L'émergence d'un modèle européen d'interrégulation en matière de protection des données personnelles

Olivia Tambou

Liber Amicorum
en l'honneur
du Professeur
Joël Monéger

L'ÉMERGENCE D'UN MODÈLE EUROPÉEN D'INTERRÉGULATION EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

Olivia TAMBOU

La notion d'interrégulation[1] caractérise en général les relations entre les autorités de régulation. L'interrégulation rend compte de la nécessité de dépasser la segmentation initiale de la régulation en raison de l'évolution de la complexité et de l'interdépendance des marchés. Il y a alors une dialectique entre interrégulation sectorielle et régulation intersectorielle[2]. La première vise à faire le lien entre les régulations sectorielles tout en les maintenant. La seconde tend à prôner la fusion des autorités intervenant dans des secteurs connexes pour des raisons d'efficacité. Les phénomènes d'interrégulation ont été principalement étudiés dans le cadre des domaines traditionnels de la régulation, à savoir la concurrence, et les secteurs tels que les télécommunications, l'audiovisuel, le secteur bancaire et financier[3]. Le droit européen de la protection des données personnelles est un droit récent né avec le développement de l'informatique puis de l'Internet. Cela explique sans doute que l'interrégulation dans le domaine de la protection des données personnelles ait été délaissée par la doctrine.

L'interrégulation est au cœur de la réforme du droit européen de la protection des données personnelles. En effet, le renforcement de la régulation de la protection des données personnelles par les autorités dites de contrôle constitue l'un des

1. Pour une analyse approfondie de ce concept, cf. H. DELZANGLES, *La notion d'interrégulation*, *in* G. ECKERT et J.-Ph. KOVAR, *L'interrégulation*, L'Harmattan, coll. « Logiques juridiques », 2015.
2. Cf. É. MULLER, *Interrégulation sectorielle ou régulation intersectorielle ? Réflexion sur les configurations institutionnelles de la régulation : ibid.*, p. 117.
3. Cf. *L'interrégulation*, ouvrage préc., ou encore les travaux de M.-A. Frison Roche qui n'intègrent que très récemment et partiellement la protection des données personnelles. Cf. M.-A. FRISON-ROCHE (ss dir.), *Internet, espace d'interrégulation*, Dalloz, coll. « Thèmes et commentaires », Série « Régulations », mai 2016.

trois piliers de cette réforme[4]. Initiée en 2012, cette réforme globale repose sur deux textes :

– le règlement définissant le cadre général de l'Union européenne pour la protection des données (ci-après RGPD)[5], et

– la directive sur le traitement des données 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 libre circulation des données (ci-après directive CJPP)[6].

L'objet de cette contribution est d'analyser cette réforme pour déterminer les contours d'un modèle européen d'interrégulation en matière de protection des données.

Le caractère transversal des traitements de données personnelles permet difficilement de parler d'interrégulation sectorielle. En effet, la collecte, l'enregistrement, la conservation, la modification d'informations permettant d'identifier une personne couvrent tous les secteurs d'activités. Ce caractère transversal n'est pas remis en cause par l'existence de types de données spécifiques telles que les données concernant la santé, ou l'existence d'obligations relatives à certains secteurs comme le secteur bancaire.

Enfin, dès l'origine, l'interrégulation européenne en matière de protection des données personnelles a été transnationale. La directive n° 95/46 avait pour objectif à la fois de faciliter les flux des données personnelles entre les États membres de l'Union européenne et vers des pays tiers.

Dans ce contexte, le modèle européen d'interrégulation de la protection des données personnelles a été d'emblée conçu comme une interrégulation multiniveau : à l'échelle des États et à l'échelle de l'Union européenne.

Les nouvelles bases juridiques introduites par le traité de Lisbonne marquent une nouvelle étape dans l'émergence du modèle européen d'interrégulation multiniveau (I). L'interrégulation disciplinaire, c'est-à-dire entre autorités de protection des données personnelles, reste privilégiée. Les potentialités d'interrégulation transdisciplinaire avec d'autres autorités de contrôle, notamment celles de la concurrence, n'ont pas encore été véritablement exploitées. L'évolution du cadre juridique se traduit également par l'émergence du développement des techniques d'interrégulation. Si certaines sont assez classiques telles que le développement des coopérations souples entre les autorités de régulation, d'autres mécanismes permettent une coordination inédite (II).

4. Les autres piliers de la réforme sont : le renforcement des droits des individus et le renforcement des obligations des responsables des traitements des données personnelles.
5. Règl. n° 2016/679, 27 avr. 2016 : *JOUE* n° L 199, p. 1.
6. Dir. n° 2016/680, 27 avr. 2016 : *JOUE* n° L 119, p. 89.

