Le CEPD en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations: tirer profit de dix années d'expérience

Document stratégique

Bruxelles, le 4 juin 2014

Synthèse

Le présent document stratégique explique, en se fondant sur dix années d'expérience, la manière dont le Contrôleur européen de la protection des données (CEPD) conseille les institutions de l'UE en ce qui concerne les politiques et la législation.

Le CEPD est l'autorité indépendante de protection des données de l'Union européenne. Nous contrôlons et assurons la protection des données à caractère personnel et de la vie privée dans le cadre du traitement des informations personnelles des individus effectué par les institutions et organes de l'UE et nous conseillons les institutions de l'UE en ce qui concerne les propositions de textes législatifs et de nouvelles politiques.

Depuis la création du CEPD en 2004, le contexte juridique, économique et technologique a connu des évolutions majeures. L'entrée en vigueur du traité de Lisbonne a confirmé la protection des données en tant que principe général du droit de l'UE (voir principalement l'article 8 de la Charte et l'article 16 du TFUE) et un certain nombre de décisions historiques rendues par la Cour de justice européenne a souligné l'importance que revêtent le respect de la vie privée et la protection des données en tant que parties intégrantes du processus de prise de décision de la législature de l'UE.

Conformément à l'article 28, paragraphe 2, du règlement, la Commission a l'obligation de consulter le CEPD dès qu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. La portée de cette obligation est étendue. Conformément à l'article 41 du règlement, le CEPD est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés, ainsi que de conseiller les institutions et organes de l'UE «pour toutes les questions concernant le traitement des données à caractère personnel», et, conformément à l'article 46, point e), nous surveillons les faits nouveaux qui pourraient avoir une incidence sur la protection des données à caractère personnel.

Conformément à la pratique établie, le CEPD est également consulté *de manière informelle* avant l'adoption de ces propositions par la Commission. Nous coopérons de manière constructive avec le Parlement européen, le Conseil et la Commission et restons disponibles pour fournir des conseils ciblés en temps voulu à toutes les étapes du processus de décision de l'UE. Nous agissons de manière sélective sur la base des priorités énoncées dans notre stratégie, dans le plan de gestion annuel et dans notre inventaire. En conséquence, nous centrons notre attention et nos efforts sur des domaines où les risques de non-respect des règles de protection des données ou les répercussions sur la vie privée et la protection des données sont les plus élevés. En vue d'optimiser l'impact et l'utilité de notre travail, nous élaborons **une «boîte à outils des politiques»** - qui comprend des orientations générales à l'attention du législateur, par exemple sous la forme de **lignes directrices** thématiques ou sectorielles - en vue d'aider les institutions à prendre des décisions éclairées sur les incidences des nouvelles propositions en matière de protection des données. À titre d'exemple, nous envisageons de rédiger un **document de référence sur la nécessité et la proportionnalité**.

L'objectif stratégique qui sous-tend les interventions du CEPD est de veiller à ce que la Commission européenne, en sa qualité d'initiateur le plus fréquent, comme le Parlement européen et le Conseil, en leur qualité de co-législateurs, connaissent les exigences relatives à la protection des données et intègrent cette notion aux nouvelles dispositions législatives. Nous

visons à développer une culture de responsabilisation dans laquelle ces institutions reconnaissent la responsabilité qui leur incombe de veiller à la protection des données à caractère personnel lors de l'élaboration de nouvelles politiques de l'UE. À cette fin, nous sommes disposés à conclure un **mémorandum d'accord** avec les trois principales institutions, lequel énoncerait la manière dont nous pouvons, dans la pratique, apporter une valeur ajoutée au processus législatif de l'UE en exerçant notre rôle consultatif.

Table des matières

Le CEPD en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations: tirer profit de dix années d'expérience

1. Introduction

Le présent document stratégique[1] explique, dix ans après la création de l'institution, la manière dont le CEPD conseille les institutions de l'UE en ce qui concerne les politiques et la législation. Il met à jour et remplace un précédent document sur ce sujet, qui a été adopté le 18 mars 2005 et visait à définir le contexte des activités consultatives du CEPD, lesquelles se sont développées depuis cette date[2]. Le présent document stratégique s'adresse à l'ensemble de nos parties prenantes et de nos interlocuteurs dans le processus d'élaboration des politiques de l'UE, y compris à nos collègues des institutions et organes de l'UE dans la mesure où ils connaissent des dossiers qui présentent une pertinence en relation avec la protection des données, et aux autorités nationales chargées de la protection des données qui sont membres du groupe de travail «Article 29».

Le rôle de conseiller des institutions et organes de l'UE qu'assume le CEPD doit être observé au regard de l'importance croissante de la protection des droits fondamentaux au sein de l'ordre juridique de l'UE, de la nécessité de cohérence en tant qu'élément constitutif d'une protection des données efficace et des conclusions de la révision stratégique effectuée par le CEPD en 2011-2012, que nous avons prises en compte dans notre stratégie pour la période 2013-2014 («la stratégie»). Les avis, qui recouvrent un large éventail de domaines politiques de l'UE[3], sont l'expression la plus visible de ce rôle, que nous exerçons conformément à notre règlement intérieur[4] (le «RI du CEPD»).

2. Le contexte juridique

Le CEPD agit en qualité d'autorité indépendante[5], en application de l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne (la «Charte»). Notre rôle consultatif est énoncé dans plusieurs dispositions du règlement n° 45/2001[6], et notamment dans son article 28, paragraphe 2, et dans ses articles 41 et 46. Conformément à l'article 28, paragraphe 2, la consultation du CEPD constitue un élément obligatoire de la procédure législative ordinaire et des procédures spécifiques prévues par les traités lorsque la Commission adopte une proposition de législation. L'article 28, paragraphe 2, doit être lu en combinaison avec l'article 41 du règlement, en application duquel le CEPD est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés, ainsi que

[1] Conformément à l'article 16 du règlement intérieur du CEPD, le CEPD adopte des documents stratégiques pour donner une orientation sur la manière dont des activités spécifiques doivent être exercées.
[2] «Le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes», adopté le 18 mars 2005, disponible sur le site web du CEPD.
[3] Voir le site web du CEPD, rubrique Consultation.
[4] JO L 273 du 15.10.2013, p. 41.
[5] Concernant la nécessité, pour les autorités chargées de la protection des données, de disposer d'une totale indépendance et de compétences suffisantes pour exercer leurs différentes fonctions, voir arrêts du 9 mars 2010, Commission / Allemagne (C-518/07, Rec. p. I-1885); du 16 octobre 2012, Commission / Autriche (C-614/10, non encore publié au Recueil), et du 8 avril 2014, Commission / Hongrie (C-288/12, non encore publié au Recueil).
[6] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

de conseiller les institutions et organes communautaires «pour toutes les questions concernant le traitement des données à caractère personnel»[7].

