Montrer l'exemple

1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

CEPD 2015 - 2019

Le Contrôleur européen de la protection des données

Un résumé du présent rapport, qui donne un aperçu des principales évolutions intervenues dans le cadre des activités du CEPD au cours de la période 2015-2019, est également disponible.

Des informations supplémentaires sur le CEPD figurent sur notre site web à l'adresse : https://edps.europa.eu/edps-homepage_fr.

De plus amples informations sur la manière de s'abonner au bulletin d'information du CEPD figurent également sur le site web.

Luxembourg : Office des publications de l'Union européenne, 2019

Print: ISBN 978-92-9242-451-0 doi:10.2804/4452 QT-04-19-470-FR-C
PDF: ISBN 978-92-9242-443-5 doi:10.2804/370572 QT-04-19-470-FR-N
HTML: ISBN 978-92-9242-446-6 doi:10.2804/21611 QT-04-19-470-FR-Q

Montrer l'exemple

1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

CEPD 2015 - 2019

TABLE DES MATIÈRES

GRAPHIQUES

AVANT-PROPOS

Giovanni Buttarelli et moi-même avons publié une stratégie pour notre mandat dans les 100 jours suivant notre prise de fonction.

Le contenu de ce court document reflétait notre vision du respect de la vie privée à l'ère numérique. C'était la vision d'une UE dotée de normes de niveau mondial en matière de protection des données, qui montre l'exemple. Elle consacrait le CEPD, dans notre rôle d'autorité de contrôle et de conseiller politique, comme un centre d'excellence pour la protection des données.

Au cours des cinq dernières années, les citoyens et les décideurs politiques ont pris de plus en plus conscience de la réalité et du potentiel des technologies numériques.

Les révélations d'Edward Snowden en 2013 ont mis en évidence la profondeur et l'ampleur des intrusions de l'État dans notre vie privée. En 2018, le scandale Facebook/Cambridge Analytica a révélé la fragilité de notre démocratie, où la sphère publique est pervertie par des manœuvres de suivi, de profilage et de ciblage complexe échappant à tout contrôle. Les entreprises les plus prisées au monde sont désormais celles qui ont obtenu les meilleurs résultats dans

la collecte et la monétisation des informations à caractère personnel, tout en acquérant des milliers de jeunes entreprises qui auraient pu les concurrencer et diversifier les modèles économiques disponibles.

Nous savons à présent que le prix caché de la *commodité* tant vantée de la numérisation se concrétise par des pratiques injustifiables et souvent peu scrupuleuses en matière de données et par un fossé croissant entre les gagnants et les perdants. La *mise en réseau du monde* a eu pour effet annexe des algorithmes opaques de maximisation des recettes, jouant le rôle de facteurs de division sociale et d'outils d'oppression.

De nombreuses régions du monde, et pas seulement l'UE, étudient actuellement la manière dont elles peuvent donner aux citoyens un plus grand contrôle sur leurs données et leur vie numérique, et instaurer une discipline dans des marchés qui, pendant près de 20 ans, ont pu se développer et désorganiser grâce à une surveillance minimale. Au début de notre mandat, l'Afrique du Sud venait de devenir le 101e pays à adopter une législation exhaustive sur la protection des données à caractère personnel. Cette année, le Nigeria est devenu le 134e pays à adopter une telle législation.

Notre mot d'ordre au cours des cinq dernières années a été la *responsabilisation*. La responsabilisation des responsables du traitement pour ce qu'ils font avec les données à caractère personnel de tierces personnes, et la responsabilisation des autorités de contrôle dans l'exercice, avec intégrité et cohérence, des pouvoirs renforcés qui nous sont confiés par le règlement général sur la protection des données (RGPD).

Notre stratégie était également un exercice de responsabilisation vis-à-vis des objectifs dont nous avons déclaré que nous les poursuivrions et les actions prioritaires dont nous avons déclaré que nous les mettrions en œuvre – en mettant l'accent sur la numérisation, les partenariats mondiaux et la modernisation de la protection des données. À de nombreux niveaux, je pense que nous avons été à la hauteur de nos ambitions.

Nous avons enquêté sur les relations contractuelles des organismes de l'UE avec les prestataires de services, mis en place un forum permettant aux agences d'échanger leurs points de vue sur la réglementation des marchés numériques et veillé à ce que le nouveau comité européen de la protection des données (le « Comité ») dispose des ressources nécessaires pour mener à bien ses travaux. Par-dessus tout, nous avons porté la question de l'éthique et des nouvelles technologies, en particulier l'intelligence artificielle, au centre du débat politique public.

Je tiens à rendre hommage à notre excellent et dévoué personnel qui a joué un rôle déterminant dans nos efforts pour faire de notre vision une réalité sur le terrain.

Toutefois, nous devons garder à l'esprit que ce n'est que le début de ce qui sera un très long processus. Au cours des prochaines années, il nous faudra veiller à ce que les citoyens soient en mesure d'exercer un plus grand contrôle sur leur vie numérique et faire en sorte que les données à caractère personnel soient mises à profit pour la société en général, et pas uniquement pour un petit nombre d'intérêts privés puissants.

Wojciech Wiewiórowski
Contrôleur européen adjoint de la protection des données

1. À PROPOS DU CEPD

Le contrôleur européen de la protection des données (CEPD) veille à ce que les institutions, organes et organismes de l'Union respectent les droits fondamentaux au respect de la vie privée et à la protection des données, qu'ils traitent des données à caractère personnel ou qu'ils participent à l'élaboration de nouvelles politiques pouvant impliquer le traitement de données à caractère personnel. Le CEPD a quatre grands domaines de travail :

- **Contrôle :** Nous surveillons le traitement des données à caractère personnel par l'administration de l'UE et veillons à ce qu'elle respecte les règles en matière de protection des données. Nos tâches vont de la réalisation d'enquêtes à la gestion des réclamations et des consultations préalables concernant les opérations de traitement.
- **Consultation :** Nous conseillons la Commission européenne, le Parlement européen et le Conseil sur les propositions de nouvelle législation et d'autres initiatives en matière de protection des données.
- **Suivi de la technologie :** Nous contrôlons et évaluons les évolutions technologiques, lorsqu'elles ont une incidence sur la protection des données à caractère personnel, à un stade précoce, en mettant particulièrement l'accent sur le développement des technologies de l'information et de la communication.
- **Coopération :** Entre autres partenaires, nous travaillons avec les autorités chargées de la protection des données (APD) au niveau national afin de promouvoir une protection cohérente des données dans l'ensemble de l'UE. Notre principale plate-forme de coopération avec les APD est le comité européen de la protection des données (le «Comité»), dont nous assurons également le secrétariat.

Jusqu'au 11 décembre 2018, les institutions de l'UE devaient se conformer aux règles en matière de protection des données énoncées dans le règlement (CE) 45/2001. Le 11 décembre 2018, le règlement (CE) 45/2001 a été remplacé par le règlement (UE) 2018/1725. Il appartient au CEPD de faire respecter ces règles.

Le règlement (UE) 2018/1725 est l'équivalent pour les institutions de l'UE du règlement général sur la protection des données (RGPD). Le RGPD est devenu pleinement applicable dans toute l'UE le 25 mai 2018 et définit les règles en matière de protection des données que tous les organismes privés et la plupart des organismes publics opérant dans l'UE doivent respecter. Il charge également le CEPD d'assurer le secrétariat du Comité.

Pour les services répressifs des États membres, la législation applicable est la directive 2016/680 relative à la protection des données dans les secteurs de la police et de la justice pénale. L'article 3 et le chapitre IX du règlement (UE) 2018/1725 s'appliquent au traitement des données opérationnelles à caractère personnel par les organes et organismes de l'UE participant à la coopération policière et judiciaire, et ces dispositions s'inspirent étroitement des règles énoncées dans la directive 2016/680.

En outre, des règles distinctes existent en ce qui concerne le traitement des données à caractère personnel pour les activités opérationnelles menées par l'Agence de l'Union européenne pour la coopération des services répressifs, Europol. Ces activités incluent la lutte contre les formes graves de criminalité et le terrorisme touchant plus d'un État membre. La législation pertinente en l'espèce est le règlement 2016/794, qui prévoit également la surveillance par le CEPD de ces activités de traitement des données. Comme pour les autres institutions et organes de l'UE, le CEPD est également chargé de la surveillance du traitement des données à caractère personnel relatives aux activités administratives d'Europol, y compris des données à caractère personnel relatives au personnel d'Europol, conformément au règlement (UE) 2018/1725. Un régime de protection des données similaire et spécifique est en place pour le Parquet européen et Eurojust.

2. STRATÉGIE DU CEPD POUR LA PÉRIODE 2015-2019

La stratégie 2015-2019 du CEPD a défini nos priorités pour le mandat et a fourni un cadre permettant de promouvoir une nouvelle culture de la protection des données au sein des institutions et organes de l'UE. Elle a résumé :

- les principaux défis en matière de protection des données et de respect de la vie privée attendus au cours du mandat ;
- trois objectifs stratégiques et dix actions d'accompagnement en vue de relever ces défis ;
- la façon dont la stratégie peut être mise en œuvre par la gestion efficace des ressources, une communication claire et l'évaluation de nos performances.

Afin de concrétiser notre vision d'une UE qui montre l'exemple dans le dialogue mondial sur la protection des données et le respect de la vie privée à l'ère numérique, nous avons défini trois objectifs stratégiques et dix points d'action :

1 La protection des données se numérise

(1) promouvoir les technologies qui améliorent le respect de la vie privée et la protection des données ;
(2) identifier des solutions interdisciplinaires ;
(3) augmenter la transparence, le contrôle des données par les utilisateurs et la responsabilisation dans les traitements de *Big Data*.

2 Forger des partenariats à grande échelle

(1) développer une dimension éthique de la protection des données ;
(2) parler d'une seule voix sur la scène internationale ;
(3) intégrer la protection des données dans les politiques internationales.

3 Ouvrir un nouveau chapitre dédié à la protection des données dans l'UE

(1) adopter des règles de protection des données modernes et les mettre en œuvre ;
(2) accroître la responsabilisation des organes de l'UE qui collectent, utilisent et stockent des données à caractère personnel ;
(3) faciliter l'élaboration responsable et éclairée de politiques ;
(4) promouvoir un dialogue mûr sur la sécurité et le respect de la vie privée.

@EU_EDPS

#EDPS strategy envisions #EU as a whole not any single institution, becoming a beacon and leader in debates that are inspiring at global level

3. 2015-2019 RÉALISER NOTRE VISION

La protection des données touche presque tous les domaines politiques de l'UE. Elle joue également un rôle essentiel dans la légitimation et l'accroissement de la confiance dans les politiques de l'UE. L'Europe est le plus fervent défenseur au monde de la protection des droits fondamentaux et de la dignité humaine. Il est donc essentiel que l'UE joue un rôle de premier plan dans l'élaboration d'une norme mondiale en matière de respect de la vie privée et de protection des données, centrée sur ces valeurs.

Giovanni Buttarelli a été nommé Contrôleur européen de la protection des données par décision conjointe du Parlement européen et du Conseil du 4 décembre 2014. Le contrôleur adjoint, Wojciech Wiewiórowski, a été nommé à la même date. Nommés pour un mandat de cinq ans, ils ont été confrontés à la tâche difficile de faciliter la transition de l'UE vers une nouvelle ère de la pratique en matière de protection des données.

Dans cette perspective, leur première action, en tant que CEPD et contrôleur adjoint, a consisté à élaborer une stratégie pour le mandat de cinq ans (voir chapitre 2). Le 2 mars 2015, nous avons publié la stratégie 2015-2019 du CEPD, et avons présenté cette stratégie lors d'un événement réunissant des commissaires de l'Union européenne et d'autres parties prenantes influentes. La tâche exigeante de la mise en œuvre de la stratégie a alors commencé.

3.1 Vision d'une nouvelle ère pour la politique de l'UE en matière de protection des données

Au début du mandat, les discussions sur un nouveau cadre pour la protection des données de l'UE étaient enlisées. L'une de nos priorités absolues a donc été d'aider la Commission européenne, le Parlement et le Conseil à surmonter leurs divergences et à parvenir à un accord (voir section 6.1).

Agissant dans notre rôle de conseiller du législateur de l'UE, nous n'avons pas seulement publié, article par article, des recommandations sur les propositions de textes pour le règlement général sur la protection des données (RGPD), nous avons également fourni ces recommandations sous la forme d'une application mobile. Utilisée par les négociateurs comme guide de référence, cette application a également contribué à promouvoir une plus grande transparence législative.

Un accord sur le texte du RGPD et de la directive relative à la protection des données dans les secteurs de la police et de la justice a été dégagé en décembre 2015 et les textes définitifs ont été publiés en mai 2016. Les préparatifs ont donc commencé en 2016 pour faire en sorte que l'UE soit prête à mettre en œuvre les nouvelles règles lorsqu'elles sont devenues pleinement applicables en mai 2018. Il s'agissait à la fois de rédiger des orientations sur les nouvelles règles et de mettre en place le nouveau comité européen de la protection des données (le « Comité »), dont le CEPD assurerait le secrétariat.

Travaillant en étroite coopération avec nos collègues au sein du groupe de travail « article 29 » (GT29), nous avons pu veiller à ce que le comité européen de la protection des données soit opérationnel à temps pour la journée de lancement du RGPD le 25 mai 2018 (voir section 6.1.3). En plus d'assumer plusieurs nouvelles tâches visant à garantir l'application cohérente du RGPD dans l'ensemble de l'UE, le comité européen de la protection des données a remplacé le GT29 en tant que principal forum de coopération entre les autorités nationales de protection des données (APD) de l'UE et le CEPD.

Le RGPD s'applique aux organisations et aux entreprises opérant dans les États membres de l'UE. Il ne s'applique toutefois pas aux institutions de l'UE elles-mêmes, qui sont soumises à un ensemble de règles différent. En 2017, avec les préparatifs bien avancés pour

le RGPD, nous avons intensifié nos efforts pour aider le législateur européen à réviser les règles applicables aux institutions de l'UE, afin de les aligner sur le RGPD.

Toutefois, les législateurs n'ont pu parvenir à un consensus concernant ce qui deviendrait le règlement (UE) 2018/1725 avant mai 2018. Les nouvelles règles pour les institutions de l'UE ne sont donc entrées en vigueur que le 11 décembre 2018, soit un peu plus de six mois après que le RGPD fut devenu pleinement applicable (voir section 6.1.4).

Le RGPD, la directive relative à la protection des données dans les secteurs de la police et de la justice pénale et le règlement (UE) 2018/1725 suivent les mêmes principes. Le CEPD, en tant que contrôleur de la protection des données pour les institutions de l'UE, a donc été en mesure de formuler une hypothèse informée de ce que les règles révisées pour les institutions de l'UE entraîneraient et de commencer à préparer les institutions de l'UE à leurs nouvelles responsabilités dès un stade précoce.

Cette préparation comprenait des sessions de formation, des visites et des orientations sur les nouvelles règles. L'accent était placé sur le principe de responsabilisation, qui consistait à veiller à ce que les institutions de l'UE respectent non seulement les nouvelles règles, mais puissent aussi démontrer ce respect (voir section 6.2). Nous voulions veiller à ce que les institutions de l'UE soient prêtes à montrer l'exemple dans l'application des règles en matière de protection des données, en fixant la norme à suivre pour d'autres dans l'UE.

Toutefois, les efforts déployés pour parvenir à un accord sur un règlement relatif à la vie privée et aux communications électroniques (le règlement « vie privée et communications électroniques ») ont été moins fructueux. Bien que le CEPD ait beaucoup œuvré pour encourager les colégislateurs à aller de l'avant dans ce dossier, parvenir à un accord final sur le texte avant les élections du Parlement européen de mai 2019 s'est finalement révélé impossible.

Un domaine que le règlement (UE) 2018/1725 ne couvre pas est le traitement de données opérationnelles à caractère personnel au sein de l'organe répressif de l'UE, Europol. En vertu du règlement Europol, le CEPD a pris en charge la supervision de ce type de traitement de données à caractère personnel le 1er mai 2017. Au cours des deux ans et demi écoulés, le CEPD a noué des relations constructives avec Europol, en l'aidant à remplir ses missions réglementaires, sans compromettre les droits fondamentaux à la protection des données et au respect de la vie privée (voir section 6.4.3).

3.2 Une approche internationale de la protection des données

Cependant, dans le monde numérique, la législation ne suffit plus à elle seule. Les cadres traditionnels utilisés pour garantir le respect des droits fondamentaux peuvent ne pas être suffisamment solides pour résister aux défis posés par la révolution numérique. Dans le cadre de la stratégie du CEPD, nous nous sommes donc engagés à lancer un débat mondial sur la manière de garantir la protection des droits fondamentaux et des valeurs à l'ère numérique, en développant une dimension éthique de la protection des données.

Pour y remédier, nous avons lancé l'initiative en matière d'éthique du CEPD (voir section 5.1). Dans un avis publié le 11 septembre 2015, nous avons appelé au développement d'une nouvelle éthique numérique, plaçant la dignité humaine au cœur de l'évolution technologique personnelle et fondée sur les données. L'avis annonçait également notre intention de créer un groupe consultatif sur l'éthique (GCE), un groupe d'experts issus d'horizons différents, chargé d'examiner les relations entre les droits de l'homme, la technologie et les marchés, et d'identifier les menaces qui pèsent sur les droits à la protection des données et au respect de la vie privée à l'ère numérique.

Le GCE a été constitué au début de l'année 2016 et, au début de l'année 2018, il a publié son rapport final, qui reflète les enjeux. Cette initiative a été suivie d'une consultation publique sur l'éthique numérique, destinée à ouvrir le débat à toutes les composantes de la société, dans le monde entier.

En tant que coorganisateurs de la Conférence internationale 2018 des commissaires à la

Guide de la réglementation européenne en vigueur en matière de protection des données

La législation européenne relative à la protection des données est définie dans un certain nombre de règlements et directives de l'Union. Si les règles applicables aux organismes privés et publics opérant dans les États membres sont similaires à celles régissant la protection des données dans les institutions de l'Union européenne, elles ne sont toutefois pas identiques. Vous trouverez ci-dessous une liste des actes réglementaires actuellement applicables dans l'Union européenne ainsi que les types d'organisations auxquelles ils s'appliquent.

Règlement général sur la protection des données (RGPD) - Règlement (UE) 2016/679: s'applique à la majorité des organismes publics et à l'ensemble des organismes privés opérant dans les États membres de l'UE. Ce règlement est mis en application par l'autorité nationale chargée de la protection des données (APD) de l'État membre concerné, laquelle est indépendante.

Règlement (UE) 2018/1725: s'applique à l'ensemble des institutions, organes et organismes de l'Union européenne. Ce règlement est mis en application par le Contrôleur européen de la protection des données (CEPD).

Directive (UE) 2016/680 relative à la protection des données dans les domaines de la police et de la justice pénale: s'applique aux activités répressives menées par les organismes compétents dans les États membres de l'UE. Elle est mise en application par l'APD nationale indépendante de l'État membre concerné.

Article 3 et chapitre IX du règlement (UE) 2018/1725: s'applique au traitement des données à caractère personnel à des fins répressives par une institution, un organe, un office ou une agence de l'Union européenne. Ces règles sont mises en application par le CEPD.

Règlement (UE) 2016/794 relatif à Europol: Sfixe les règles du traitement des données à caractère personnel opérationnelles au sein d'Europol, l'autorité répressive de l'Union européenne. Ce règlement est mis en application par le CEPD.

Règlement (UE) 2017/1939 concernant le Parquet européen: fixe les règles du traitement des données à caractère personnel opérationnelles au sein du Parquet européen. Ce règlement sera mis en application par le CEPD.

Règlement (UE) 2018/1727 relatif à Eurojust: établit quelques règles particulières qu'Eurojust appliquera dans certains cas spécifiques à compter du 12 décembre 2019. Dans tous les autres cas, ses activités opérationnelles seront régies par le chapitre IX du règlement (UE) 2018/1725. Ce règlement sera mis en application par le CEPD.

Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques): définit les règles relatives à la protection des données et de la vie privée dans le secteur des communications électroniques. Certaines règles, telles que celles qui concernent le traitement des données relatives au trafic et des données de localisation, s'appliquent uniquement aux opérateurs de télécommunications et aux prestataires de services internet. D'autres règles, telles que celles relatives à la confidentialité, au suivi en ligne et aux courriers indésirables, s'appliquent à l'ensemble des organismes publics et privés opérant dans les États membres. L'article 5, paragraphe 3, s'applique directement aux institutions européennes.

protection des données et à la vie privée, nous avons décidé de consacrer la session publique de la conférence au thème de l'éthique numérique. Notre objectif était de tirer parti des travaux réalisés grâce à l'initiative en matière d'éthique pour susciter un débat mondial sur les défis de l'ère numérique.

Pour tirer parti du succès de la conférence, nous avons lancé un podcast en 2019. Chaque conversation #DebatingEthics explorait un sujet de préoccupation spécifique relevé lors de la conférence et a donné lieu à la publication, fin 2019, d'un deuxième avis sur l'éthique numérique. Le sujet étant désormais solidement ancré dans le programme international relatif à la protection des données, nous comptons sur de nouvelles évolutions dans ce domaine dans un proche avenir.

Toutefois, ce n'est pas seulement dans le domaine de l'éthique numérique que nos efforts pour dialoguer avec les partenaires internationaux se sont intensifiés. De meilleures relations avec la Commission européenne, le Parlement européen et le Conseil signifient que nous sommes désormais consultés beaucoup plus fréquemment sur les propositions politiques de l'UE, y compris les politiques internationales, et que nous n'hésitons pas à faire entendre notre voix dans les cas où nous nourrissons des préoccupations légitimes qui ne sont pas prises en considération.

Avec le comité européen de la protection des données actuellement en place, l'UE est également mieux à même de coordonner ses efforts et de synchroniser ses messages sur la protection des données, ce qui donne plus de poids à notre voix sur la scène internationale.

3.3 Une réponse collaborative au défi numérique

Nos capacités technologiques évoluent à un rythme de plus en plus rapide. Les progrès accomplis au cours des cinq années qui se sont écoulées depuis le début du mandat du CEPD sont stupéfiants en soi. Pourtant, si les nouvelles technologies ont profondément modifié notre mode de vie, déterminer la meilleure manière de réglementer le développement de ces technologies n'est pas une tâche aisée.

Par l'intermédiaire du réseau d'ingénierie de la vie privée sur l'internet (IPEN), qui réunit des experts issus de différents domaines, le CEPD s'est efforcé de promouvoir les technologies renforçant le respect de la vie privée et la protection des données. En facilitant la mise en œuvre des principes de protection des données dès la conception et de protection des données par défaut, obligatoires en vertu du RGPD, de la directive sur la protection des données dans les secteurs de la police et de la justice et du règlement (UE) 2018/1725, le réseau vise à garantir que la protection des données est prise en compte dès la conception et lors du développement de toutes les nouvelles technologies (voir section 4.1.1).

Le CEPD a également pour objectif de développer et de partager l'expertise technologique dans le domaine de la protection des données, que ce soit au moyen d'avis, d'observations, de documents d'information ou de notre bulletin d'information TechDispatch (voir section 4.1.2).

La *Digital Clearinghouse* (Centre d'échange d'informations numériques) est une autre de nos initiatives collaboratives. Créée par le CEPD en 2016, et lancée officiellement l'année suivante, la Clearinghouse (chambre de compensation numérique) se réunit deux fois par an et sert de forum de coopération entre les autorités chargées de la concurrence, de la protection des consommateurs et de la protection des données. En travaillant ensemble, il est à espérer que les autorités de réglementation dans ces domaines seront mieux à même de relever les défis posés par l'économie numérique et de faire appliquer de manière cohérente les règles de l'UE relatives aux droits fondamentaux dans le monde numérique (voir section 4.2.1).

Montrer l'exemple, cependant, commence par les institutions de l'UE. Étant leur autorité de contrôle, il nous incombe de veiller à ce qu'elles définissent la norme à suivre, en les aidant à renforcer la responsabilisation et la transparence de leurs travaux. En offrant une formation et une orientation et en travaillant en étroite coopération avec les délégués à la protection des données (DPD) des institutions de l'UE, nous entendons leur fournir les outils nécessaires pour y parvenir. Nous contrôlons également de près les activités des institutions et organes de l'UE et, en 2019, nous avons lancé deux enquêtes

de premier plan. Elles visaient à s'assurer que les institutions de l'UE appliquent les niveaux les plus élevés de respect de la protection des données, garantissant ainsi les niveaux de protection les plus élevés pour toutes les personnes vivant dans l'UE (voir section 4.3.1).

Grâce à nos travaux avec les institutions de l'UE, nous espérons non seulement améliorer les pratiques en matière de protection des données des institutions de l'UE, mais aussi contribuer aux efforts visant à améliorer la protection des données dans l'ensemble de l'UE et dans le monde, en faisant mieux connaître les principes de protection des données, ainsi que les éventuels problèmes et préoccupations.

3.4 Mise en œuvre de la stratégie

Une gestion rigoureuse des ressources et une communication efficace font partie intégrante de la réalisation des objectifs définis dans la stratégie du CEPD. De cette manière, nous avons pu nous assurer que nous disposions des ressources adéquates pour mener à bien les travaux en question et que nos messages atteignaient les publics visés.

Au tout début du mandat, nous avons participé à un projet de remise en valeur (voir section 7.1.1). Nous voulions développer une nouvelle identité visuelle pour l'institution, qui refléterait notre statut de chef de file mondial en matière de protection des données et de respect de la vie privée. La première phase du projet a été achevée en 2015, avec l'élaboration d'un nouveau logo. Nous avons lancé, en mars 2017, un nouveau site web doté d'une nouvelle présentation conviviale, puis avons adopté une nouvelle approche dans le cadre de notre bulletin d'information en juin 2017. De nouvelles initiatives, telles qu'un blog et l'application du CEPD, ont également contribué à accroître la transparence des travaux du CEPD et de la politique de l'UE en général.

Afin d'assumer de nouvelles responsabilités et de s'en acquitter à un niveau élevé, le CEPD a besoin de recruter davantage d'experts en matière de protection des données (voir section 7.2.1). Par l'organisation de deux concours d'experts en matière de protection des données, par l'intermédiaire de l'Office européen de sélection du personnel (EPSO), nous avons pu nous assurer que nous disposions d'une liste d'experts compétents en matière de protection des données dans laquelle puiser pour pourvoir toute fonction vacante. Cette liste a été particulièrement utile dans la mise en place du secrétariat du Comité. En outre, nous avons investi du temps et des efforts pour développer les compétences et les connaissances de nos membres du personnel actuels afin de nous assurer que nous sommes à même de montrer la voie à suivre concernant la responsabilisation en matière de protection des données.

En tant qu'institution de l'UE elle-même, le CEPD est également lié par les nouvelles règles en matière de protection des données pour les institutions de l'UE. Notre crédibilité et notre autorité en tant qu'autorité de l'UE chargée de la protection des données dépendent de la mise en œuvre de ces règles selon les normes les plus strictes. Une collaboration à l'échelle de l'institution était donc nécessaire pour garantir que nous étions prêts à montrer la voie à suivre en matière de respect de la protection des données de manière responsable.