I. – L'ÉMERGENCE D'UNE INTERRÉGULATION MULTINIVEAU RENOUVELÉE

Depuis le traité de Lisbonne, la protection des données personnelles repose sur des bases juridiques spécifiques. D'une part, l'article 8 de la Charte des droits fondamentaux consacre la protection des données personnelles comme un droit fondamental dissocié de celui du respect de la vie privée[7]. D'autre part, l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) permet l'adoption de normes de droit dérivé afin de protéger ce droit fondamental. Ces nouveautés renouvellent l'interrégulation européenne multiniveau en matière de protection des données (B) dont il faut au préalable rappeler la progressive construction (A).

A. – L'émergence d'une interrégulation européenne multiniveau

L'émergence d'une interrégulation multiniveau découle de la mise en place progressive d'un modèle européen de régulation lui-même multiniveau de la protection des données personnelles.

1° Les contours du modèle européen de régulation de la protection des données personnelles

Le modèle européen de régulation multiniveau de la protection des données repose principalement sur trois caractéristiques.

Premièrement, cette régulation multiniveau s'est construite par étapes des États vers l'Union. Tout d'abord, certains États européens ont adopté des législations spécifiques sur la protection des données personnelles dans les années 1970. Le *Land* de Hesse en Allemagne, la Suède, l'État fédéral allemand et la France ont ainsi été précurseurs en la matière[8]. Chacune de ces lois a introduit une autorité de contrôle, le *Datenschutzbeauftragter* dans le *Land* du Hesse, le *Bundesbeauftragter fiir den Datenschutz* pour la RFA, la *Datainspektionen* en Suède, et la *Commission nationale de l'informatique et des libertés* (*CNIL*) en France. Autrement dit, dès l'origine, l'existence d'une autorité de contrôle a constitué un élément essentiel.

Ensuite, la directive n° 95/46 a généralisé à l'échelle communautaire l'institutionnalisation des autorités nationales de régulation. L'ambition de ce texte était de créer une régulation multiniveau avec des autorités de contrôle au sein de chaque État membre et à l'échelle européenne avec le groupe dit de l'article 29 (G29).

---

7. G. Gonzalez Fuster, *The emergence of Personal Data Protection as a fundamental Right of the EU*, Springer, 2014.
8. Sur cette approche historique, cf. *op. cit.* G. Gonzalez Fuster, spéc. p. 55 et s.

Enfin, une régulation de la protection des données pour les institutions et organes de l'Union a été mise en place par le règlement n° 45/2001/CE. Ce dernier institue le *Contrôleur européen des données personnelles* (CEPD) en tant qu'autorité de contrôle indépendante qui a pour mission de garantir le respect dudit règlement. La régulation verticale entre l'échelon national et celui de l'Union européenne est ainsi complétée par une régulation horizontale à l'échelle de l'Union européenne elle-même.

Deuxièmement, cette régulation générale a été complétée par des régulations spécifiques liées au système de compétences des Communautés, puis de l'Union européenne[9]. La décision-cadre n° 2008/977 JAI du Conseil a été adoptée dans le cadre de la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. En outre, il existe des régulations *sui generis* dans le cadre du domaine des migrations et du contrôle des frontières. Ces régulations sont liées à l'existence de bases de données sensibles telles que le Système d'information Schengen (SIS II)[10], le Système d'information visa (VIS)[11], Eurodac[12]. L'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'Espace de liberté, de sécurité et de justice (EU-Lisa)[13] a été créée en 2012 afin d'assurer un haut niveau de protection des données autour de ces trois fichiers. Dans le domaine de la coopération judiciaire, la création d'Europol et d'Eurojust a aussi été accompagnée de deux autorités de contrôle communes.

Troisièmement, cette construction historique ancrée dans les traditions juridiques des États membres explique qu'il n'existe pas véritablement de modèle unique d'autorité de régulation en matière de protection des données personnelles dans l'Union européenne. Ainsi, ces autorités peuvent avoir une forme collégiale, telle que la CNIL, ou unipersonnelle, telle que le Commissaire à la protection des données de l'Irlande.

Face à la multiplication des niveaux et des domaines de régulation de la protection des données personnelles, une interrégulation a été envisagée à l'échelle européenne.