Depuis la création du CEPD en 2004, le contexte juridique, économique et technologique a connu des évolutions majeures. À la suite de l'entrée en vigueur du traité de Lisbonne, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel ont été renforcés au sein de l'ordre juridique de l'UE (voir principalement l'article 8 de la Charte et l'article 16 du traité sur le fonctionnement de l'Union européenne – le «TFUE») et un certain nombre de décisions importantes rendues par la Cour européenne de justice ont souligné l'importance du respect de la vie privée et de la protection des données en tant que parties intégrantes du processus de prise de décision de la législature de l'UE[8]. Ces éléments ont été pris en compte dans le cadre de la réforme en cours du cadre juridique de la protection des données[9].

3. Le rôle consultatif du CEPD: tirer profit de dix années d'expérience

Au cours de la dernière décennie, nous avons suivi de près la préparation des principaux instruments de protection des données de l'UE, en publiant parfois des contributions successives à différentes étapes de la procédure législative[10]. Nous avons également apporté des contributions aux principaux dossiers législatifs et politiques ayant des répercussions en matière de protection des données[11]. Sur le fondement de cette expérience et dans un esprit d'utilisation efficace des ressources, nous élaborons actuellement une nouvelle **«boîte à outils des politiques»** - qui comprend des **lignes directrices** thématiques ou sectorielles[12] - en vue, d'une part, d'aider le législateur à prendre des décisions éclairées sur les incidences en matière de protection des données de nouvelles propositions, conformément aux principaux principes

[7] Dans ses ordonnances du 17 mars 2005, Parlement / Conseil (C-317/04, Rec. p. I-2457) et Parlement / Commission (C-318/04, Rec. p. I-2467), la Cour a confirmé le champ d'application étendu de cette notion en affirmant expressément que la «mission consultative ne vise pas uniquement les traitements de données à caractère personnel effectués par ces institutions ou organes».

[8] Voir, par exemple, arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, Rec. p. I-11063) et, plus récemment, du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a. (C-293/12 et C-594/12, non encore publié au Recueil).

[9] Communication de la Commission du 25 janvier 2012 «Protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle», COM(2012) 9 final; 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; proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final.

[10] À titre d'exemple, nous avons formulé trois avis distincts sur la décision-cadre 2008/977/JAI (projet) relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale et deux avis sur la dernière révision de la directive 2002/58/CE «vie privée et communications électroniques», et nous sommes intervenus à de multiples reprises au sujet du paquet de mesures pour une réforme de la protection des données (en cours).

[11] P. de Hert et V. Papakonstantinou, «The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations», *Data protection Anno 2014: How to Restore Trust?* (en français, «Le CEPD, en tant que seule partie prenante dans le paysage européen de la protection des données, répond aux attentes explicites comme implicites», *Protection des données - année 2014: comment restaurer la confiance?*) Intersentia 2014, p. 249.

[12] Par exemple, des lignes directrices sectorielles sur la protection des données dans le domaine des services financiers seront adoptées en 2014.

énoncés dans la partie 4 ci-après et, d'autre part, de mettre davantage l'accent sur notre consultation.

Lorsque nous exerçons le rôle de conseiller, nous nous appuyons non seulement sur l'expérience que nous avons accumulée en matière de conseil aux institutions, mais également sur l'expertise que nous avons acquise dans le domaine du contrôle. Ces deux rôles principaux sont complémentaires et nous nous efforçons de tirer parti des synergies qu'ils présentent et d'assurer la cohérence entre les principes préconisés dans notre politique et notre travail de contrôle.

3.1. Nos valeurs fondamentales et nos principes directeurs

Conformément à notre stratégie[13], nos activités reposent sur les valeurs fondamentales d'impartialité, d'intégrité, de transparence et de pragmatisme. Ces principes sont mis en œuvre de la manière suivante:

- ***Impartialité***: *travailler au sein du cadre législatif et politique existant tout en faisant preuve d'indépendance et d'objectivité et en trouvant le juste équilibre entre les différents intérêts en jeu*.
  - Tout au long du processus législatif, nous coopérons de manière constructive avec le Parlement européen, le Conseil et la Commission européenne, en conservant la même distance vis-à-vis de chacune des trois institutions.
  - L'impartialité est également un principe directeur lorsque nous choisissons, le cas échéant, d'agir également de manière anticipatoire.

- ***Intégrité***: *observer les normes de conduite les plus élevées et faire ce qui est juste même si cela s'avère impopulaire*.
  - Nous conseillons sur la clarté de la formulation des textes législatifs pour assurer le traitement univoque et cohérent des questions de protection des données.
  - Nous formulons nos conseils en temps opportun afin d'être utiles aux étapes appropriées de la procédure législative.
  - Sur le fond, nous fournissons des conseils cohérents sous la forme appropriée. En ce qui concerne les propositions législatives de la Commission ayant une incidence sur la protection des données, nous formulerons généralement des avis formels.
  - Nous appliquons le principe de sélectivité et fixons des priorités dans notre inventaire[14]. En particulier, nous centrons notre attention et nos efforts sur des domaines où les risques de non-respect des règles de protection des données ou les répercussions sur la vie privée et la protection des données sont les plus élevés.
  - Nous visons à fournir des conseils pertinents faisant autorité en nous fondant sur l'expertise unique que nous avons développée au cours des dix dernières années concernant la législation et la pratique de la protection des données - y compris le contrôle - ainsi que la technologie pertinente.

[13] Stratégie, p. 15.
[14] Voir partie 5 ci-après.

- ***Transparence:*** *expliquer ce que nous faisons et pourquoi nous le faisons dans un langage clair et accessible à tous.*
  - Nous nous appuyons sur un inventaire annuel, un instrument qui garantit la cohérence de nos décisions d'intervenir ou de nous abstenir et leur transparence vis-à-vis de nos parties intéressées.
  - Nous coopérons de manière constructive avec les institutions de l'UE et d'autres autorités chargées de la protection des données, des organes de contrôle, des organisations internationales et d'autres parties prenantes, en recherchant la cohérence de la protection des données et l'application de normes exigeantes en la matière dans toute l'UE.
  - En ce qui concerne la procédure, nous nous efforçons de nous tenir à tout moment à la disposition de toute partie prenante pour aider à identifier des solutions.
  - Nous expliquons des questions techniques complexes d'une manière qui soit compréhensible pour les non-spécialistes, tout en demeurant exacte d'un point de vue technique et scientifique.

- ***Pragmatisme:*** *comprendre les besoins des parties prenantes et rechercher des solutions qui fonctionnent dans la pratique.*
  - Nous donnons des conseils objectifs fondés sur une analyse et non sur des perceptions.
  - Nous nous appuyons sur l'expérience acquise dans le cadre de nos fonctions de contrôle pour recommander des solutions qui soient réalisables dans la pratique. Nous œuvrons pour trouver des solutions pratiques, notamment dans des domaines politiques complexes où il peut s'avérer difficile de trouver le juste équilibre.
  - Nous cherchons à garantir que la protection des données fera partie intégrante de l'élaboration des politiques et du processus législatif, tout en garantissant un juste équilibre avec d'autres intérêts publics et droits fondamentaux.

L'objectif stratégique qui sous-tend ces valeurs est de veiller à ce que la Commission européenne, en sa qualité d'initiateur le plus fréquent, comme le Parlement européen et le Conseil, en leur qualité de co-législateurs, connaissent les exigences relatives à la protection des données et intègrent cette notion aux nouvelles dispositions législatives[15]. Nous visons à développer une culture de responsabilisation dans laquelle ces institutions reconnaissent la responsabilité qui leur incombe de veiller à la protection des données à caractère personnel lors de l'élaboration de nouvelles politiques de l'UE.