3.5 Indicateurs clés de performance

Après l'adoption de notre stratégie 2015-2019, en mars 2015, nous avons réévalué nos indicateurs clés de performance (ICP) existants et établi une nouvelle série d'ICP, reflétant nos nouveaux objectifs et priorités. Ils ont été conçus afin de nous permettre de contrôler et de rectifier, si nécessaire, les conséquences de nos activités et l'efficacité avec laquelle nous utilisons les ressources.

Tout au long du mandat, nous avons présenté chaque année un rapport sur nos ICP, dans notre rapport annuel. Certains ICP ont été adaptés pour tenir compte des changements ou des évolutions importantes ayant une incidence sur l'exécution de certaines activités.

Les ICP se rapportant au premier objectif stratégique (« La protection des données doit

Objectif 1 – *La protection des données doit devenir numérique*

Nombre d'initiatives visant à promouvoir les technologies destinées à améliorer le respect de la vie privée et la protection des données organisées ou coorganisées par le CEPD

Objectif	Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
9 initiatives par an	9 initiatives	9 initiatives	9 initiatives	9 initiatives

Nombre d'activités axées sur des solutions stratégiques interdisciplinaires (internes et externes)

Objectif	Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
8 initiatives par an	9 initiatives	8 initiatives	8 initiatives	8 initiatives

Illustration 1. Évolution des ICP relatifs à l'objectif stratégique « La protection des données doit devenir numérique »

devenir numérique ») se sont concentrés sur des initiatives visant à promouvoir les technologies pour renforcer le respect de la vie privée et la protection des données, ainsi que sur des solutions stratégiques interdisciplinaires. Ils n'ont pas changé tout au long du mandat et ont régulièrement atteint les objectifs fixés (voir illustration 1).

Pour les ICP se rapportant au deuxième objectif stratégique (« Forger des partenariats à grande échelle »), nous avons décidé de rationaliser le suivi de nos travaux au niveau international et, en 2017, nous sommes passés de deux ICP à un seul. Cela signifie que les contributions sur les accords internationaux étaient contrôlées conjointement avec d'autres contributions au niveau international. Dans tous les cas, nous avons enregistré des résultats supérieurs ou nettement supérieurs à l'objectif fixé (voir illustration 2).

Les ICP faisant référence au troisième objectif stratégique (« Ouvrir un nouveau chapitre dédié à la protection des données dans l'UE ») ont porté sur les missions de contrôle et de consultation.

En ce qui concerne les missions de contrôle, nous avons conservé le même ICP sur l'ensemble du mandat, au niveau de satisfaction des DPD, des coordinateurs de la protection des données (CPD) et des responsables du traitement en ce qui concerne la coopération avec le CEPD et les orientations. Les résultats ont constamment dépassé les objectifs fixés, ce qui démontre clairement la satisfaction de nos parties prenantes.

Pour les missions de consultation, les ICP concernés ont connu un certain nombre de modifications tout au long du mandat. Premièrement, l'ICP initial, portant sur l'incidence des avis du CEPD, dépendait de l'évolution du processus législatif, ce qui a rendu difficile le respect du calendrier fixé pour le suivi de nos IPC. Deuxièmement, les ICP se rapportant à l'inventaire du CEPD des propositions législatives pertinentes (sur

Objectif 2 – *Forger des partenariats à grande échelle*

Nombre d'initiatives adoptées concernant les accords internationaux (utilisées en 2015-2016 uniquement)

Résultat au 31.12.2015	Résultat au 31.12.2016
3 initiatives	8 initiatives

Le résultat de 2015 a servi de point de référence, avec un objectif déÿni de 5 initiatives pour 2016

Nombre d'a˜aires traitées au niveau international (comité européen de la protection des données, CdE, OCDE, GPEN, conférences internationales) pour lesquelles le CEPD a fourni une contribution écrite importante

Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
13 affaires	18 affaires	31 affaires	31 affaires

Le résultat de 2015 a servi de point de référence, avec un objectif déÿni de 13 a°aires à partir de 2016

Illustration 2. Évolution des ICP relatifs à l'objectif stratégique consistant à forger des partenariats à grande échelle

la base du programme de travail public de la Commission européenne) ont été visés par des changements, tant internes qu'externes, dans la manière dont nous avons effectué et contrôlé nos activités de conseil stratégique, ce qui a également eu une incidence sur notre capacité à surveiller cet ICP. Toutefois, lorsqu'ils ont été mesurés, les résultats ont atteint ou dépassé leurs objectifs (voir illustration 3).

Certaines modifications ont également eu lieu en ce qui concerne les ICP relatifs aux instruments stratégiques (« Communication et gestion des ressources »).

En ce qui concerne les activités de communication, entre 2017 et 2018, nous avons lancé un nouveau site web, puis mis en œuvre les modifications à la politique en matière de cookies et de suivi afin d'accroître la sensibilisation des utilisateurs et d'être plus respectueux de la protection des données. Cela a eu une incidence sur la manière dont nous avons suivi l'ICP relatif aux visites sur notre site web. Après avoir analysé nos activités de communication, nous avons recensé les résultats concernant nos activités dans les médias sociaux en tant qu'ICP plus significatif, et nous procéderons à cette mesure dans les résultats de notre ICP pour 2019.

Pour nos ICP relatifs à la gestion des ressources, l'un - sur la satisfaction du personnel - a fait l'objet d'un suivi sur une base bisannuelle, fondé sur les résultats de notre enquête auprès du personnel. Le deuxième ICP, portant sur le taux d'exécution budgétaire, a été introduit en 2018 en reconnaissance de l'importance de cette activité. Dans les deux cas, les résultats ont atteint ou dépassé les objectifs fixé (voir illustration 4).

Objectif 3 – *Ouvrir un nouveau chapitre dédié à la protection des données dans l'UE*

Niveau de satisfaction du DPD/du CPD/des responsables du traitement au sujet de la coopération avec le CEPD et des lignes directrices, y compris la satisfaction des personnes concernées en ce qui concerne les formations

Objectif	Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
60% (2015-2017) 70% (2018-2019)	79,5 %	88 %	92,3 %	95 %

Analyse de l'incidence de la contribution du CEPD au RGPD (utilisée en 2015-2016 uniquement

Résultat au 31.12.2015	Résultat au 31.12.2016
Sans objet	RGPD: forte incidence Directive: incidence moyenne

Analyse de l'incidence de la contribution des avis du CEPD (utilisée en 2017 uniquement)

Résultat au 31.12.2017
Sans objet

Niveau d'intérêt des parties prenantes (utilisé en 2018 uniquement)

Objectif	Résultat au 31.12.2018
10 consultations	15 consultations

Taux d'exécution des dossiers dans la liste de priorité du CEPD (régulièrement mise à jour) sous la forme de commentaires informels et d'avis formels

Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
83 %	93 %	100 %	Sans objet

Illustration 3. Évolution des ICP relatifs à l'objectif stratégique « Ouvrir un nouveau chapitre dédié à la protection des données dans l'UE »

Facteurs – *Communication et gestion des ressources*

Nombre de visites sur le site web du CEPD (utilisé en 2015-2017)

Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017
195 715	459 370	181 805

Le résultat de 2015 a servi de point de référence

Nombre d'abonnés au compte Twitter du CEPD (utilisé en 2015-2018)

Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
3 631	6 122	9 407	14 000

Niveau de satisfaction du personnel

Objectif	Résultat au 31.12.2015	Résultat au 31.12.2016	Résultat au 31.12.2017	Résultat au 31.12.2018
75 %	Sans objet	75 %	Sans objet	75 %

Exécution du budget (utilisée en 2018-2019 uniquement)

Objectif	Résultat au 31.12.2018
90 %	93,8 %

Illustration 4. Évolution des ICP relatifs aux instruments stratégiques de communication et gestion des ressources

4. LA PROTECTION DES DONNÉES SE NUMÉRISE

Le monde dans lequel nous vivons est incontestablement numérique. La technologie évolue à un rythme de plus en plus rapide, transformant notre mode de vie d'une manière que nous n'aurions jamais pu prévoir. Pourtant, bien que les avancées technologiques présentent des avantages incontestables, elles ne sont pas dénuées de risques.

De nombreuses nouvelles technologies reposent sur la collecte et l'utilisation généralisées de quantités massives de données à caractère personnel. Alors que l'innovation technologique a fait des progrès fulgurants, la réaction institutionnelle a été lente et le maintien du contrôle sur nos données à caractère personnel est devenu sans cesse plus difficile.

Au cours des cinq dernières années, nous avons déployé des efforts considérables pour aider les citoyens à reprendre le contrôle. Dans la stratégie du CEPD pour la période 2015-2019, nous avons conclu à la nécessité urgente de tenir compte, et de gérer, l'incidence de la révolution technologique sur le respect de la vie privée et la protection des données. Nous avons appelé les autorités de réglementation à travers le monde à se coordonner en vue d'apporter une réponse rapide et innovante visant à protéger les droits fondamentaux et à rétablir l'équilibre. Nous devrions tous pouvoir bénéficier des nouvelles technologies sans pour autant compromettre nos droits fondamentaux. Nous avons fait valoir que la protection des données doit devenir numérique.

La stratégie établit trois points d'action visant à élaborer une approche réglementaire efficace à l'ère numérique. Ces actions mettent l'accent sur le développement de technologies respectueuses de la vie privée, la coopération avec d'autres organismes de réglementation et la promotion d'une approche transparente et responsable concernant les traitements de *Big Data*. Nous estimons avoir accompli des progrès significatifs dans ces trois domaines, en jetant les bases sur lesquelles les autorités chargées de la protection des données (APD) et les autres organismes de réglementation s'appuieront dans les années à venir.

@EU_EDPS

Time for #eudatap to go digital. Technology is not neutral and must not be allowed to dictate ethics #CPDP2015

4.1 Promouvoir les technologies qui améliorent le respect de la vie privée et la protection des données

Dans tous les domaines de la vie économique et privée, le nombre de services qui utilisent des technologies traitant, d'une façon ou d'une autre, les données à caractère personnel est en constante augmentation. Dans de nombreux cas, les organisations qui traitent ces données le font en vue d'en retirer un avantage, qu'il soit économique ou autre. Le défi pour les régulateurs consiste à garantir la protection des individus malgré les risques que comportent ces activités de traitement des données, toujours plus nombreuses.

Relever ce défi suppose de veiller à ce que les mesures de protection des données et de respect de la vie privée soient dûment prises en considération dans le cadre des évolutions technologiques actuelles et nouvelles. Le CEPD a apporté sa contribution dans ce domaine, en surveillant et en répondant aux enjeux technologiques, en promouvant l'élaboration de mesures d'ingénierie de la vie privée et en collaborant avec d'autres organismes pour établir une interprétation commune de ce qu'il convient de considérer comme l'état de l'art de la protection des données dès la conception.

4.1.1 Ingénierie de la vie privée

L'ingénierie de la vie privée est une discipline émergente. Elle porte essentiellement sur la promotion de nouvelles solutions d'ingénierie visant à garantir et à renforcer la protection des données et de la vie privée en ligne. Au cours des cinq dernières années, le CEPD a pris part à plusieurs initiatives d'ingénierie de la vie privée, dans le but partagé d'intégrer les principes de protection des données et de respect de la vie privée dans les évolutions technologiques.

Le réseau d'ingénierie de la vie privée sur l'internet

Conformément à la nouvelle législation de l'UE en matière de protection des données, les responsables du traitement sont tenus de respecter les principes de la protection des données dès la conception et par défaut. Quant aux concepteurs et aux fabricants de technologies, ils doivent tenir compte du respect de la vie privée et de la protection des données lors de la conception et de l'élaboration de solutions technologiques. Pour les aider à se préparer à ces nouvelles exigences, le CEPD a mis sur pied le réseau d'ingénierie de la vie privée sur l'internet (IPEN).

Lancé en 2014, l'IPEN rassemble des experts venus d'horizons divers pour encourager la recherche de solutions techniques aux problèmes de protection de la vie privée. En soutenant les projets qui intègrent le respect de la vie privée dans les outils numériques existants et nouveaux, le réseau vise à promouvoir et à faire évoluer les pratiques actuelles en matière d'ingénierie de la vie privée.

Depuis la tenue du premier atelier en 2014, l'IPEN a grandi et évolué. Le réseau se concentrait dans un premier temps sur l'examen des concepts pertinents pour l'ingénierie de la vie privée, en clarifiant leur interprétation et en mettant à disposition une plate-forme visant à promouvoir les solutions disponibles respectueuses de la vie privée. Des ateliers annuels, couplés à d'autres réunions, événements et débats (voir illustration 5), ont préparé le terrain à l'adoption d'une approche plus ciblée lors de l'atelier organisé à Rome en 2019.

Les nouvelles règles de l'UE en matière de protection des données étant à présent pleinement applicables, l'atelier de 2019 s'est attaché à comprendre plus précisément et plus concrètement l'évolution des technologies respectueuses de la vie privée. Il avait pour objectif de parvenir à une convergence de vues entre les responsables du traitement et les concepteurs, les régulateurs et les experts juridiques, sur ce qui constitue la technologie de pointe en matière de protection des données dès la conception. C'est cette vision commune qui aidera tous les acteurs concernés à créer de nouveaux processus de conception, de nouvelles technologies et de nouveaux modèles économiques intelligents, qui protégeront plus efficacement les individus et leur dignité.

Partenaires dans le cadre de l'ingénierie de la vie privée

En plus de travailler sur l'initiative IPEN, nous avons collaboré avec d'autres organisations impliquées dans la promotion de l'élaboration de solutions d'ingénierie de la vie privée et de technologies renforçant la protection de la vie privée. L'Institut national des normes et des technologies (US-NIST), une division du ministère américain du commerce, qui s'est doté de son propre programme d'ingénierie de la vie privée, en est un partenaire important.

Nous suivons les travaux menés par le NIST depuis le lancement de son programme d'ingénierie de la vie privée et nous collaborons avec lui dans le cadre de plusieurs projets. En plus de participer à l'un des ateliers organisés par le NIST en 2018, nous avons pris part avec lui à plusieurs événements consacrés à l'ingénierie de la vie privée au cours des trois dernières années. Le CEPD et le NIST évoluent dans des environnements juridiques et institutionnels radicalement différents. Cependant, en matière d'ingénierie de la vie privée, nos méthodes et nos objectifs ont beaucoup en commun, ce qui ne peut avoir qu'une incidence positive sur l'évolution de l'ingénierie de la vie privée.

Le travail accompli par le NIST ne s'applique légalement qu'au secteur public des États-Unis d'Amérique, mais les secteurs à forte intensité de données semblent également s'intéresser

Illustration 5. Ateliers, réunions, événements et débats de l'IPEN, 2015-2019

de plus en plus à l'ingénierie de la vie privée. La création de sections consacrées à l'ingénierie de la vie privée au sein des associations sectorielles pertinentes illustre bien ce phénomène. Pour promouvoir davantage ces initiatives, l'IPEN a contribué à plusieurs événements pertinents, notamment à des conférences organisées par l'International Association of Privacy Professionals (IAPP) en 2017, 2018 et 2019 ainsi qu'aux éditions 2015-2018 de la conférence « *Computers, Privacy and Data Protection* » (CPDP).

4.1.2 Suivre les avancées technologiques et y faire face

Le CEPD ne contribue pas seulement à promouvoir et à faire prendre conscience de la nécessité de disposer de technologies respectueuses de la vie privée au travers de diverses initiatives en matière d'ingénierie de la vie privée. Nous avons également pour objectif de suivre les avancées, les événements et les incidents technologiques et d'y faire face, et d'évaluer leur incidence sur la protection des données. Nos travaux ont donné lieu à plusieurs notes d'orientation, avis et rapports, qui ont été publiés au cours du présent mandat.

Développer et partager l'expertise technologique

Il est désormais impossible de garantir une protection efficace des données en l'absence d'expertise technologique. La révolution numérique a contraint les APD et les autres autorités de réglementation à renforcer leurs compétences dans ce domaine. Le CEPD s'est toujours efforcé d'être à la pointe de cette tendance, en fournissant une analyse utile des nouvelles avancées technologiques.

Notre document de veille technologique sur les lunettes intelligentes et la protection des données, publié en janvier 2019, en est un exemple. Bien que les lunettes intelligentes puissent sembler sortir tout droit d'un film de science-fiction, elles sont en réalité de plus en plus accessibles et de plus en plus utilisées, que ce soit par les pouvoirs publics, les entreprises ou les particuliers. L'intérêt affiché par les services répressifs à travers le monde illustre les possibilités que cette technologie peut offrir. Cependant, bien qu'elles puissent se révéler utiles dans de nombreux contextes, notamment dans les secteurs de la maintenance technique, de l'éducation et de la construction, les lunettes intelligentes peuvent avoir de graves répercussions sur le respect de la vie privée, notamment lorsque l'approche retenue pour leur élaboration ne tient pas compte de la vie privée dès la conception.

Notre rapport sur les lunettes intelligentes analyse ces répercussions. Il présente également une synthèse des fabricants concernés et des cas dans lesquels ces lunettes sont actuellement utilisées, et évalue les évolutions possibles.

Nous espérons apporter notre pierre à l'édifice d'une manière différente par notre bulletin d'information TechDispatch. Dans chaque numéro de TechDispatch, publié depuis juillet 2019, nous visons à expliquer une nouvelle technologie émergente. TechDispatch fournit des informations sur la technologie elle-même, une évaluation préliminaire de son incidence éventuelle sur le respect de la vie privée et la protection des données à caractère personnel et des liens qui permettent d'approfondir le sujet.

Le logiciel d'inspection de sites web du CEPD est une autre initiative visant à encourager l'expertise technologique. Pour la première fois de son histoire, le CEPD a publié en 2019 un outil logiciel destiné à soutenir le travail des professionnels de la protection des données, tels que les responsables du traitement, les délégués à la protection des données (DPD), les APD et les chercheurs.

Notre outil *Website Evidence Collector*, initialement conçu pour procéder à l'inspection des sites web des institutions européennes (voir section 6.2.3), fonctionne sous Linux, MacOS X et Windows. Une fois installé, et après une brève présentation, cet outil permet aux novices sur le plan technique de collecter automatiquement des preuves du traitement de données à caractère personnel, telles que des cookies ou des demandes adressées à des tiers. Les données collectées sont documentées dans un format lisible pour les humains et les machines. Cet outil est un logiciel libre, que nous avons publié sous la licence publique de l'UE sur le site web du CEPD et sur GitHub, la plate-forme de partage de code.

En publiant ce type d'informations, nous voulons contribuer au réservoir commun de connaissances dont l'ensemble des APD et d'autres parties intéressées pourront bénéficier.

Le respect de la vie privée dès la conception

Ces dernières années, plusieurs scandales concernant l'utilisation abusive de données à caractère personnel à des fins de suivi et de profilage ont fait la une de la presse. Les débats qui s'en sont suivis ont soulevé un certain nombre de questions concernant le rôle que la technologie devrait jouer au sein de la société. La question a notamment été posée de savoir si les entreprises devaient utiliser la technologie exclusivement pour accroître leurs bénéfices.

La protection des données dès la conception et la protection des données par défaut sont deux principes qui pourraient contribuer au bénéfice sociétal et humain des avancées technologiques, plutôt que le seul profit des entreprises en tant que moteur principal de ces avancées. Mises en place au titre de la nouvelle législation de l'UE en matière de protection des données, ces obligations juridiques imposent aux entités chargées de la collecte et du traitement de données à caractère personnel de mettre en place des mesures techniques et organisationnelles pour garantir et démontrer le respect des règles en matière de protection des données. Dans le cas de la protection des données dès la conception, cela implique de planifier la manière d'intégrer la protection des données à caractère personnel dans les nouveaux systèmes et processus technologiques tout au long du cycle de vie d'un projet, tandis que la protection des données par défaut suppose d'intégrer la protection de la vie privée dans l'ensemble des produits et services technologiques comme paramètre par défaut.

Le 31 mai 2018, quelques jours après que le règlement général sur la protection des données (RGPD) de l'UE fut devenu pleinement applicable, nous avons publié un avis préliminaire sur le respect de la vie privée dès la conception. Cet avis se fonde sur les travaux de l'IPEN et sur l'initiative en matière d'éthique du CEPD (voir section 5.1). Il encourage les législateurs, les autorités de réglementation, l'industrie, le monde universitaire et la société civile à travailler ensemble en vue d'adopter une approche commune en matière de progrès technologique, qui serait d'abord centrée sur la dignité des êtres humains.

Des travaux visant à élaborer cette approche commune sont actuellement en cours au sein de plusieurs plates-formes collaboratives. Il s'agit notamment de l'IPEN, du comité européen de la protection des données et du groupe de travail international sur la protection des données et les télécommunications (également connu sous le nom de « *Berlin Group* »).

Intelligence artificielle

Ces dernières années, des développements significatifs ont été enregistrés dans les domaines de l'intelligence artificielle (IA) et de la robotique. Bien que les nouvelles technologies, lorsqu'elles sont associées à l'intelligence artificielle, ouvrent incontestablement la voie à des perspectives d'avenir enthousiasmantes, elles présentent néanmoins des défis de taille en ce qui concerne la protection des données.

Pour prendre des décisions, l'IA s'appuie sur des algorithmes, plutôt que sur l'esprit humain. En l'absence de tout système décisionnel humain ou prévisible, il nous est pratiquement impossible d'obtenir des informations quant à la manière dont les technologies basées sur l'intelligence artificielle traitent nos données à caractère personnel. Par conséquent, il nous est souvent impossible d'accorder notre consentement éclairé au traitement de nos données à caractère personnel par ces technologies.

En 2016, la Conférence internationale annuelle des commissaires à la protection des données et à la vie privée (ICDPPC) a classé l'IA et la robotique parmi les principaux sujets de discussion, au cours de sa session fermée à laquelle ont participé des membres accrédités et des observateurs de l'ICDPPC. Les participants à la conférence en session fermée souhaitaient adopter une position commune sur ces nouvelles technologies. Pour éclairer les discussions, le CEPD a préparé un document d'information détaillant les utilisations qui sont faites de l'IA et de la robotique et proposant des pistes de réflexion.

En 2018, la Conférence internationale est revenue sur le sujet. Cette année-là, les débats tenus lors de la conférence en session fermée ont donné lieu à une déclaration de l'ICDPPC sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle. Cette déclaration énonce six principes relatifs à l'évolution de l'IA et appelle à une action concertée à l'échelle internationale pour mettre ces principes en œuvre. L'ICDPPC a créé un nouveau groupe de travail permanent sur l'éthique et la protection des données dans le secteur de l'IA pour contribuer à cet effort. Le CEPD est l'un des coprésidents de ce groupe, dont il assure également le secrétariat.

4.2 Trouver des solutions stratégiques interdisciplinaires

Les progrès technologiques posent de nombreux défis que les APD ne peuvent relever seules. La coopération entre les régulateurs, les autorités et d'autres experts est nécessaire pour trouver des solutions et les mettre en œuvre.

À l'ère numérique, la protection des données ne peut être traitée comme un domaine de compétence isolé. Il convient de transcender les frontières disciplinaires pour aborder les questions stratégiques liées à la vie privée et à la protection des données et pour développer des approches coordonnées et communes aux défis qui se posent à nous.

Ces cinq dernières années, nous avons élaboré et lancé plusieurs initiatives visant à renforcer la coopération et à concevoir des solutions en collaboration avec divers partenaires. L'IPEN en est un bon exemple (voir section 4.1.1), mais nous avons également travaillé avec la société civile, des autorités de la concurrence et de protection des consommateurs et d'autres autorités de réglementation en vue d'atteindre nos objectifs communs.

@EU_EDPS

.@Buttarelli_G #DigitalClearingHouse to bring together independent authorities to discuss & promote interests of individuals online #EDPD17

4.2.1 Le centre d'échange d'informations numérique (« *The Digital Clearinghouse* »)

Il existe des synergies naturelles entre la protection des données, la protection des consommateurs et la politique de la concurrence. Cependant, les autorités compétentes dans ces différents domaines fonctionnent depuis longtemps en vase clos. Pour améliorer notre compréhension des dynamiques du marché et pour apporter des réponses cohérentes et conséquentes aux défis posés par l'économie numérique, il s'impose de renforcer la coopération entre ces autorités.

En septembre 2016, Giovanni Buttarelli, le contrôleur européen de la protection des données, a fait part de son intention de créer un centre d'échange d'informations numérique. L'objectif poursuivi était de promouvoir une application plus cohérente des règles de l'UE en matière de droits fondamentaux. Regroupant des autorités de réglementation bénévoles, le centre d'échange d'informations a été conçu comme un réseau permettant aux autorités de réglementation dans les domaines de la protection des consommateurs, de la concurrence et de la protection des données de partager des informations et d'examiner la meilleure manière d'appliquer les règles dans l'intérêt des personnes. Le Parlement européen et l'ICDPPC ont tous deux pris acte des efforts que nous avons déployés pour regrouper les différents volets des activités déjà entreprises dans ce domaine.

Le centre d'échange d'informations numérique s'est réuni pour la première fois le 29 mai 2017 ; l'ensemble des régulateurs de l'espace numérique, qu'ils soient basées dans l'UE ou ailleurs, ont été invitées à prendre part aux discussions. Cette réunion, qui a marqué l'aboutissement de plusieurs années de discussions importantes quant à la manière de relever les défis numériques, s'est attachée à recenser les préoccupations et les lacunes communes en matière de réglementation qui orienteront les futures réunions.

Le nombre de participants et le thème de la réunion, qui est organisée deux fois par an, ont progressivement évolué (voir illustration 6). La troisième réunion a été la première à accueillir des autorités de pays tiers ; lors de la quatrième

réunion, la participation a été étendue aux autorités électorales afin de discuter, notamment, de l'incidence de la manipulation en ligne sur la liberté et l'équité des activités politiques. Le centre d'échange d'informations étant désormais bien établi, l'accent est désormais mis sur le recensement des domaines se prêtant à une coopération pratique, sur la base de cas concrets, pour veiller à ce que les intérêts des personnes soient au centre de toutes les nouvelles évolutions technologiques.

4.2.2 Rencontre avec la société civile

Le CEPD, à l'instar des groupes de défense des libertés civiles, croit fermement que les droits des personnes doivent être au cœur de toutes les politiques de l'UE. Dès le début de l'actuel mandat du CEPD, Giovanni Buttarelli a fait du dialogue ouvert avec les groupes de défense des libertés civiles l'instrument privilégié permettant de mieux comprendre les préoccupations des citoyens et de veiller à ce que celles-ci soient prises en considération au niveau de l'Union.

Des rencontres entre des groupes de la société civile et le CEPD sur l'état de la protection des données et du respect de la vie privée dans l'UE ont régulièrement eu lieu depuis mai 2015. Le thème central de nos rencontres avec la société civile change chaque année, en fonction du débat politique.

La première rencontre s'est tenue le 27 mai 2015. Les nouvelles règles en matière de protection des données étant toujours en cours de discussion, cette réunion a été pour nous l'occasion de veiller à ce que les préoccupations et les avis de la société civile soient entendus et pris en considération par le législateur de l'UE. Les réunions suivantes ont mis l'accent sur une série de questions législatives, notamment sur l'application du RGPD, la réforme de la directive relative à la vie privée et aux communications électroniques, le bouclier de protection des données (« *Privacy Shield* ») et le contrôle des contenus illicites et préjudiciables en ligne.