---

9. Cf. *Manuel européen de la protection des données*, Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, Office des publications de l'Union européenne, 2014, spéc. p. 161.
10. SIS est une base de données contenant des informations sur les personnes, les véhicules et les objets recherchés ou disparus sur le territoire Schengen.
11. VIS est une base de données qui aide les pays situés dans l'espace sans frontières de Schengen à échanger des données en matière de visas concernant les demandes introduites par des ressortissants de pays tiers en vue de recevoir un visa de court séjour pour séjourner ou circuler dans cette zone.
12. Eurodac (base de données DACtyloscopiques EUROpéenne en matière d'asile) est une base de données à grande échelle d'empreintes digitales, destinée à faciliter la comparaison des empreintes digitales des demandeurs d'asile et de plusieurs catétories d'immigrants clandestins.
13. Règl. n° 1077/2011, portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice : *JOUE* n° L 286, p. 1.

2° Une interrégulation multiniveau des différentes formes de régulation

L'institutionnalisation d'une régulation multiniveau s'est accompagnée d'une interrégulation, elle aussi multiniveau. Cette interrégulation trouve son fondement dans le droit dérivé. Elle s'est développée principalement au sein du G29 et du CEPD.

Le G29, qualifié par la directive n° 95/46 de groupe « consultatif et indépendant », a été conçu pour assurer une forme d'interrégulation multiniveau. Il se compose d'un représentant d'une autorité de contrôle nationale par État membre, d'un représentant de la Commission et du CEPD. En outre, il a permis une certaine interrégulation transdisciplinaire. Son domaine d'action s'étend aux communications électroniques en vertu de l'article 15 de la directive n° 2002/58 dite « directive vie privée et communications électroniques ». Le G29 s'est notamment donné pour tâche de « promouvoir l'application uniforme des principes généraux des directives dans tous les États membres à travers une coopération avec les autorités nationales de contrôle ».

Dans la pratique, cette interrégulation a joué un rôle important. Cela dit, le G29 souffre d'une faiblesse de moyens tant budgétaires qu'administratifs[14]. Son secrétariat est assuré par la Commission européenne et sa capacité de travail repose essentiellement sur celles des autorités nationales.

Le CEDP assure également plusieurs fonctions d'interrégulation. À l'échelle européenne, il a un rôle qu'il qualifie lui-même de supervision des traitements des données personnelles effectués par les institutions et les organes européens. Les traitements comportant des risques spécifiques des institutions ou organes de l'Union européenne ne peuvent être mis en œuvre sans son contrôle préalable. En outre, il coordonne l'action des délégués à la protection personnelle qui doivent être obligatoirement nommés dans chaque institution et organe. Enfin, en dehors du G29, le CEDP coopère avec les autorités de protection nationales compétentes pour les systèmes d'informations européens, notamment ceux précités (Eurodac, SISII, VIS,). Le CEPD est un membre actif des groupes de supervision de ces systèmes. Au 1er mai 2017, Europol sera également placé sous la supervision du CEPD.

La Cour de justice de l'Union européenne a aussi eu l'occasion de rappeler à plusieurs reprises que le contrôle des autorités indépendantes constitue un élément essentiel du modèle européen de protection des données personnelles. L'exigence d'une régulation de la protection des données assurée par un organe indépendant semble nécessaire pour qualifier la protection des données dans un pays tiers équivalente à celle de l'Union européenne[15]. La promotion d'une certaine forme d'interrégulation pourrait alors s'imposer pour faciliter le transfert des données vers des pays tiers comme les USA par exemple.

---

14. S. Nerbonne, *Le « Groupe de l'article 29 » est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? : Légicom* 2009/1, n° 42, p. 37-46.
15. Cf. CJUE, 6 oct. 2015, aff. 362/74, *Schrems*.

B. – Le renouvellement de cette interrégulation multiniveau

L'article 16 TFUE constitue désormais la base juridique de droit commun du droit européen de la protection des données personnelles.

Le premier paragraphe de cette disposition reprend les termes de l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Il consacre le droit pour toute personne « à la protection des données personnelles la concernant ». Le second paragraphe consacre une nouvelle base juridique pour l'adoption de « règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel… ». Ces règles doivent être adoptées par le Parlement et le Conseil statuant à la procédure législative ordinaire, sauf dans le domaine de la PESC où elles nécessitent une décision du Conseil[16]. Enfin, l'ensemble de ces règles est soumis « au contrôle d'autorités indépendantes ».