À cette fin, nous nous sommes disposés à conclure un **mémorandum d'accord** avec les trois principales institutions (le Parlement, le Conseil et la Commission) qui énoncerait la manière dont nous pouvons, dans la pratique, apporter une valeur ajoutée au processus législatif de l'UE en exerçant notre rôle consultatif.

[15] Stratégie, p. 11.

3.2. La portée étendue de notre rôle consultatif

Dans tous les domaines. Conformément à l'article 28, paragraphe 2, du règlement, toutes les propositions de législation qui comprennent des dispositions sur le traitement de données à caractère personnel, qui s'appuient sur le cadre juridique existant en matière de protection des données, qui le complètent ou qui le modifient ou qui ont une incidence significative sur la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel doivent être soumises à la consultation du CEPD. En d'autres termes, il n'est pas nécessaire, pour qu'une proposition de législation déclenche l'examen du CEPD, qu'elle ait une incidence directe sur les règles de l'UE relatives à la protection des données elles-mêmes. En conséquence, au fil des années, nous avons couvert un grand nombre de domaines politiques.

Anticipatoire. Notre rôle de conseiller général concernant toutes les questions de protection des données au niveau de l'UE signifie que nous ne conseillons pas uniquement en réponse à une consultation de la Commission (ou à une demande de conseil formulée par une autre institution), mais également de notre propre initiative, lorsqu'une question revêt une importance significative dans ce domaine. En outre, dans les domaines dans lesquels l'activité législative est intense ou qui ont une incidence particulièrement significative sur la protection des données à caractère personnel, nous développons des orientations générales dans des lignes directrices thématiques ou sectorielles ou d'autres instruments adaptés.

À toutes les étapes. Afin de réaliser au mieux nos objectifs de sensibilisation et de renforcer la qualité des politiques de l'UE, nous sommes prêts à donner des conseils à toutes les étapes de la procédure législative, des premières phases de l'élaboration des politiques jusqu'aux discussions au sein du Parlement et du Conseil aux différentes étapes du processus d'élaboration des lois de l'UE. Dans certains cas, ceci peut supposer d'intervenir à plusieurs reprises au cours des différents stades de la procédure.

Auprès de multiples parties prenantes. Par nos avis, observations et autres formes d'intervention, nous visons à sensibiliser non seulement les membres des institutions et organes de l'UE, mais également le grand public aux questions de protection des données[16].

Évaluer la complexité (technologique). L'incidence d'une proposition de législation sur la protection des données à caractère personnel n'est pas toujours claire, compte tenu en particulier de la nature technique du traitement des données, de l'incidence des technologies de l'information et de la complexité de nombreux dossiers législatifs. Pour répondre à ce défi, nous disposons de l'expertise et des connaissances nécessaires dans le domaine des technologies de l'information pour suivre les évolutions technologiques et évaluer leurs incidences sur la protection des données et le respect de la vie privée.

4. Analyser l'incidence sur le respect de la vie privée et la protection des données

La présente partie expose en termes généraux la manière dont nous évaluons, au regard de la jurisprudence de la Cour de justice, l'incidence des mesures proposées sur les droits au respect de la vie privée et à la protection des données personnelles[17].

[16] Voir ci-après partie 6.5 «Transparence et confidentialité».

[17] Elle peut être lue conjointement à la «"check-list" droits fondamentaux» proposée par la Commission dans sa stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne (COM(2010) 573).

4.1. Les mesures supposent-elles le traitement de données à caractère personnel?

Lorsque les parties prenantes s'interrogent sur l'opportunité de faire intervenir le CEPD dans une procédure d'élaboration d'une législation ou d'une politique, la première question à laquelle elles doivent répondre porte sur le point de savoir si l'instrument (proposé) suppose le traitement de données à caractère personnel.

L'expression «traitement de données à caractère personnel» recouvre toute opération, automatisée ou non, telle que la collecte, l'enregistrement, la conservation, l'utilisation, la communication, la transmission ou toute autre forme de mise à disposition appliquée à toute information concernant une personne physique identifiée ou identifiable[18].

En conséquence, la notion de «données à caractère personnel» englobe beaucoup plus d'informations que les données permettant d'identifier directement une personne, comme un nom[19], un numéro national d'enregistrement ou un numéro d'identification fiscal. La Cour de justice a établi que la notion de données à caractère personnel englobe également, entre autres éléments: les informations concernant la rémunération[20], les montants des subventions agricoles perçues[21], les informations biométriques[22], les adresses IP[23], les données relatives au trafic et les données de localisation[24], le montant des revenus du travail et du capital et celui du patrimoine des personnes physiques[25], les périodes de travail journalières, les périodes de repos ainsi que les interruptions et pauses correspondantes[26]. Dans ce contexte, nous renvoyons à l'avis n° 4/2007 du groupe de travail «Article 29», qui fournit une analyse approfondie et de nombreux exemples[27]. L'avis comporte en particulier une analyse des quatre principaux éléments de la définition, à savoir «toute information», «concernant», «[personne physique] identifiée ou identifiable» et «personne physique», dont chacun doit être évalué afin de déterminer si des «données à caractère personnel» sont en jeu dans une situation donnée.

4.2. Le droit de l'UE sur le respect de la vie privée et la protection des données

Lorsqu'une proposition de législation ou une autre mesure suppose le traitement de données à caractère personnel, cette mesure doit être conforme au droit primaire de l'UE, et en particulier aux articles 7 et 8 de la Charte. Le droit au respect de la vie privée prévu à l'article 7 de la Charte sera applicable dans de nombreux cas et le droit à la protection des données le sera dans tous les cas.

Les articles 7 et 8 sont étroitement liés, mais sont de nature différente et définissent des exigences distinctes qui doivent être satisfaites pour assurer la conformité.

L'article 7 peut être considéré comme un droit fondamental classique qui protège les personnes physiques, en premier lieu, contre toute ingérence de l'État. L'article 7 correspond globalement

[18] Article 2, points a) et b), commun à la directive 95/46/CE et au règlement n° 45/2001.
[19] Arrêts du 6 novembre 2003, Lindqvist (C-101/01, Rec. p. I-12971, point 24), et du 7 mai 2009, Rijkeboer (C-553/07, Rec. p. I-3889, point 42).
[20] Arrêt du 20 mai 2003, Österreichischer Rundfunk e.a. (C-465/00, C-138/01 et C-139/01, Rec. p. I-4989, point 64).
[21] Arrêt Volker und Markus Schecke, précité, note 8 ci-dessus, point 60.
[22] Arrêt du 17 octobre 2013, Schwarz (C-291/12, non encore publié au Recueil, point 27).
[23] Arrêt du 24 novembre 2011, Scarlet Extended (C-70/10, Rec. p. I-11959, point 51).
[24] Arrêt Digital Rights Ireland, précité, note 7 ci-dessus, points 26 et 29.
[25] Arrêt du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia (C-73/07, Rec. p. I-9831, points 35 et 37).
[26] Arrêt du 30 mai 2013, Worten (C-342/12, non encore publié au Recueil, point 19).
[27] Avis 4/2007 sur le concept de données à caractère personnel, WP 136, adopté le 20 juin 2007.

