LE GROUPE DE TRAVAIL DE L'ARTICLE 29

par Julien ROSSI

Ce texte est l'un des chapitres du livre "Correspondant Informatique et Libertés : bien plus qu'un métier", publié en 2015 par l'AFCDP.

Le groupe de travail de l'article 29 (ou G29), prévu par la directive 95/46/CE, regroupe les autorités nationales de protection des données personnelles. Cette structure originale dans l'architecture européenne, semble à mi-chemin entre une agence structurée et un comité classique conseillant la Commission. Récemment, un contrôle conjoint de la politique de confidentialité de Google a attiré l'attention du public sur le rôle joué par ce groupe dans la protection des données en Europe. Cet article tente d'explorer le rôle du G29 dans la politique européenne de protection des données. Ce travail permet de montrer que le réseau institutionnalisé sous la forme du G29 actuel préexistait à la directive européenne le créant formellement, et qu'il a eu un rôle majeur dans l'adoption de celle-ci. Aujourd'hui, le projet de règlement entérine plusieurs évolutions de facto expérimentées par ce groupe, mais la montée en puissance du G29, bien qu'apparemment très forte, est à nuancer. On ne peut en effet pas parler d'unité du G29, qui ressemble plus à une ressource politique et matérielle à disposition des autorités nationales. Il n'en demeure pas moins que ce groupe est capable de produire des outils utiles à l'intention des responsables de traitement et des CIL.

La directive 95/46/CE 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 oblige les États membres de l'Union Européenne (UE) qui n'en étaient pas encore dotés de créer une ou plusieurs autorités chargées de contrôler le respect, par les responsables de traitement, des obligations découlant de la directive.

L'article 29 de cette même directive prévoit la constitution d'un groupe de travail composé des représentants de ces autorités nationales. Ce groupe, qui peut prendre ses décisions à la majorité simple, élit son propre président, mais ne dispose pas de son propre secrétariat – lequel est assuré par la Commission européenne – ni d'un budget propre. La directive ne prévoit que des missions *consultatives* : ce groupe conseille la Commission, émet des avis sur la conformité du niveau de protection des données dans les États tiers, peut émettre de sa propre initiative des recommandations, contribue à la mise en œuvre homogène de la directive et produit un rapport annuel, qui est en fait pour une très large part la compilation d'extraits de rapports annuels en provenance des États membres.

Concrètement, ce groupe de travail, connu en France sous son abréviation « G29 », a un rôle dans cinq domaines :

- L'interprétation de la directive par l'adoption d'avis sur différents thèmes, allant de la biométrie à la définition de la notion personnelle ou du consentement ;
- L'évaluation du niveau de protection des données personnelles des États tiers, cadre dans lequel le G29 entretient une correspondance avec les autorités de ces États et formule des avis à leur encontre, participant à une forme de « diplomatie des données personnelles » au niveau international ;

- La correspondance avec certains responsables de traitement établis dans les États tiers (ICANN[1], Microsoft, Google…) ;
- La formulation d'avis sur la politique européenne, sous l'angle de la protection des données ;
- Enfin, le G29 est un forum d'échange d'expertise entre autorités nationales et a un rôle primordial dans la mise en réseau de celles-ci.

I. Le G29 à l'origine de la directive 95/46/CE

I.1. L'entrepreneuriat transgouvernemental

Abraham Newman, universitaire américain ayant étudié les Autorités nationales de Protection des Données Personnelles (APDP), propose dans son ouvrage *Protectors of Privacy* (2008) une explication alternative aux récits classiques, intergouvernementaux[2] et néofonctionnalistes[3] pour expliquer l'adoption de la directive 95/46/CE, auquel il donne le nom de *la théorie de l'entrepreunariat transgouvernemental*. Cette explication repose sur les éléments suivants :

- une volonté politique d'acteurs publics sub-étatiques ;
- une mise à l'agenda politique passant par l'expertise ;
- l'utilisation de ressources politiques nationales pour modifier le *statuquo* réglementaire international ;
- la contribution aux négociations internationales.

I.2. Le G29 avant la directive

Le rôle joué par le réseau des APDP européennes dans l'adoption de la directive 95/46/CE illustre la théorie de l'entrepreneuriat transgouvernemental d'Abraham Newman.