L'article 16 TFUE constitue un fondement juridique pour le renouvellement de l'interrégulation multiniveau. D'une part, cet article a été introduit dans un chapitre intitulé « Dispositions d'application générale ». Cela signifie que le traité ne se contente pas de consacrer le droit de la protection des données personnelles comme un droit fondamental. Il encourage aussi l'adoption de règles permettant de rendre effectif ce droit fondamental dans l'ensemble des politiques de l'Union européenne[17] et non plus seulement au sein du Marché intérieur. En outre, il consacre le rôle central des autorités indépendantes qui doivent assurer le contrôle de ces règles.

À l'heure actuelle, les potentialités offertes par l'article 16 TFUE n'ont encore été que partiellement exploitées. L'article 16 TFUE a été utilisé pour approfondir l'interrégulation disciplinaire préexistante[18]. En revanche, cet article n'est pas exploité pour développer une interrégulation transdisciplinaire.

1° L'article 16 TFUE : fondement exploité pour l'approfondissement de l'interrégulation disciplinaire

L'article 16 TFUE a été exploité dans le cadre de la réforme de la protection des données personnelles pour développer l'interrégulation disciplinaire de deux façons[19].

16. Cf. TUE, art. 39.
17. Cf. les récentes conclusions dans l'avis n° 1/15 dans lesquelles l'avocat général Mengozi a rappelé la nécessité de fonder sur l'article 16, § 2 TFUE, l'acte de conclusion de l'accord PNR-Canada, relevant de la dimension externe de l'ELSJ, pts 112 à 117.
18. L'adoption de règles particulières dans le domaine de la PESC sur la base de l'article 39 TUE n'a pas encore eu lieu, malgré les incitations en ce sens. Cf. l'avis du CEPD du 24 novembre 2010 sur la communication de la Commission au Parlement européen et au Conseil intitulée « La politique antiterroriste de l'UE : principales réalisations et défis à venir », pt 31.
19. Cf. A. Guirgiu et T. Larsen, *Roles and Powers of National Data Protection Authorities, moving from Directive 95/46 EC to GDPR : Stronger and More « European » DPAs as Guardians of Consistency ?*, EDPL, 3/2016, p. 342.

Premièrement, la réforme procède à une importante harmonisation des statuts, compétences et missions des autorités nationales de régulation de la protection des données. Les difficultés générées par les différences de pouvoirs et de moyens entre les vingt-huit autorités nationales de protection des données avaient été dénoncées[20]. L'objectif de cette harmonisation est clairement de faciliter la coopération horizontale entre les autorités nationales. En outre, l'article 52, § 4 RGPD impose à chaque État membre de veiller à ce que « chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaire à l'exercice effectif de ses missions et de ses pouvoirs », y compris dans le cadre des coopérations avec les autres autorités.

D'une manière générale, l'harmonisation des statuts, compétences et pouvoirs constitue le terreau nécessaire sur lequel l'interrégulation va pouvoir prospérer. L'alignement des statuts, pouvoirs et compétences doit notamment créer une confiance mutuelle entre les autorités, élément incontournable pour l'interrégulation.

Le RGPD[21] permet de mieux garantir l'indépendance des autorités nationales de protection des données[22]. Il organise une certaine homogénéité des missions[23] et des pouvoirs des autorités nationales de contrôle[24]. Ainsi chaque autorité devra être dotée de trois types de pouvoirs. Elle doit disposer de pouvoirs d'investigations. Elle doit aussi pouvoir prendre des mesures correctives. Il peut s'agir d'imposer des sanctions administratives. Le montant ainsi que les modalités de mise en œuvre de ces sanctions ont fait l'objet d'une harmonisation. Cela implique aussi le pouvoir d'imposer la cessation d'un traitement, voire de suspendre le transfert des données vers un État tiers. Enfin, les autorités bénéficient de pouvoirs d'autorisations et de conseils.

Deuxièmement, la réforme institutionnalise une nouvelle autorité de régulation européenne : le Comité européen de la protection des données (ci-après le Comité) qui remplace le G29. Une certaine forme de continuité est assurée en ce qui concerne la composition de ce nouvel organe de l'Union européenne. Il s'agit toujours de réunir les autorités nationales de protection des données, avec le contrôleur européen des données. En revanche, si la directive n° 95/46 ajoutait également la présence d'un représentant de la Commission, la formulation choisie par le RGPD diffère légèrement. L'article 68, § 5 précise que : « La Commission a le droit de participer aux activités et réunions du Comité sans droit de vote ». Le représentant de la Commission acquiert ainsi d'emblée un statut particulier

20. *Access to Data protection remedies in EU Member States*, European Union Agency for fundamental rights, Luxembourg publications Office of the European Union, 2013.
21. Des dispositions similaires ont été introduites aux articles 41-47 de la directive n° 2016/680/UE.
22. RGPD, art. 51 et s.
23. RGPD, art. 57.
24. RGPD, art. 58.

au sein du Comité. Cette précaution est un indice supplémentaire de la transformation institutionnelle du Comité en une véritable autorité de contrôle indépendante au sens de l'article 16, § 2 TFUE. Cela implique que le Comité puisse statuer sans la présence du représentant de la Commission[25].