à l'article 8 de la Convention européenne des droits de l'homme (la «CEDH»). Il doit être lu conjointement à l'article 52, paragraphe 1, de la Charte[28], qui autorise l'apport de limitations aux droits fondamentaux sous réserve que ces limitations, en plus d'être prévues par la loi:

- respectent le «contenu essentiel» du ou des droits;
- répondent effectivement à des objectifs d'intérêt général reconnus par l'UE ou au besoin de protection des droits et libertés d'autrui; et
- dans le respect du principe de proportionnalité, aient un caractère nécessaire[29].

La Cour de justice a précisé en outre que les législateurs doivent rechercher s'il est possible d'atteindre ces objectifs par des mesures moins intrusives[30]. Il découle également de la jurisprudence que les limitations apportées aux droits fondamentaux doivent être interprétées de manière restrictive[31]. Dans cette limite, le législateur de l'UE demeure libre de faire des choix politiques. Cependant, le contrôle judiciaire de tout exercice de ce pouvoir discrétionnaire est susceptible d'être particulièrement strict dans le cadre du traitement d'une masse de données concernant un nombre de personnes très important, et concernant l'accès à ces données et leur utilisation par les autorités judiciaires[32].

L'article 8, en revanche, doit être considéré comme un droit à la protection horizontal et anticipatoire qui n'est pas limité à des ingérences de l'État. Il accorde aux personnes physiques le droit que leurs données à caractère personnel ne puissent être traitées que sous réserve de la satisfaction de certaines conditions. Leurs données à caractère personnel ne peuvent faire l'objet d'un traitement - par l'État ou par quelque autre acteur - que si les normes énoncées aux paragraphes 2 et 3 de l'article 8 sont satisfaites, à savoir i) le traitement est loyal et licite et est effectué à des fins déterminées, ii) la transparence est assurée par l'octroi aux personnes physiques des droits d'accès et de rectification, et iii) le contrôle d'une autorité indépendante est assuré. Ces principes sont exposés plus en détail dans plusieurs instruments de la législation de l'UE en matière de protection des données, en particulier dans la directive 95/46/CE, le règlement n° 45/2001, la décision-cadre 2008/977/JAI et la directive 2002/58/CE. La conformité à l'article 8 de la Charte doit donc être évaluée en se référant spécifiquement au système de garanties exposé dans ces instruments. Ces règles constituent le point de référence pour le législateur, et il convient, de manière générale, d'éviter ou, à tout le moins, de justifier de manière appropriée, toute dérogation à ces règles.

4.3. Les étapes de l'analyse

Lors de l'évaluation d'une proposition de mesure qui comprend le traitement de données à caractère personnel, il convient de suivre un certain nombre d'étapes d'analyse:

1. Quel est le **fondement juridique** du traitement de données? Conformément à l'article 8, paragraphe 2, de la Charte, il peut s'agir du consentement de la personne concernée ou d'un autre fondement légitime prévu par la loi. Ce point est précisé à l'article 7 de la

[28] En ce qui concerne les droits fondamentaux au respect de la vie privée et à la protection des données, voir, à titre d'exemple, arrêt Digital Rights Ireland, précité, note 8 ci-dessus.

[29] L'article 52, paragraphe 1, suit l'article 8, paragraphe 2, de la CEDH, selon lequel il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

[30] Arrêt Volker und Markus Schecke, précité, note 8 ci-dessus, point 81.

[31] Arrêts Satakunnan Markkinapörssi et Satamedia, précité, note 26 ci-dessus, point 56, et Volker und Markus Schecke, précité, note 8 ci-dessus, points 77 et 86.

[32] Arrêt Digital Rights Ireland, précité, note 8 ci-dessus, points 57 à 61.

directive 95/46/CE et à l'article 5 du règlement n° 45/2001. Le cas échéant, il doit également être tenu compte de l'article 7 et des autres dispositions pertinentes de la Charte.

2. Le «**contenu essentiel**» du droit (c'est-à-dire son identité de base ou le fond d'un droit qui lui donne toute sa signification) est-il respecté? Une mesure peut avoir une incidence sérieuse sur un droit sans toutefois porter atteinte à son contenu essentiel[33]. Par exemple, la Cour a indiqué que la conservation des données relatives au trafic et à la localisation en application de la directive 2006/24/CE était gravement attentatoire au droit au respect de la vie privée mais que, dès lors qu'elle ne s'appliquait pas au contenu des communications électroniques, elle ne portait pas intrinsèquement atteinte au contenu essentiel du droit au respect de la vie privée.

3. La proposition de mesure est-elle **suffisamment précise**? Les règles régissant la portée et l'application de la mesure sont-elles claires et précises? Le type des données qui seront réunies, traitées ou échangées, et les personnes par lesquelles elles le seront, sont-ils indiqués de manière explicite?

4. L'objectif de la proposition de mesure est-il suffisamment clair? La **finalité du traitement** est-elle décrite de manière explicite et spécifique? S'il est prévu un traitement ultérieur, la finalité de celui-ci est-elle **compatible** avec la finalité initiale et, dans le cas contraire, existe-t-il des fondements suffisants pour une limitation[34]?

5. Le traitement de données prévu par la mesure est-il **adéquat, pertinent et non excessif** au regard des finalités pour lesquelles les données concernées sont collectées ou pour lesquelles elles sont traitées ultérieurement?

6. Le choix de la proposition de mesure est-il approprié? Serait-il possible d'atteindre le résultat souhaité par d'autres mesures qui seraient moins intrusives et moins attentatoires au droit fondamental en jeu? Ces points sont liés au critère de la **proportionnalité**, expliqué de manière plus détaillée ci-après.

7. Lorsqu'une mesure vise à protéger **d'autres intérêts publics ou droits fondamentaux**, comment l'équilibre entre ces intérêts ou droits et le respect de la vie privée et la protection des données est-il assuré?

8. En cas d'incidence sérieuse sur un droit fondamental et outre les points précédents, des **garanties appropriées** sont-elles prévues au niveau de l'UE (par opposition à l'hypothèse dans laquelle il serait simplement laissé aux États membres le soin de les définir)?

9. Existe-t-il des garanties suffisantes de la possibilité pour les personnes concernées d'exercer leurs **droits d'accès et de rectification**, ainsi que les autres droits pertinents?

[33] Arrêt Digital Rights Ireland, précité, note 8 ci-dessus, points 39 et 40.

[34] Il s'agit du principe désigné sous le nom de limitation de la finalité, actuellement énoncé à l'article 6, paragraphe 1, point b), de la directive 95/46/CE et à l'article 4, paragraphe 1, point b), du règlement n° 45/2001. Voir également article 13, paragraphe 1, de la directive 95/46/CE et article 20, paragraphe 1, du règlement n° 45/2001 concernant les restrictions possibles.

10. Existe-t-il des garanties suffisantes du fait que la conformité du traitement de données à la législation en matière de protection des données pourra être effectivement **contrôlée par une autorité indépendante**[35]?