Lorsqu'au milieu des années 1970 ont commencé les négociations au Conseil de l'Europe sur ce qui allait devenir la Convention 108 sur la protection des données à caractère personnel, le réseau des experts de ce sujet ne pouvait s'appuyer que sur une autorité nationale de protection des données personnelles, celle de la Suède, puisqu'il n'en existait aucune autre à l'exception de celle du Land de Hesse, qui n'avait qu'une autorité régionale. En 1988, il y avait déjà onze autorités, dont la coopération avait débuté par l'organisation à Bonn, en 1979, lors de la première conférence internationale des commissaires à la protection des données.

À partir du milieu des années 1970, le Parlement européen a adopté plusieurs résolutions demandant à la Commission de proposer un texte visant à harmoniser les règles de protection des données personnelles en Europe[4]. Le Parlement européen, même s'il n'est élu au suffrage universel direct que depuis 1979, avait déjà théoriquement vocation à devenir un élément supranational dans l'architecture institutionnelle de la CEE, qui devint l'Union européenne. La Commission, que celui-ci appelait à agir, n'a cependant pas souhaité le faire, la direction générale Marché Intérieur ayant considéré à l'époque

[1] *Internet Corporation for Assigned Names and Numbers* (en français, la Société pour l'attribution des noms de domaine et des numéros sur Internet) est une autorité de régulation de l'Internet. C'est une société de droit californien à but non lucratif ayant pour principales missions d'administrer les ressources numériques d'Internet, tels que l'adressage IP et les noms de domaines de premier niveau, et de coordonner les acteurs techniques.

[2] Le récit intergouvernemental suppose une volonté politique des États, poursuivant leurs propres intérêts. Or, il n'y avait aucune demande par les États au niveau du Conseil en faveur d'une législation harmonisée au niveau européen sur la protection des données.

[3] Le récit néofonctionaliste part du principe que l'intégration européenne favorise la naissance de groupes d'intérêts paneuropéens susceptibles de faire pression pour obtenir des évolutions législatives européennes, entraînant un cercle (vicieux ou vertueux, selon l'interprétation politique de chacun) favorable à une intégration européenne croissante. Or, l'étude d'Abraham Newman montre qu'il n'y avait pas de demande particulière, à l'époque, ni de la part d'ONG, ni, encore moins, de la part des industriels.

[4] La première est la résolution du 8 avril 1976 relative à la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique.

que la protection des données personnelles ne concernait que le secteur public. En outre, l'absence d'appel à une harmonisation européenne par les représentants de l'industrie contribue elle aussi à invalider l'explication néofonctionnaliste de l'adoption de la directive 95/46/CE. L'explication intergouvernementale est invalidée par l'absence de volonté française ou allemande d'imposer un cadre européen, et l'opposition du gouvernement britannique au Conseil.

Mais, à partir de la fin des années 1980, les autorités nationales de protection des données prennent le relais du Parlement européen pour exiger une harmonisation européenne. En 1989, à Berlin, les autorités de protection des données personnelles adoptent une résolution appelant la Commission à agir, et jouant sur les objectifs du marché unique. L'année suivante, les mêmes autorités menacent, si la CEE ne se dote pas d'une réglementation garantissant un niveau minimum de protection des données avant 1992, de bloquer les flux de données transfrontaliers qui sont alors déjà en pleine expansion :

> *If there are no common rules by 1992 amongst the twelve Community members then quite simply five of the countries of the European Community without such laws will have to be treated in exactly the same way as those with no rules for data privacy. Therefore, there will no personal data transfers to those countries because data commissioners will oppose such transfers*[5].

Cette menace a eu des effets concrets. Invoquant l'article 24 de la loi Informatique et Libertés de l'époque, la CNIL a bloqué un transfert de données personnelles de Fiat France vers Fiat Italie (CNIL, délibération 89-78). De telles menaces ont également pesé à la fin des années 1980 sur l'accord Schengen, des autorités nationales ayant menacé d'interdire les transferts vers la Belgique prévus dans le cadre du *Schengen Information System* (SIS).

C'est à la lumière de ces efforts coordonnés que doit s'analyser la proposition du 13 septembre 1990 de la Commission européenne portant sur une directive relative à la protection des données à caractère personnel[6], qui allait aboutir à la directive 95/46/CE que nous connaissons. Les autorités nationales de protection des données ont su ainsi imposer aux gouvernements réunis au sein du Conseil leur agenda politique dans un domaine où ces derniers avaient déjà, dans un premier temps, délégué leurs compétences en interne à une entité sub-étatique, indépendante d'eux.