Le statut, l'organisation, les missions et les pouvoirs du Comité ont été considérablement améliorés par rapport au G29. Le Comité est doté de la personnalité juridique. Le Comité obtient officiellement le statut d'organe de l'Union européenne, un peu comme les autres agences de régulation[26]. L'indépendance du Comité est désormais garantie à l'article 69 RGPD. Son secrétariat n'est plus assuré par la Commission, mais par le CEPD[27]. Ce mode d'organisation atteste clairement de la volonté du législateur d'asseoir l'indépendance du Comité vis-à-vis de la Commission. Il favorise la naissance d'une interrégulation à l'échelle européenne entre le CEPD et les autorités nationales de protection sans aller jusqu'à l'émergence d'une structure unique de régulation à l'échelle de l'Union européenne.

En outre, le Comité acquiert une compétence globale puisqu'il est l'organe de régulation non seulement dans le champ d'application du RGPD, mais aussi de la directive CJPP. Cela illustre encore une fois que l'article 16 TFUE permet une interrégulation disciplinaire de la protection des données au-delà du marché intérieur.

Enfin, le Comité acquiert de véritables pouvoirs de décisions comme nous le verrons ultérieurement.

Au-delà de cette interrégulation disciplinaire, l'article 16 TFUE pourrait aussi constituer le fondement juridique pour développer une interrégulation transdisciplinaire.

2° L'article 16 TFUE : fondement non encore exploité pour une interrégulation transdisciplinaire

Une telle interrégulation transdisciplinaire semble découler de la lettre même de l'article 16 TFUE. D'une part, l'article 16 TFUE prévoit que « toute personne a droit à la protection des données personnelles la concernant ». D'autre part, il précise que « le respect de ces règles est soumis au contrôle d'autorités indépendantes ». La généralité de ces termes constitue une sorte d'habilitation pour l'ensemble des autorités indépendantes et non seulement celles spécialisées dans la protection des données personnelles à exercer leurs compétences en prenant soin de veiller au respect des règles de la protection des données personnelles.

---

25. En ce sens cf. H. Hijmans, *The European Union as a constitutional guardian of internet privacy and data protection*, PhD Thesis, University of Amsterdam 2016, http://hdl.handle.net/11245/2.169421, p. 389.
26. Cf. RGPD, art. 68.
27. RGPD, art. 75.

Les autorités indépendantes de la concurrence, mais aussi en matière de protection de la consommation tant à l'échelle nationale qu'à l'échelle européenne pourraient ainsi s'appuyer sur cette disposition pour créer des mécanismes d'interrégulation en matière de protection des données personnelles. Le CEPD a récemment proposé la mise en place d'une chambre numérique des compensations, *Digital Clearing House*[28]. Il s'agirait d'un nouveau réseau ouvert aux autorités de régulation nationales et européennes compétentes dans la régulation du numérique. Ce réseau permettrait ainsi une interrégulation avec les autorités de régulation de la concurrence, du droit de la consommation, mais aussi des télécommunications. Cette première proposition de structuration d'interrégulation transdisciplinaire repose néanmoins sur une base volontaire et n'a pas été explicitement fondée sur l'article 16, § 2 TFUE. Des régulateurs nationaux ont également souhaité, voire mené de telles interrégulations transdisciplinaires de façon spontanée[29].

L'article 16, § 2 pourrait être utilisé par le législateur de l'Union européenne pour adopter des règles matérielles ou procédurales pour cette interrégulation.

Enfin, l'article 16, § 2 TFUE pourrait inciter au développement d'une interrégulation transdisciplinaire avec des autorités non européennes.

La décision de la Commission européenne dite *EU-US Privacy Schield* a renforcé les mécanismes d'interrégulation entre, d'une part, les autorités européennes de protection des données personnelles et, d'autre part, le ministère du Commerce, la *Federal Trade Commission* et le ministère des Transports[30]. En outre, un médiateur (*Privacy Schield Ombudsperson*) est institué pour permettre la surveillance et la conformité des activités des autorités de renseignement américaines. La saisine de ce médiateur transitera par les autorités nationales européennes, qui devront coopérer avec lui notamment en cas de plaintes individuelles. Enfin, le niveau de protection des transferts de données personnelles vers les États-Unis est soumis à un réexamen conjoint annuel entre l'ensemble de ces organismes américains et la Commission européenne. La participation des autorités nationales de contrôle, voire de représentant du G29 est envisagée.