11. Lorsqu'il est fait usage de systèmes d'information complexes, la nécessité de **sécurité** et les principes de **protection des données dès la conception et de protection des données par défaut** sont-ils suffisamment pris en compte?

4.4. La notion de proportionnalité

Comme il est indiqué au point 6 ci-dessus, les responsables politiques doivent évaluer la proportionnalité de la mesure. Une «mesure proportionnelle» peut s'entendre d'une mesure qui est «apte à réaliser l'[es] objectif[s] visé[s] par la législation en cause et [qui ne va] pas au-delà de ce qui est nécessaire pour l'[les] atteindre»[36].

Pour évaluer la proportionnalité conformément à l'article 52, paragraphe 1, de la Charte, la Cour a appliqué un critère plus strict, dans des arrêts comme Volker und Markus Schecke[37] et Digital Rights Ireland[38], que celui qu'elle avait appliqué antérieurement conformément au principe de proportionnalité énoncé à l'article 5, paragraphe 4, du traité sur l'Union européenne (le «TUE») dans l'arrêt Österreichischer Rundfunk[39].

Compte tenu de l'importance fondamentale que revêt la proportionnalité en matière de protection des données, nous envisageons de publier **un document de référence** afin de développer plus avant la présente orientation.

4.5. Un juste équilibre avec les autres intérêts publics et droits fondamentaux

Veiller à ce que la protection des données devienne une partie intégrante de l'élaboration des politiques de l'UE nécessite non seulement de comprendre les principes exprimés dans le cadre juridique et la jurisprudence, mais également de rechercher des solutions pratiques et créatives à des problèmes complexes en présence de priorités politiques fréquemment concurrentes.

La Cour de justice a reconnu que la législation européenne doit souvent réaliser plusieurs objectifs d'intérêts public qui peuvent parfois être contradictoires et qui nécessitent d'assurer un juste équilibre entre les différents intérêts publics et droits fondamentaux protégés par l'ordre juridique de l'UE[40]. Ces droits et intérêts peuvent comprendre: la protection de la vie et de la

[35] Arrêts Commission / Allemagne, point 23; Commission / Autriche, point 37, et Commission / Hongrie, point 47, tous précités, note 5 ci-dessus. Au point 68 de l'arrêt Digital Rights Ireland, précité, note 8 ci-dessus, la Cour a affirmé que dans les circonstances du cas d'espèce, ce contrôle indépendant n'était pas pleinement garanti dès lors que la mesure en cause n'imposait pas que les données traitées soient conservées sur le territoire de l'UE.

[36] Arrêt Volker und Markus Schecke, précité, note 8 ci-dessus, point 74.

[37] Arrêt Volker und Markus Schecke, précité, note 8 ci-dessus, points 77 et 86. La Cour a indiqué au point 81 que, lors de l'adoption de mesures imposant la publication obligatoire de certaines informations relatives aux bénéficiaires de fonds de l'UE, les législateurs de l'UE auraient dû prendre en considération des modalités de publication de ces informations qui seraient conformes à l'objectif d'une telle publication tout en étant moins attentatoires au droit de ces bénéficiaires au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier.

[38] Voir note 8 ci-dessus.

[39] Arrêt Österreichischer Rundfunk, précité, note 21 ci-dessus, point 94. Dans cette affaire, l'objectif légitime d'un État membre de garantir une utilisation optimale des fonds publics devait être mis en balance avec la gravité de l'atteinte au droit des personnes concernées par les mesures de transparence des salaires au respect de leur vie privée.

[40] Arrêt du 29 janvier 2008, Promusicae (C-275/06, Rec. p. I-271, point 68).

santé; la prévention et la lutte contre la grande criminalité et la criminalité organisée, le maintien de l'ordre public et la protection de la sécurité; l'ouverture, la transparence et le droit d'accès aux documents; la propriété, y compris la propriété intellectuelle; la liberté d'expression; la liberté d'entreprise.

Nous travaillons avec les institutions de l'UE et les autres parties prenantes pour nous assurer de comprendre les priorités et les objectifs qui sous-tendent les mesures ayant une incidence sur la protection des données et pour contribuer à trouver des solutions qui limitent les conflits entre ces priorités. Dans ce cadre, nous tenons à souligner que des garanties solides en matière de protection des données peuvent également renforcer l'efficacité des mesures destinées à protéger ces intérêts.

4.6. Les technologies et le droit à la protection des données

Notre objectif est de veiller à ce que les aspects technologiques qui sont pertinents pour les décisions législatives soient présentés de façon exacte et complète et soient actualisés.

Lorsque nous formulons des conseils, nous évaluons l'incidence sur la protection des données des éléments technologiques des systèmes d'information créés pour soutenir les politiques de l'UE (par exemple, dans le domaine de la liberté, de la sécurité et de la justice ou pour le marché intérieur). Nous évaluons également l'incidence sur la protection des données des politiques de l'UE qui sont liées à des technologies spécifiques (par exemple, la RFID, l'informatique en nuage, les réseaux intelligents, le système «eCall», les scanners corporels) ou qui pourraient entraîner des évolutions techniques (par exemple, les initiatives en matière de services rendus par une tierce partie de confiance, la cybersécurité, le commerce électronique, les questions liées au droit d'auteur numérique ou la législation «vie privée et communications électroniques»). Les éléments technologiques peuvent également jouer un rôle dans d'autres politiques, comme les bases de données ouvertes.

Dans certains cas, l'incidence d'une technologie ne peut être détectée et évaluée qu'à l'issue d'une analyse approfondie. Nous considérons que les choix en matière de solutions technologiques devraient être fondés sur cette analyse. Le législateur doit être conscient des choix technologiques existants et il ne doit pas être porté à croire qu'une technologie impose une législation spécifique, sans option possible. En particulier, nous visons à promouvoir les principes de respect de la vie privée dès la conception et de respect de la vie privée par défaut.

5. Définition des priorités

Le CEPD est confronté au défi de fournir des conseils efficaces en se fondant sur des ressources de plus en plus limitées. Une approche sélective fondée sur des critères clairs et une planification rigoureuse est une condition indispensable pour que nous puissions accomplir notre mission consultative de manière efficace.

Compte tenu du nombre significatif de propositions de législation présentées par la Commission, nous établissons une liste de priorités[41] sur une base annuelle, en signalant un nombre limité de questions stratégiques auxquelles nous souhaitons consacrer une énergie significative. Cet *inventaire* est un outil de planification et d'évaluation des performances. Il est préparé sur la base du programme annuel de travail de la Commission, de l'examen à

[41] Article 29 du RI du CEPD.

mi-parcours du programme et des autres outils de programmation et de planification utilisés par la Commission, ainsi que des contacts bilatéraux que nous entretenons avec les services de la Commission. L'inventaire se compose d'une liste des propositions de législation et des documents connexes pour lesquels nous avons l'intention de donner des conseils, classés selon leur priorité, et d'un document explicatif exposant notre approche stratégique dans le domaine de la consultation pour l'année suivante.