L'absence de dispositions portant sur des autorités de supervision dans la Convention 108 du Conseil de l'Europe, comparée à l'importance de ces dernières dans l'architecture réglementaire de la directive 95/46/CE, est elle aussi un indice qui rappelle l'absence des autorités dans les négociations de ce premier texte, qui vient renforcer la thèse de Newman.

II. Le G29 aujourd'hui : une ressource plus qu'un lieu uni de décision, ou qu'un embryon d'agence fédérale européenne de protection des données

Si l'article 29 de la directive formalise et institutionnalise cette coopération informelle préexistante des autorités nationales de protection des données personnelles en Europe, elle ne lui confère cependant pas de pouvoirs d'une portée comparable à ceux de ses membres, puisqu'il ne s'agit que d'une instance consultative, présentant ses avis à la Commission et lui proposant éventuellement d'agir dans le cadre

[5] Simitis, Spiros. 1990. *Simitris Reports Data Protection Chaos*. *Transnational Data and Communications Report* (juin-juillet)

[6] 13 septembre 1990, *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and Information security*

d'actes délégués, soumis de toutes façons à une procédure de comitologie[7] fortement contrôlée et contrainte par les exécutifs nationaux des États membres.

La question se pose de savoir si cet esprit d'entrepreneuriat politique des premières heures a perduré après l'adoption de la directive. Certains signes extérieurs semblent en effet pointer vers une tentative de « fédéraliser » la supervision des données personnelles au niveau du G29.

La multiplication du nombre de comptes à des services en ligne a créé un marché pour les services permettant de se connecter avec un identifiant à plusieurs comptes en même temps. Microsoft avait au début des années 2000 lancé le produit Passport.NET pour offrir ce type de service. Les données collectées par les prestataires partenaires étaient centralisées et servaient à l'établissement d'un profil marketing. En 2002, le G29 s'est saisi de la question en publiant un rapport mettant en lumière plusieurs éléments d'inquiétude vis-à-vis de ce service, et déplorant le manque d'information des usagers. Microsoft avait alors incorporé les recommandations des superviseurs européens.

Plus récemment, le G29 a su attirer l'attention par son action conjointe à l'égard de Google. Le 2 février 2012, Jacob Kohnstamm, président du G29, a écrit à *Google Inc.* pour demander des clarifications au sujet de la fusion des règles de protection des données de plusieurs services gérés par Google[8]. Cette lettre informait le PDG de Google de l'intention du G29 d'évaluer la conformité de la nouvelle politique de confidentialité de Google à la lumière de la législation européenne, et demandait la suspension de la mise en œuvre des nouvelles règles en attente du résultat de cette analyse. Google refusa cette dernière demande et en informa le G29 par courrier[9], qui procéda malgré tout à l'évaluation prévue et conclut à la violation par Google de la directive 95/46/CE en raison d'une information insuffisante des utilisateurs, de la violation du principe de limitation des finalités, et de l'absence d'indication quant à la durée de conservation des données[10].

Suite à cela, les autorités nationales de protection des données personnelles française, italienne, espagnole, britannique et hambourgeoise se sont regroupées pour sanctionner Google chacune selon la procédure nationale[11]. L'autorité espagnole a imposé une amende de 900.000 euros[12] et la CNIL 150.000 euros[13]. Le 15 décembre 2014, le CBP néerlandais a annoncé avoir mis Google en demeure d'adapter sa politique de confidentialité avant fin février 2015, sous peine d'une astreinte dont le montant pourrait atteindre jusqu'à 15 millions d'euros[14]. Et fin février 2015, l'autorité italienne de protection des données a annoncé un accord avec Google[15], selon lequel l'entreprise avait jusqu'en janvier 2016 pour se mettre en conformité. S'il est possible d'interpréter cette décision comme un nouveau délai accordé – de près d'un an par rapport au délai contenu dans la décision néerlandaise – le fait que le *Garante Privacy* italien soit parvenu à un accord montre l'efficacité que peut revêtir une procédure à l'échelle européenne.

---

[7] Procédure selon laquelle la Commission, assistée par des représentants des États-membres, est habilitée par le Conseil des ministres à arrêter des mesures exécutives, c'est-à-dire des mesures qui appliquent les lois européennes, et qui correspondent à ce que l'on connaît, dans les États-membres, comme étant les arrêtés ministériels et les ordonnances.

[8] *Letter from the Article 29 Working Party addressed to Google regarding the upcoming change in their privacy policy*. 2 February 2012.