Par ailleurs, en 2018, en tant qu'organisation hôte de la Conférence internationale annuelle des commissaires à la protection des données et à la vie privée (voir section 5.2.1), nous nous sommes consciemment efforcés de veiller à ce que les organisations de la société civile participent à la session publique de la conférence, à la fois en qualité de participants et d'intervenants.

Le 19 décembre 2017, en réponse à une déclaration conjointe de la coalition mondiale d'associations de la société civile, nous avons adressé une lettre ouverte à la société civile. Dans cette lettre, nous avons réaffirmé l'importance de veiller à la participation active des représentants des organisations non gouvernementales, outre celle des autorités nationales de réglementation, du monde universitaire et des représentants du gouvernement et de l'industrie, au cours de la session publique de la conférence, afin de garantir un débat sérieux. Nous avons souhaité créer un environnement propice à la libre expression des opinions et à la construction de nouveaux partenariats.

En plus des initiatives visant à nouer des liens avec la société civile, le CEPD et le contrôleur adjoint ont participé à des événements organisés par des groupes de la société civile. Ils ont notamment pris part au sommet RightsCon et Wojciech Wiewiórowski, le contrôleur adjoint, a prononcé un discours liminaire lors de l'événement « *Freedom not Fear* » ainsi qu'à l'occasion de la célébration de l'anniversaire de l'EDRi.

4.3 Augmenter la transparence, le contrôle des données par les utilisateurs et la responsabilisation dans les traitements de Big Data

Pour assurer le contrôle de nos données à caractère personnel, il nous faut pouvoir déterminer quelles données sont utilisées, à quelles fins et par qui. Cela suppose également de pouvoir pleinement exercer les droits relatifs à la protection des données. Bien que l'idée puisse sembler simple en théorie, le traitement automatisé et complexe des données à caractère personnel, l'utilisation d'algorithmes pour prendre des décisions et la quantité considérable de données à caractère personnel collectées, fournies et partagées librement par de nombreux acteurs de l'économie moderne, en particulier en ligne, a considérablement compliqué ce processus.

La «Digital Clearinghouse» (chambre de compensation numérique): 2016-2019

La chambre de compensation numérique a été créée en 2016 afin de faciliter la coopération entre autorités de réglementation dans les domaines de la protection des données, de la concurrence et de la protection des consommateurs.

23 septembre 2016

Le CEPD publie un avis sur une application cohérente des droits fondamentaux à l'ère des données massives (*Big Data*). Dans cet avis, nous proposons la création d'une chambre de compensation numérique, un réseau volontaire d'autorités de réglementation qui souhaitent partager des informations et des idées sur la manière de garantir l'application cohérente des différents domaines du droit régissant l'économie numérique.

29 septembre 2016

Le CEPD et le Bureau européen des unions de consommateurs (BEUC) organisent une conférence sur le thème *Mégadonnées: droits individuels et contrôle avisé de l'application des règles*. La conférence réunit les principales autorités de réglementation dans les domaines de la concurrence, de la protection des données et de la protection des consommateurs afin de débattre d'aspects déterminants de l'évolution économique et sociale mondiale, de promouvoir une coopération et un dialogue plus étroits entre les organismes de réglementation et de répression et d'étudier les moyens de mieux répondre aux défis auxquels la société est confrontée.

29 mai 2017

La chambre de compensation numérique tient sa première assemblée. Les autorités de réglementation débattent de questions d'intérêt commun à court et long termes, dont la portabilité des données, les «fake news» et la manipulation des électeurs, l'émergence de marchés de l'attention et l'opacité des algorithmes qui déterminent la manière dont les données à caractère personnel sont collectées et utilisées. Les participants commencent à identifier des principes de coopération.

27 novembre 2017

La chambre de compensation numérique se réunit pour la deuxième fois. Les discussions portent sur plusieurs domaines où peuvent exister des chevauchements ou des lacunes sur le plan réglementaire. Il s'agit notamment de l'impact à long terme des grandes fusions dans le secteur technologique, des «fake news», des considérations de sécurité liées à l'internet des objets, des conditions préjudiciables ou déloyales appliquées sur les plateformes en ligne et de la recherche de pistes nouvelles. *online platforms* and *the generation of leads*.

21 juin 2018

La troisième réunion de la chambre de compensation numérique est la première à accueillir des représentants d'autorités de pays tiers. Les thèmes de discussion incluent la pertinence des données à caractère personnel dans le cadre de l'application des règles de concurrence et de protection des consommateurs, l'équité des politiques et conditions de confidentialité dans les services en ligne gratuits, les pratiques de tarification collusoires et personnalisées et les théories du préjudice qui s'y rapportent dans les marchés numériques, ainsi que la collecte et l'analyse de données contraires à l'éthique aux fins d'une commercialisation ciblée.

10 décembre 2018

Nous élargissons la portée de la quatrième réunion de la chambre de compensation numérique afin d'associer aux débats les autorités de réglementation électorale. La réunion traite de l'incidence de la manipulation en ligne sur les activités politiques libres et équitables, ainsi que d'autres domaines de coopération pratique, tels que le procédé déloyal qui consiste dans la présentation trompeuse d'une offre comme étant gratuite, la réglementation asymétrique en matière d'accès aux données et le recours abusif à la protection des données par les autorités nationales pour faire obstacle aux enquêtes.

5 juin 2019

Lors de la cinquième réunion de la chambre de compensation numérique, la session de la matinée est consacrée aux défis posés par la réglementation des services à tarification non monétaire. Dans l'après-midi, les débats portent sur les grandes entreprises technologiques, l'accent étant mis en particulier sur les décisions et les mesures récentes prises contre Facebook en matière de protection des consommateurs.

9 juillet 2019

En collaboration avec le Commissaire fédéral allemand à la protection des données et à la liberté de l'information, nous organisons un débat sur le thème de *la protection des données et la compétitivité à l'ère numérique*. Les participants évaluent la convergence entre la protection des données et la politique de concurrence, à une époque où les modèles d'entreprise s'appuient de plus en plus sur de grandes quantités de données à caractère personnel.

Illustration 6. Réunions et événement du centre d'échange d'informations numérique, 2016-2019

La transparence et la responsabilisation, dans le cadre du traitement des données à caractère personnel, sont plus importantes que jamais. Les institutions de l'Union doivent s'assurer de montrer l'exemple aux autres organisations et entreprises de l'UE et il incombe au CEPD, en sa qualité d'autorité de contrôle de la protection des données, de veiller à ce que les institutions indiquent la voie à suivre. Le CEPD peut, notamment, dispenser des formations, fournir des orientations (voir section 6.2.2), mener des enquêtes sur les activités des institutions de l'Union et rechercher des solutions susceptibles de faciliter le traitement transparent et responsable des données.

4.3.1 Enquêtes menées par le CEPD

En tant qu'autorité de contrôle de l'ensemble des institutions européennes, le CEPD est chargé de faire appliquer et de contrôler le respect des règles relatives à la protection des données. Il est également tenu de veiller à ce que le public ait conscience des risques éventuels que le traitement des données à caractère personnel peut présenter pour les droits et libertés individuels et sociétaux. C'est à ce titre que, en 2019, le CEPD a ouvert deux enquêtes très médiatisées sur le respect, par les institutions de l'UE, des règles en matière de protection des données.

Activités de communication en vue des élections parlementaires européennes

En 2019, en vue des élections parlementaires européennes, le Parlement européen a lancé plusieurs actions de communication. L'une de ces actions consistait à promouvoir la participation au scrutin à travers un site web appelé *thistimeimvoting.eu*, qui a collecté les données à caractère personnel de citoyens intéressés par la campagne électorale.

Nous avons découvert que le Parlement européen a confié la tâche à NationBuilder, une société basée aux États-Unis spécialisée dans les campagnes électorales, d'assurer la prestation de services liés à ce site web. Ces services comprenaient notamment le traitement des données à caractère personnel pour le compte du Parlement. Compte tenu de la controverse qui a précédemment entouré NationBuilder, en février 2019, nous avons ouvert une enquête sur le recours du Parlement à cette société, afin de veiller à ce que l'utilisation du site web par le Parlement et le traitement connexe des données à caractère personnel soient licites et conformes aux règles applicables aux institutions de l'UE, établies dans le règlement (UE) 2018/1725.

Les élections parlementaires européennes ont eu lieu après qu'une série de controverses de nature électorale a éclaté dans les États membres de l'UE et à l'étranger. Il était, par conséquent, primordial que le CEPD intervienne pour veiller à ce que le Parlement européen collecte et utilise les données à caractère personnel de manière transparente et légale. C'est dans cette optique que le CEPD a, pour la première fois de son histoire, infligé un blâme à une institution de l'UE : une violation par le Parlement de l'article 29 du règlement (UE) 2018/1725 concernant la sélection et l'agrément de sous-traitants utilisés par NationBuilder.

Le CEPD a également ordonné au Parlement de publier une notice d'information relative à la protection de la vie privée conforme au règlement. Le Parlement européen ayant omis de publier cette notice d'information dans le délai fixé, le CEPD a émis un deuxième blâme à son encontre.

Nous prévoyons de contrôler les procédures du Parlement en matière de protection des données fin 2019, dès que celui-ci aura terminé d'informer les personnes physiques de son intention révisée de conserver les données à caractère personnel collectées par le site web jusqu'en 2024. Il sera possible de tirer des conclusions supplémentaires une fois que ce processus sera terminé.

Cette enquête nous a permis de tester le rôle de surveillance qui nous incombe au titre du nouveau règlement. Au fil de l'enquête, la compréhension et la coopération entre le Parlement européen et le CEPD ont gagné en efficacité, ce qui est essentiel pour garantir et protéger les intérêts des citoyens de l'UE.

Accords contractuels avec des prestataires de service extérieurs

En avril 2019, nous avons ouvert une enquête sur le respect des accords contractuels et pratiques

conclus entre les institutions de l'UE et Microsoft quant à l'utilisation des produits et services de Microsoft.

Lorsqu'elles s'en remettent à des tiers pour fournir des services, les institutions de l'UE restent responsables du traitement des données effectué pour leur compte. Elles sont également tenues de veiller à ce que les accords contractuels respectent la nouvelle législation en matière de protection des données et de prendre des mesures visant à réduire et atténuer les risques. Les clauses contractuelles doivent donc inclure des mesures organisationnelles et techniques spécifiques pour protéger la vie privée et les droits des personnes à la protection des données et veiller à ce que, dans la pratique, le traitement de leurs données à caractère personnel soit conforme aux règles.

Les institutions européennes utilisent les services et produits de Microsoft pour mener leurs activités quotidiennes, qui incluent le traitement de grandes quantités de données à caractère personnel. Compte tenu de la nature, de l'étendue, du contexte et de la finalité du traitement de ces données, il est particulièrement important de veiller à ce que des garanties contractuelles appropriées et des mesures d'atténuation des risques soient en place. Notre enquête s'est, par conséquent, attachée à recenser les produits et services de Microsoft utilisés par les institutions de l'UE et à contrôler la conformité des accords contractuels conclus entre Microsoft et les institutions de l'UE aux règles de protection des données. En outre, nous avons évalué si les mesures convenues avec Microsoft, et les mesures appliquées par les institutions de l'UE, permettaient de réduire et d'atténuer les risques posés aux individus par le traitement de leurs données à caractère personnel par les produits et services de Microsoft.

Nous avons adopté différentes approches dans le cadre de cette enquête ; nous avons notamment réalisé des contrôles sur place pour vérifier les faits et les pratiques et pour contrôler les mesures mises en œuvre par les institutions de l'UE. Les résultats de cette enquête devraient contribuer à améliorer le respect par l'ensemble des institutions de l'UE de la protection des données, mais nous voulons également être en première ligne des changements positifs en cours en dehors des institutions de l'Union, de manière à en faire profiter le plus grand nombre. En collaborant avec les autres institutions, nous espérons faire en sorte que les modifications nécessaires apportées aux produits et les garanties contractuelles et techniques supplémentaires puissent être utilisées par l'ensemble des pouvoirs publics qui opèrent dans l'espace économique européen (EEE).

4.3.2 Systèmes de gestion des informations personnelles

Notre vie en ligne s'inscrit actuellement dans un système centré sur les prestataires, dans lequel les politiques de confidentialité tendent à servir les intérêts du prestataire ou d'un tiers, plutôt que ceux des citoyens. Grâce aux données qu'ils collectent, les réseaux publicitaires, les fournisseurs de réseaux sociaux et d'autres entreprises sont en mesure d'établir des profils individuels de plus en plus exhaustifs, de sorte qu'il est compliqué pour les citoyens d'exercer leurs droits ou de gérer leurs données à caractère personnel en ligne.

Bien que le RGPD et le règlement (UE) 2018/1725 renforcent le contrôle que les citoyens peuvent exercer sur la manière dont leurs données à caractère personnel sont collectées et utilisées en ligne, il est possible et nécessaire d'en faire davantage pour veiller à ce que les citoyens puissent reprendre le contrôle de leurs identités numériques. Le RGPD et le règlement (UE) 2018/1725 doivent être considérés comme un point de départ pour l'élaboration d'une approche plus humaine, fondée sur la transparence et le contrôle par les utilisateurs.

Dans notre avis sur une application cohérente des droits fondamentaux à l'ère des données massives (« *Big Data* ») de septembre 2016, nous avons souligné les difficultés associées à l'exercice des droits relatifs à la protection des données dans l'environnement numérique actuel. Toutefois, notre avis sur les systèmes de gestion des informations personnelles (PIMS) d'octobre 2016 incitait à un certain optimisme. Dans cet avis, nous avons répertorié les efforts déployés pour élaborer une nouvelle vision de la réalité, dans laquelle les citoyens, plutôt que les prestataires de services en ligne, sont en mesure de gérer et de contrôler leurs identités numériques.

La mise au point de PIMS permettrait aux citoyens d'entreposer leurs données à caractère personnel dans des systèmes de stockage en ligne sécurisés et de décider quand et avec qui ils souhaitent partager ces informations. Cette technologie émergente est caractérisée par une variété de configurations et de modèles opérationnels, qui partagent tous le même objectif, à savoir renforcer les droits fondamentaux dans le monde numérique tout en créant de nouveaux débouchés commerciaux pour les fournisseurs de PIMS.

Dans notre avis, nous avons exhorté la Commission européenne à soutenir l'élaboration d'outils numériques innovants, tels que les PIMS, et à adopter des initiatives stratégiques favorisant la conception de modèles opérationnels économiquement viables pour faciliter l'utilisation de ces outils. Il convient d'encourager l'élaboration d'initiatives technologiques, commerciales et juridiques visant à garantir la mise en œuvre efficace des règles en matière de protection des données, qui nous aideront à reprendre le contrôle de nos identités numériques.

Le CEPD continue de suivre l'évolution des PIMS et d'autres initiatives ayant pour but de renforcer la transparence et le contrôle des utilisateurs. L'IPEN (voir section 4.1.1), par exemple, constitue un forum utile aux fins du suivi de ces évolutions.

4.3.3 La manipulation en ligne

Le 20 mars 2018, nous avons publié un avis sur la manipulation en ligne et la protection des données. Compte tenu des *fausses informations* et de la manipulation en ligne, deux sujets qui préoccupaient de plus en plus l'opinion publique dans les mois qui précédèrent l'application du RGPD, nous avons affirmé que le problème fondamental auquel nous sommes confrontés n'est pas les *fausses nouvelles* en soi, mais l'utilisation abusive, à grande échelle, des données à caractère personnel et du droit à la liberté d'expression.

Cette utilisation abusive est une constante à tous les niveaux de l'écosystème numérique. Au cours des deux dernières décennies, cet écosystème a évolué pour devenir une structure extrêmement complexe, contrôlée par un nombre restreint d'entreprises technologiques très puissantes et faisant preuve d'un manque de responsabilisation. Cette structure repose sur un cycle constant de suivi, de profilage et de ciblage des individus, les données collectées permettant de déterminer les informations qui doivent être présentées en ligne aux différents individus.

Les publicités ciblées illustrent le mode de fonctionnement de ce système. Cependant, il est devenu évident en 2018 que cet écosystème était utilisé non seulement à des fins commerciales, mais aussi à des fins politiques, dans le but de perturber le processus démocratique et de fragiliser la cohésion sociale.

Une technique algorithmique opaque est utilisée pour décider du contenu que nous voyons en ligne. Ce processus privilégie les contenus qui suscitent l'indignation, étant donné qu'ils accroissent les *réactions* et, par conséquent, génèrent des revenus pour l'entreprise technologique concernée. Il comporte des risques évidents pour la protection des valeurs fondamentales et la démocratie.

Dans notre avis, nous avons souligné la nécessité de renforcer la coopération entre régulateurs afin que les acteurs commerciaux et politiques soient responsables de la manière dont ils traitent les données à caractère personnel. Il convient de renforcer la coopération entre les APD elles-mêmes, mais également d'accroître la coopération au-delà des frontières disciplinaires, en définissant les rôles des autorités de la concurrence, des autorités de réglementation des services audiovisuels et des autorités de contrôle électoral.

Craignant que les campagnes politiques tirent parti des espaces numériques centralisés et des données largement accessibles pour contourner la loi, nous nous sommes intéressés de près à un cas très concret : l'élection du Parlement européen, qui a eu lieu en mai 2019.

En février 2019, nous avons organisé un atelier sur la manière de démasquer et de combattre la manipulation en ligne, pas uniquement dans le cadre de l'élection du Parlement européen, mais aussi des différentes élections nationales prévues en 2019. Cet atelier avait pour objectif de faciliter

les échanges entre les APD, les autorités de contrôle électoral, les autorités de réglementation des services audiovisuels, les médias et les plates-formes en ligne et de coordonner la lutte contre la manipulation en ligne dans le cadre des élections. Les participants ont été sensibilisés à la manière dont les fausses informations sont générées et diffusées et différentes sessions ont été consacrées aux défis auxquels la démocratie doit faire face, aux vulnérabilités numériques et à la manière dont les autorités de réglementation dans différents secteurs peuvent collaborer pour combattre la manipulation en ligne et préserver l'intégrité de la démocratie.

Le 13 mars 2019, le comité européen de la protection des données a adopté une déclaration sur l'utilisation des données à caractère personnel lors des campagnes politiques, à laquelle le CEPD a activement contribué. Par ailleurs, dans le cadre de notre fonction de surveillance, nous avons déployé des efforts considérables pour contrôler l'utilisation au sein des institutions de l'Union des données à caractère personnel tout au long de la campagne électorale, en prenant des mesures le cas échéant (voir section 4.3.1).

Nous cherchons à faire en sorte que la coopération avec l'ensemble des parties concernées se poursuive, dans le cadre du centre d'échange d'informations numérique (voir section 4.2.1) et d'autres forums, afin de protéger la démocratie et la cohésion sociale à travers le monde.

5. FORGER DES PARTENARIATS À GRANDE ÉCHELLE

Les législations relatives à la protection des données sont établies au niveau national ou régional. Cependant, les données à caractère personnel circulent au-delà des frontières. Il est, par conséquent, essentiel de forger des partenariats à grande échelle pour garantir la protection efficace des droits individuels au sein de l'UE et ailleurs dans le monde.

La question de savoir comment les acteurs de la protection des données peuvent mieux s'investir pour parvenir à une plus grande convergence à l'échelle mondiale dans notre approche en matière de protection des données est depuis longtemps un sujet de discussion. En 2015, le CEPD a décidé qu'il était temps de joindre les actes à la parole. Nous voulions définir une norme numérique mondiale pour le respect de la vie privée et la protection des données, une norme axée sur les individus, leurs droits et leurs libertés ainsi que sur leur identité personnelle et leur sécurité. L'Europe doit être au premier plan de ces efforts, montrant l'exemple en tant que figure phare du respect des droits fondamentaux.

Notre stratégie 2015-2019 a établi trois points d'action contribuant à la réalisation de cet objectif. Elle prévoit, notamment, de développer une dimension éthique de la protection des données, de veiller à ce que les principes de la protection des données soient intégrés dans tous les accords internationaux négociés par l'UE et d'améliorer la coopération avec les alliés de l'UE afin de parler d'une seule voix sur la scène internationale.

Le respect du principe de responsabilisation dans le traitement des données à caractère personnel est un enjeu mondial, mais étant donné le nombre croissant de pays qui adoptent des législations en matière de protection des données, bon nombre d'entre eux s'inspirant du règlement général sur la protection des données (RGPD) de l'UE, il y a tout lieu de croire que nos efforts vont dans la bonne direction.

5.1 Développer une dimension éthique de la protection des données

Ces dernières années, les réseaux sociaux sont devenus un outil puissant de manipulation politique et commerciale (voir section 4.3.3). Les assistants virtuels et les systèmes de gestion automatisés ont commencé à remplacer les interactions humaines, les activités de surveillance publique se sont intensifiées, à l'instar des investissements des secteurs public et privé dans le développement des technologies de guerre numérique, et l'incidence des technologies gourmandes en données sur notre écosystème naturel est également devenue une source d'inquiétude.

La révolution numérique modifie les cadres traditionnels utilisés pour garantir le respect de nos droits à la protection des données et à la vie privée. Il est absolument indispensable de s'interroger sur la manière dont nous utilisons les nouvelles technologies, d'évaluer leur incidence sur nos droits et nos valeurs et de définir la façon de traiter cette question.

Nous pourrions, par exemple, encourager un débat continu sur ce qui est éthique dans l'univers numérique. Le CEPD a déployé des efforts importants à cette fin au cours de son mandat. Nous voulions lancer un débat à l'échelle mondiale sur la manière de garantir la protection des droits humains et des valeurs fondamentales à l'ère numérique.

5.1.1 L'initiative en matière d'éthique

En 2015, le CEPD a lancé l'initiative en matière d'éthique. Ce programme quinquennal couvrant la totalité du mandat du CEPD avait pour but d'aller au-delà des préoccupations traditionnelles en matière de protection des données tout en étudiant les conséquences des technologies numériques existantes et émergentes sur les individus et la société dans son ensemble.

Notre objectif était de promouvoir la conscience et la compréhension des risques auxquels nous sommes actuellement confrontés en tant que population. Nous voulions évaluer les liens existant entre la protection des données et de la vie privée et la préservation de la dignité humaine dans le monde numérisé, mais aussi étudier la signification et l'importance de ces liens, en tenant compte des avancées technologiques, telles que les pratiques répandues de suivi et profilage, l'internet des objets, les données massives, l'intelligence artificielle (IA), les systèmes autonomes, la robotique et la biométrie.

L'éthique consiste à distinguer le bien du mal, à la fois en théorie et en pratique, dans des circonstances particulières. Bien qu'elle ne se substitue pas à la loi, l'éthique éclaire la conception, l'interprétation et la révision des législations. Elle peut également servir de guide aux personnes et aux organisations qui doivent déterminer ce qu'il convient de faire dans un domaine où le droit est muet ou imprécis. Tout au long de l'initiative en matière d'éthique, nous avons cherché à dépasser le cercle immédiat des fonctionnaires, juristes et spécialistes informatiques de l'UE et à créer un dialogue au niveau mondial sur le sujet.

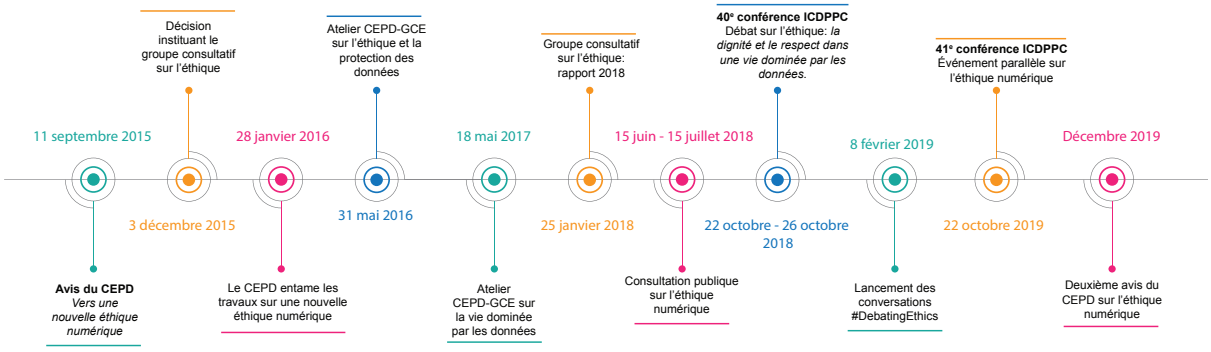
5.1.2 Le groupe consultatif sur l'éthique

En septembre 2015, nous avons lancé l'initiative en matière d'éthique avec la publication d'un avis intitulé *Vers une nouvelle éthique numérique : données, dignité et technologie*. Dans cet avis, nous avons recensé les tendances technologiques qui soulèvent de nouvelles questions éthiques et nous avons exhorté l'UE ainsi que d'autres organisations internationales à promouvoir une approche éthique en matière d'élaboration et d'utilisation des nouvelles technologies. Dans ces avis, nous avons également fait part de notre intention de créer un groupe consultatif indépendant sur l'éthique (GCE).

En janvier 2016, nous avons dévoilé la composition du GCE lors de la conférence annuelle « *Computers, privacy and data protection* » - (CPDP). Composé de six experts issus de différentes disciplines, le GCE avait pour mission d'étudier les relations entre les droits humains, la technologie et les marchés et de recenser les menaces qui pèsent sur les droits à la protection des données et de la vie privée à l'ère numérique.

Pendant deux ans, le groupe s'est penché sur l'éthique numérique selon des points de vue académiques et professionnels différents. Ces discussions avaient pour objectif de contribuer au débat plus large sur l'environnement numérique et ses implications éthiques. Au cours de cette période, le secrétariat du GCE, assuré par le CEPD, a organisé deux ateliers sur l'éthique numérique. Le premier, tenu en juillet 2016, s'est intéressé à la relation entre l'éthique et la protection des données, tandis que le second, organisé en juillet 2017, a couvert le sujet plus vaste de la vie dominée par les données.

Initiative en matière d'éthique du CEPD:
Trois ans de préparation



Le GCE a mis fin à ses travaux en janvier 2018, avec la présentation de son rapport final lors de la conférence CPDP 2018. Ce rapport n'avait pas pour but de fournir des réponses définitives ni de définir de nouvelles normes, mais bien de promouvoir une réflexion volontariste sur différents enjeux. Il a mis l'accent sur les conséquences de la révolution numérique et sur l'incidence que ces conséquences ont sur les valeurs auxquelles nous sommes attachés, en tant que citoyens et en tant que société.

Le GCE a répertorié les principaux changements socioculturels introduits par les récents progrès technologiques et a déconseillé d'adopter une approche instrumentale en matière d'éthique incluant des listes de contrôle éthiques, arguant du fait qu'une telle approche limiterait la réflexion éthique. Il a attiré l'attention sur les risques que les nouvelles technologies numériques font peser sur l'autonomie des individus et leur autodétermination et il a soutenu que le respect de l'humanité et de la dignité individuelles ne saurait être préservé lorsque les individus sont considérés comme des agrégats temporaires de données, traités à l'échelle industrielle à l'aide d'un système de profilage algorithmique pour accroître toute possibilité d'interaction avec ces individus.