L'objectif de cette interrégulation est de veiller à ce que le niveau de la protection des données personnelles qui sont transférées aux États-Unis soit équivalent à celui qui existe dans l'Union européenne. Or, il n'est pas certain que l'interrégulation proposée permette de parvenir à cet objectif. Tant le G29 que le CEDP ont émis de sérieuses réserves sur l'indépendance du médiateur. Il est vraisemblable que cette nouvelle décision de la Commission européenne fasse l'objet de

28. Cf. EDPS opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 sept. 2016.
29. Cf. I. FALQUE-PIERROTIN, *Des problématiques concurrentielles imposant la mise en place d'une véritable interrégulation : Concurrences* 2-2013, p. 30 ou encore opinion 8/2016 préc., p. 9.
30. Cette décision ne cite pas expressément l'article 16, § 2 TFUE, mais fait globalement référence au Traité sur le fonctionnement de l'Union européenne.

contentieux. Il appartiendra à la Cour de justice de l'Union européenne de vérifier sa conformité.

Cet exemple illustre que l'émergence du développement des techniques d'interrégulation peut aussi s'étendre dans les relations entre l'Union européenne et ses partenaires. L'émergence des techniques d'interrégulation au sein de l'Union est néanmoins renforcée par la mise en place actuelle du marché unique du numérique.

II. – L'ÉMERGENCE DU DÉVELOPPEMENT DES TECHNIQUES D'INTERRÉGULATION

D'une part, des coopérations souples entre les autorités se développent de plus en plus. D'autre part, de véritables techniques de coordination émergent.

A. – Le renforcement de la coopération souple

L'échange d'informations constitue le premier stade de ces coopérations souples entre les autorités de contrôle[31]. L'étendue du renforcement actuel des échanges d'informations a été récemment étudiée[32]. Ces échanges peuvent avoir lieu de façon informelle ou dans le cadre du G29. Il existe d'ailleurs un sous-groupe dédié à ces coopérations au sein du G29. Dernièrement, les échanges d'informations ont eu lieu autour de cas emblématiques tels que l'affaire *Google Spain* ou l'affaire *Schrems*. La formalisation de ces coopérations s'est traduite par l'adoption par le G29 de lignes directrices afin d'aider les autorités nationales à mettre en œuvre ses arrêts. Plus concrètement encore, les autorités ont élaboré des outils internes pour pouvoir échanger sur ces cas tels que des points de contact ou des tableaux de bord pour suivre le traitement des affaires similaires pendantes devant les autres autorités.

Aujourd'hui, de plus en plus de responsables de traitement de données personnelles ont des activités qui affectent des individus résidant dans plusieurs États membres. Cela renforce le besoin d'échanger des informations entre autorités. Dans sa jurisprudence *Weltimmo*[33], la Cour de justice de l'Union européenne a rappelé qu'une autorité nationale peut traiter de plaintes à l'encontre des traitements effectués par une société inscrite au registre des sociétés d'un autre État membre. En l'espèce, l'autorité hongroise souhaitait sanctionner une société slovaque exploitant un site

31. La promotion de ces échanges d'information, y compris avec des autorités non européennes, constitue l'une des missions attribuées au nouveau Comité européen de la protection des données personnelles par le RGPD, cf. art. 70 1. u) v) w).
32. Cf. *Best Practices for cooperation between EU DPAs*, deliverable 2.2. January 2016, spéc. p. 10 et s. Http ://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II_D2.2-report_2016.02.15.pdf.
33. CJUE, 1er oct. 2015, aff. C-230/14, *Weltimmo*.

Internet d'annonces immobilières pour des biens situés en Hongrie. La Cour a considéré que l'autorité hongroise pouvait examiner cette réclamation indépendamment du droit applicable en vertu de l'article 28, § 6 de la directive n° 95/46. En revanche, elle devait coopérer avec l'autorité de l'État du siège social de l'entreprise (ici la Slovaquie) si elle souhaitait infliger à l'entreprise des sanctions.