L'inclusion d'un projet de proposition déterminé dans l'inventaire et le niveau de priorité qui lui est attribué sont le fruit d'une analyse fondée sur un certain nombre de critères. En premier lieu, il est tenu compte des objectifs stratégiques du CEPD et du plan de gestion annuel[42]. Il est également tenu compte de l'incidence prévue de la proposition sur le niveau effectif de protection des données dans l'UE. Un projet de mesure ayant des incidences importantes et/ou un caractère très intrusif et un domaine d'application étendu se verra normalement attribuer un niveau de priorité élevé. Enfin, les initiatives qui revêtent une importance stratégique pour les politiques de l'UE et/ou une dimension politique significative sont susceptibles de faire l'objet d'un contrôle renforcé.

6. Forme et moment de l'intervention du CEPD

Sans préjudice de l'article 28, paragraphe 2, du règlement n° 45/2001, une consultation concernant une proposition ou une question unique comprend normalement les étapes ci-après[43]:

6.1. *Étape 1*: consultation informelle[44] par le service responsable de la Commission

Pour que nos interventions soient efficaces, il est important que nous puissions apporter une contribution à un stade précoce, idéalement avant l'adoption formelle d'une proposition. Cette consultation précoce nous permet d'attirer l'attention, de manière informelle, sur des aspects de la protection des données à caractère personnel qui présentent une pertinence en ce qui concerne la proposition et - le cas échéant - de formuler des propositions de modifications d'un texte, sans participer aux négociations politiques entre les co-législateurs de l'UE, le Parlement européen et le Conseil.

En conséquence, conformément à une procédure bien établie[45], le CEPD est normalement consulté par la Commission à un stade précoce de la préparation d'un instrument, à savoir au cours de la consultation interservices, et en tout état de cause avant que le collège des commissaires ne décide définitivement d'adopter une mesure, une proposition législative ou un document politique. En réponse, nous adressons au service responsable de la Commission des observations informelles sur le projet de document. Ces observations se concentrent généralement sur les aspects techniques de la proposition en cause, même si nous pouvons effectuer une analyse plus approfondie dans les cas où une proposition soulève des préoccupations graves concernant la nécessité et la proportionnalité du traitement de données proposé. Les observations informelles donnent une bonne indication des questions que nous sommes susceptibles de soulever dans notre avis ou dans nos observations formels.

[42] Chaque année, il est établi un plan de gestion annuel (interne) qui traduit la stratégie à long terme du CEPD en objectifs généraux et spécifiques (article 13, paragraphe 1, du RI du CEPD).
[43] Article 26 du RI du CEPD.
[44] Article 27 du RI du CEPD.
[45] Note du Secrétaire général de la Commission aux directeurs généraux et aux chefs de service du 8 décembre 2006, SEC(2006)1771.

6.2. *Étape 2*: consultation formelle[46] par la Commission

En réponse à une consultation formelle par la Commission à la suite de l'adoption d'une proposition de législation soumise à la procédure législative ordinaire (article 294 du TFUE), nous formulerons, en règle générale, un avis formel. L'approche adoptée est la même pour les propositions soumises par la Commission au Conseil et/ou au Parlement dans le cadre de procédures législatives spécifiques. Un avis est normalement publié dans les trois mois suivant l'adoption par la Commission et comporte une analyse aussi exhaustive que possible des aspects d'une proposition liés à la protection des données.

Outre les actes législatifs stricto sensu (à savoir les règlements, les directives ou les décisions), nous pourrons également formuler un avis sur des documents comme, par exemple, une communication de la Commission ou un document de travail des services de la Commission lorsque la protection des données constitue, ou devrait constituer, un élément fondamental du projet d'instrument. Il en va de même concernant les recommandations et les avis, ainsi que les actes délégués (article 290 du TFUE) et les actes d'exécution (article 291 du TFUE).

Compte tenu de la nécessité d'adopter une approche sélective pour mener nos missions consultatives de manière efficace, nous pouvons, dans certains cas, fournir des conseils plus limités, sous une forme autre qu'un avis (par exemple, des observations formelles ou un courrier). Pour les autres instruments, les observations ou courriers seront privilégiés, sauf s'il existe une raison spécifique d'adopter un avis, par exemple si le document sur lequel nous formulons des observations est susceptible d'avoir des conséquences particulièrement importantes en matière de protection des données. Les observations formelles sont normalement formulées dans les deux mois suivant l'adoption du document en question et se concentrent sur des aspects spécifiques d'une proposition.

Le cas échéant, nous pouvons utiliser *d'autres instruments* pour communiquer notre opinion, y compris des présentations verbales, des courriers ou des communiqués de presse (qui ne se rapportent pas directement à un avis ou à des observations). En particulier, à des étapes plus avancées du processus législatif (par exemple, à la suite de l'adoption d'une proposition modifiée par la Commission, de conciliations/trilogues, etc.), un courrier explicatif sur un sujet spécifique peut suffire. Ces courriers seront également publiés sur notre site web.

6.3. Procédures spécifiques[47]

6.3.1. Actes délégués et actes d'exécution (articles 290 et 291 du TFUE)

Les actes législatifs peuvent prévoir l'adoption d'actes délégués et/ou de mesures d'exécution destinés à apporter des précisions aux dispositions générales de l'instrument. Certains de ces aspects peuvent concerner le traitement de données à caractère personnel, dont les modalités peuvent être définies de manière plus précise dans l'acte délégué/d'exécution que dans l'acte de base. L'acte de base devrait normalement comporter une disposition prévoyant l'exigence de conformité du traitement à la législation en matière de protection des données. Cependant, il est possible que cette disposition ne définisse pas suffisamment précisément les garanties nécessaires compte tenu des modalités qui seront ultérieurement énoncées dans les actes délégués et les actes d'exécution. En conséquence, nous devrions être impliqués dans la préparation des actes délégués et des actes d'exécution susceptibles d'avoir des incidences en matière de protection des données à un stade précoce du processus.

[46] Article 28 du RI du CEPD.
[47] Article 26, paragraphe 1, du RI du CEPD.

À cette fin, nous indiquons généralement dans notre avis sur l'acte de base que nous souhaitons être consultés sur ces projets d'actes. Dans certains cas, nous pouvons participer à des groupes (d'experts) au sein desquels se tiennent des discussions concernant la préparation de ces actes. En tout état de cause, nous devrions être consultés de manière informelle par la Commission avant l'adoption de l'acte délégué ou de l'acte d'exécution, dès lors qu'il s'agit souvent de la seule occasion dont nous disposons d'apporter une contribution qui pourra être prise en compte.

Nous pouvons également décider de réagir publiquement après l'adoption de l'acte délégué ou de l'acte d'exécution par la Commission, en particulier pour indiquer au législateur si l'acte délégué ou l'acte d'exécution constitue ou non une menace pour le respect de la vie privée et de la protection des données des personnes physiques et, dans l'affirmative, s'il a été apporté la preuve de sa nécessité et de sa proportionnalité et si les garanties appropriées ont été prévues. Ce faisant, nous cherchons à guider le législateur pour qu'il prenne une décision éclairée concernant l'acceptation ou le rejet d'un acte délégué ou d'un acte d'exécution.