@EU_EDPS

.@Buttarelli_G keynote speech at #EDPS #DataDrivenLife workshop. #DigitalEthics is essential & one of #EDPS priorities for this mandate

5.1.3 Débattre des aspects éthiques

Une fois les travaux du GCE terminés, nous nous sommes employés à encourager le débat sur l'éthique numérique à travers le monde. Sur la base des résultats du rapport du GCE, le 15 juin 2018, nous avons lancé une consultation publique mondiale sur l'éthique numérique, ouvrant le débat aux contributions de citoyens et d'organisations représentant tous les pans de la société.

Dans le cadre de cette consultation, nous avons reçu 76 réponses de sources très variées provenant du monde entier, notamment de centres de santé, de jardins d'enfants, d'universités, de pouvoirs publics, d'ONG, de bureaux d'avocats et de développeurs de logiciels. Il est ressorti des résultats de la consultation que, en matière de protection des données, une nette majorité des personnes interrogées avait adopté une approche fondée sur l'éthique afin de renforcer le respect de la législation et d'anticiper les nouveaux enjeux.

La 40e Conférence internationale des commissaires à la protection des données et à la vie privée (voir section 5.2.1) a marqué un tournant dans le débat sur l'éthique numérique. La session publique de la conférence, organisée en octobre 2018 par le CEPD, a porté sur le thème «*Débattre des aspects éthiques : la dignité et le respect dans une vie dominée par les données*». Notre objectif était de tirer parti des travaux réalisés grâce à l'initiative en matière d'éthique du CEPD pour susciter une réaction mondiale face aux enjeux de l'ère numérique.

Parmi les orateurs figuraient des militants, des universitaires, des représentants du secteur privé, des présidents de tribunaux, des autorités chargées de la protection des données (APD) et de nombreux autres intervenants venus des quatre coins du monde. En outre, les participants à la conférence étaient issus d'horizons très divers. Des débats passionnants ont eu lieu sur les défis que pose la préservation de la dignité et du respect des êtres humains dans nos sociétés actuelles dominées par les données, ainsi que sur la manière de relever ces défis. Notre rapport détaillé sur la conférence résume les principaux messages de chaque orateur et de chaque session.

Les défis posés par la révolution numérique demandent une réponse à l'échelle planétaire. La conférence a suscité, de bout en bout, un débat intense, global et pluridisciplinaire pouvant servir de source d'inspiration pour surmonter ces défis. Les efforts de communication déployés tout au long de la conférence nous ont permis de mobiliser un large éventail d'interlocuteurs, pas uniquement au sein de la communauté de la protection des données en Europe, mais aussi dans un grand nombre de disciplines à travers le monde, et d'avancer à grands pas vers la réalisation d'un objectif commun, à savoir

l'élaboration d'une approche éthique en matière de protection des données.

@EU_EDPS

.@Buttarelli_G #GDPR represents an important inspiration worldwide. However, laws are not enough. "Debating #Digital #Ethics" Intl Conference aims at facilitating discussion on how technology is affecting us as individuals and our societies @icdppc2018

5.1.4 Au-delà de la Conférence internationale

Il était important de tirer parti des progrès accomplis lors de la conférence et de continuer d'alimenter le débat sur l'éthique numérique. Sur la base des questions soulevées au cours de la conférence, nous avons répertorié plusieurs sujets de préoccupation sur lesquels nous avons centré une série de webinaires publics, que nous avons appelés les «conversations #DebatingEthics».

Ces *conversations* nous ont permis d'approfondir chacun des sujets sélectionnés, avec l'assistance d'experts invités. Elles étaient articulées autour de thèmes tels que la surveillance sur le lieu de travail et l'incidence des technologies numériques sur l'environnement. Toutes les conversations sont disponibles sous forme de podcasts sur le site web du CEPD.

Une fois les conversations #DebatingEthics terminées, nous avons publié fin 2019 un deuxième avis sur l'éthique numérique, dans lequel nous mettons en évidence les principales préoccupations relevées dans le cadre de l'initiative en matière d'éthique et la manière de procéder.

La Conférence internationale reste un forum de discussion important pour faire progresser le débat. La création du groupe de travail de l'ICDPPC sur l'intelligence artificielle (IA), l'éthique et la protection des données en 2018 (voir sections 4.1.2 et 5.2.4) assure le maintien des débats sur l'éthique numérique à l'ordre du jour de la communauté internationale.

Nous avons également organisé un événement en marge de l'édition 2019 de la conférence, qui a eu lieu à Tirana, en Albanie. Cet événement avait pour thèmes centraux l'incidence de facteurs tels que le réchauffement climatique et le déplacement massif de populations qu'il provoque, la tendance en faveur de l'utilisation de la technologie biométrique et de surveillance dans la gestion des frontières ainsi que notre capacité à faire respecter le droit à la vie privée, mais aussi la dignité humaine et d'autres droits et valeurs fondamentaux.

L'initiative du CEPD en matière d'éthique a obligé la communauté de la protection des données à ouvrir les yeux. Nous sommes parvenus à lancer le débat très attendu sur les valeurs et les droits dans le monde numérique qui, nous l'espérons, garantira une innovation responsable et des technologies apportant de réels bienfaits à la société.

5.2 Intégrer la protection des données dans les politiques internationales

Ces cinq dernières années, la protection des données a réellement commencé à s'imposer comme une partie intégrante des politiques publiques. À l'ère numérique, tout et tout le monde est connecté et cette connexion est rendue possible par les données. Alors que la protection des données était autrefois considérée comme une question politique distincte, il s'agit désormais d'une préoccupation politique majeure. Les discussions sur la politique commerciale de l'UE illustrent bien ce phénomène, ainsi que Giovanni Buttarelli l'a expliqué dans une publication de fin 2017.

Nous nous efforçons, depuis le début du mandat actuel, de conseiller clairement le législateur européen quant à la manière d'appliquer de manière cohérente et conséquente les principes de la protection des données de l'UE dans le cadre de la négociation d'accords internationaux comportant des flux transfrontaliers de données. Par ailleurs, nous avons suivi de près la mise en œuvre des accords internationaux existants, tout en renforçant notre coopération avec les partenaires internationaux en vue de

mieux coordonner l'approche internationale en matière de protection des données et de respect de la vie privée.

@EU_EDPS

> #Dataprotection **should not be subject to** #trade **negotiations. Read about the relationship between trade &** #data **in the latest blogpost by** @Buttarelli_G**: 'Less is sometimes more'** http://europa.eu/!YW39rf

5.2.1 La Conférence internationale 2018 des commissaires à la protection des données et à la vie privée

La Conférence internationale annuelle des commissaires à la protection des données et à la vie privée (ICDPPC) se réunit chaque année afin d'assurer, au niveau mondial, la direction des initiatives en faveur de la protection des données et de la vie privée, en mettant en relation les autorités chargées de la protection des données et de la vie privée du monde entier. Le CEPD participe activement à cette conférence depuis longtemps. En octobre 2018, nous avons eu le privilège d'organiser la Conférence internationale à Bruxelles, en partenariat avec la commission bulgare de protection des données à caractère personnel.

La conférence a débuté par une session fermée de deux jours, à laquelle seuls les membres accrédités ont participé. Des délégués venus des quatre coins du monde ont ensuite pris part à la session publique de la conférence. Parmi les participants figuraient des représentants de différents gouvernements, de la société civile, d'autorités de réglementation, de l'industrie, du monde universitaire, des médias et d'APD. Quarante événements portant sur des questions liées à la vie privée ont également eu lieu en marge de la conférence tandis que des événements supplémentaires ont été organisés à Sofia, en Bulgarie, par le coorganisateur de la conférence.

La conférence en session fermée – Éthique et intelligence artificielle

Il incombe au comité exécutif de l'ICDPPC d'établir l'ordre du jour de la conférence en session fermée. Cependant, en 2018, le thème central de la conférence en session fermée était, pour la première fois, directement lié au thème de la session publique.

En 2018, un nombre record de délégués a pris part à la conférence en session fermée, soit un total de 206 participants issus de 76 pays. Le sujet du débat était « L'éthique et l'intelligence artificielle ».

À l'heure actuelle, peu d'autorités supervisent l'incidence des nouvelles technologies sur les droits fondamentaux aussi étroitement et aussi intensivement que les autorités chargées de la protection des données et de la vie privée. En 2018, la conférence a donc été consacrée à la poursuite de la discussion sur l'IA entamée deux années plus tôt, à Marrakech (voir section 4.1.2).

En plus d'élaborer une déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle (voir section 4.1.2), les participants à la conférence en session fermée ont adopté trois résolutions sur les plates-formes d'apprentissage en ligne, sur l'enquête de la conférence sur la collaboration entre les autorités chargées de la protection des données et les autorités de protection des consommateurs pour une meilleure protection des citoyens et des consommateurs dans l'économie numérique ainsi qu'une résolution concernant une feuille de route sur l'avenir de la Conférence internationale.

Nous espérons que les décisions prises au cours de la conférence en session fermée l'aideront à se développer de façon à renforcer la coopération au niveau mondial, à la fois à l'intérieur et à l'extérieur de la communauté de la protection des données.

La session publique – Débattre des aspects éthiques

Le choix du thème de la session publique étant laissé à la discrétion des organisateurs, nous avons choisi le thème suivant : « Débattre des aspects éthiques : la dignité et le respect dans une vie dominée par les données ». Nous souhaitions susciter un débat inclusif, pluridisciplinaire et interactif sur la révolution numérique et son incidence sur les citoyens et la société (voir section 5.1.3).

La session publique a réuni des délégués de diverses origines et nationalités. Parmi les participants figuraient des représentants des secteurs public et privé, du monde universitaire, de la société civile et des médias ainsi que des invités, des membres et des observateurs de l'ICDPPC. Les débats ont porté sur les notions du bien et du mal à travers le monde et dans différentes disciplines ainsi que sur la manière dont ces notions sous-tendent les législations, les technologies et les comportements humains.

L'exclusivité du thème, du programme et du format de la conférence ainsi que la palette d'excellents orateurs ont attiré les foules, y compris un nombre record de délégués d'ONG. Au total, 85 pays étaient représentés, donnant ainsi tout son sens à cette conférence internationale.

La couverture médiatique de la conférence a été, elle aussi, internationale. Quatre-vingt-un organes d'information de 23 pays différents, notamment des radiodiffuseurs, des agences de presse et des quotidiens de premier plan ont couvert la conférence.

Un rapport détaillé sur la conférence est disponible sur le site web du CEPD.

@EU_EDPS

#EDPS @Buttarelli_G opens the 2018 Olympic Games on #Privacy - "Choose humanity: putting the dignity back into digital". The 40th International Conference will explore the human dimension of new technologies. #DebatingEthics @icdppc2018

Événements parallèles

Généralement, des événements parallèles ont lieu en marge de la Conférence internationale,

et la conférence de 2018 n'a pas fait exception à la règle. Les événements ont mis l'accent non seulement sur l'éthique numérique, le thème de la conférence, mais aussi sur un vaste éventail d'autres sujets liés à la protection des données. Avec plus de 40 événements parallèles, il y en avait pour tous les goûts.

Organisés par différents groupes et organisations des quatre coins du monde, les événements parallèles qui ont eu lieu durant la semaine de la Conférence internationale ont offert une occasion unique aux participants d'interagir avec des collègues issus de disciplines et de régions différentes et de s'inspirer de leur expérience dans toute une série de domaines liés à la protection des données. Les événements parallèles ont été organisés par huit APD issues de différents pays, 18 ONG et organisations internationales, six groupes de réflexion et de recherche et huit entreprises privées et bureaux d'avocats. Plus de 160 orateurs ont pris la parole.

@EU_EDPS

More than 200 delegates from #DPAs represented at 40th International Conference of #DataProtection & #Privacy Commissioners in Brussels. Warm thank you to more than 1400 delegates, speakers, participants for fruitful discussions & inspiring atmosphere! #DebatingEthics #icdppc2018

5.2.2 Protection des données et commerce

Au début de 2018, la Commission européenne a présenté les résultats des travaux réalisés par son équipe de projet concernant un chapitre distinct sur les flux transfrontaliers de données et la protection des données à caractère personnel, qui figurera dans les futurs accords sur le commerce et les investissements. L'équipe de projet a proposé que le chapitre soit constitué de deux articles, qui couvriront les flux transfrontaliers de données et la protection des données à caractère personnel.

La protection des données à caractère personnel et le respect de la vie privée sont des droits fondamentaux; ils sont, par conséquent, non négociables. Cela signifie que, idéalement, ils ne devraient pas être inclus dans les accords internationaux sur le commerce ou les investissements. Néanmoins, le CEPD salue l'approche proposée, qui établit un équilibre entre la nécessité d'éliminer les obstacles aux flux internationaux de données d'une part, et la nécessité de préserver les droits fondamentaux de l'UE, y compris le droit à la protection des données, d'autre part. Nous nous sommes également félicités du fait que la Commission confirme que les décisions relatives à l'adéquation du niveau de protection des données (voir section 5.2.3) doivent constituer l'instrument juridique privilégié dans le cadre de transferts internationaux de données, dans le cadre de négociations distinctes relatives à la protection des données. Cela signifie qu'il convient d'envisager l'ajout de dispositions horizontales dans les accords sur le commerce ou les investissements uniquement lorsque l'objectif d'adéquation ne peut pas être réellement atteint.

Cette nouvelle approche a été appliquée pour la première fois dans le cadre des négociations sur l'accord de partenariat économique entre l'UE et le Japon, qui est entré en vigueur le 1er février 2019. Parallèlement à ces discussions, la Commission a adopté une décision d'adéquation concernant le Japon (voir section 5.2.3). Le CEPD a activement participé aux discussions du comité européen de la protection des données sur la proposition de décision afin que cette nouvelle approche en matière de protection des données et d'accords commerciaux soit couronnée de succès.

5.2.3 Évaluation des décisions d'adéquation

La Commission européenne peut décider si un pays tiers offre un niveau de protection des données essentiellement équivalent à celui de l'UE, permettant ainsi aux données à caractère personnel de circuler librement entre l'UE et le pays tiers en question. Ces décisions sont appelées «décisions d'adéquation».

Cependant, conformément au RGPD et à la directive en matière de protection des données pour les secteurs de la police et de la justice, la Commission doit, avant d'adopter une décision

d'adéquation, solliciter l'avis du comité européen de la protection des données, dont le CEPD fait partie, en ce qui concerne sa proposition.

Au cours des cinq dernières années, nous avons fourni des conseils à la Commission dans deux affaires portant sur des décisions d'adéquation (Japon et États-Unis).

La décision d'adéquation UE-Japon

En septembre 2018, la Commission européenne a publié un projet de décision d'adéquation portant sur le transfert de données à caractère personnel depuis l'UE vers le Japon. Utilisant comme point de repère son document d'orientation actualisé sur les décisions d'adéquation, le comité européen de la protection des données a adopté le 5 décembre 2018 un avis concernant le projet de décision d'exécution de la Commission européenne.

En ce qui concerne la première décision d'adéquation depuis l'entrée en vigueur du RGPD, il était essentiel de veiller à ce que l'accord entre l'UE et le Japon établisse des normes aussi rigoureuses que possible. Le comité européen de la protection des données voulait s'assurer de donner le ton des futurs accords d'adéquation et de l'examen à venir des décisions d'adéquation déjà en vigueur. Bien que le comité européen de la protection des données ait salué les efforts déployés par la Commission européenne et la commission japonaise de protection des données à caractère personnel (PPC) pour harmoniser leurs cadres juridiques respectifs, il a également souligné un certain nombre de préoccupations, notamment la question de savoir si la protection des données à caractère personnel transférées depuis l'UE vers le Japon pouvait être garantie tout au long de leur cycle de vie. Le 4 septembre 2018, le CEPD a, par ailleurs, formulé des observations préliminaires informelles sur la proposition de décision d'adéquation.

En tant que membre du comité européen de la protection des données, le CEPD a activement contribué aux discussions sur l'avis du Comité, en attirant particulièrement l'attention sur le rôle du Comité ainsi que sur la responsabilisation de la Commission dans la négociation des accords d'adéquation. Le CEPD était particulièrement conscient de l'importance des négociations en cours pour l'accord de partenariat économique entre l'UE et le Japon, qui avaient lieu en parallèle, et de la nécessité de veiller à ce que la nouvelle approche européenne en matière de protection des données dans les accords commerciaux, approuvée par la Commission, puisse être bien appliquée dans la pratique (voir section 5.2.2).

La Commission a modifié la proposition de décision après que le comité européen de la protection des données a publié son avis et, le 23 janvier 2019, elle a adopté la décision d'adéquation UE-Japon.

@EU_EDPS

Glad #EDPS has strongly contributed to a balanced @EU_EDPB opinion of paramount importance on the first #GDPR adequacy finding: Not a red light, but improvements are recommended to achieve a robust #EU & #Japan #dataprotection deal

La « sphère de sécurité » est déclarée invalide

Le 24 mars 2015, la Cour de justice de l'Union européenne (CJUE) a invité le CEPD à intervenir dans l'affaire C-362/14 Schrems contre Data Protection Commissioner, en sa qualité de conseiller des institutions de l'UE en matière de protection des données.

L'affaire avait pour objet la décision concernant la « sphère de sécurité », négociée avec le gouvernement des États-Unis et adoptée par la Commission plus de 15 ans auparavant pour veiller à ce que les données à caractère personnel transférées depuis l'UE vers les États-Unis bénéficient aux États-Unis du même niveau de protection que celui dont elles auraient bénéficié dans l'UE. S'il ne s'agissait pas de la seule façon de transférer des données entre les deux pays, le cadre de la « sphère de sécurité » était largement utilisé, en particulier par de nombreuses grandes entreprises technologiques américaines.

L'affaire avait pour origine une plainte concernant des transferts de données effectués par Facebook

Ireland Ltd. Le plaignant, un étudiant autrichien, Maximilian Schrems, soutenait que les données à caractère personnel transférées aux États-Unis dans le cadre de la « sphère de sécurité » n'étaient pas suffisamment protégées. Pour étayer sa thèse, il s'est appuyé sur des révélations concernant la surveillance de masse exercée par les États-Unis. Le commissaire à la protection des données irlandais considérant qu'il n'était pas en mesure de procéder à une enquête sur les faits dénoncés, Schrems a introduit un recours devant la Haute Cour de justice d'Irlande, qui a adressé une demande de décision préjudicielle à la CJUE.

Dans les observations soumises à la CJUE par le CEDP, nous avons formulé les observations suivantes :

- la « sphère de sécurité » soulevait des doutes depuis longtemps ; le groupe de travail « article 29 » (GT29) avait précédemment formulé un certain nombre de critiques, qui n'ont jamais été prises en considération ;
- il est possible que la portée et l'envergure de la surveillance aient été si considérables que la «sphère de sécurité» ne soit pas parvenue à respecter l'essence du droit fondamental à la vie privée et à la protection des données consacré par la charte des droits fondamentaux de l'Union européenne ;
- les autorités indépendantes compétentes en matière de protection des données peuvent déterminer les mesures qui s'imposent pour assurer un équilibre entre le respect de la vie privée et la protection des données à caractère personnel et, dans le cas présent, toute perturbation du marché intérieur.

Nous sommes parvenus à la conclusion que la négociation d'un accord international assurant une protection adéquate contre une surveillance arbitraire constituerait une solution efficace. Nous avons précisé que des obligations concernant les droits en matière de surveillance, de transparence, de recours et de protection des données devraient figurer dans cet accord.

Le 6 octobre 2015, la CJUE a déclaré nulle la décision relative à la « sphère de sécurité ». La Cour a précisé que, lorsqu'elle négocie une décision d'adéquation relative au transfert de données entre l'UE et un pays tiers, la Commission européenne doit évaluer tant le contenu des règles de protection des données du pays en question que les mesures visant à assurer le respect de ces règles. Il convient de procéder périodiquement à cette évaluation pour s'assurer que la situation n'a pas changé.

La Cour a également jugé que les APD nationales doivent être habilitées à examiner et à contester la validité des décisions d'adéquation de la Commission pour le compte de toute personne exprimant des préoccupations.

@EU_EDPS

Careful attention should be given to modalities #international transfers of personal #data in line with #CJEU ruling in @maxschrems #EUdataP

Une approche coordonnée à l'égard du bouclier de protection des données UE-États-Unis

Au début de 2016, la Commission européenne est parvenue à un accord politique avec les États-Unis au sujet d'un nouveau cadre régissant les transferts de données à caractère personnel. Conformément à la procédure établie, la Commission a soumis l'accord, connu sous le nom de « bouclier de protection des données UE-États-Unis », à la consultation du CEPD et du groupe de travail « article 29 ».

Au terme de sa réunion plénière des 2 et 3 février 2016, le GT29 a publié une déclaration commune sur la proposition. Peu de temps après, il a publié un avis (13 avril 2016). Bien que le groupe se soit félicité d'un certain nombre d'améliorations significatives, par rapport à la décision relative à la « sphère de sécurité », il a également fait part de sérieuses réserves quant à la proposition d'accord, soulignant que des principes importants de la protection des données prévus par la législation de l'UE étaient absents de la proposition.

Le CEPD a publié son propre avis le 30 mai 2016, en se fondant sur les recommandations contenues dans l'avis du GT29 et en donnant plus de poids à bon nombre d'entre elles. Bien que nous ayons salué les efforts consentis pour remplacer

adéquatement la « sphère de sécurité », nous sommes parvenus à la conclusion que les améliorations proposées dans le nouveau cadre étaient insuffisantes. Nous avons recommandé, en particulier, de renforcer les principes clés du nouveau système d'autocertification, notamment les dispositions relatives à la conservation des données, à la limitation de la finalité et aux droits des individus, et nous avons plaidé en faveur de la mise en œuvre de règles strictes quant à l'accès des autorités publiques américaines aux données à caractère personnel.

Le bouclier de protection des données UE-États-Unis est entré en vigueur le 1er août 2016 ; depuis lors, un examen conjoint, organisé par le GT29 et ensuite par le comité européen de la protection des données, est réalisé chaque année. Cet examen a pour objectif de veiller à ce que le bouclier de protection soit mis en œuvre de manière à assurer un niveau adéquat de protection des données à caractère personnel, conformément aux règles de l'UE. Le CEPD a, jusqu'à présent, pris part à tous les exercices d'évaluation.

Le 28 novembre 2017, le GT29 a publié son rapport sur le premier examen conjoint annuel du bouclier de protection des données UE-États-Unis, à la suite de la publication du rapport de la Commission européenne sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis.

Ce rapport met l'accent sur les préoccupations exprimées dans les précédents avis du GT29 concernant les aspects commerciaux du bouclier de protection et l'accès des pouvoirs publics aux données de l'UE à des fins répressives et de sécurité nationale. Dans ce rapport, le GT29 recommande que la Commission européenne et les autorités américaines reprennent les discussions et appelle de ses vœux la désignation d'un médiateur, la clarification du règlement intérieur et l'attribution des postes vacants au sein du Conseil américain de surveillance de la vie privée et des libertés civiles (PCLOB) avant le 25 mai 2018. Les autres préoccupations devaient être abordées au plus tard à la date du deuxième examen conjoint. L'incapacité à répondre à ces préoccupations dans les délais impartis pourrait amener le GT29 à saisir les tribunaux nationaux afin qu'ils soumettent une question préjudicielle à la CJUE concernant la décision d'adéquation relative au bouclier de protection.

Le rapport du comité européen de la protection des données sur le deuxième examen annuel, publié le 22 janvier 2019, a reconnu les progrès accomplis dans la mise en œuvre du bouclier de protection, grâce aux efforts déployés pour adapter la procédure de certification initiale, engager d'office des actions de surveillance et de contrôle de l'application et publier un certain nombre de documents importants. La désignation d'un nouveau président et de trois nouveaux membres du PCLOB, ainsi que la désignation d'un médiateur permanent, ont également été saluées comme une évolution positive.

Cependant, des préoccupations subsistaient quant à la mise en œuvre du bouclier de protection, compte tenu notamment de l'absence d'assurances concrètes concernant la collecte arbitraire de données à caractère personnel et l'accès aux données à caractère personnel à des fins de sécurité nationale. Par ailleurs, les informations fournies à l'époque n'ont pas permis de démontrer que le médiateur disposait de pouvoirs suffisants pour agir en cas de non-respect. En outre, certains points soulevés après le premier examen conjoint étaient encore en suspens.

Le troisième examen conjoint a eu lieu les 12 et 13 septembre 2019. Un rapport sera publié en temps opportun.

5.2.4 Le PNR UE-Canada fait l'objet d'un examen attentif

Le 25 novembre 2014, le Parlement européen a demandé l'avis de la CJUE quant à la compatibilité avec les traités de l'Union européenne de l'accord envisagé entre l'UE et le Canada relatif au transfert et au traitement des données du dossier passager (PNR). Le Parlement européen souhaitait également savoir si la base juridique proposée pour l'accord envisagé était appropriée. La Commission européenne a négocié ce projet d'accord en remplacement de l'accord précédent, qui est arrivé à expiration en 2009.

En 2013, le CEPD a publié un avis sur le projet d'accord et, en avril 2016, la CJUE nous a invités à intervenir à l'audience. Dans notre plaidoirie, nous avons formulé les observations suivantes :

- l'accord envisagé servirait de référence pour des accords bilatéraux semblables conclus avec des pays tiers au nom de la sécurité publique et pour faciliter les transferts de données à caractère personnel ;
- les garanties visées à l'article 8 de la charte des droits fondamentaux de l'UE doivent être respectées, y compris lorsque des règles relatives aux transferts de données sont définies dans un accord international ;
- le contrôle judiciaire des législations de l'UE relatives au PNR doit être strict, le traitement des données PNR étant systématique et intrusif et susceptible de permettre aux autorités d'engager des actions de *police prédictive*.

Nous avons conclu que l'accord envisagé ne garantissait pas le niveau de protection requis au titre de l'article 8 de la Charte.

Dans son avis publié le 26 juillet 2017, la Cour a conclu que l'accord entre l'UE et le Canada sur les données PNR était incompatible avec les articles 7, 8, 21 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, en tant qu'il n'exclut pas le transfert des données sensibles depuis l'Union vers le Canada ni l'utilisation et la conservation de ces données. Il aurait dû être fondé conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), de la Charte. Par ailleurs, plusieurs autres aspects auraient dû être modifiés pour garantir sa compatibilité avec la Charte.

Les types de données PNR pouvant être transférés, notamment, auraient dû mieux répondre aux exigences de clarté. La Cour a relevé que les passagers devraient avoir le droit de se voir informer du traitement de leurs données PNR durant ou après leur séjour au Canada et elle a mis en lumière la nécessité de disposer d'une autorité de contrôle indépendante pour surveiller l'utilisation des données PNR au Canada.

Les conclusions auxquelles la Cour est parvenue ont constitué une étape importante pour l'UE, en établissant des normes pour tout autre accord similaire entre l'UE et des pays tiers. Le CEPD, qui suit de près l'évolution des négociations en cours entre la Commission européenne et le Canada, publiera un avis après avoir été consulté.

5.2.5 Travailler avec les organisations internationales

Les organisations internationales ne sont généralement pas soumises aux législations européennes et bénéficient de privilèges et d'immunités, qui ont une incidence sur l'applicabilité des législations nationales, y compris des règles en matière de protection des données. Cependant, ces organisations prônent avec un certain succès le développement d'une culture de protection de la vie privée et elles disposent souvent de leurs propres règles internes en matière de protection des données à caractère personnel.