Le RGPD règle cette situation par l'instauration de la figure de l'autorité chef de file qui est celle dans laquelle le responsable des traitements a son établissement principal. L'autorité chef de file constitue un guichet unique pour l'entreprise qui ne relève plus des autorités nationales des autres États membres. L'article 60 RGPD institue alors une obligation d'échanges d'information entre l'autorité chef de file et les autres autorités nationales concernées par le traitement en cause. Plus globalement, l'article 61 RGPD établit une obligation d'assistance mutuelle entre l'ensemble des autorités de contrôle. Il s'agit de transmettre des informations utiles pour la conduite d'une enquête, mais également de demander à une autorité de prendre des mesures de contrôle. Enfin, l'article 67 précise que la Commission peut adopter des actes d'exécution pour définir les modalités des échanges d'information par voie électronique entre les autorités de contrôle. Autrement dit, on assiste au développement de plateformes numériques d'échanges d'information entre les autorités de contrôle[34].

Les échanges d'informations constituent le premier stade de coopérations souples dont l'objectif est désormais de faciliter l'émergence d'une véritable coordination.

B. – L'émergence de la coordination

La pratique récente des autorités de contrôle des données personnelles révèle le développement d'opérations conjointes. En outre, le RGPD consacre une nouvelle forme de coordination : la prise de décisions communes.

1° Le développement des opérations conjointes

Les autorités de protection des données ont mené ces dernières années plusieurs opérations conjointes. Les autorités des pays nordiques ont par exemple mené une opération conjointe auprès des banques en 2012[35]. Le changement des termes de la politique relative à la protection des données personnelles et les *cookies* de Facebook ont donné lieu à la création d'un groupe de contact au sein de cinq autorités de protection qui ont adopté une déclaration commune[36]. Cette forme

34. Pour un aperçu de l'étendue du développement de ces plateformes, y compris à l'échelle mondiale, cf. rapport préc. Phaedra, p. 15 et s.
35. Cf. rapport préc. Phaedra, p. 13.
36. *The Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands. France, Spain, Hamburg and Belgium*. Https ://www.datenschutz-hamburg.de/uploads/media/Common_Statement_of_the_Contact_Group_on_Facebook_-_4.12.2015.pdf.

de coordination a néanmoins ces limites. Chacune des autorités a par la suite mis en demeure ou condamné Facebook sur son territoire et sur la base de sa législation nationale[37].

Il est aussi possible de citer une forme de coordination concrète telle que la mise en place d'audits en ligne concertés par des autorités de protection dans le monde entier. L'Internet *Sweep Day* a été initié en 2013 par le *Global Privacy Enforcement Network* (GPEN). Il a successivement porté sur les sites Internet et applications mobiles les plus visités, les applications mobiles, l'utilisation de *cookies*, les sites pour enfants et sur les objets connectés en 2016.

L'article 62 RGPD donne une nouvelle base juridique aux opérations conjointes des autorités de contrôle. Ainsi, les autorités concernées par des traitements effectués par un responsable ou un sous-traitant établi dans plusieurs États membres peuvent prendre part à des opérations conjointes. Ces opérations conjointes peuvent donner lieu à l'exercice par une autorité de contrôle d'un État membre de pouvoirs notamment d'enquête sur le territoire de l'autorité de contrôle d'accueil. Une telle coordination est néanmoins soumise à trois conditions. D'une part, le droit de l'État d'accueil doit pouvoir le permettre, d'autre part, les pouvoirs d'enquête doivent être exercés sous l'autorité et en présence des agents de l'autorité de contrôle d'accueil. Enfin, les agents de l'autorité de contrôle d'origine sont soumis au droit de l'autorité de contrôle d'accueil.

2° La consécration de prises de décisions communes dans le RGPD

Le RGPD met en place un système complexe dit « de coopération et cohérence », notamment pour gérer les cas transfrontaliers entre les autorités de contrôle. Ce mécanisme s'articule avec l'institution de l'autorité chef de file[38] et le mécanisme du guichet unique évoqués précédemment. Le RGPD précise les modalités d'adoption de décisions par l'autorité chef de file en coordination avec d'autres autorités concernées. Il s'agit d'autorités locales de contrôle, c'est-à-dire celle saisie par une personne concernée par une violation dans un autre État membre ou celle de l'État qui sera plus substantiellement affecté par le traitement.

L'article 60 RGPD décrit en détail comment l'autorité chef de file et les autorités des autres États membres concernées doivent se coordonner pour arriver à une décision commune. Le projet de décision est élaboré par l'autorité chef de file, puis soumis aux avis des autres autorités. Ensuite, l'adoption de la décision commune et sa diffusion sont réparties entre les différentes autorités. L'autorité chef de file demeure l'interlocuteur du responsable de traitement. C'est elle qui

37. Cf. Délib. n° 2016-026, 4 févr. 2016, du bureau de la Commission nationale de l'informatique et des libertés décidant de rendre publique la mise en demeure n° 2016-007 du 26 janvier 2016 prise à l'encontre des sociétés Facebook Inc. et Facebook Ireland.