[9] *Reply from Google addressed to the Article 29 Working Party regarding the upcoming changes in their privacy policy*. 3 February 2012.

[10] *Letter from the Article 29 Working Party*. 16 October 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf

[11] *Der Hamburgische Beauftragte für Datenschutz un Informationsfreiheit* (HmbBfDI). Communiqué de presse : *Google's Privacy Policy under Scrutiny*. 2 avril 2013 : http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2013-04-02_Google_PrivacyPolicy.pdf

[12] Agencia Española de Protección de Datos (AEPD). 18 décembre 2013. *Resolución* R/02892/2013 *Procedimiento* Nº PS/00345/2013.

[13] Commission Nationale Informatique et Libertés (CNIL). 2014. Délibération n° 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc.

[14] Voir https://cbpweb.nl/en/news/cbp-issues-sanction-google-infringements-privacy-policy

[15] Voir www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740585

L'analyse détaillée de la procédure à l'encontre de *Google Inc.* illustre cependant le fait que le G29 sert en fait souvent à « démultiplier » le rôle d'une autorité nationale. C'est en effet la CNIL qui a pris la direction de l'enquête sur *Google Inc.*, qui ne s'y trompe pas : c'est Google France qui a répondu à la lettre à la lettre du président du G29 du 2 février 2012 sur sa nouvelle politique de confidentialité, par un courrier envoyé à la CNIL. Le communiqué de presse publié le 16 octobre 2012 sur le site du G29[16] est un communiqué de la CNIL. Et à l'heure actuelle, seules quelques autorités ont sanctionné Google dans le cadre de sa nouvelle politique de confidentialité[17], la plupart n'ayant même pas enclenché de procédure interne !

L'absence de véritable procédure commune de sanction peut s'expliquer par l'absence de caractère contraignant des décisions du G29. De plus, l'analyse par une autorité chef-de-file, et les éléments de dossiers qu'elle collecte, ne peuvent généralement pas être légalement utilisés dans leur ordre juridique interne et leurs procédures internes par les autorités d'autres États membres. Plusieurs acteurs étrangers de la protection des données – qui ont préféré garder l'anonymat pour ne pas engager les autorités pour lesquelles ils travaillent – ont indiqué que selon eux, cette procédure est une tentative dont le but réel est de pallier l'absence de moyens de l'autorité irlandaise de protection des données. Mais Google Irlande n'a par exemple aucune obligation de laisser entrer des agents d'une autorité étrangère, même membre de l'Union européenne et mandatés par le président du G29, pour une inspection sur place. Enfin, la coordination entre les autorités nationales n'est à l'heure actuelle même pas appuyée par un système cohérent de partage d'informations. Il n'existe pas, contrairement à d'autres domaines de la coopération européenne, d'extranet commun à ces autorités qui permettrait un partage sécurisé des données.

Cette utilisation du G29 comme « démultiplicateur » des capacités d'une autorité nationale se voit aussi dans la façon dont les « petites autorités » font un usage plus systématique des avis du G29 que les « grandes ». Le G29 a adopté, depuis sa création, un nombre important d'avis visant à clarifier certaines des notions de la directive 95/46/CE ou à définir des lignes directrices propres à un secteur d'activité. Il arrive que ces opinions contiennent des recommandations qui vont au-delà de ce que prescrit explicitement la directive. C'est le cas notamment de l'avis 10/2004 sur l'harmonisation des dispositions en matière d'information[18]. La question se pose alors pour un responsable de traitement de savoir s'il peut se baser de façon fiable sur ces avis pour sa propre politique de confidentialité. Traduit d'une façon plus « politique », il s'agit de savoir si les autorités nationales répercutent, utilisent et se basent dans leurs décisions sur ces avis du G29. Quinze décisions de trois autorités ont été étudiées. Toutes les décisions hongroises analysées faisaient référence à un ou plusieurs avis du G29, ainsi que deux des cinq décisions françaises, mais aucune des décisions espagnoles. Comme la CNIL française dispose de plus de moyens que l'AEPD espagnole[19], le facteur « ressources » n'est pas le seul qui semble entrer en jeu. Cependant, si l'AEPD et la CNIL ont des ressources similaires (respectivement 14,4 millions et 15,8 millions d'euros en 2011), la NAIH ne disposait en 2012, date de sa création, que de 1,3 million d'euros pour exercer des compétences qui vont au-delà de celles de la CNIL ou l'AEPD, puisqu'elle est aussi responsable de l'accès aux documents administratifs. Il faudrait vérifier avec les