Pour aider les organisations internationales à développer leurs propres cadres de protection des données et pour leur donner la possibilité de partager leurs connaissances et leurs expériences, le CEPD a lancé une série d'ateliers. Au début du mandat, nous avons donné une nouvelle impulsion à cette initiative, qui a vu le jour en 2005.

Le cinquième atelier du CEPD destiné aux organisations internationales, organisé en collaboration avec le comité international de la Croix-Rouge, a eu lieu le 5 février 2016, après une interruption de quatre ans. Depuis lors, cet atelier est organisé chaque année, en collaboration avec une organisation internationale différente (voir illustration 7).

Ces ateliers s'avèrent être un outil précieux pour les organisations internationales, qui peuvent partager leur expérience et leurs bonnes pratiques en matière de protection des données et analyser les défis communs auxquels elles sont confrontées. Ils leur permettent également d'évaluer la situation de la protection des données au sein des organisations internationales.

La taille et la pertinence de ces ateliers progressent constamment depuis 2005. Ce constat confirme la nécessité de ce genre de plate-forme et démontre, par ailleurs, que les organisations internationales perçoivent de plus en plus l'importance de mettre en place des protections solides en ce qui concerne les données à caractère personnel. Les organisations internationales font preuve d'une volonté commune d'intégrer la protection des données dans leur culture de travail et de répondre de leurs actes. Le CEPD continuera d'appuyer sans réserve ces efforts.

Protection des données au sein des organisations internationales

Le CEPD collabore avec les organisations internationales dans le cadre d'une série d'ateliers visant à sensibiliser à la protection des données et à promouvoir l'adoption de règles en matière de protection des données.

Premier atelier - Genève, 13 septembre 2005

En coopération avec: le Conseil de l'Europe et l'Organisation de coopération et de développement économiques (OCDE)
À l'ordre du jour: la protection des données à caractère personnel du personnel et d'autres personnes et le traitement des données sensibles relatives à la santé, au statut de réfugié et à des condamnations pénales.

Deuxième atelier - Munich, 29 mars 2007

En coopération avec: l'Office européen des brevets
À l'ordre du jour: le rôle du délégué à la protection des données, comment mettre en place un régime de protection des données et la coopération avec les organisations et les pays qui n'appliquent pas les mêmes normes en matière de protection des données.

Troisième atelier - Florence, 27-28 mai 2010

En coopération avec: l'Institut universitaire européen
À l'ordre du jour: la gouvernance de la protection des données dans les organisations internationales, la conformité dans la pratique, les défis technologiques et les mesures de sûreté connexes dans les organisations internationales et l'utilisation de la biométrie aux frontières et pour la sécurité intérieure.

Quatrième atelier - Bruxelles, 8-9 novembre 2012

En coopération avec: l'Organisation mondiale des douanes (OMD)
À l'ordre du jour: le paquet de réformes de l'UE sur la protection des données, les initiatives du Conseil de l'Europe et de l'OCDE sur la protection des données, la conformité et les transferts de données à des tiers, le traitement des données concernant le personnel, les procédures de notification des violations de la sécurité et l'informatique en nuage.

Cinquième atelier - Genève, 5 février 2016

En coopération avec: le Comité international de la Croix-Rouge (CICR)
À l'ordre du jour: l'état d'avancement de la protection des données dans les organisations internationales, les développements récents en matière de protection des données et de la vie privée, et l'impact de ces développements sur les organisations internationales.

Sixième atelier - Genève, 11-12 mai 2017

En coopération avec: l'Organisation internationale pour les migrations (OIM)
À l'ordre du jour: les développements récents en matière de protection des données et de la vie privée dans les organisations internationales, l'informatique en nuage, le traitement des données relatives à la santé, le rôle du délégué à la protection des données et l'impact du règlement général sur la protection des données (RGPD) sur les transferts internationaux de données à des organisations internationales.

Septième atelier - Copenhague, 12 juillet 2018

En coopération avec: le Haut-Commissariat des Nations unies pour les réfugiés
À l'ordre du jour: les normes de protection de la vie privée et les mécanismes de contrôle pour les organisations internationales, la mise en pratique du principe de responsabilité, les transferts internationaux et les motifs légaux pour autoriser le traitement de données à caractère personnel dans le cadre des travaux des organisations internationales.

Huitième atelier - Paris, 17-18 juin 2019

En coopération avec: l'Organisation de coopération et de développement économiques (OCDE)
À l'ordre du jour: les défis posés par l'utilisation des services web et des réseaux sociaux, les dispositions contractuelles avec les fournisseurs de logiciels, les transferts de données à caractère personnel à des organisations internationales et la mise au point des évaluations des risques.

Illustration 7. La protection des données dans les ateliers destinés aux organisations internationales

5.3 Parler d'une seule voix sur la scène internationale

Si elle dispose d'un ensemble unique de règles en matière de protection des données applicable à l'ensemble de ses États membres, l'Union devrait être en mesure de parler d'une seule voix sur la scène internationale. Cela ne signifie pas qu'une seule personne ou une seule organisation doit s'exprimer au nom de l'UE, mais plutôt que l'ensemble des autorités de l'Union chargées de la protection des données doit promouvoir de manière cohérente la même approche en matière de protection des données, en accordant la priorité à la protection des droits fondamentaux.

Une approche coordonnée nous permettra de mieux faire entendre notre voix; elle aidera l'UE à jouer un rôle positif et de premier plan dans l'élaboration d'une norme numérique mondiale garantissant le respect de la vie privée et la protection des données. Pour que cela devienne une réalité, il est essentiel que la coopération et la communication entre le CEPD et les autres APD de l'UE soient efficaces. Depuis le 25 mai 2018, le comité européen de la protection des données est le principal forum de coopération entre les APD. Avant cette date, c'est le GT29, le prédécesseur du Comité, qui a jeté les bases de cette coopération.

5.3.1 Travailler avec les APD

Chaque État membre de l'UE possède au moins une APD indépendante. Certains États membres en ont davantage, en fonction des exigences constitutionnelles de rigueur dans ces États. Les APD sont des autorités chargées d'assurer et de contrôler le respect des règles en matière de protection des données dans leur État membre respectif. Le rôle du CEPD correspond à celui des APD des États membres, dans la mesure où nous sommes chargés d'assurer et de contrôler le respect des règles en matière de protection des données au sein des institutions et des organes de l'UE.

Les APD de l'UE et le CEPD collaborent de plusieurs façons pour favoriser une protection plus systématique et cohérente des données à caractère personnel dans l'ensemble de l'Union européenne.

@EU_EDPS

.@Buttarelli_G: #EDPS is proud to provide a modern and highly responsive secretariat to the new Data Protection Board #EDPB #data2016

Le CEPD en tant que membre actif du groupe de travail «article 29»

Le GT29 a été institué en vertu de la directive 95/46 relative à la protection des données, qui a précédé le RGPD. Il a servi de forum de coopération privilégié aux APD de l'UE entre 1996 et le début de l'année 2018. Depuis le début de son mandat en 2015 jusqu'à la création du comité européen de la protection des données en mai 2018, le CEPD a n'a cessé de contribué activement aux activités du GT29, en coordonnant le sous-groupe sur les dispositions clés, en prenant part aux travaux des autres sous-groupes du GT29 et en déployant ses efforts là où il pouvait apporter une importante valeur ajoutée. Il a ainsi collaboré aux avis du GT29 sur «l'accord parapluie» entre l'UE et les États-Unis, le bouclier de protection des données UE-États-Unis et l'interopérabilité.

Entre 2015 et 2018, la plupart des travaux du GT29 ont porté sur la préparation du RGPD et du comité européen de la protection des données, dont le CEPD allait assurer le secrétariat. La coopération avec le GT29 était essentielle pour que l'UE soit en mesure d'appliquer le RGPD à partir du 25 mai 2018.

L'essentiel des travaux relatifs à ces préparatifs a été assuré par le sous-groupe sur les dispositions clés, coordonné par le CEPD, ainsi que par le sous-groupe sur l'avenir du respect de la vie privée, au sein duquel le CEPD a joué un rôle actif. Le CEPD, qui a assumé le rôle de co-rapporteur, a rédigé plusieurs lignes directrices du GT29, conçues pour aider les entreprises et les organisations opérant dans l'UE à mieux comprendre et mettre en œuvre les exigences du RGPD.

Il s'est également associé aux efforts entrepris par le GT29 pour fournir des éclaircissements quant à l'incidence des technologies émergentes sur la protection des données. Le GT29 s'est attaché,

en particulier, à interpréter les règles de l'UE en matière de protection des données, neutres d'un point de vue technologique, et à s'en inspirer, en abordant des sujets tels que l'anonymisation, l'informatique dans les nuages et l'internet des objets.

Le GT29 devait veiller à ce que le comité européen de la protection des données et son secrétariat soient opérationnels dès l'entrée en vigueur du RGPD. Les préparatifs pratiques se sont intensifiés en 2017, l'accent ayant été mis sur la conclusion d'un protocole d'accord entre le Comité et le CEPD. Le protocole d'accord définit les conditions de la coopération entre le Comité et le CEPD. Il jette les bases de notre coopération, en garantissant la confiance, la bonne foi et la collégialité entre les deux parties. Le CEPD a également contribué à la rédaction du règlement intérieur du Comité ainsi qu'à la définition des différentes procédures relatives au mécanisme de cohérence, qui a pour but de garantir l'application cohérente du RGPD dans l'ensemble de l'UE.

Cependant, au cours de cette période, les travaux du GT29 n'ont pas porté uniquement sur les préparatifs en vue de l'entrée en vigueur du RGPD. En septembre 2017, par exemple, un représentant du CEPD s'est rendu à Washington D.C. avec la délégation de l'UE qui a réalisé le premier examen conjoint de la mise en œuvre du bouclier de protection (voir section 5.2.3). Cette délégation était composée de représentants de la Commission européenne et de plusieurs APD européennes. Les conclusions de l'examen conjoint ont été présentées à l'occasion d'une réunion plénière du GT29 et, le 28 novembre 2017, le groupe a publié un rapport sur le bouclier de protection, dans lequel nous avons demandé que des améliorations soient apportées à la mise en œuvre de cet accord.

Le comité européen de la protection des données se met au travail

Créé par le RGPD, le comité européen de la protection des données a remplacé, le 25 mai 2018, le GT29 en tant que forum de coopération entre le CEPD et les APD des États membres de l'UE. Il a également pris en charge un grand nombre de nouvelles tâches dans le but d'assurer l'application cohérente du RGPD et de la directive relative à la protection des données par les secteurs de la police et de la justice dans l'UE. Le comité européen de la protection des données est un organe de l'UE doté de la personnalité juridique qui, dans certains cas, est habilité à adopter des décisions contraignantes. Le Comité peut également publier des orientations, des recommandations et des déclarations sur un vaste éventail de sujets.

Les autorités de contrôle des États membres de l'EEE et de l'AELE (Islande, Liechtenstein et Norvège) sont également membres du Comité en ce qui concerne les questions relatives au RGPD, mais elles n'ont ni le droit de vote ni celui d'être élues à la présidence ou à la vice-présidence.

Le CEPD est un membre du comité européen de la protection des données, dont il assure également le secrétariat. En 2017, nous avons nommé un agent de liaison chargé de coordonner l'ensemble des travaux du CEPD relatifs à la préparation du secrétariat du Comité. Nous avons notamment travaillé avec le GT29 pour créer le site web et le logo du Comité (voir section 7.1.5) et nous avons préparé le protocole d'accord entre le CEPD et le Comité. Giovanni Buttarelli, le contrôleur européen de la protection des données, et Andrea Jelinek, présidente du comité européen de la protection des données, ont signé ce protocole d'accord lors de la première réunion plénière du Comité, qui a eu lieu le 25 mai 2018.

Le CEPD étant membre du comité européen de la protection des données, nos représentants participent à la fois aux réunions plénières et aux réunions des sous-groupes et y contribuent activement. Nous avons continué de coordonner le sous-groupe d'experts sur les dispositions clés et nous coordonnons également le sous-groupe d'experts sur les utilisateurs de programmes informatiques. Notre participation active dans l'ensemble des sous-groupes nous a permis d'apporter notre contribution aux avis, aux orientations et aux autres documents du Comité qui ont été adoptés en 2018 et 2019. Parmi ceux-ci, citons notamment l'avis de 2018 sur le projet de décision d'adéquation UE-Japon concernant

les transferts internationaux de données (voir section 5.2.3) et l'avis de 2019 sur le projet d'arrangement administratif (AA) concernant les transferts de données à caractère personnel entre les autorités de l'Espace économique européen (EEE) chargées de la surveillance financière et les autorités de pays tiers chargées de la surveillance financière, auxquels nous avons contribué de manière significative.

Le nombre de réunions plénières et de réunions des sous-groupes ayant augmenté en 2019, notre charge de travail s'est également accrue. Nous nous sommes, dès lors, efforcés de concentrer nos efforts sur les dossiers dans lesquels notre contribution sera probablement la plus précieuse et concernant lesquels la nécessité de présenter et de défendre la perspective de l'UE est manifeste (voir illustration 8).

Le règlement (UE) 2018/1725 offre la possibilité à la Commission de solliciter l'avis conjoint du CEPD et du comité européen de la protection des données dans certaines circonstances. En juillet 2019, le premier avis conjoint du Comité et du CEPD concernant le traitement des données des patients et le rôle de la Commission européenne dans l'infrastructure de services numériques dans le domaine de la santé en ligne (eHDSI) a été adopté.

Cependant, les documents conjoints du Comité et du CEPD ne se limitent pas aux consultations menées au titre du règlement (UE) 2018/1725. Nous avons également transmis une réponse conjointe à la commission des libertés civiles du Parlement européen (LIBE) concernant l'incidence sur le cadre juridique européen, en matière de protection des données à caractère personnel, de la loi américaine « *US Cloud Act* ».

Supervision coordonnée

L'UE exploite plusieurs systèmes d'information à grande échelle, à l'appui de ses politiques en matière d'asile, de gestion des frontières, de coopération policière et de douanes. Grâce à ces

Illustration 8. Contributions du CEPD aux travaux du comité européen de la protection des données, de mai 2018 à septembre 2019

systèmes d'information, les autorités nationales, ainsi que certains organes de l'UE, sont en mesure d'échanger des informations sur ces domaines stratégiques.

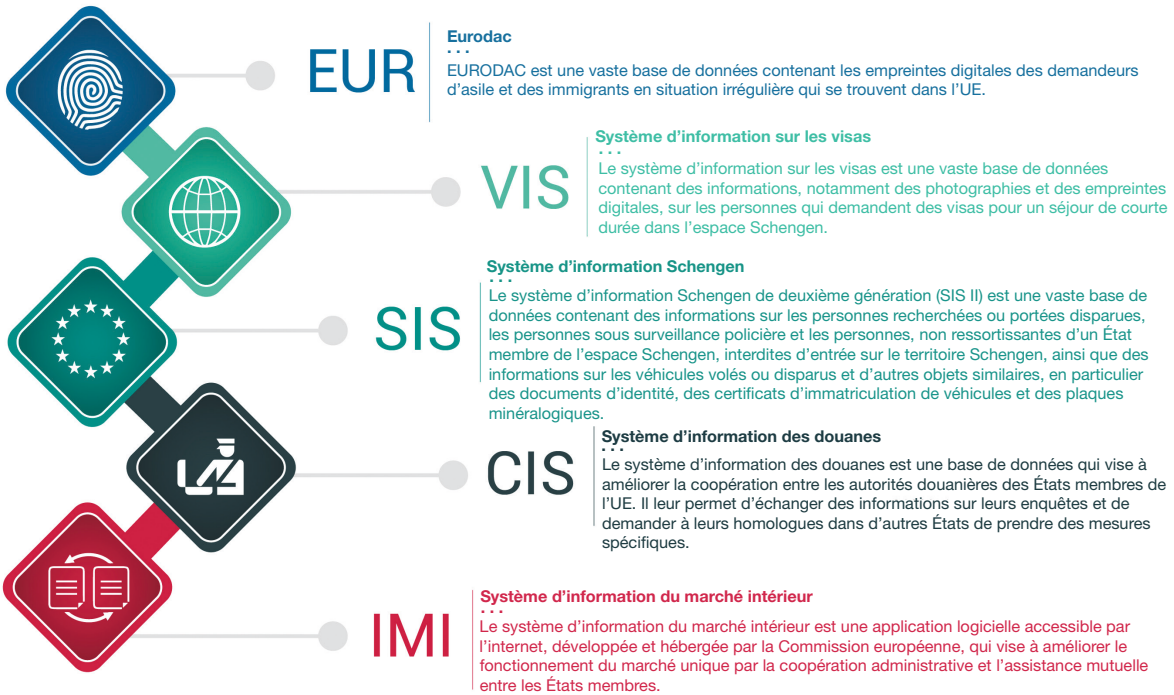
À l'heure actuelle, le CEPD et les APD nationales se partagent la responsabilité de la supervision de ces systèmes d'information. Tandis que le CEPD supervise le traitement des données à caractère personnel dans les unités centrales, les APD nationales sont chargées de superviser la manière dont leurs autorités nationales respectives utilisent ces systèmes d'information et de contrôler les composantes nationales de ces systèmes.

Toutes les autorités de contrôle concernées, y compris le CEPD, coopèrent dans le cadre des groupes de coordination de la supervision (GCS). Chacun de ces groupes est chargé d'un système d'information spécifique de l'UE et a pour mission d'assurer la cohérence des efforts de supervision à chaque niveau.

Le CEPD assure également le secrétariat de chacun de ces groupes, qui travaillent sous l'autorité de leur président respectif. Les groupes « Eurodac », « Système d'information sur les visas » (VIS), « Système d'information Schengen » (SIS) et « Système d'information des douanes » (SID) se réunissent en moyenne deux fois par an. Nous publions les conclusions de leurs réunions sur la page web qui leur est consacrée sur le site web du CEPD.

Dans le cadre de notre travail avec Europol, nous participons également à des activités impliquant une supervision coordonnée. Tandis que le CEPD est chargé de superviser le traitement par Europol des données opérationnelles à caractère personnel, les APD nationales ont pour mission de surveiller le traitement des données à caractère personnel par leurs services répressifs nationaux respectifs (voir section 6.4.3).

La plupart des données traitées par Europol étant communiquées par les services répressifs nationaux, il est essentiel de pouvoir coopérer efficacement avec les APD dans ce domaine. Cette coopération s'organise en grande partie au sein du comité de coopération d'Europol, dont le CEPD assure le secrétariat. Ce comité a une fonction consultative et il offre un cadre pour discuter de sujets communs et élaborer des lignes



directrices et des bonnes pratiques. Ses membres se réunissent au moins deux fois par an.

L'avenir de la supervision coordonnée

Les nouvelles règles en matière de protection des données pour les institutions et les organes de l'UE, qui sont établies dans le règlement (UE) 2018/1725, prévoient un modèle unique de supervision coordonnée pour les agences et systèmes d'information à grande échelle de l'UE, dans le cadre du comité européen de la protection des données. Ce modèle unique remplacera le système actuel des GCS individuels.

Il ne s'appliquera pas immédiatement à l'ensemble des systèmes et des agences d'information de l'UE, mais progressivement, en fonction de la date à laquelle la version révisée de la loi portant création de chaque système et agence d'information de l'UE, prévoyant son application, entrera en vigueur.

Depuis 2018, les travaux préparatoires visant à organiser ce modèle, qui n'est applicable actuellement qu'au système d'information du marché intérieur (IMI), sont en cours au sein du comité européen de la protection des données Le but est de définir des solutions pratiques permettant de mettre en pratique le modèle unique de supervision coordonnée envisagé par le législateur. Le CEPD continue de jouer un rôle actif dans ce processus.

En janvier 2019, pour compléter les discussions du comité européen de la protection des données, nous avons organisé, lors de la conférence annuelle « *Computers, Privacy and Data Protection* » (CPDP), une réunion-débat intitulée *Checks and balances in the area of freedom security and justice : rethinking governance* (L'équilibre des pouvoirs dans les domaines de la liberté, de la sécurité et de la justice : repenser la gouvernance). Au cours de cette réunion-débat, nous avons discuté de la façon d'instaurer une collaboration étroite entre les organes de supervision, tout en préservant l'indépendance et le rôle de chacun d'entre eux, et de la manière de simplifier les systèmes de supervision actuels.

5.3.2 Une coopération plus étroite avec l'Agence des droits fondamentaux de l'Union européenne

Le CEPD n'est pas le seul organe de l'UE dont le mandat est axé sur la protection des droits fondamentaux. L'Agence des droits fondamentaux de l'Union européenne (FRA) a pour mission de fournir des avis indépendants sur les droits visés dans la charte des droits fondamentaux, notamment sur la protection des données.

La protection des données, le respect de la vie privée et les autres libertés et droits fondamentaux énoncés dans la Charte sont interdépendants. Le 30 mars 2017, Giovanni Buttarelli, le contrôleur européen de la protection des données, et Michael O'Flaherty, le directeur de la FRA, ont signé un protocole d'accord concernant le renforcement de la coopération entre les deux organisations. Ce document reflète la relation étroite et constructive entre le CEPD et la FRA, mais il traduit également leur engagement à coopérer pour protéger plus efficacement les droits et les intérêts des citoyens de l'Union européenne.

Leur collaboration dans le cadre de la révision du manuel de droit européen en matière de protection des données de la FRA, publié en mai 2018, a permis de renforcer cet engagement. Nous avons coparrainé la préparation de ce manuel avec le Conseil de l'Europe et nous avons mis à disposition nos ressources et notre expertise en matière de législation et de jurisprudence de l'UE relatives à la protection des données.

@EU_EDPS

#EDPS & @EURightsAgency strengthen ties to improve #DataProtection #cooperation - Read blogpost by @Buttarelli_G https://t.co/FAPKQm2QBt

5.3.3 Coopération avec d'autres organisations

En plus de coopérer étroitement avec nos partenaires au sein des APD de l'EEE, nous travaillons aussi avec d'autres organisations et partenaires au rayonnement international. Ce type de collaboration permet à l'Union européenne de parler d'une voix forte et unie sur la scène internationale, montrant ainsi que la protection des données va au-delà du travail des APD.

Le Conseil de l'Europe

Le 28 janvier 1981, le Conseil de l'Europe a adopté la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Connue sous le nom de «Convention 108», cette convention est le premier instrument international juridiquement contraignant dans le domaine de la protection des données.

Tous les pays peuvent adhérer à la convention ; 55 pays sont désormais partis à la convention et à son protocole additionnel sur les autorités de contrôle et les flux transfrontières de données. Ce nombre passe à 70, si l'on tient compte des pays qui participent au Comité de la Convention 108 en qualité d'observateurs.

Le CEPD participe aux groupes d'experts du Conseil de l'Europe sur la protection des données, tels que le Comité consultatif (T-PD) de la Convention 108, en tant qu'observateur. Notre rôle consiste à garantir un niveau élevé de protection des données et de compatibilité avec les normes de l'UE en matière de protection des données. Le CEPD a, par ailleurs, été associé au processus de modernisation de la Convention 108, qui s'est achevé le 18 mai 2018.

Depuis mars 2018, le CEPD représente également la Conférence internationale annuelle des commissaires à la protection des données et à la vie privée auprès du T-PD.

L'OCDE

Le CEPD suit les activités du groupe de travail sur la sécurité et la vie privée dans l'économie numérique (GTSVPEN) de l'Organisation pour la coopération et le développement économiques (OCDE). L'OCDE, qui participe activement aux ateliers organisés chaque année par le CEPD pour les organisations internationales, collabore avec celui-ci dans le cadre de l'édition 2019 de cet événement (voir section 5.2.5).

Le 1er juillet 2019, il a été décidé de remplacer le GTSVPEN par deux nouveaux groupes d'experts :

- le groupe de travail sur la gouvernance des données et la vie privée dans l'économie numérique (GDVP) ;
- le groupe de travail sur la sécurité dans l'économie numérique (SEN), qui dépend du Comité de la politique de l'économie numérique (CPEN).

Le GDVP continuera de traiter les questions relatives à la protection des données et à la vie privée, tandis que le SEN mettra davantage l'accent sur la cybersécurité et les questions informatiques, telles que la cryptographie. Le CEPD suivra les activités de ces deux groupes.

Nous avons également pris part aux travaux du groupe d'experts de l'OCDE sur les lignes directrices régissant la protection de la vie privée (GELDVP), depuis sa création au début de l'année 2019. Nous avons participé à plusieurs téléconférences préparatoires ainsi qu'au premier atelier du GELDVP sur la responsabilisation, qui s'est tenu à Paris le 6 mai 2019. Nous continuerons de suivre les discussions et la progression de ce groupe, en coopération avec la Commission européenne et d'autres APD de l'UE participantes.

Évolutions technologiques

Le CEPD travaille également avec plusieurs groupes au niveau de l'UE et à l'échelle internationale pour étudier l'incidence de la technologie sur les droits fondamentaux et soutenir l'intégration du respect de la vie privée dans l'évolution technologique, y compris dans l'évolution des structures de l'internet.

Le groupe de haut niveau sur l'internet de l'UE (HLIG), composé de représentants des institutions de l'Union et d'États membres

de celle-ci, est l'un de ces groupes. Le CEPD y participe en tant qu'observateur. Grâce à ce groupe, l'UE est mieux à même de coordonner sa position sur certains sujets et, par conséquent, de parler d'une seule voix.

Le cas de la Société pour l'attribution des noms de domaines et des numéros sur l'internet (ICANN) en est un bon exemple. Du 13 au 15 mars 2017, Giovanni Buttarelli, le contrôleur européen de la protection des données, a participé, avec les représentants d'autres organisations internationales de protection des données, à une série de réunions et de sessions de haut niveau dans le cadre de la 58e réunion de l'ICANN à Copenhague. Ces réunions avaient pour thème les règles et les procédures de l'ICANN relatives au système WHOIS, qui contient des données sur les propriétaires de domaines internet et d'adresses IP. Les règles et les procédures en vigueur à l'époque, qui prévoyaient un accès non contrôlé aux données à caractère personnel des individus fournissant des ressources sur l'internet, plaçaient certains fournisseurs en porte-à-faux avec les règles de l'UE en matière de protection des données. En parlant d'une seule voix, l'UE est parvenue à convaincre l'ICANN d'engager un processus visant à adapter ses règles et procédures, pour les aligner sur le RGPD.

Le CEPD est également membre du groupe de travail international sur la protection des données dans les télécommunications (le *« Berlin Group »*). Cet organisme mondial rassemble des experts provenant d'autorités chargées du respect de la vie privée et de la protection des données, du monde universitaire, de la société civile et d'organisations internationales de normalisation. Le débat concernant le rôle de la technologie et son incidence sur les droits fondamentaux s'étant intensifié ces dernières années, les travaux du groupe ont gagné en importance.

Le groupe de Berlin publie des documents de travail, sur la base d'une analyse des caractéristiques technologiques du sujet faisant l'objet d'un examen. Il définit des principes et des recommandations visant à atteindre des objectifs communs. Au cours des cinq dernières années, le groupe de Berlin a adopté des documents de travail sur des questions de sécurité et de protection de la vie privée concernant la téléphonie par l'internet, la biométrie dans le cadre de l'authentification en ligne, les plates-formes d'apprentissage en ligne, les principes ou instruments internationaux régissant la collecte et le traitement de données dans les véhicules connectés, auxquels le CEPD a contribué.