38. Pour savoir comment déterminer l'autorité chef de file, cf. *Guidelines for identifying a controller or processor's lead supervisory authority adopted by the G29 on 13 December 2016*.

adopte en principe la décision commune. Lorsqu'un individu a déposé une plainte devant une autre autorité, cette autorité locale communique avec l'individu et lui fait part de la décision commune prise. En revanche, s'il s'agit d'une décision de rejet ou refus de la réclamation, c'est l'autorité locale qui doit adopter la décision et la notifier au plaignant. Il s'agit de lui permettre de pouvoir attaquer cette décision dans son État membre et selon le droit de son État.

Enfin, l'article 65 RGPD institue une procédure de règlement des litiges entre l'autorité chef de file et les autorités concernées devant le Comité européen de la protection des données personnelles. Cela vise les cas où les autorités ne sont pas d'accord sur la décision commune à adopter pour un traitement particulier. Cela concerne également les désaccords portant sur la détermination de l'établissement principal d'un responsable de traitement. Dans ce cas, l'enjeu du litige est la détermination de l'autorité chef de file. La procédure de règlement des litiges est aussi applicable lorsqu'une autorité de contrôle ne respecte pas les cas de saisine obligatoire pour demander un avis préalable du Comité européen de la protection des données. Ces cas, énumérés à l'article 64, § 1 RGPD, visent principalement l'adoption de décisions susceptibles de produire des effets sur de nombreuses personnes dans plusieurs États membres. Il s'agit par exemple de la liste des traitements devant faire l'objet d'une étude d'impact en matière de protection de la vie privée, ou l'approbation de règles contraignantes d'entreprises. Dans ces cas, la procédure de règlement des différends permet au Comité de renforcer la cohérence des décisions prises par les autorités de contrôle en évitant les contradictions.

Dans toutes ces hypothèses de conflit, le Comité rend une décision contraignante à la majorité des deux tiers de ses membres et dans un délai d'un mois.

* *

*

À l'issue de ces analyses, plusieurs conclusions peuvent être tirées. Premièrement, l'émergence du modèle d'interrégulation européenne de la protection des données personnelles est travaillée par trois dynamiques dont l'articulation n'est pas toujours très claire. D'une part, une interrégulation horizontale entre les autorités de contrôle nationales généralistes avec une coordination du futur Comité européen de la protection des données. D'autre part, une interrégulation entre des autorités de contrôle spécifiques et le Contrôleur européen de la protection des données. Enfin, des initiatives d'interrégulation transdisciplinaires émergent tant à l'échelle nationale qu'à l'échelle de l'Union européenne, voire dans les relations avec les pays tiers. Deuxièmement, l'article 16, § 2 TFUE n'a pas encore été exploité pour structurer ces initiatives d'interrégulation transdisciplinaires alors qu'il pourrait l'être. Troisièmement, l'émergence d'un modèle européen d'interrégulation n'échappe pas à l'ambivalence intrinsèque de l'interrégulation qui vise à relier des régulations aux objectifs différents. Analysée sous cet angle, l'interrégulation apparaît tantôt comme un échec de la régulation intersectorielle, tantôt comme un complément de celle-ci. Quatrièmement, cette présentation

illustre les forces et faiblesses du recours à l'interrégulation. L'interrégulation peut permettre la création d'une culture mondiale de la régulation de la protection des données. Il est néanmoins difficile de prédire s'il s'agit d'une solution intermédiaire ou non. La création d'un instrument international relatif à la protection des données relève encore de l'utopie[39]. Il semble néanmoins perceptible que l'interrégulation européenne comporte une volonté de l'Union européenne de peser en tant que modèle à l'échelle mondiale.

Enfin, l'émergence d'une interrégulation en matière de protection des données comporte aussi un risque de création d'une communauté épistémique[40]. La transparence du fonctionnement actuel des autorités chargées de la régulation de la protection des données laisse parfois à désirer. Le renforcement à l'avenir de leur rôle amènera à se poser une question. Qui doit contrôler les régulateurs et comment prévenir un risque de déficit démocratique ?

39. La Convention 108, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe qui pourrait être cet instrument juridique n'a été ratifiée que par trois États non européens (Uruguay, Sénégal et Maurice).
40. Cf. G. MARCOU, *Différenciation des régulations et interrégulation*, in *L'interrégulation*, *op. cit.*, note 1, p. 234.