[16] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[17] Aux Pays-Bas, le régulateur se demande encore quelles mesures il va prendre : http://www.dutchdpa.nl/Pages/pb_20131128-google-privacypolicy.aspx L'autorité italienne a donné dix-huit mois à Google pour se mettre en conformité. En Angleterre, l'ICO avait donné à Google jusqu'au 20 septembre 2013 pour apporter les changements demandés, mais n'a, à l'heure actuelle, pas encore donné suite : http://www.theregister.co.uk/Print/2014/07/22/uk_watchdog_is_still_probing_googles_2012_privacy_tweak/

[18] Avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations ». http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_fr.pdf

[19] Rossi. Julien. 2013. Les autorités nationales de protection des données personnelles dans l'Union européenne - Étude des causes des manquements constatés par la cour de justice de l'Union Européenne, Lille : Institut d'Etudes Politiques. Disponible en ligne sur le site de l'AFCDP : http://afcdp.net/IMG/pdf/rossi_julien_memoire_autorites_nationales_de_pdp.pdf

autres « petites » autorités nationales si la même propension à se référer aux avis du G29 se retrouve, mais il est possible de formuler l'hypothèse selon laquelle les autorités disposant de peu de moyens trouvent dans le G29 un vivier d'expertise utile et permettant de compenser en partie le manque de moyens internes. Quoiqu'il en soit, le résultat de cette courte enquête prouve que contrairement à ce qu'avance Newman dans son ouvrage publié en 2008, les avis du G29 n'ont pas le même impact interne dans chaque État membre.

La participation au G29 des autorités disposant de moyens limités est aussi contrainte par le fait qu'il ne dispose pas de son propre budget. La participation aux travaux et les déplacements sont financés par les autorités elles-mêmes. La présidence du G29 est assurée par le budget et le personnel de l'autorité dont le dirigeant a été élu, et seuls les déplacements sont pris en charge par la Commission.

III. Des outils pour les CIL

Bien que cela soit rare, il convient tout d'abord de souligner qu'il arrive au G29 de prendre contact directement avec des responsables de traitement. Les cas précédemment décrits de Microsoft, avec Passport.Net, et de Google plus récemment, en sont des illustrations. Il arrive également que le contact avec le G29 soit à l'initiative du responsable de traitement, ou d'associations professionnelles. C'est ainsi que le G29 a été amené à se prononcer sur une proposition de cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID). De tels contacts sont cependant relativement rares et, étant donné le faible poids au quotidien du G29 sur l'immense majorité des responsables de traitement, c'est ailleurs que les CIL peuvent aujourd'hui trouver un intérêt à ses travaux.

Deux catégories d'outils proposés par le G29 paraissent dès aujourd'hui pertinentes pour les Correspondants Informatique et Libertés : les avis du G29, et la procédure européenne de reconnaissance mutuelle des règles contraignantes d'entreprise comme base légale permettant le transfert de données vers des pays tiers.

III.1. Les avis du G29

Le groupe a été amené à adopter un grand nombre d'avis sur des thèmes variés[20], des données biométriques à la protection des données des enfants. Une présentation plus intuitive sur le site Internet du G29 permettrait sans doute de mieux faire le tri entre les avis encore pertinents et utiles aux responsables de traitement, et ceux qui sont soit périmés (comme l'avis 3/1997 sur l'anonymat sur Internet, techniquement dépassé depuis longtemps), soit destinés à la Commission et donc sans grand intérêt pour les CIL.

Les avis du G29 contiennent parfois des recommandations pragmatiques à l'usage des responsables de traitement. C'est le cas par exemple de l'avis 4/2004 sur la vidéosurveillance[21] qui propose un guide concret de la réflexion à suivre pour aboutir à une politique de confidentialité conforme à la directive. L'avis 10/2004[22], qui porte sur l'information à donner aux personnes concernées, propose lui aussi des exemples. Plus récent, l'avis 5/2014 présente les avantages et les inconvénients de plusieurs techniques d'anonymisation.