En octobre 2019, le CEPD a organisé la réunion du groupe de Berlin à Bruxelles. Les discussions ont porté sur des sujets tels que le nouveau concept de la portabilité des données, établi par le RGPD, et ses possibles répercussions au niveau mondial. En ce qui concerne les évolutions technologiques, le groupe s'est penché sur les assistants vocaux, tels que les haut-parleurs intelligents, dont nous avons parlé dans le premier numéro de TechDispatch (voir section 4.1.2), l'intensification des activités de profilage et de suivi et les évolutions concernant la technologie des chaînes de blocs.

Depuis 2019, le CEPD copréside le groupe de travail de l'ICDPPC sur l'intelligence artificielle, dont il assure également le secrétariat (voir section 4.1.2). Ce groupe de travail a été créé à la suite de l'adoption de la déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle, lors de la 40e ICDPPC qui s'est tenue à Bruxelles. Le CEPD était l'un des auteurs du projet de déclaration, à l'instar d'autres membres de l'ICDPPC.

Le CEPD prend également part aux événements du Dialogue européen sur la gouvernance de l'internet (EuroDIG). Cette initiative fournit une plate-forme de dialogue informel sur les politiques publiques dans le domaine de la gouvernance de l'internet. Il s'agit d'un forum qui permet d'échanger des connaissances et de bonnes pratiques et de parvenir à des positions communes.

6. OUVRIR UN NOUVEAU CHAPITRE DÉDIÉ À LA PROTECTION DES DONNÉES DANS L'UE

L'Union européenne montre la voie à suivre en matière de protection des données et de respect de la vie privée. Nos réglementations accordent la priorité à l'individu, en veillant à ce que chaque personne soit en mesure d'exercer les droits fondamentaux visés dans la charte des droits fondamentaux de l'UE et d'en bénéficier. Cependant, pour conserver cette position privilégiée, l'UE doit s'assurer que ses réglementations continuent, à l'ère numérique, d'offrir une protection adéquate aux citoyens.

Au début du mandat, les règles portant sur la protection des données en vigueur dans l'UE dataient encore de l'ère pré-numérique. Le CEPD s'est donc fixé pour objectif principal d'établir et d'appliquer, dès que possible, de nouvelles règles. Pour cela, nous avions besoin d'ouvrir un nouveau chapitre dédié à la protection des données dans l'Union. Il nous a fallu élaborer une nouvelle norme, plus stricte, concernant la protection des données à l'ère numérique, susceptible de faire des émules à travers le monde.

Dans notre stratégie 2015-2019, nous avons défini quatre points d'action concernant cette question, le premier d'entre eux prévoyant de soutenir la Commission européenne, le Parlement et le Conseil dans la recherche d'un accord sur un nouveau cadre de l'UE pour la protection des données. Nous nous sommes également engagés à travailler avec les institutions et les organes de l'UE que nous supervisons afin qu'ils soient prêts à appliquer ces nouvelles règles, à émettre des avis pour faciliter l'élaboration de politique de l'UE éclairée et responsable et à aider l'UE à définir des approches stratégiques qui à la fois amélioreront la sécurité de l'UE et protégeront la vie privée.

@EU_EDPS

Our experience as a supervisor gives us knowledge and credibility to advise on the reform of #EUdataP @Buttarelli_G #EDPS

6.1 Adoption et mise en œuvre des règles modernes de protection des données

En janvier 2012, la Commission européenne a présenté des propositions législatives concernant de nouvelles règles de l'UE pour la protection des données, adaptées à l'ère numérique. Ces règles devaient constituer un train de réformes législatives couvrant la protection des données à travers l'UE, y compris la protection des données dans les secteurs de la police et de la justice pénale.

Cette réforme a fait l'objet de débats intenses et prolongés. En tant que conseiller du législateur de l'Union, nous avons suivi l'ensemble du processus, en émettant des avis à différents stades de la procédure. Le processus législatif étant encore dans l'impasse au début du mandat, nous nous sommes fixé comme priorité d'aider le Parlement européen, le Conseil et la Commission à surmonter leurs divergences et à conclure un accord sur un nouvel ensemble de règles. Ces règles devaient être suffisamment flexibles pour encourager l'innovation technologique et pour ne pas entraver les flux transfrontaliers de données, mais surtout, elles devaient permettre aux citoyens d'appliquer et d'exercer leurs droits plus efficacement, à la fois en ligne et hors ligne.

PROTECTION DES DONNÉES DANS L'UNION EUROPÉENNE

Chronologie

24 octobre 1995

Adoption de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

7 décembre 2000

La Charte des droits fondamentaux de l'Union européenne est publiée. Elle énonce les droits personnels, civiques, politiques, économiques et sociaux de toutes les personnes vivant dans l'UE. Ceux-ci incluent les droits à la protection des données et au respect de la vie privée

31 octobre 2003

La directive 2002/58/CE sur la protection de la vie privée et les communications électroniques devient pleinement applicable dans l'ensemble de l'UE. Elle remplace la directive 97/66/CE

25 novembre 2009

Publication de la directive 2009/136/CE, qui met à jour la directive sur la protection de la vie privée et les communications électroniques. Elle requiert en particulier qu'un consentement soit donné en connaissance de cause avant qu'un «cookie» puisse être installé sur un dispositif.

25 janvier 2012

La Commission européenne propose une réforme exhaustive des règles de l'UE en matière de protection des données, en vue de renforcer les droits en matière de respect de la vie privée dans l'environnement en ligne et de donner un coup d'accélérateur à l'économie numérique européenne

27 juillet 2015

Le CEPD publie des recommandations concernant le règlement général sur la protection des données (RGPD) et délivre une application mobile permettant aux utilisateurs de comparer son texte avec les textes de négociation proposés par la Commission européenne, le Parlement européen et le Conseil

15 décembre 1997

Adoption de la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

18 décembre 2000

Entrée en vigueur du règlement (CE) nº 45/2001, définissant les règles relatives à la protection des données dans les institutions de l'UE et instituant le CEPD

19 janvier 2009

Entrée en vigueur de la décision-cadre 2008/977/JHA du Conseil, applicable au traitement des données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale

1er décembre 2009

Le traité de Lisbonne entre en vigueur, donnant pleinement force juridique à la Charte des droits fondamentaux de l'UE. Les institutions et les États membres de l'UE sont à présent tenus de respecter la Charte lorsqu'ils mettent en œuvre le droit de l'UE

Mars 2012

Le CEPD et le groupe de travail «article 29» (GT art. 29) adoptent des avis sur le train de mesures de la Commission européenne pour une réforme de la protection des données

28 octobre 2015

Le CEPD publie des recommandations concernant la directive relative à la protection des données pour les secteurs de la police et de la justice pénale

15 décembre 2015

Le Parlement européen et le Conseil s'accordent sur un texte pour le RGPD, qui définit les règles en matière de protection des données applicables à toutes les organisations et à toutes les entreprises opérant dans l'UE, ainsi que sur un texte pour la directive relative à la protection des données pour les secteurs de la police et de la justice pénale.

2 février 2016

Le GT art. 29 publie un plan d'action pour la mise en œuvre du GDPR

22 juillet 2016

Le CEPD publie un avis sur la révision de la directive sur la protection de la vie privée et les communications électroniques

10 janvier 2017

La Commission européenne propose deux nouveaux règlements, l'un sur la protection de la vie privée et les communications électroniques et l'autre sur la protection des données dans les institutions de l'UE

15 mars 2017

Le CEPD rend un avis sur la proposition de la Commission relative à un nouveau règlement sur la protection des données dans les institutions de l'UE

24 avril 2017

Le CEPD rend un avis concernant la proposition de règlement de la Commission européenne sur la protection de la vie privée et les communications électroniques

6 mai 2018

La nouvelle directive sur la protection des données pour les secteurs de la police et de la justice pénale devient pleinement applicable, remplaçant la décision-cadre 2008/977/JHA

22 mai 2018

Le Parlement européen et le Conseil s'accordent sur un texte pour un nouveau règlement sur la protection des données dans les institutions de l'UE, qui aligne les règles énoncées dans le règlement (CE) nº 45/2001 sur le règlement général sur la protection des données.

25 mai 2018

Le RGPD s'applique pleinement à toutes les organisations et à toutes les entreprises opérant dans l'UE et le comité européen de la protection des données débute ses activités

11 décembre 2018

Le règlement (CE) nº 2018/1725 remplace le règlement (CE) nº 45/2001, énonçant les règles relatives à la protection des données dans les institutions de l'UE

6.1.1 Le règlement général sur la protection des données

En 2018, nous sommes entrés dans une nouvelle ère européenne de la protection des données. Le 25 mai 2018, le règlement général sur la protection des données (RGPD) est devenu pleinement applicable à l'ensemble des entreprises, des organisations et des institutions opérant dans l'Union européenne, remplaçant la directive 95/46/CE sur la protection des données.

Au terme de près de quatre ans de négociation, le législateur de l'UE est parvenu, en décembre 2015, à un accord sur le texte final du RGPD. Le CEPD a suivi l'ensemble du processus, en conseillant le législateur de l'UE à différents stades.

Le 27 juillet 2015, nous avons publié nos recommandations sur la proposition législative, pour aider les colégislateurs de l'UE à négocier le texte final. Nous avons également lancé une application mobile permettant aux utilisateurs de comparer facilement les textes proposés par la Commission européenne, le Parlement européen et le Conseil avec les recommandations du CEPD. Nous souhaitions garantir la transparence du processus de négociation.

Le texte final du RGPD a été publié au *Journal officiel de l'Union européenne* le 4 mai 2016 et le compte à rebours en vue de la pleine application du RGPD (25 mai 2018) s'est enclenché. Dans le cadre de ce processus, nous avons actualisé notre application mobile afin d'y inclure le texte final du RGPD.

En plus de renforcer les droits des personnes à la protection des données et de la vie privée, le RGPD a consolidé les prérogatives des autorités nationales chargées de la protection des données (APD), en leur donnant le droit de conseiller les parlements nationaux, les gouvernements et d'autres institutions et organes sur les mesures législatives et administratives relatives à la protection des données à caractère personnel. Ces prérogatives sont semblables à celles qui sont dévolues au CEPD par rapport aux institutions de l'UE. Le groupe de travail « article 29 » (GT29), composé de l'ensemble des APD de l'UE et du CEPD, s'est donc fixé comme objectif la préparation au RGPD. Il a notamment fourni une assistance en matière de mise en œuvre et d'interprétation des nouvelles règles (voir section 5.3.1).

Depuis le 25 mai 2018, en notre qualité de membre du comité européen de la protection des données, qui a remplacé le GT29 en vertu du RGPD, nous continuons de contribuer pleinement aux efforts déployés pour fournir orientation et conseil concernant le RGPD (voir section 5.3.1).

@EU_EDPS

#EDPS app : recommendations support EU to achieve best possible outcome #EUdataP within the boundaries of the 3 texts

6.1.2 La directive en matière de protection des données dans le domaine pénal

En plus du RGPD, le législateur de l'UE a également adopté de nouvelles règles en matière de protection des données dans les domaines de la police et de la justice pénale. La directive en matière de protection des données dans le domaine répressif garantit la protection adéquate des données à caractère personnel des individus concernés par des procédures pénales à titre de témoin, de victime ou de suspect. Elle vise également à faciliter l'échange d'informations entre les autorités policières et judiciaires des États membres, en améliorant la coopération dans la lutte contre le terrorisme et d'autres formes graves de criminalité en Europe.

La directive établit un cadre complet garantissant un niveau élevé de protection des données tout en tenant compte de la nature spécifique du domaine de la police et de la justice pénale. Elle remplace la décision-cadre 2008/977/JAI, qui régissait auparavant le traitement des données par les autorités policières et judiciaires, et elle couvre tant le traitement national que le traitement transfrontalier des données à caractère personnel. Elle ne couvre pas les activités des institutions, organes, bureaux et agences de l'Union européenne.

À la suite de l'adoption d'un accord général sur la nouvelle directive, le CEPD a publié ses

recommandations le 28 octobre 2015. Nous avons également publié un tableau comparant nos recommandations avec les propositions soumises pour négociation par le Parlement européen et le Conseil ; nous les avons incluses dans notre application mobile, comme nous l'avions fait pour le RGPD (voir section 6.1.1).

La directive est entrée en vigueur le 5 mai 2016 et les États membres avaient jusqu'au 6 mai 2018 pour la transposer dans leur législation nationale.

@EU_EDPS

#data protection in police & justice sectors should be fully consistent with general rules contained in #GDPR #EUdataP

6.1.3 Création du secrétariat du comité européen de la protection des données

Le RGPD a également institué le comité européen de la protection des données (EDPB), un nouvel organe de l'Union chargé de faciliter la coopération entre les APD nationales de l'UE. Le 25 mai 2018, le Comité s'est vu confier les responsabilités du GT29, en plus de nombreuses nouvelles tâches visant à garantir l'application cohérente du RGPD à travers l'UE (voir section 5.3.1).

Chargé d'assurer le secrétariat du Comité, le CEPD a nommé, au début de 2017, un agent de liaison ayant pour mission de coordonner l'ensemble des travaux du CEPD relatifs à la mise en place du secrétariat du Comité. Sous la supervision de l'agent de liaison, nous avons créé, au deuxième semestre de 2017, un secteur EDPB, qui est devenu, le 25 mai 2018, le secrétariat du Comité. Le secrétariat a pour mission de fournir un soutien logistique et administratif au Comité et de mener les travaux pertinents de recherche et d'analyse.

L'unité « Ressources humaines, budget et administration » (HRBA) du CEPD soutient les activités du secrétariat du Comité. Elle a veillé à ce que l'infrastructure de ressources humaines nécessaire au fonctionnement du Comité soit en place avant le 25 mai 2018 (voir section 7.2.3).

Le CEPD était également chargé de mettre au point l'infrastructure informatique du comité européen de la protection des données. Il a notamment défini les exigences spécifiques du nouveau système d'information, tant pour le Comité que pour les APD, et il a réalisé une analyse approfondie des options technologiques qui s'offraient à nous. Nous avons privilégié la solution la plus appropriée, qui nous a permis de garantir que le système soit opérationnel en mai 2018.

6.1.4 Règlement (UE) 2018/1725

Le RGPD n'a pas été le seul événement marquant de l'année 2018 en ce qui concerne la protection des données. Deux jours avant le lancement du RGPD, le législateur de l'UE est parvenu à un accord sur des règles équivalentes pour les institutions, organes et agences de l'UE. Cette législation, qui définit également le rôle et les prérogatives du CEPD en tant qu'autorité de contrôle des institutions de l'UE, est devenue pleinement applicable le 11 décembre 2018, remplaçant le règlement (CE) nº 45/2001.

Le RGPD, qui établit les règles de la protection des données dans les entreprises et les organisations opérant dans l'ensemble de l'Union, ne s'applique pas aux institutions et organes de l'UE, qui sont soumis à leurs propres règles, désormais établies par le règlement (UE) 2018/1725. Ces règles, qui sont équivalentes à celles du RGPD, garantissent que, lorsqu'ils ont affaire aux institutions de l'UE, tous les agents de l'UE et toute personne résidant dans l'UE bénéficient de droits renforcés, comme cela serait le cas avec le RGPD.

La Commission européenne avait initialement prévu de faire appliquer le RGPD et le règlement (UE) 2018/1725 à compter de la même date, la révision des règles visées au règlement (CE) nº 45/2001 et leur harmonisation avec les règles établies par le RGPD ont pris plus de temps que prévu.

En 2015, le CEPD a mis sur pied un groupe de travail informel composé, entre autres, de plusieurs délégués à la protection des données (DPD) issus d'institutions de l'UE, pour échanger des points de vue sur la révision du règlement. En avril 2016, ce groupe de travail a soumis un

rapport à la Commission. Dans ce rapport, le groupe comparait les dispositions du règlement (CE) nº 45/2001 et celles du RGPD et avançait plusieurs recommandations concernant le règlement actualisé.

Le 10 janvier 2017, la Commission a adopté une proposition de règlement actualisé, à laquelle nous avons répondu le 15 mars 2017 avec notre avis. Même si nous estimions que la proposition garantissait un juste équilibre entre les différents intérêts en jeu, nous avons également mis en lumière plusieurs domaines susceptibles d'être améliorés, notamment en ce qui concerne la limitation des droits des personnes et la nécessité de donner la possibilité aux institutions de l'UE d'utiliser des mécanismes de certification dans certains contextes. En ce qui concerne les missions et les prérogatives du CEPD, nous avons estimé que la proposition établissait un équilibre raisonnable entre les intérêts en jeu et qu'elle reflétait les fonctions normales d'une autorité indépendante chargée de la protection des données.

Les discussions portant sur le règlement révisé sont entrées en phase de *trilogue* en novembre 2017. Nous avons répondu en demandant au Parlement européen, à la Commission et au Conseil d'aboutir aussi rapidement que possible à un accord sur le nouveau règlement, afin que les institutions de l'UE montrent l'exemple en ce qui concerne l'application des nouvelles règles en matière de protection des données. Les trois institutions ne sont, toutefois, pas parvenues à s'accorder sur le texte avant le 23 mai 2018. Publié le 21 novembre 2018 au *Journal officiel de l'Union européenne*, le règlement (UE) 2018/1725 est pleinement applicable depuis le 11 décembre 2018, faisant converger les règles applicables aux institutions de l'UE vers celles du RGPD.

Le nouveau règlement comporte, par ailleurs, un chapitre spécifique sur le traitement des données opérationnelles à caractère personnel par les agences de l'UE actives dans le domaine du maintien de l'ordre et de la coopération judiciaire en matière pénale, telles qu'Eurojust, qui fait également l'objet d'un règlement spécifique, le règlement(UE) 2018/1727. Ces règles sont alignées sur les règles établies par la directive en matière de protection des données dans le domaine pénal qui, à l'instar du RGPD, est devenue applicable en mai 2018.

À l'heure actuelle, le traitement des données opérationnelles à caractère personnel par Europol et le parquet européen ne relève pas du champ d'application de ces nouvelles règles ; il est prévu que la Commission européenne examine la situation d'ici à 2022.

@EU_EDPS

Regulation 2018/1725 on protection of natural persons w/ regard to processing of #personaldata by #EUInstitutions, bodies, offices & agencies enters into force today, bringing #dataprotection rules for #EUI in line w/ standards imposed by #GDPR https://europa.eu/!Kx84fu #GDPRforEUI

6.1.5 Vie privée et communications électroniques

Les nouvelles règles, en vigueur depuis 2018, renforcent la position de l'UE en tant que leader mondial dans le domaine de la protection des données et du respect de la vie privée. Cependant, une pièce du puzzle réglementaire fait toujours défaut. Le RGPD ne régissant pas la confidentialité des communications électroniques, un nouveau règlement sur la vie privée et les communications électroniques, qui reflète fidèlement et soutient les principes énoncés dans le RGPD, est essentiel pour que les droits fondamentaux des personnes à la protection des données et de la vie privée soient pleinement respectés.

En vertu des règles actuelles en matière de vie privée et de communications électroniques, les communications électroniques traditionnelles sont soumises à des limitations claires en ce qui concerne la manière dont elles utilisent les données à caractère personnel. Cependant, les entreprises considérées comme étant des *services de la société de l'information* ont prospéré du fait de leur capacité à exploiter les lacunes du cadre juridique actuel. Il existe, par conséquent, un besoin réel et urgent de combler

ces lacunes et de renforcer la protection de la vie privée et la sécurité des communications en ligne.

Le 22 juillet 2016, à la demande de la Commission européenne, nous avons publié un avis sur le réexamen de la directive «vie privée et communications électroniques», qui est en vigueur dans sa forme actuelle depuis 2009. Dans cet avis, nous avons précisé notre position quant aux principales questions relatives à son réexamen. Nous avons souligné la nécessité d'un nouveau cadre juridique pour la vie privée et les communications électroniques, plus intelligent, plus clair et plus solide, et nous avons recommandé que le champ d'application de ce cadre soit étendu, à la fois pour tenir compte des mutations technologiques et sociétales et pour faire en sorte que les individus bénéficient du même niveau de protection pour l'ensemble des services équivalents d'un point de vue fonctionnel. Nous avons également souligné la nécessité de protéger la confidentialité sur tous les réseaux accessibles au public et de veiller à ce que le consentement des utilisateurs soit, le cas échéant, explicite, libre et éclairé.

Le 10 janvier 2017, la Commission a publié sa proposition de nouveau règlement relatif à la vie privée et aux communications électroniques et, le 24 avril 2017, nous avons publié notre réponse. Bien que nous ayons accueilli favorablement cette proposition, nous avons exposé certaines de nos principales préoccupations. Celles-ci avaient trait au champ d'application et aux définitions, à la nécessité de garantir un consentement réellement libre, au besoin de clarté quant à la relation entre le règlement relatif à la vie privée et aux communications électroniques et le RGPD et à la nécessité d'inclure la protection de la vie privée par défaut.

Le 27 octobre 2017, le Parlement européen a répondu en approuvant son rapport sur le nouveau règlement relatif à la vie privée et aux communications électroniques. Nous avons constaté avec satisfaction que ce rapport faisait suite aux nombreuses recommandations contenues dans nos avis. Il s'appuyait également sur les recommandations concernant les propositions d'amendements du Parlement, qui ont été publiées le 5 octobre 2017, ainsi que sur les recommandations formulées par le GT29, auxquelles nous avons activement contribué en tant que corapporteur. Il a cependant été plus difficile d'obtenir le feu vert du Conseil.

En ce qui concerne de nombreux points de la proposition, la marge de négociation est restreinte, car elle est susceptible d'entacher les principes clés du secret des communications. Compte tenu de l'importance de garantir la confidentialité des communications et étant donné la nature particulièrement sensible des métadonnées concernées, nous avons besoin de toute urgence d'une législation assurant un niveau de protection équivalent, voire supérieur, à celui du RGPD.

Malgré tous les efforts que nous avons déployés pour encourager les colégislateurs à faire avancer ce dossier, la révision de la législation concernant la vie privée et les communications électroniques n'a pas été finalisée avant la tenue des élections du Parlement européen, en mai 2019. Une nouvelle période législative étant désormais en cours, l'avenir du règlement concernant la vie privée et les communications électroniques est de plus en plus incertain. Cependant, le CEPD continuera de plaider en faveur d'une solution satisfaisante garantissant que l'UE assure le niveau le plus élevé possible de protection des données et de la vie privée.

@EU_EDPS

#ePrivacy will help fix, not exacerbate, #digital market imbalances through a more consistent and more economically sustainable approach among #EU Member States

6.2 Accroître la responsabilisation des organes de l'UE qui collectent, utilisent et stockent des données à caractère personnel

En tant qu'autorité de contrôle de la protection des données des institutions et organes de l'UE, nous sommes chargés de veiller à ce que les institutions de l'Union respectent les règles pertinentes en matière de protection des données. Nous croyons fermement que les

institutions de l'UE doivent montrer l'exemple, en établissant des normes auxquelles d'autres organisations et entreprises dans l'UE devront se conformer.

Le CEPD dispose de plusieurs instruments lui permettant de surveiller et d'appliquer les règles en matière de protection des données au sein des institutions de l'Union. Parmi ceux-ci, citons les inspections, les visites et le pouvoir de traiter les réclamations. Cependant, nous nous efforçons également de fournir aux institutions les outils dont elles ont besoin pour mettre en œuvre de manière efficace les règles en matière de protection des données, que ce soit par l'intermédiaire de réunions régulières avec les DPD, de sessions de formation avec les responsables de l'UE ou la publication de lignes directrices. Au cours du mandat, nous nous sommes attachés à encourager les institutions de l'UE à agir de manière responsable, en veillant non seulement à ce qu'elles respectent les règles en matière de protection des données, mais aussi à ce qu'elles soient en mesure d'en apporter la preuve.

6.2.1 Contrôler et garantir le respect du règlement (CE) nº 45/2001

Jusqu'au 11 décembre 2018, le règlement (CE) nº 45/2001 définissait les règles en matière de traitement des données à caractère personnel applicables aux institutions et organes de l'UE. Il définissait également le rôle et les prérogatives du CEPD, en tant que leur autorité de contrôle de la protection des données, en matière de surveillance et de respect des règles. Les contrôles préalables, les consultations, les inspections et l'élaboration de lignes directrices faisaient notamment partie des attributions du CEPD.

Contrôles préalables

Le règlement (CE) nº 45/2001 disposait que les traitements effectués par les institutions de l'UE susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités étaient soumis au contrôle préalable du CEPD. Le traitement envisagé devait être notifié au CEPD afin qu'il puisse l'évaluer et émettre un avis sur la manière de garantir le respect des règles en matière de protection des données.

Entre 2015 et 2018, lorsque le règlement (CE) nº 45/2001 était en vigueur, nous avons reçu 267 notifications et émis 298 avis relatifs aux contrôles préalables. Ces derniers traitaient de questions très diverses, des activités fondamentales des institutions de l'Union aux opérations de traitement administratif, telles que la gestion du personnel (voir illustration 11).