6.3.2. Accords internationaux et autres arrangements bilatéraux et multilatéraux

Conformément à l'article 218 du TFUE, les accords internationaux sont négociés par la Commission et soumis à l'approbation du Parlement avant leur ratification par le Conseil. Les accords internationaux peuvent avoir une incidence sur le respect de la vie privée et la protection des données des personnes physiques, y compris lorsque leur champ d'application ne concerne pas les droits fondamentaux en tant que tels[48]. Il en va ainsi, en particulier, lorsque ces accords comportent des dispositions prévoyant l'échange de données à caractère personnel avec des destinataires situés dans des pays tiers[49].

Le CEPD devrait être consulté *de manière informelle* sur le projet de mandat donné à la Commission et sur l'évolution des négociations avant que le texte ne soit paraphé, et *de manière formelle* sur l'issue des négociations avant que la Commission n'adopte une proposition finale de décision du Conseil relative à la conclusion et à la signature de l'accord. En outre, pour que notre contribution permette effectivement de prévoir les garanties appropriées dans l'accord, nous devrions être tenus informés de l'avancement des négociations, à tout le moins concernant les aspects les plus importants liés à la protection des données. En outre, la Commission peut attirer notre attention, en toute confidentialité, sur des questions précises pour que nous formulions une opinion spécifique.

Il convient de suivre une procédure similaire pour les autres arrangements bilatéraux et multilatéraux qui n'ont pas la nature formelle d'accords internationaux. Cela vaut par exemple pour les positions que doit prendre l'UE au sein de comités mixtes de coopération douanière créés sur le fondement d'accords bilatéraux et prévoyant l'échange d'informations comportant des données à caractère personnel.

Une fois que la Commission a adopté la proposition de décision du Conseil ayant une incidence importante en matière de protection des données, nous formulons un avis.

[48] Par exemple, le respect de la vie privée et la protection des données constituent des éléments fondamentaux des négociations en cours d'un accord-cadre entre l'UE et les États-Unis.

[49] Par exemple, les accords sur les dossiers passagers (PNR), le programme de traque du financement du terrorisme (TFTP), les accords sur les précurseurs de drogues (entre l'UE et la Russie) et les accords de coopération douanière entre l'UE et des pays tiers.

6.3.3. Communications de la Commission

Le CEPD devrait être consulté, de manière informelle et formelle, sur les communications de la Commission susceptibles d'avoir une incidence sur le respect de la vie privée et la protection des données à caractère personnel. La Commission adopte généralement des communications avant que ne soient adoptés de nouveaux instruments législatifs. En donnant des conseils avant et après l'adoption de la communication, nous apportons une contribution d'experts pour aider à guider les choix législatifs ultérieurs.

6.3.4. Consultations publiques

Nous pouvons, à notre propre initiative, répondre aux consultations publiques lancées par la Commission européenne ou par d'autres parties prenantes[50] dans des domaines susceptibles d'avoir une incidence sur le respect de la vie privée et la protection des données des personnes physiques. Notre apport peut avoir une influence particulièrement importante dans tous les cas où des consultations publiques sont lancées avant l'adoption d'instruments législatifs ou juridiques. Il contribue à l'élaboration de la décision à venir en soulignant les questions de protection des données qui doivent être résolues ainsi que les garanties qu'il est possible de prévoir pour y répondre.

6.3.5. Initiatives des États membres et coopérations renforcées

Les traités prévoient encore des procédures législatives dans lesquelles l'initiative est prise par les États membres [par exemple, l'article 76, point b), du TFUE concernant la coopération policière et judiciaire]. Ils comportent également des dispositions détaillées concernant les coopérations renforcées (article 20 du TUE et articles 326 à 334 du TFUE). Dans ces procédures, même si la Commission a un rôle plus limité, le CEPD devrait jouer le même rôle consultatif que dans les autres procédures. Nous visons à définir les modalités de l'exercice de ce rôle dans le **mémorandum d'accord**, comme mentionné ci-dessus.

6.4. Suivi de nos interventions[51]

Notre rôle consultatif ne prend pas fin avec la formulation de notre avis formel (ou d'une autre intervention). Nous continuons à surveiller toutes les évolutions pertinentes et nous tenons prêts à réagir, le cas échéant, en particulier dans le cas d'avis, afin d'en optimiser l'impact. Notre degré de participation et l'importance des ressources consacrées à ce suivi dépendent de la priorité que nous accordons à une proposition déterminée. Cependant, nous sommes prêts à examiner toutes les demandes de conseils (supplémentaires) que nous adressent les institutions de l'UE au cours des étapes ultérieures du processus législatif, lorsque des questions de protection des données sont en jeu.

En premier lieu, nous restons disponibles pour présenter nos conseils aux co-législateurs et en discuter avec eux, ou pour fournir toute autre contribution dont il nous serait fait la demande. Cette coopération prend généralement la forme de réunions avec les personnes qui assument la responsabilité directe du dossier au sein du Parlement européen (la commission compétente, le rapporteur et les rapporteurs fictifs) et/ou du Conseil (le groupe de travail compétent et le Secrétariat du Conseil). Pour les affaires qui présentent une haute importance stratégique (par exemple, celles qui sont identifiées comme telles dans l'inventaire), nous rechercherons activement l'opportunité de présenter nos avis au cours de réunions de haut niveau.

[50] Lesquelles peuvent également comprendre des organisations internationales.
[51] Article 30 du RI du CEPD.

En outre, nous prenons l'initiative de communications régulières avec la commission du Parlement européen compétente et le Secrétariat général du Conseil afin de pouvoir suivre les évolutions du processus législatif. Une fois encore, en raison des contraintes budgétaires, nous accorderons la priorité aux affaires qui présentent une haute importance stratégique. Lorsque ce suivi aboutit à l'introduction de modifications substantielles dans une mesure législative en cours de discussion qui pourraient avoir des incidences graves, le cas échéant, en matière de protection des données, nous pourrons examiner l'opportunité de formuler des conseils supplémentaires sous la forme la plus adaptée au vu des circonstances.

6.5. Transparence et confidentialité

La transparence est l'une des valeurs fondamentales du CEPD[52]. Nous sommes convaincus qu'agir de manière transparente, en expliquant ce que nous faisons et pourquoi nous le faisons dans un langage clair et accessible à tous[53], peut améliorer grandement l'efficacité du CEPD dans son rôle de conseiller.

En règle générale, les documents politiques clés, les lignes directrices, les avis législatifs, les observations formelles, les articles, les courriers, les discours et les autres documents produits sont publiés sur le site web du CEPD[54]. La publication intervient en principe dans les langues de travail du CEPD. En outre, les résumés des avis législatifs sont traduits dans toutes les langues officielles de l'UE et publiés au *Journal officiel de l'Union européenne* (série C)[55].

Cependant, en vue de protéger la confidentialité du processus de décision interne de la Commission, les observations informelles - formulées lors des étapes précoces du processus de décision interne en réaction à des projets de documents qui ne sont pas encore tombés dans le domaine public - sont généralement communiquées à titre confidentiel et ne sont pas publiées (bien que les règles de transparence et d'accès aux documents consacrées par les traités et par le droit dérivé[56] restent pleinement applicables)[57]. Nous disposons également de procédures internes pour assurer la plus stricte confidentialité des documents au sujet desquels nous sommes consultés dans des affaires spécifiques, par exemple des (projets d')accords internationaux ou des documents sensibles[58], ou toutes les fois que les conditions d'une affaire déterminée l'exigent.