[20] Les avis et recommandations du G29 sont en ligne sur le site Internet de la Commission : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[21] *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

[22] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_fr.pdf

D'autres avis sont quant à eux intéressants car ils sont des éléments de doctrine qui ont une influence forte sur les autorités nationales à l'échelle de l'Union, même si celle-ci varie d'une autorité à l'autre en fonction de la connaissance qu'en ont les agents. L'avis 1/2010 présente ainsi les notions de responsable de traitement et de sous-traitant et décrit en détail les situations dans lesquelles un sous-traitant peut être requalifié de responsable de traitement. L'avis 4/2007 sur le concept de donnée personnelle est lui aussi intéressant, car il entérine à un niveau européen une évolution de la notion, qui ne saurait être conçue de façon absolue (donnée personnelle / donnée non-personnelle) mais de façon relative : est une donnée personnelle toute donnée que le détenteur est en mesure de relier à une personne physique.

Il serait difficile de dresser un tableau exhaustif des avis pouvant intéressant les responsables de traitement, car nombre de ces avis sont des avis sectoriels (vidéosurveillance, RFID[23], données PNR[24]…) et ne concernent pas tous les CIL. Quoiqu'il en soit, ils peuvent s'avérer une ressource utile pour une mise en conformité pensée en rapport avec la directive, et donc à un niveau européen.

III.2. Les règles contraignantes d'entreprise

Les règles contraignantes d'entreprise de l'Union européenne[25], ou BCR (de l'anglais *Binding Corporate Rules*) sont un moyen pour un groupe d'entreprises international de faciliter les transferts de données personnelles en son sein, entre ses filiales situées dans et hors de l'Union européenne. Elles ne sont pas prévues par la directive, mais se fondent sur l'article 26 paragraphe 2 qui dispose que :

> […] un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

Les BCR sont un moyen de prouver la garantie offerte par le responsable de traitement, au même titre que les clauses contractuelles types de la Commission européenne. Cet outil a été créé en 2003 par le G29, et la procédure de reconnaissance mutuelle date de 2005[26].

Cette procédure se déroule en plusieurs étapes[27] :

- dans un premier temps, le groupe ayant rédigé un projet de BCR doit désigner une autorité chef-de-file là où il a son établissement principal sur le territoire de l'Union ;
- ensuite, l'autorité chef-de-file envoie son analyse à deux autres autorités, qui analysent à leur tour les BCR ;

---

[23] *Radio frequency identification*, ou radio-identification : méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (*RFID tag* ou *RFID transponder* en anglais).

[24] *Passenger Name Record* : les données des dossiers passagers sont des données personnelles concernant tous les détails d'un voyage pour des passagers voyageant ensemble. Les États-Unis, le Canada, l'Australie et le Royaume-Uni se sont dotés d'un tel système de surveillance, le Royaume-Uni dans le cadre du programme e-borders, dont fait partie le système Semaphore et les États-Unis dans le cadre du programme US-VISIT.

[25] Il existe un équivalent, au niveau de l'Association francophone des autorités de protection des données personnelles (AFAPDP) et de l'APEC (les *Cross Border Privacy Rules*, CBPR). Attention toutefois : des règles contraignantes approuvées par l'AFAPDP ou par l'APEC ne sont pas automatiquement valables au niveau du G29.

[26] *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules*

[27] Le détail de la procédure est en ligne sur le site de la CNIL : http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/les-bcr/

- puis, le projet de BCR et l'analyse sont envoyés à toutes les autorités participant au mécanisme de reconnaissance mutuelle, puis à toutes les autorités du G29 ;
- des commentaires sont envoyés au groupe candidat, qui doit alors les prendre en compte et proposer des modifications ;
- une fois que l'autorité chef-de-file est satisfaite des modifications apportées, elle propose aux autres autorités de les approuver. Un consensus entre autorités est nécessaire pour cette étape.

Une fois les BCR approuvés, le groupe doit cependant toujours procéder aux demandes d'autorisation de transfert dans chaque État membre d'où il veut transférer des données, mais les autorités nationales participant au mécanisme de reconnaissance mutuelle s'engagent à accorder l'autorisation dès lors que les BCR ont été préalablement approuvés au niveau du G29. Ceci montre les limites du pouvoir du G29, qui ne peut pas lui-même créer du droit. L'existence de BCR devrait être entérinée par le projet de règlement actuellement en cours de négociation, mais en l'attente de cette réforme, les BCR sont une construction nouvelle, non prévue par la législation actuelle, mais devant s'insérer dans le cadre fourni par cette dernière.

En règle générale, l'autorité chef-de-file prend cinq mois pour analyser une candidature de BCR. Ensuite, il faut attendre en moyenne trois mois et demi pour que la procédure de reconnaissance mutuelle suive son cours, après quoi le plus long est la prise en compte des remarques par le groupe candidat, puisque ce délai est en moyenne de sept mois et demi (Privacy Laws & Business, 2013).