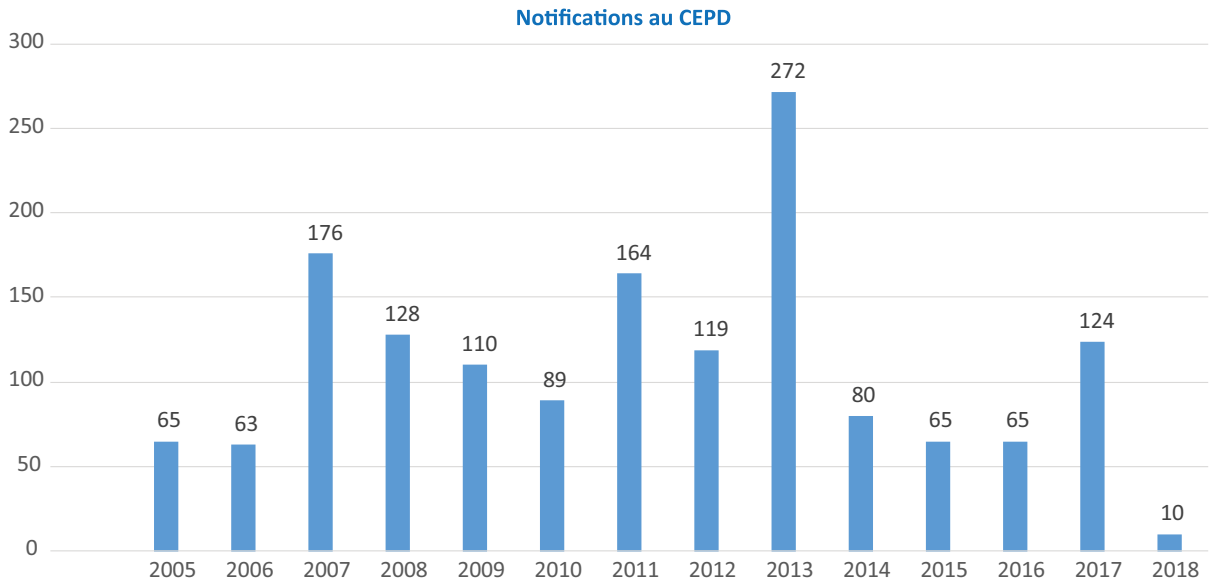


Illustration 9. Évolution des notifications reçues par le CEPD au titre du règlement (CE) nº 45/2001

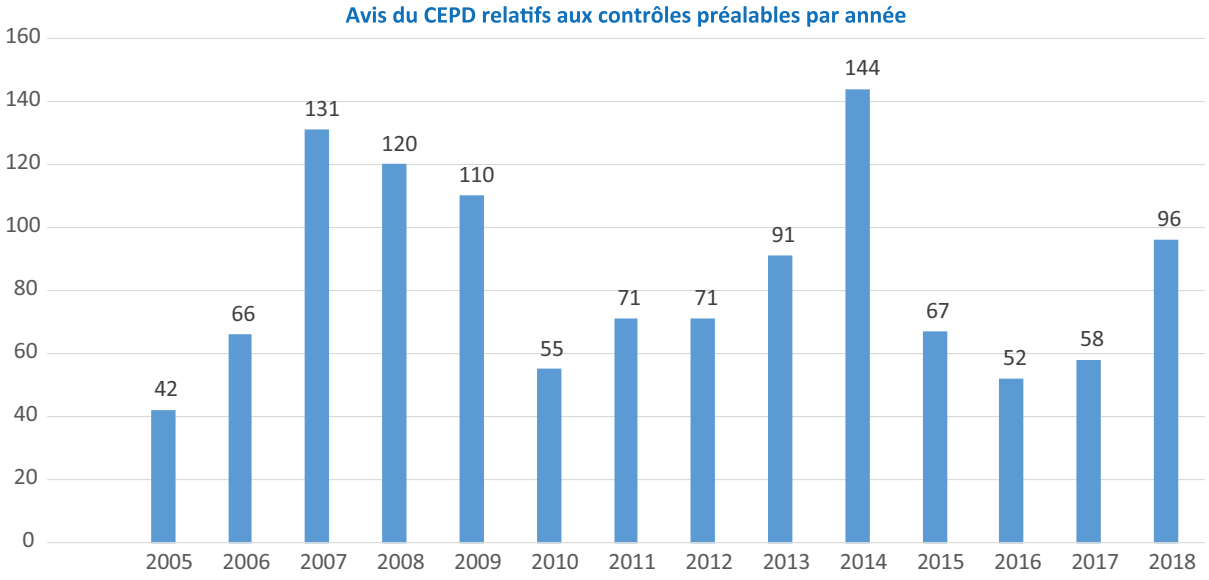


Illustration 10. Évolution des avis relatifs aux contrôles préalables émis par le CEPD au titre du règlement (CE) nº 45/2001

Consultations

Le règlement (CE) nº 45/2001 disposait que, dans certains cas, les institutions de l'UE étaient tenues de consulter le CEPD. Les institutions de l'UE pouvaient également consulter le CEPD à titre volontaire, si elles avaient des doutes quant à la manière d'appliquer le règlement. Ces consultations pouvaient être formelles ou informelles, en fonction des circonstances propres à chaque cas. Les consultations étaient obligatoires dans les circonstances suivantes :

- si une institution de l'UE doutait s'il convenait de notifier le CEPD en vue d'un avis relatif à un contrôle préalable, elle pouvait saisir de l'affaire son DPD, lequel pouvait demander l'avis du CEPD ;
- lors de l'élaboration de mesures administratives relatives au traitement de données à caractère personnel impliquant une institution de l'UE.

Les institutions de l'UE avaient également la possibilité de consulter le CEPD sur toute autre question concernant un traitement de données à caractère personnel. Entre 2015 et le 10 décembre 2018, nous avons reçu 162 demandes de consultation et nous avons présenté 160 réponses.

Au cours de la même période, nous avons reçu 29 demandes de consultation concernant la nécessité d'effectuer des contrôles préalables et émis 30 avis, en ce qui concerne les mesures administratives visées au règlement (CE) nº 45/2001, nous avons reçu 20 demandes de consultation et rendu 21 avis.

Bien que certaines demandes de consultation nous soient parvenues avant le 10 décembre 2018, nous y avons répondu après cette date. Cela explique la disparité entre le nombre de demandes de consultation reçues et le nombre de réponses.

Réclamations

L'une des principales fonctions du CEPD consiste à recevoir et à traiter les réclamations ainsi qu'à mener des enquêtes. Cette obligation reste inchangée, que ce soit au titre du règlement (CE) nº 45/2001 ou du nouveau règlement (UE) 2018/1725. Toute personne ayant le sentiment qu'une institution de l'Union n'a pas respecté ses droits en matière de protection des données peut déposer une réclamation auprès du CEPD.

Entre 2015 et 2018, nous avons reçu 748 réclamations portant sur diverses questions de protection des données ; 573 d'entre elles

Thèmes de contrôles préalables, de consultations et de réclamations au titre du règlement (CE) nº 45/2001

Les institutions de l'UE traitent des données à caractère personnel pour diverses raisons. Voici quelques exemples de thèmes de contrôles préalables, de consultations et de réclamations que nous avons reçus au titre du règlement (CE) nº 45/2001.

Contrôles préalables

Conformément au règlement (CE) nº 45/2001, tous les traitements effectués par les institutions de l'UE et susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées sont soumis au contrôle préalable du CEPD. Par exemple:

- la surveillance des médias sociaux par une institution de l'UE
- les recherches menées sur certains problèmes médicaux par une institution de l'UE
- une campagne en faveur de la non-discrimination lancée par une institution de l'UE
- la dénonciation des dysfonctionnements dans les institutions de l'UE
- les mesures de vigilance concernant le blanchiment d'argent et le financement du terrorisme
- Confluence – un espace de collaboration pour l'échange d'informations sur la situation administrative des assistants parlementaires accrédités
- le répertoire aéromédical européen

Consultations

Dans certains cas, le règlement (CE) nº 45/2001 impose aux institutions de l'UE de consulter le CEPD de manière formelle ou informelle au sujet des traitements prévus. Par exemple:

- la divulgation de données à caractère personnel par des travailleurs sociaux dans les institutions de l'UE
- les conditions de partage des données au sein d'un syndicat d'une institution de l'UE
- le traitement de données à caractère personnel par une autorité nationale au moyen d'un outil en ligne fourni par une institution de l'UE
- les activités d'enquête menées par les institutions de l'UE, notamment dans les domaines de la lutte contre la fraude, de la concurrence et du commerce
- l'alignement des clauses contractuelles dans les marchés de service sur les conditions énoncées dans le RGPD

Réclamations

Le règlement (CE) nº 45/2001 exige que le CEPD examine les réclamations relatives au traitement illicite de données à caractère personnel par les institutions de l'UE. Exemples de réclamations reçues:

- la procédure d'inscription à une conférence internationale organisée par une institution de l'UE
- le respect de la vie privée et la protection des données à caractère personnel sur les sites web de certaines institutions et organes de l'UE
- la publication du nom d'un candidat ayant réussi un concours de l'Office européen de sélection du personnel (EPSO) pour devenir fonctionnaire européen
- une violation du caractère privé de la correspondance d'un membre du personnel de l'UE par son employeur
- le traitement de données médicales dans le cadre de procédures disciplinaires et la communication de telles données à des tiers
- le traitement de données d'entreprises permettant d'identifier une personne
- une violation possible du principe de minimisation des données par une des agences exécutives de l'UE
- l'accès aux données dans le cadre d'une procédure de recrutement d'un organe de l'UE

Illustration 11. Exemples de contrôles préalables, de consultations et de réclamations au titre du règlement (CE) nº 45/2001

ont été rejetées comme irrecevables. La plupart de ces plaintes concernaient le traitement de données au niveau national plutôt que le traitement de données par une institution ou un organe de l'UE.

Au cours de cette période, nous avons donc reçu 175 réclamations recevables et rendu 134 décisions. L'objet de ces réclamations variait d'une année à l'autre. Citons notamment la limitation des droits des personnes, la confidentialité et la sécurité du traitement des données, le droit d'accès aux données à caractère personnel, le recrutement et le transfert de données (voir illustration 12).

Inspections et visites

Les inspections et les visites sont deux instruments qui permettent au CEPD de surveiller les institutions de l'Union et de veiller à ce qu'elles respectent les règles en matière de protection des données. Les visites peuvent également contribuer à sensibiliser aux questions relatives à la protection des données au sein des institutions de l'Union.

Entre 2015 et juin 2019, nous avons effectué 29 inspections et 22 visites visant à vérifier le respect des règles et leurs responsabilités de plusieurs institutions et organes de l'UE. Les inspections ont servi à la fois à garantir le respect du règlement (CE) nº 45/2001 et, dans le cadre de la préparation des nouvelles règles en matière de protection des données, à s'assurer que les institutions de l'UE disposaient des outils adéquats pour mettre en œuvre une approche en matière de protection des données fondée sur la responsabilisation. Nous communiquons les résultats de nos inspections aux institutions concernées et nous assurons un suivi en temps utile pour veiller à ce que nos recommandations soient mises en œuvre.

Dans le cadre des visites visant à vérifier le respect des règles, nous collaborons avec l'institution de l'Union concernée pour établir une feuille de route de conformité. Nous assurons le suivi de ces visites à une date ultérieure pour vérifier que cette feuille de route a été mise en œuvre de manière efficace. Les visites visant à vérifier la responsabilisation de l'institution ou de l'organe de l'UE concerné avaient pour objectif de préparer leur transition vers le nouveau règlement.

Parmi les responsabilités qui nous incombent en matière de surveillance, nous sommes chargés de mener des inspections périodiques des bases

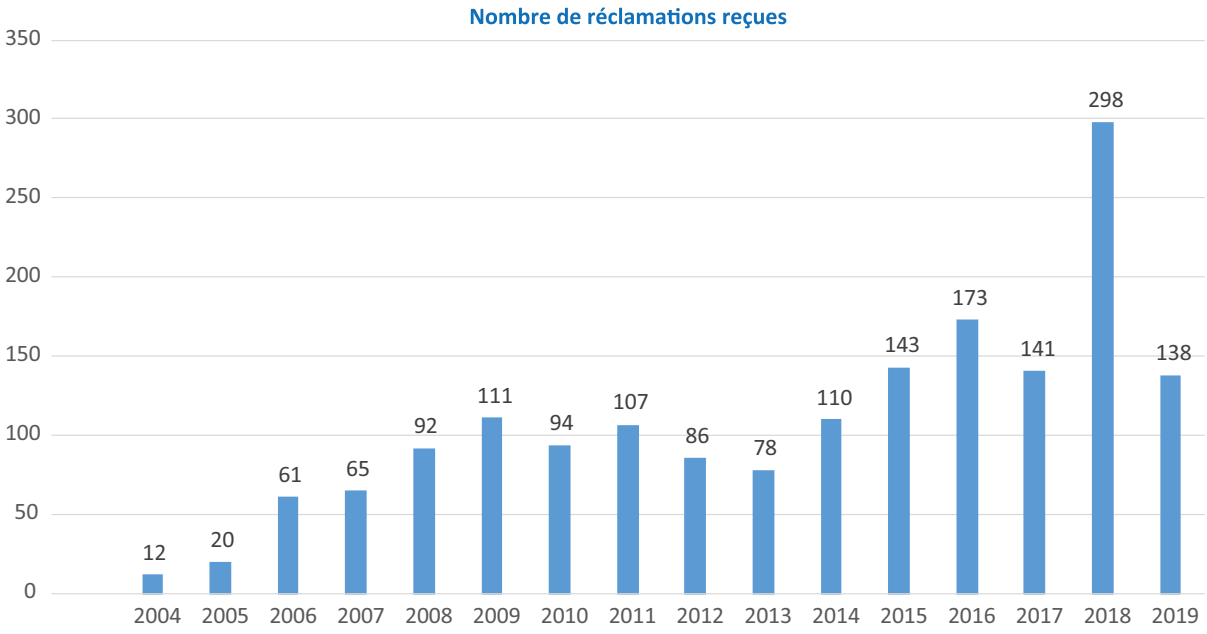


Illustration 12. Évolution du nombre de réclamations reçues par le CEPD, y compris de réclamations irrecevables (jusqu'au 31 août 2019)

de données centrales des systèmes d'information à grande échelle de l'UE (voir section 5.3.1). Ces inspections portent principalement sur la sécurité et la gestion des systèmes ; les autorités nationales sont responsables de l'exactitude des données saisies dans ces systèmes. Ces inspections nous permettent de contrôler le respect de la protection des données, mais également de travailler directement avec l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) pour valider leur responsabilisation dans le cadre de la gestion de ces bases de données.

Les inspections et les visites se poursuivent au titre du règlement (UE) 2018/1725, l'accent étant davantage mis sur la promotion et la garantie d'une approche en matière de protection des données fondée sur une responsabilisation accrue. Cela implique non seulement de respecter les règles en matière de protection des données, mais aussi d'être en mesure d'en apporter la preuve.

L'enquête de printemps

En 2015 et 2017, nous avons mené notre enquête de printemps. Il s'agit d'un examen périodique des progrès accomplis par l'ensemble des institutions et organes de l'UE concernant la mise en œuvre des règles de l'UE en matière de protection des données. Cette enquête nous permet de recenser les problèmes et de prendre des mesures pour y remédier.

Dans le cadre de chaque enquête, nous ciblons également certains thèmes bien précis sur lesquels nous mènerons des études. Il s'agit de thèmes jugés particulièrement pertinents pour l'activité des institutions de l'Union. En 2015, nous avons mis l'accent sur les transferts internationaux de données à caractère personnel, les mesures de sécurité de l'information, la suppression effective des données à caractère personnel et la relation entre les institutions et leurs DPD. En 2017, nous nous sommes à nouveau penchés sur les transferts internationaux de données, à la lumière des dernières évolutions dans ce domaine (voir section 5.2.3), et nous nous sommes également intéressés à la collecte de documents d'identification par les institutions de l'UE ainsi qu'aux besoins spécifiques en matière de formation recensés par les institutions de l'UE pour s'assurer d'être préparées à l'introduction du règlement (UE) 2018/1725.

Les résultats des deux enquêtes montrent que des progrès réguliers continuent d'être enregistrés en ce qui concerne le respect des règles. Les enquêtes nous fournissent des informations précieuses qui nous permettent de dégager des tendances et de mieux planifier nos activités de supervision et de contrôle de l'application des règles.

Coopération avec les DPD au titre du règlement (CE) nº 45/2001

Chaque institution de l'UE doit désigner un DPD indépendant ayant pour mission de s'assurer que les règles de protection des données sont appliquées au sein de l'institution. Ces DPD rencontrent le CEPD deux fois par an, dans le cadre des réunions du réseau des DPD (voir illustration 13). Ces réunions servent à renforcer la coopération entre les DPD et à garantir que les institutions de l'UE disposent des outils nécessaires pour montrer l'exemple en matière d'application de la législation sur la protection des données.

Entre 2015 et le 11 décembre 2018, lorsque les nouvelles règles en matière de protection des données destinées aux institutions de l'UE sont entrées en vigueur, les DPD ont rencontré le CEPD à sept reprises, chaque réunion ayant été organisée par une institution, un organe ou une agence de l'UE distinct. La première de ces réunions se déroulant dans le cadre du nouveau mandat a été organisée par le Fonds européen d'investissement, au Luxembourg. Inspirés par la stratégie du CEPD, nous avons profité de cette occasion pour lancer une nouvelle approche innovante ayant pour but de rendre ces réunions plus dynamiques, interactives et efficaces grâce à des études de cas pratiques et des ateliers interactifs.

Convaincus que la responsabilisation serait une composante clé des nouvelles règles de protection des données destinées aux institutions de l'UE, nous nous sommes efforcés d'aider les

Réunions DPD-CEPD 2015-2019

2015

Afin d'aider les institutions de l'UE à passer d'une conception de la protection des données fondée uniquement sur le respect des règles à une démarche axée sur la responsabilité, nous avons lancé en 2015 une approche nouvelle et innovante des réunions DPD-CEPD, qui recourt à des ateliers interactifs.

37e réunion – 8 mai, Fonds européen d'investissement (FEI), Luxembourg
Thèmes de discussion: lignes directrices du CEPD sur les dispositifs mobiles, la responsabilité, la sécurité des opérations de traitement des données, le rôle du DPD dans le traitement des plaintes

38e réunion – 5 novembre, Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), Athènes
Thèmes de discussion: traitement des plaintes portant sur des aspects juridiques et informatiques, lignes directrices du CEPD sur les questions disciplinaires, lien entre la sécurité de l'information et la protection des données

2016

Les réunions de 2016 ont suivi le même format que celui introduit l'année précédente. Diverses lignes directrices du CEPD ont inspiré de nombreuses activités et ont permis de mettre en pratique ces orientations en les appliquant à des études de cas.

39e réunion – 28 avril, Eurofound, Dublin
Thèmes de discussion: lignes directrices du CEPD en matière de communications électroniques, évaluations du personnel, dénonciation des dysfonctionnements, informatique en nuage

40e réunion – 27 octobre, Office de l'Union européenne pour la propriété intellectuelle (EUIPO), Alicante
Thèmes de discussion: droit d'accès aux données à caractère personnel, lignes directrices du CEPD sur les applications mobiles et les services web, analyses d'impact relatives à la protection des données (AIPD)

2017

En janvier 2017, une proposition de nouvelles règles en matière de protection des données pour les institutions de l'UE a été publiée. Les implications de ces nouvelles règles étant désormais plus claires, les réunions de 2017 visaient à fournir aux DPD les connaissances et les outils nécessaires pour montrer l'exemple en ce qui concerne leur application.

41e réunion – 1er juin, Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), Tallinn
Thèmes de discussion: AIPD, responsabilité, droits des personnes au titre des nouvelles règles de protection des données de l'UE

42e réunion – 13 octobre, Agence européenne des médicaments (EMA), Londres
Thèmes de discussion: AIPD, responsabilité, notifications de violation de données à caractère personnel

2018

Une semaine à peine avant notre première réunion de l'année, un accord politique sur les nouvelles règles de protection des données dans les institutions de l'UE a été conclu. Ces règles devant s'appliquer à partir de la fin 2018, notre première réunion visait à garantir que les institutions de l'UE étaient prêtes à les mettre en pratique. La seconde réunion, tenue le lendemain de l'entrée en vigueur de ces nouvelles règles, a permis aux DPD de réfléchir aux nouveaux défis qui les attendaient.

43e réunion – 31 mai, CEPD, Bruxelles
Thèmes de discussion: surveillance des médias sociaux, registre de protection des données, AIPD, gouvernance informatique

44e réunion – 12 décembre, Parlement européen et CEPD, Bruxelles
Thèmes de discussion: règles internes, procédure de notification de violations de données à caractère personnel, contrôle conjoint, protection des données à caractère personnel traitées par les services web des institutions de l'UE

2019

Les nouvelles règles étant désormais en vigueur, les réunions de 2019 nous ont permis de faire le point sur les difficultés rencontrées par les DPD dans leur application et de trouver les moyens de les surmonter.

45e réunion – 17 mai, Autorité européenne des assurances et des pensions professionnelles (AEAPP), Francfort
Thèmes de discussion: organisation d'événements, notifications de violations de données à caractère personnel, responsabilité conjointe du traitement, passation de marchés, obligations du responsable du traitement et du sous-traitant

46e réunion – 7 novembre, Archives historiques de l'Union européenne (AHUE), Florence
Thèmes de discussion: jurisprudence récente, archives, contrats avec des fournisseurs de logiciels

Illustration 13. Réunions CEPD-DPD 2015-2019

institutions de l'Union à ne pas se limiter à une approche purement fondée sur le respect des règles, mais à adopter une approche privilégiant la démonstration de cette conformité. À mesure que les nouvelles règles se faisaient plus précises, nous avons pu organiser nos réunions avec les DPD pour qu'ils disposent de l'ensemble des connaissances et des outils nécessaires à leur préparation. Parmi les sujets des exercices pratiques conçus pour aider les DPD à acquérir une expérience concrète leur permettant d'affronter les défis potentiels, citons notamment les réseaux sociaux, le microciblage, les analyses d'impact relatives à la protection des données, la gouvernance informatique, les droits des personnes et les notifications en cas de violation de données.

Pour apporter un soutien supplémentaire aux DPD dans leur préparation en vue de l'introduction des nouvelles règles, le 30 septembre 2018, nous avons publié une version actualisée de notre document de référence sur le rôle joué par les délégués à la protection des données au sein des institutions de l'UE. Ce document explique la relation qui unit les DPD et le CEPD et fournit des orientations quant au profil des DPD et aux ressources dont ils doivent disposer pour mener à bien leur mission.

Lignes directrices thématiques

Le CEPD publie des lignes directrices thématiques sur plusieurs sujets communs à la plupart des institutions de l'UE, tels que le recrutement, les évaluations, l'utilisation du matériel informatique sur le lieu de travail et les procédures disciplinaires. Ces lignes directrices consolident les orientations fournies dans le cadre de nos consultations et avis relatifs aux contrôles préalables, ainsi que les orientations publiées par le GT29 et la jurisprudence des tribunaux européens. Un grand nombre de nos lignes directrices peuvent également servir de source d'inspiration à des organisations autres que les institutions de l'Union, ou compléter les orientations fournies par les APD nationales.

Au cours du mandat, nous avons publié 17 séries de lignes directrices (voir illustration 14). Bien que la grande majorité de ces lignes directrices ait été publiée avant l'entrée en vigueur du règlement (UE) 2018/1725, elles n'en restent pas moins pertinentes aujourd'hui, les principes clés n'ayant pas changé. Les lignes directrices formulées depuis la publication de la proposition devenue par la suite le règlement (UE) 2018/1725 ont été rédigées en ayant à l'esprit les nouvelles règles.

Un grand nombre de lignes directrices portent sur les évolutions technologiques. Tel est le cas des lignes directrices sur la gouvernance informatique et la gestion informatique, sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'UE et sur la protection des données à caractère personnel traitées au moyen des services web fournis par les institutions de l'UE (voir section 6.2.3). Citons également les lignes directrices sur la procédure d'alerte éthique, sur les enquêtes administratives et les procédures disciplinaires et sur les opérations de traitement de documents. (voir illustration 14).

6.2.2 Faciliter la transition vers le règlement (UE) 2018/1725

Le 11 décembre 2018, le règlement (UE) 2018/1725 a remplacé le règlement (CE) nº 45/2001. À l'instar du règlement (CE) nº 45/2001, le règlement (UE) 2018/1725 définit les règles de la protection des données au sein des institutions de l'UE ainsi que le rôle et les prérogatives du CEPD, en les alignant sur les règles établies par le RGPD.

En tant qu'autorité de contrôle de la protection des données pour les institutions de l'Union européenne, le CEPD a vu ses responsabilités s'accroître. Désormais, il doit non seulement veiller à la mise en application des nouvelles règles une fois celles-ci en place, mais aussi aider les institutions de l'UE à se préparer en vue des nouvelles règles.

Assurer la responsabilisation sur le terrain

Tant le RGPD que le règlement (UE) 2018/1725 soulignent l'importance de la responsabilisation, l'idée étant que le responsable du traitement des données, l'organisation chargée de traiter les données à caractère personnel, doit non seulement respecter les règles en matière de protection des données, mais aussi être en mesure d'apporter la preuve qu'il les applique.

Lignes directrices du CEPD 2015-2019

Les lignes directrices du CEPD abordent une série de sujets communs à de nombreuses institutions de l'UE. Elles fournissent aux membres du personnel de l'UE des conseils pratiques leur indiquant comment garantir le respect des règles en matière de protection des données.

Décembre 2019 - Proportionnalité des mesures limitant les droits fondamentaux à la protection des données et de la vie privée

Les décideurs politiques doivent être capables de démontrer que toute proposition de mesure qui limiterait les droits fondamentaux est proportionnelle, compte tenu des objectifs stratégiques et de la finalité de l'opération de traitement de données proposée. Ces lignes directrices aident les décideurs politiques à évaluer la proportionnalité de toute nouvelle mesure et à adapter leur proposition en conséquence.

17 juillet 2019 - Liste des analyses d'impact relatives à la protection des données

Des analyses d'impact relatives à la protection des données ont été introduites à la fois dans le cadre du RGPD et du règlement (UE) 2018/1725 pour que les institutions de l'UE veillent à ce que les responsables du traitement tiennent dûment compte des risques liés au respect de la vie privée et à la protection des données lors de certaines opérations de traitement à haut risque. La liste des analyses d'impact relatives à la protection des données du CEPD peut êtreutilisée afin de déterminer les cas dans lesquels la réalisation d'une analyse d'impact relative à la protection des données est nécessaire.

20 décembre 2018 - Article 25 du règlement (UE) 2018/1725

La limitation des droits en matière de protection des données n'est possible qu'en cas de circonstances exceptionnelles. Toute limitation doit être fondée sur un acte juridique ou sur des règles internes. Nos lignes directrices mettent l'accent sur les conditions dans lesquelles des règles internes peuvent être utilisées pour limiter les droits en matière de protection des données, sur la manière de rédiger des règles internes et sur la manière d'interpréter et d'appliquer en pratique des limitations.

23 mars 2018 - Gouvernance informatique et gestion informatique

Conformément au RGPD, les organisations chargées du traitement des données à caractère personnel doivent veiller à mettre en place des politiques efficaces en matière de gestion des risques afin de protéger les libertés et les droits fondamentaux des personnes concernées. Cela inclut la gestion des risques liés à la sécurité informatique, abordés dans ces lignes directrices.

Novembre 2019 - Notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement

Les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement désignent différents rôles que les entités peuvent assumer lors d'opérations de traitement spécifiques. Nos lignes directrices servent d'appui aux institutions et aux organes de l'UE pour cibler leur rôle et déterminer leurs responsabilités ainsi que les mesures à prendre pour garantir les meilleures pratiques en matière de protection des données.

16 juillet 2019 - Responsabilité sur le terrain

Tant le RGPD que le règlement (UE) 2018/1725 soulignent l'importance du principe de responsabilité. Celui-ci prévoit que non seulement les organisations doivent respecter les règles en matière de protection des données, mais qu'elles doivent également être en mesure de démontrer que celles-ci sont respectées. Ce guide est conçu pour assurer que les institutions de l'UE mettent en pratique ce principe de responsabilité, en les aidant à documenter correctement leurs activités de traitement des données.

7 décembre 2018 - Notifications des violations de données à caractère personnel

En vertu des nouvelles règles en matière de protection des données, toutes les institutions de l'UE sont tenues de signaler au CEPD certaines violations de données à caractère personnel. Il s'agit de veiller à ce que des mécanismes de prévention et de détection soient mis en place, ainsi que des procédures d'enquête et de rapport interne. Ces lignes directrices fournissent les informations et les conseils pratiques nécessaires pour leur permettre d'agir en conséquence.

16 mars 2018 - L'utilisation des services d'informatique en nuage

L'informatique en nuage est devenue un outil de plus en plus attrayant pour denombreuses institutions de l'UE, mais elle soulève de nombreuses questions complexes en matière de protection des données. Nos lignes directrices fournissent des instructions et des conseils pratiques sur l'évaluation et la gestion des risques liés à la protection des données, au respect de la vie privée et à d'autres droits fondamentaux que présente le traitement de données à caractère personnel effectué par des services d'informatique en nuage.