[52] Article 15, paragraphe 1, du RI du CEPD.
[53] Stratégie, p. 15.
[54] Article 54, paragraphe 1, du RI du CEPD.
[55] Article 55, point a), du RI du CEPD.
[56] Conformément à l'article 56 du RI du CEPD, tous les documents détenus par le CEPD peuvent faire l'objet de demandes d'accès du public, dans le respect des principes énoncés par le règlement n° 1049/2001.
[57] Article 27, paragraphe 2, du RI du CEPD. Dans des cas particuliers, par exemple si des observations informelles présentent un intérêt général, peuvent fournir des orientations utiles à d'autres parties prenantes ou ont une incidence dans d'autres domaines d'activité du CEPD, nous pouvons décider de publier notre contribution sous une forme adaptée, après avoir consulté la Commission.
[58] Voir article 9 du règlement n° 1049/2001 du Parlement européen et du Conseil du 10 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.05.2001, p. 43).

6.6. Autres interventions

Si les documents adoptés dans le cadre des missions de contrôle du CEPD sont généralement des *documents d'orientation*, nous pouvons également publier un *document de référence*[59] pour faire part de notre opinion sur la manière de parvenir à une approche équilibrée et proportionnée de la protection des données dans un domaine particulier, lorsqu'il est nécessaire d'effectuer une analyse préliminaire ou plus poussée. Enfin, nous pouvons adopter un *document stratégique* pour préciser la manière dont le CEPD entend accomplir ses missions et exercer ses pouvoirs, comme les tâches relevant de notre rôle consultatif à l'égard de propositions de nouvelles dispositions législatives[60]. Ces instruments renforcent l'efficacité des travaux consultatifs du CEPD et semblent particulièrement adaptés pour promouvoir une culture générale de protection des données au sein des institutions et organes de l'UE.

En outre, nous nous employons à recenser certains thèmes stratégiques et à agir de façon plus anticipatoire en formulant des conseils d'office, en l'absence de proposition officielle de législation, souvent sous la forme d'un *avis*[61] ou d'un *avis préliminaire*[62].

L'approche communautaire de la protection des données est guidée par les arrêts de la Cour de justice de l'Union européenne qui interprètent les dispositions du cadre juridique applicable, y compris de la directive 96/45/CE et du règlement n° 45/2001. Nous visons à jouer un rôle anticipatoire dans ce domaine, par la mise en œuvre de l'article 47, paragraphe 1, point i) du règlement n° 45/2001 qui donne compétence au CEPD pour intervenir dans les affaires portées devant la Cour de justice[63]. Dans ce contexte, nous nous efforçons de fournir des conseils d'experts et impartiaux sur les questions relevant de notre compétence, d'une manière similaire aux mémoires des *amicus curiae* («amis de la cour») que l'on connaît dans certaines juridictions. Nos interventions doivent donc être considérées comme relevant de notre rôle consultatif au sens le plus large, c'est-à-dire recouvrant également la mise à disposition de notre expertise en matière de protection des données dans le cadre de procédures judiciaires devant la Cour[64].

Enfin, nous utilisons un certain nombre d'autres moyens pour sensibiliser aux questions de protection des données, y compris les publications sur notre site web et l'organisation d'ateliers, de réunions et de séminaires.

---

[59] Par exemple, «Accès du public aux documents contenant des données à caractère personnel après l'arrêt rendu dans l'affaire Bavarian Lager», 24 mars 2011, disponible à l'adresse https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_FR.pdf.

[60] Par exemple, le document stratégique de 2005, note 3 ci-dessus.

[61] Par exemple, l'avis relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», 16 novembre 2012, disponible à l'adresse: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_FR.pdf.

[62] Par exemple, l'avis préliminaire «Vie privée et compétitivité à l'ère de la collecte de données massives: l'interaction entre le droit à la protection des données, le droit de la concurrence et la protection des consommateurs dans l'économie numérique», mars 2014, disponible à l'adresse: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_FR.pdf

[63] Voir également article 41 du RI du CEPD.

[64] Des informations sur les interventions du CEPD devant la Cour sont disponibles à l'adresse: https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Consultation/Court.

7. Coopération

Les autorités de contrôle indépendantes qui contrôlent l'application de la législation en matière de protection des données dans les États membres de l'UE collaborent dans le cadre du groupe de protection des personnes à l'égard du traitement des données à caractère personnel (également désigné sous le nom de «groupe de travail "Article 29"») institué par l'article 29 de la directive 95/46/CE. Le groupe de travail «Article 29» conseille la Commission sur le niveau de protection offert dans les pays tiers, sur tout projet de modification de la directive 95/46/CE, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, *ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés*[65] (mise en italique ajoutée).

En tant que membre du groupe de travail «Article 29»[66], nous apportons notre contribution au programme de travail du groupe et nous participons aux réunions plénières et de sous-groupes (y compris en rédigeant et/ou en apportant notre contribution à des avis et à d'autres textes) de la manière adaptée pour assurer une parfaite cohérence et fournir le point de vue unique de l'UE. Nous veillons également à assurer une coordination régulière, en particulier avec le président du groupe de travail «Article 29», afin de développer des synergies.

En janvier 2012, la Commission a adopté une proposition de règlement général sur la protection des données et une proposition de directive dans le domaine de l'application de la législation. L'un des éléments clés de ces propositions a été la création d'un comité européen de la protection des données qui remplacerait le groupe de travail «Article 29». En application du mécanisme désigné sous le nom de «mécanisme de contrôle de la cohérence», le comité européen de la protection des données deviendrait l'instance centrale de l'application de la législation en matière de protection des données dans les affaires revêtant une dimension européenne.

En application de la proposition de la Commission, le secrétariat du comité européen de la protection des données (y compris le soutien analytique, administratif et logistique) sera assuré par le CEPD[67]. Cette disposition permettra au comité européen de la protection des données d'exercer ses fonctions avec une totale indépendance et en disposant de pouvoirs juridiques solides, tout en tirant profit des synergies et des économies de coûts découlant du soutien d'une structure existante pour les missions de secrétariat.

Enfin, nous collaborons avec d'autres organes de l'UE qui conseillent les institutions de l'UE et les États membres sur certains aspects liés aux droits fondamentaux (comme l'Agence des droits fondamentaux - «la FRA») ou à la sécurité de l'information (l'Agence européenne chargée de la sécurité des réseaux et de l'information - «l'ENISA»), et nous participons aux activités d'un certain nombre d'organisations internationales comme le Conseil de l'Europe. Nous suivons les discussions du comité consultatif de la convention 108, de son bureau et du comité ad hoc sur la protection des données, auxquelles nous contribuons activement en tant qu'observateur.

[65] Article 30, paragraphe 1, point c), de la directive 95/46/CE.
[66] Article 46, point g), du règlement n° 45/2001.
[67] Article 71, paragraphe 2, de la proposition de règlement général sur la protection des données.