Les BCR peuvent être un outil efficace pour nombre de responsables de traitement. Il convient toutefois de souligner que toutes les autorités ne participent pas au mécanisme de reconnaissance mutuelle. Seuls les vingt-et-un pays suivants participaient au moment de la rédaction de cet article : l'Allemagne, l'Autriche, la Belgique, la Bulgarie, Chypre, l'Espagne, l'Estonie, la France, la Grande Bretagne, l'Irlande, l'Islande, l'Italie, la Lettonie, le Liechtenstein, le Luxembourg, Malte, la Norvège, les Pays-Bas, la République tchèque, la Slovaquie et la Slovénie. La plupart des autres États membres de l'Union acceptent quand même les BCR, mais selon une procédure différente, qui varie d'un État à l'autre. Le droit hongrois pose plus particulièrement problème, puisque l'article 8 de la loi hongroise sur la protection des données (loi CXII de 2011) ne reconnaît que le consentement, les décisions de conformité de la Commission et les traités internationaux conclus entre la Hongrie et des États tiers comme base légale permettant le transfert de données personnelles. Bien que l'autorité hongroise de protection des données demande depuis plusieurs années la possibilité de participer au mécanisme de reconnaissance mutuelle des BCR, cette demande n'a toujours pas été prise en compte par le législateur. Les données en provenance de ce pays doivent donc être exclues des transferts vers des pays tiers, ce qui prouve que malgré tout l'intérêt de l'outil que sont les BCR, en dehors des vingt-et-un États participant au mécanisme de reconnaissance mutuelle du G29, il convient de demeurer vigilant dans l'utilisation des BCR et de vérifier le droit national applicable au cas-par-cas.

IV. Le futur du G29

Le projet de règlement européen devrait transformer le G29 d'aujourd'hui en Comité européen de la protection des données, ou *European Data Protection Board* en anglais (EDPB[28]). Cette transformation fait suite à des demandes de la part du G29 d'avoir, notamment, plus de poids dans la résolution d'affaires touchant plusieurs États membres[29]. L'article 66 de la proposition de règlement,

[28] L'acronyme EDPB est préférable à CEPD, puisque CEPD désigne aussi le Contrôleur européen de la protection des données.

[29] Les demandes du G29 adressées à la Commission préalablement à la publication de la communication 2012 011 COM contenant le projet de règlement réformant la directive 95/46/CE actuellement en vigueur peuvent être trouvées dans la lettre adressée à la commissaire Reding en 2011 (G29, 2011a).

qui liste les tâches du futur EPDB, n'inclut aucune mission de nature à le mettre en contact avec des responsables de traitement, ni aucune responsabilité vis-à-vis, par exemple, des CIL.

Le règlement introduit plusieurs modifications, comme par exemple le fait que le secrétariat ne sera plus assuré par la Commission, mais par le Contrôleur Européen de la Protection des Données (CEPD). La principale nouveauté consiste en la consécration du mécanisme de reconnaissance mutuelle des BCR, décrit à l'article 43 du règlement. La nouvelle procédure de reconnaissance mutuelle se base sur celle – nouvelle elle aussi – de la procédure du mécanisme de contrôle de la cohérence.

Selon la procédure de cohérence, les autorités nationales sont habilitées à prendre les décisions portant sur les responsables de traitement ayant leur établissement principal dans leur aire de compétence géographique (art. 51-2 de la proposition de règlement). La certification de BCR est au nombre de ces décisions pour lesquelles sont compétentes les autorités nationales. L'EDPB dispose ensuite d'un mois au maximum pour donner un avis sur la décision affectant la protection des données au niveau européen (art. 58-7). Il ne s'agit que d'un avis simple, que l'autorité nationale compétente n'est pas tenue de respecter. La Commission peut cependant décider (art. 59) de suspendre la décision de l'autorité nationale compétente pendant une durée pouvant aller jusqu'à un an (art. 60). Ceci diminue le pouvoir qui est celui actuel du G29 dans le processus de certification des BCR, réduit considérablement la durée de la consultation par rapport aux délais actuels, et accroît les pouvoirs de la Commission en matière de protection des données. Cette dernière peut en effet intervenir non seulement en matière de BCR, mais dans toute autre procédure relative à des traitements de données affectant plusieurs États membres. La Commission étant un organe politique, ceci semble difficilement compatible avec la jurisprudence de la CJUE[30] sur l'indépendance des autorités de protection des données[31]…

En créant cette nouvelle procédure, ainsi qu'une procédure permettant aux autorités de mettre en commun des ressources humaines sous l'autorité d'un chef-de-file pour l'organisation de contrôles conjoints, la réforme proposée par la Commission accentue la transformation du G29 en une ressource matérielle et politique utilisée à disposition des autorités nationales, et renforce la Commission tout comme le CEPD. La production d'avis ne devrait pas être affectée par ce changement, mais il incombera au premier président de l'EDPB de faire en sorte que le G29 ne perde pas ce qu'il avait d'unité si ce forum de décision souhaite demeurer pertinent pour définir la mise en œuvre de la politique européenne de protection des données.

V. Conclusion

On ne peut pas dire que le G29 soit une entité singulière, disposant d'une identité propre. En l'état actuel des choses, le G29 reste avant tout un réseau transgouvernemental, c'est-à-dire, selon Keohane et Nye[32] « Un jeu d'interactions parmi des sous-unités de différents gouvernements qui ne sont pas contrôlées ou guidées de près par les politiques gouvernements ou par ses ministres[33] ».

[30] La Cour de justice de l'Union européenne (CJUE), anciennement Cour de justice des Communautés européennes (CJCE), est l'une des sept institutions de l'Union européenne. Elle regroupe trois juridictions : la Cour de justice, le Tribunal et le Tribunal de la fonction publique. Le siège de l'institution et de ses différentes juridictions, est à Luxembourg.

[31] Voir à ce sujet les décisions : CJUE 9 mars 2010, Commission contre République Fédérale d'Allemagne, aff. C-518/07, Rec. p. I- 01885 ; CJUE 16 octobre 2012, Commission contre République d'Autriche, aff. C-614/10, non encore publiée au recueil ; CJUE 8 avril 2014, Commission contre Hongrie, aff. C-288/12, non encore publiée au recueil

[32] Keohane, R.O. & Nye, J.S. 1974. *Transgovernmental relations and international organizations*. World Politics 27: 39–62

[33] Traduction de l'auteur

Ce réseau représente avant tout une ressource pour les autorités nationales qui peuvent s'en servir de levier pour leurs activités d'entrepreunariat intergouvernemental, à l'image de la façon dont la CNIL a expérimenté dans l'affaire Google mentionnée ci-dessus ce que pourraient être des contrôles conjoints dans le futur. Cet « activisme institutionnel » d'autorités nationales a un effet puisque le projet de règlement officialise certaines des évolutions informelles du G29 qui sont le fait de telles entreprises politiques. Il peut aussi servir de ressource matérielle et en expertise pour des autorités nationales à taille et moyens réduits, et cette tendance est appelée à s'accentuer si la réforme proposée par la Commission est adoptée.

Il n'est cependant pas à négliger. Ce forum de discussion entre membres des autorités nationales – car ce sont bien les agents qui travaillent dans les sous-groupes préparant les décisions et avis du G29 – contribue à unifier la vision qu'ont les autorités nationales de certaines questions techniques ou légales en matière de protection des données. Les avis du G29 sont des éléments incontournables de doctrine en la matière, et ils ont l'avantage d'être valables sur tout le territoire de l'Union. Enfin, le G29 s'est montré capable à plusieurs reprises d'influencer des réformes législatives. S'il continue à développer une logique d'entrepreneuriat, il pourrait devenir un partenaire incontournable des CIL, tant au niveau de CEDPO qu'au niveau des responsables de traitement qui, par leur importance et leur échelle européenne ou mondiale, ne peuvent efficacement être supervisés qu'à un niveau européen.

Julien ROSSI, Membre de l'AFCDP. Lors de la rédaction de ce texte, il était chargé de missions pédagogiques à l'université de Szeged (Hongrie). Il est actuellement Doctorant au laboratoire COSTECH de l'Université de technologie de Compiègne (UTC). Julien a suivi un Master en Affaires européennes à l'Institut d'Études Politiques de Lille où il a publié un mémoire de recherche sur la jurisprudence de la Cour de justice de l'Union européenne sur les autorités nationales de protection des données personnelles, avant de faire un stage de fin d'études à l'Autorité nationale pour la protection des données et la liberté de l'information, en Hongrie, puis au service international de la Commission Nationale Informatique et Libertés.