15 janvier 2018 - Obligations et droits en matière de transparence

Tous les membres du personnel des institutions de l'UE chargés du traitement des données à caractère personnel pour le compte de leur institution doivent appliquer les nouvelles règles en matière de protection des données. Ces lignes directrices les aident à s'initier au respect de leurs nouvelles obligations, en mettant l'accent sur la manière de fournir des informations transparentes sous la forme d'une déclaration relative à la protection des données.

18 novembre 2016 - Enquêtes administratives et procédures disciplinaires

L'ensemble du personnel de l'UE doit se conformer au statut des fonctionnaires. Toutefois, bien que ce statut permette de repérer des cas d'infraction aux règles, il ne précise pas comment les institutions de l'UE doivent gérer les contrevenants. Nos lignes directrices abordent cette problématique, en proposant aux institutions de l'UE un cadre pour mener des enquêtes administratives et des procédures disciplinaires conformément aux règles en matière de protection des données.

7 novembre 2016 - Services sur le web

Les institutions de l'UE et les autres organisations ont de plus en plus recours aux outils en ligne pour communiquer et interagir avec les citoyens. Les transactions en ligne étant de plus en plus complexes, des politiques efficaces en matière de protection des données sont nécessaires pour protéger les droits des utilisateurs. Cet aspect est particulièrement important en ce qui concerne les cookies, le suivi en ligne, la sécurité et les transferts de données à caractère personnel, comme le démontrent ces lignes directrices.

17 décembre 2015 - Dispositifs mobiles

Les dispositifs mobiles étant de plus en plus utilisés dans les activités quotidiennes des institutions de l'UE et d'autres organisations, nous avons publié des lignes directrices contenant des conseils pratiques sur l'intégration de principes relatifs à la protection des données dans la gestion des dispositifs mobiles sur le lieu de travail.

11 avril 2017 - Guide pour l'évaluation de la nécessité

Dans le cadre de notre engagement à faciliter l'élaboration responsable et éclairée de politiques, le CEPD a publié un guide pour l'évaluation de la nécessité. Le guide est conçu pour aider les décideurs politiques à mesurer l'effet des nouvelles règles sur le droit fondamental à la protection des données et à déterminer les cas dans lesquels la limitation de ces droits est réellement nécessaire.

7 novembre 2016 - Applications mobiles

La plupart des applications mobiles sont conçues pour interagir de manière spécifique avec un large éventail de ressources en ligne et pour échanger des informations avec d'autres dispositifs connectés. Cette interaction entraîne souvent la collecte d'une quantité importante de données à caractère personnel. Dans nos lignes directrices, nous fournissons des conseils sur les manières de garantir que les applications mobiles traitent ces données en respectant la vie privée.

18 juillet 2016 - Procédures d'alerte éthique

La confidentialité est le moyen le plus efficace pour inciter le personnel à signaler des actes répréhensibles sur le lieu de travail. Nos conseils sur les procédures d'alerte éthique visent à garantir que les institutions de l'UE soient en mesure de proposer des filières sûres permettant au personnel de l'UE ou aux autres informateurs de signaler des fraudes, des cas de corruption ou d'autres manquements graves survenus au sein des organisations.

21 mars 2016 - Mesures de sécurité pour le traitement de données à caractère personnel

Plusieurs organisations doivent faire face à différents risques de sécurité liés aux informations qu'elles utilisent. Nos lignes directrices fournissent aux institutions de l'UE des conseils sur la manière de créer et de maintenir un environnement numérique sûr et fiable pour les informations qui sont essentielles au fonctionnement de leurs services.

16 December 2015 - Communications électroniques

Dans la plupart des organisations, y compris les institutions de l'UE, les communications électroniques sont désormais incontournables. Ces lignes directrices du CEPD fournissent aux institutions de l'UE des instructions et des conseils pratiques sur le traitement des données à caractère personnel par les outils de communication électronique, pour s'assurer qu'elles respectent la législation applicable en matière de protection des données.

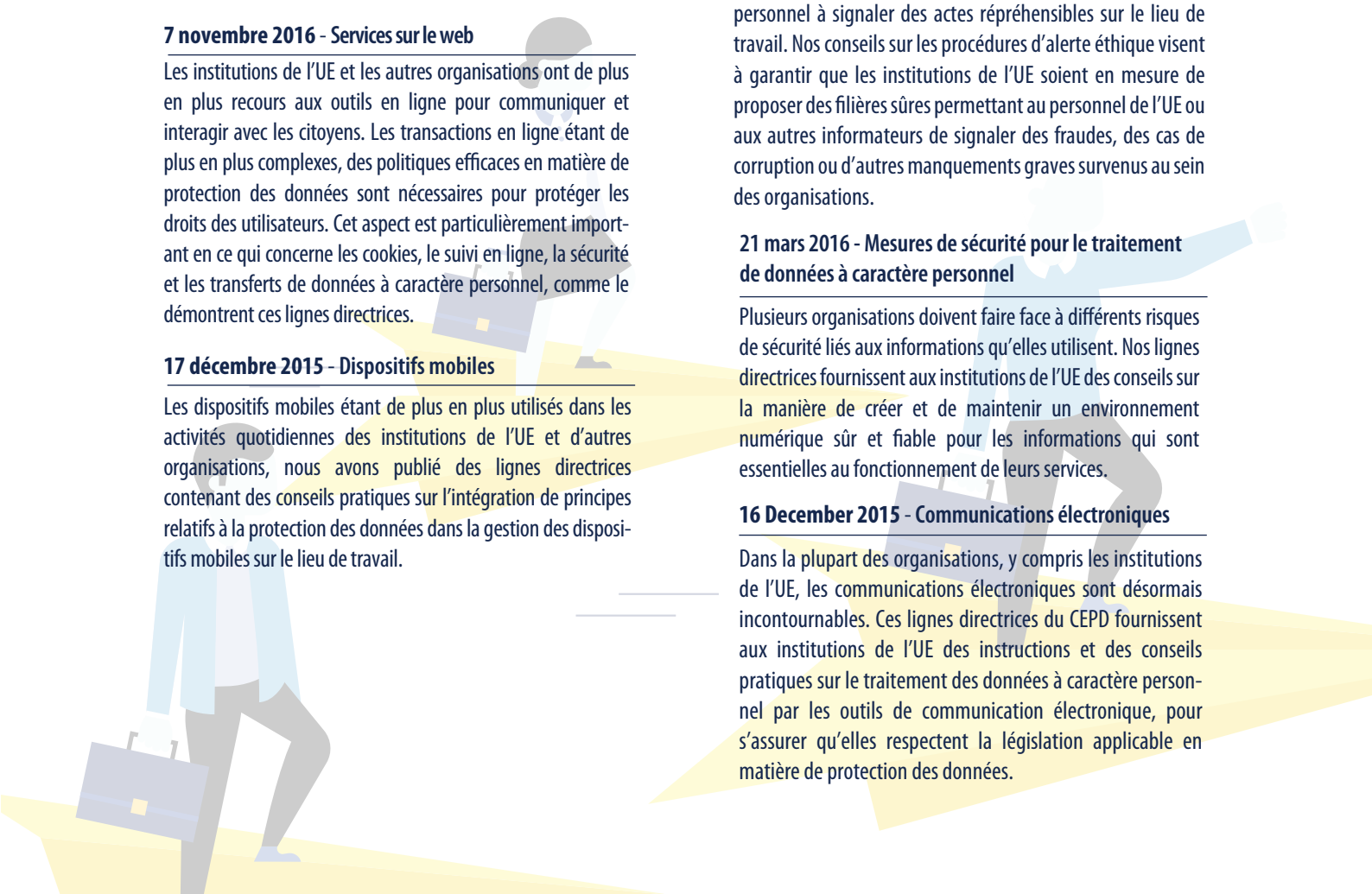


Illustration 14. Lignes directrices du CEPD

Pour que la responsabilisation devienne une réalité, l'ensemble des institutions de l'UE, à l'instar des autres organisations actives dans l'Union, doivent veiller à documenter de manière adéquate leurs activités de traitement des données. Pour les aider dans cette tâche, nous avons créé une boîte à outils concernant la responsabilisation sur le terrain.

Une première version de cette boîte à outils a été publiée en février 2018 afin d'aider les institutions de l'UE à se préparer à l'introduction des nouvelles règles. Nous l'avons actualisée pour qu'elle corresponde précisément à la version définitive du règlement (UE) 2018/1725 et, depuis lors, nous avons amélioré le texte à plusieurs reprises. La dernière version en date a été publiée le 16 juillet 2019. Elle contient des orientations quant à la manière de documenter le traitement de données au moyen de ce que l'on appelle un registre des activités de traitement et elle établit les critères permettant de déterminer s'il convient d'effectuer une analyse d'impact relative à la protection des données.

Cette boîte à outils complète les travaux que nous avons menés avec les DPD sur la responsabilisation, ainsi que les sessions de formation et les visites effectuées au cours du mandat.

Le règlement (UE) 2018/1725, à l'instar du RGPD, a introduit des changements significatifs en ce qui concerne notamment les règles régissant la sous-traitance du traitement des données à caractère personnel. En vertu des nouvelles règles, il incombe directement aux prestataires de garantir le respect des règles.

Cependant, lorsqu'elles s'en remettent à des tiers pour fournir des services, les institutions de l'UE, comme n'importe quel autre responsable du traitement des données, restent responsables du traitement des données effectué pour leur compte. Il incombe au responsable du traitement de ne choisir que des prestataires qui satisfont aux exigences de la législation applicable en matière de protection des données.

Pour aider les institutions de l'UE dans cette tâche, le CEPD a adopté des clauses contractuelles types pour les sous-traitants en décembre 2018. Ces clauses fixent les exigences minimales pour les institutions de l'UE en ce qui concerne la sous-traitance du traitement des données à caractère personnel.

Sessions de formation et visites de contrôle du principe de responsabilité

En 2017 et 2018, en prévision du règlement (UE) 2018/1725, nous avons travaillé en étroite collaboration avec les DPD et d'autres représentants de l'ensemble des institutions, organes et agences de l'Union pour veiller à ce qu'ils soient préparés. Nous avons notamment organisé des ateliers interactifs dans le cadre de nos deux réunions annuelles avec les DPD (voir sections 6.2.1 et 6.2.2), ainsi que des visites de contrôle du principe de responsabilité, des sessions de formation et des conférences. Nous voulions nous assurer que l'ensemble du personnel de l'UE intervenant dans le traitement de données à caractère personnel, quelle que soit sa position dans la hiérarchie, ait connaissance des nouvelles règles et de leurs conséquences.

Nous avons intensifié notre campagne de sensibilisation en 2018, pour que les institutions de l'Union européenne disposent des connaissances et des outils nécessaires pour appliquer aisément les nouvelles règles après leur entrée en vigueur à la fin de cette même année. La campagne a mis particulièrement l'accent sur l'importance de la responsabilité, sur l'idée que les institutions européennes doivent non seulement respecter les règles en matière de protection des données, mais aussi apporter la preuve qu'elles appliquent ces règles.

Notre programme de sessions de formation et de visites était l'un des éléments clés de notre campagne de sensibilisation. Conçu pour renforcer nos lignes directrices écrites (voir section 6.2.1), ce programme prévoyait une visite auprès des institutions et des organes de l'UE à Luxembourg effectuée par Wojciech Wiewiórowski, le contrôleur adjoint, des sessions de formation pour les institutions de l'Union à Luxembourg et pour le personnel des agences de l'UE à Athènes, un échange avec les chargés de communication des institutions de l'UE et une session de formation pour le personnel des agences de l'UE en Italie, ainsi que de nombreuses réunions bilatérales et autres avec les instances dirigeantes des institutions de l'UE.

Nous avons poursuivi les visites et les sessions de formation en 2019. Depuis l'entrée en vigueur des nouvelles règles, il est plus important que jamais de veiller à ce que tous les membres du personnel de l'UE chargés du traitement de données à caractère personnel soient conscients de leurs nouvelles obligations et qu'ils sachent comment les remplir. L'organisation d'une session de formation sur la passation des marchés publics pour les fonctionnaires de la direction générale des finances du Parlement européen chargés d'examiner les dossiers et la possibilité de collaborer avec la direction générale des ressources humaines de la Commission européenne (DG HR), l'un des secteurs les plus touchés par les nouvelles règles, illustrent bien les efforts que nous déployons sans relâche pour faciliter la transition vers les nouvelles règles.

@EU_EDPS

#EDPS training on new #dataprotection regulation for #EUinstitutions addressed to high-level management at @Europarl_EN - @W_Wiewiorowski stresses the importance of #transparency of operations and #accountability in the heart of #EU #democracy

Coopération avec les DPD au titre du règlement (UE) 2018/1725

Le 12 décembre 2018, le lendemain de l'entrée en vigueur du règlement (UE) 2018/1725, les DPD se sont réunis à Bruxelles à l'occasion de la 44e réunion CEPD-DPD (voir illustration 13). Cette réunion nous a fourni l'occasion d'examiner ensemble les défis que la nouvelle législation pose au CEPD et aux DPD.

Le programme de la journée était organisé autour d'une série d'études de cas visant à doter les DPD d'une expérience concrète quant à la manière d'aborder certains de ces défis. Parmi ces défis, citons notamment la limitation des droits des personnes, les notifications en cas de violation de données et la notion de responsable conjoint. Notre objectif était d'encourager les DPD à considérer les règles comme un outil de référence quant à la manière de garantir le respect des droits des personnes, plutôt que comme un fardeau.

Une réunion supplémentaire a eu lieu en mai 2019. Cette réunion nous a permis de dresser le bilan des défis auxquels les DPD sont confrontés lorsqu'ils appliquent les nouvelles règles et de réfléchir à la manière de les relever. Lors de cette réunion, nous avons également présenté aux DPD notre stratégie de suivi de la mise en œuvre du règlement (UE) 2018/1725.

Depuis l'entrée en vigueur des nouvelles règles, il est plus important que jamais de coopérer de manière constructive avec les DPD si nous voulons que les institutions de l'UE puissent montrer l'exemple en matière de protection des données.

@EU_EDPS

.@W_Wiewiorowski stressed the essential role of the #DPO network is ensuring the protection of fundamental rights of individuals. It's about people, not #data. As a result of their close cooperation with the controllers, they will prevent sanctions.

Gestion des connaissances

En 2019, le CEPD a célébré son quinzième anniversaire. Bien des choses ont changé depuis la création de notre petite institution en 2004. Ces dernières années, la nécessité de consolider nos connaissances et de travailler en un seul lieu facilement accessible, pour ne pas dépendre excessivement de l'expertise individuelle, est devenue de plus en plus manifeste. Cela nous permettrait de renforcer notre position en tant que spécialiste de la protection des données, en particulier quand il s'agit de sensibiliser les institutions de l'Union européenne et d'émettre des conseils sur les risques, les droits et les obligations qui découlent du règlement (UE) 2018/1725.

En 2018, nous avons donc lancé plusieurs activités liées à la gestion des connaissances. Parmi les principales activités, notons la création d'un wiki interne portant sur le nouveau règlement. L'objectif était d'encourager les collègues à partager leurs connaissances à travers la création

Formations CEPD

2018

Bruxelles - 31 janvier

Nous avons démarré l'année par une formation dispensée à Bruxelles à des agents du Médiateur européen (et également accessible, par liaison vidéo, aux agents du Médiateur européen à Strasbourg). Ce cours a été suivi par des chefs d'unités et de secteurs, ainsi que par d'autres membres du personnel concernés.

Bruxelles - 16 février (et au-delà)

Nous avons organisé à l'École européenne d'administrateurs (EUSA) une formation de deux heures destinée aux cadres de l'UE. Ce ne devait pas être la seule ... puisque nous sommes revenus à l'EUSA à six reprises au cours de l'année 2018. Grâce à nos formations, le personnel de l'EUSA est à présent plus à même de négocier les modalités liées à l'application du nouveau règlement 2018/1725.

Lisbonne - 25 mai

Le 25 mai, nous avons célébré l'entrée en vigueur du RGPD avec des collègues de l'Agence européenne pour la sécurité maritime (AESM) et de l'Observatoire européen des drogues et des toxicomanies (OEDT), en leur proposant une formation visant à les préparer à la transition vers le nouveau règlement.

Bruxelles - 7 juin

Juste avant le début de l'été, nous nous sommes rendus avenue de Beaulieu, à Bruxelles, pour y dispenser une formation sur les nouvelles obligations en matière de protection des données, destinée aux agents de la DG CLIMA, de la DG MOVE ainsi qu'aux autres collègues intéressés.

Maastricht - 26 juin

Le 26 juin, puis à nouveau le 3 décembre, le chef des inspections du CEPD s'est rendu à Maastricht pour présenter le certificat de protection des données de l'IEAP aux participants à la formation. Cette intervention de deux heures avait pour titre «Supervising data protection compliance: the role of data protection authorities» (Surveiller le respect des obligations en matière de protection des données : rôle des autorités de protection des données).

Luxembourg - 30 et 31 janvier

D'autres collègues du CEPD se sont aventurés un peu plus loin, pour proposer deux jours de formation pour des agents des institutions de l'UE en poste au Luxembourg. Plus de 200 personnes du Parlement européen, de la Commission, de la CJUE, de la Cour des comptes, de la BEI, du CDT, du FEI et de la CHAFEA ont suivi cette formation managériale de haut niveau.

Athènes - 1er et 2 mars

Cette formation de deux jours, destinée au personnel de l'ENISA et du Cedefop, a permis de réaffirmer les obligations actuelles en matière de traitement des données et de présenter les nouvelles obligations conformément au nouveau règlement. Nous avons par ailleurs démarré une étude de cas sur la gestion des événements, qui s'est révélée si utile qu'elle a été réutilisée pour d'autres sessions de formation tout au long de l'année.

Bruxelles - 29 mai

Quatre jours seulement après l'entrée en vigueur du règlement général sur la protection des données (RGPD), le CEPD a accueilli 23 délégués à la protection des données (DPD) et DPD adjoints récemment désignés, issus des institutions et organes de l'UE, à une formation sur la protection efficace des données à caractère personnel à assurer dans le cadre de leur nouveau rôle. Une seconde formation, similaire à la première et destinée aux DPD, a été dispensée le 10 décembre.

Bruxelles - 14 juin

Nous avons présenté un webinaire à l'Office des publications de l'UE ainsi qu'à d'autres membres de l'IUE en charge des publications, de la communication, des médias sociaux et du web. Mais notre action ne s'est pas arrêtée là : le même jour, nous avons organisé une formation pour le Service européen pour l'action extérieure (SEAE).

Luxembourg - 1er et 2 octobre

Répondant à une invitation de la Cour de justice de l'UE (CJUE), nous sommes revenus à Luxembourg pour y dispenser une formation sur le nouveau règlement. Plus de 400 personnes, issues de diverses institutions de l'UE, y ont assisté.

Stockholm - 18 septembre

Nous avons dispensé une formation lors de la réunion annuelle des responsables web des agences et organes de l'UE. Ce fut là une magnifique occasion de procéder à des échanges directs avec des responsables de la communication de l'UE sur des questions relatives à la protection des données.

Bruxelles - 7 novembre

Nous avons dispensé une formation sur la protection des données destinée à la DG FISMA (service de la Commission chargé de la politique de l'UE dans les secteurs bancaire et financier), qui portait sur les éléments de base en matière de protection des données, les droits des personnes concernées, et comportait une étude de cas sur la gestion des événements.

Bruxelles - 20 novembre

Juste à la veille de la publication du règlement (UE) 2018/1725, le personnel de l'Autorité de surveillance de l'AELE a bénéficié de la dernière formation organisée en 2018.

Paris - 26 novembre

En cette fin d'année, le CEPD s'est rendu à Paris pour effectuer une visite de contrôle à l'Institut d'études de sécurité de l'Union européenne. L'équipe S&E a dispensé une formation sur le nouveau règlement, en présence du contrôleur adjoint Wojciech Wiewiórowski.

Bruxelles - 23 octobre

La Commission européenne et les autorités nationales de la concurrence de tous les États membres de l'UE coopèrent dans le cadre du Réseau européen de la concurrence (REC). En octobre, nous nous sommes rendus à la DG COMP afin de présenter au Réseau européen de la concurrence les règles de protection des données applicables dans le cadre d'enquêtes ou d'inspections.

Turin - 20 et 21 septembre

Répondant à une demande de la Fondation européenne pour la formation (ETF), nous avons examiné des études de cas sur la protection des données avec un large éventail de collègues, notamment des participants de l'ETF, de l'Autorité européenne de sécurité des aliments (EFSA), du Centre commun de recherche (JRC) et de l'Institut universitaire européen (IUE).

Francfort - 12 novembre

Mi-novembre, nous étions en Allemagne pour dispenser une formation sur les modalités de la protection des données dans le cadre de la surveillance bancaire, organisée en coopération avec le délégué à la protection des données de la Banque centrale européenne (BCE) et le secteur privé (Union Investment), à l'intention du personnel de la BCE et du personnel de l'Autorité européenne des assurances et des pensions professionnelles (AEAPP) à Francfort.

Bruxelles - 21 novembre

Le 21 novembre, le CEPD a fait une présentation devant le comité pour la sûreté de l'aviation civile, à la DG MOVE.

Bruxelles - 3 décembre

Les dernières formations de l'année ont eu lieu là où les premières s'étaient déroulées, à savoir à Bruxelles, lieu d'implantation du CEPD. Nous avons dispensé des formations à la DG COMM et à d'autres représentations de la Commission européenne sur la manière dont le nouveau règlement pourrait affecter les événements qu'elles organisent.

d'une version annotée de la nouvelle législation, pour nous aider à appliquer une approche cohérente en matière de supervision et de mise en application de la protection des données au sein des institutions de l'UE.

Pour tirer parti de cette approche collaborative, nous avons organisé des ateliers internes pour permettre aux collègues de partager leurs compétences et connaissances spécifiques ainsi que pour discuter des nouveaux concepts et de la jurisprudence importante. Grâce à ces ateliers, nous nous tenons informés des dernières évolutions susceptibles d'avoir une incidence sur notre travail de supervision. Ces ateliers devraient également nous aider à sensibiliser le public aux risques que certaines technologies nouvelles font peser sur les droits et les libertés des personnes et sur la société et à promouvoir leur compréhension. Une série d'ateliers a, par exemple, mis l'accent sur l'éthique numérique. Cela nous a permis de porter notre attention au-delà de nos activités quotidiennes et de mieux comprendre l'incidence des technologies sur la société.

6.2.3 La protection des données à caractère personnel à l'ère numérique

La mise en œuvre des nouvelles règles nécessite que les instances dirigeantes de chaque institution de l'UE donnent le ton en intégrant la protection des données dans les plans de gestion des risques et en veillant à ce que la protection des données soit ancrée dans la culture de leur institution. À l'ère numérique, cet aspect revêt une importance accrue.

Pour aider les institutions de l'Union, nous avons fourni des orientations et des formations sur une série de nouveaux sujets peu familiers pour les institutions de l'UE, tels que la responsabilisation (voir section 6.2.2), l'évaluation des risques, les analyses d'impact relatives à la protection des données et les notifications en cas de violation de données. Par ailleurs, nous avons investi dans l'élaboration d'outils plus sophistiqués pour procéder à l'inspection des systèmes d'information et des sites web ; ces outils nous aident à contrôler plus efficacement l'application des nouvelles règles aux technologies numériques.

Inspection des systèmes d'information et des sites web

En tant qu'autorité de contrôle des institutions de l'Union européenne, il nous incombe notamment de procéder à l'inspection des systèmes d'information à grande échelle de l'UE, mais aussi de contrôler les activités des institutions de l'UE (voir section 6.2.1). Les outils informatiques utilisés par les institutions de l'UE étant de plus en plus pointus et le nombre de systèmes d'information de l'UE étant voué à augmenter, il nous faut, de toute évidence, améliorer notre méthode et renforcer nos capacités d'inspection.

Le *IT Policy Lab* étant désormais opérationnel, nous avons, en juillet 2018, inauguré un programme d'inspections à distance des services web fournis par les institutions de l'Union. Les lignes directrices sur la protection des données à caractère personnel traitées au moyen des services web fournis par les institutions de l'UE ayant été publiées en novembre 2016, les inspections à distance devaient servir d'exercice de suivi.

Pour mener les inspections, nous avons mis au point plusieurs logiciels spécialisés, tels que le *Website Evidence Collector*, qui collecte automatiquement des informations sur le traitement des données à caractère personnel par des sites web, comme l'utilisation de cookies, les pixels invisibles, les éléments de page téléchargés auprès de tiers et la sécurité des connexions cryptées (HTTPS). Cet outil est désormais disponible sur le site web du CEPD. Il a été publié sous une licence logicielle libre, ce qui signifie que toute personne peut le télécharger et l'utiliser (voir section 4.1.2).

Les institutions de l'UE offrant plus de 700 services web, nous avons organisé plusieurs vagues d'inspections. Nous avons divisé les services web en deux ensembles ; la première vague d'inspections a englobé les services susceptibles d'avoir la plus forte incidence sur les utilisateurs de ces services, tandis que la seconde a mis l'accent sur les sites web les plus visités des institutions et des organes de l'UE.

Les résultats de la première vague d'inspections ont montré que plusieurs sites web ne respectaient pas les dispositions du règlement

(UE) 2018/1725 ni celles de la directive relative à la vie privée et aux communications électroniques et qu'ils ne suivaient pas nos lignes directrices sur les services web. Le suivi par des tiers sans consentement préalable, qui s'avère particulièrement problématique lorsque la partie tierce concernée applique un modèle économique fondé sur le profilage et le ciblage comportemental des visiteurs de son site web, figurait parmi les problèmes recensés. Les autres points soulevés concernaient l'utilisation de traqueurs pour l'analyse du trafic web sans le consentement préalable des visiteurs ainsi que la soumission de données à caractère personnel collectées au moyen de formulaires en ligne en l'absence de connexions cryptées.

Les institutions ayant fait l'objet d'une inspection ont réagi rapidement pour remédier aux problèmes que nous avons recensés. Toutes les institutions concernées fournissent désormais des connexions HTTPS sécurisées et ont réduit de façon significative le nombre de traqueurs de tiers qu'elles utilisent. Nous assurerons le suivi des mesures adoptées tout en menant d'autres vagues d'inspections.

Nous continuons d'investir dans le *IT Policy Lab* du CEPD. Une procédure de passation de marchés publics a été lancée en vue d'actualiser les capacités du laboratoire. Cela nous permettra également d'inspecter, à distance, les applications mobiles.

Violations de données à caractère personnel

En vertu du règlement (UE) 2018/1725, il incombe à l'ensemble des institutions et des organes de l'UE de communiquer au CEPD certains types de violations de données à caractère personnel. Dans la mesure du possible, chaque institution de l'UE se doit d'informer le CEPD 72 heures au plus tard après avoir pris connaissance de la violation. Si la violation est susceptible de porter préjudice aux droits et aux libertés des personnes, l'institution de l'Union doit également en informer les personnes concernées dans les plus brefs délais.

En date du 30 septembre 2019, nous avions reçu et évalué 65 notifications de violations de données à caractère personnel au titre du règlement (UE) 2018/1725.

Le 4 avril 2019, nous avons organisé une conférence en partenariat avec l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). Cette conférence avait pour thème l'évaluation des risques en matière de violations de données à caractère personnel. L'attention s'est portée sur les enjeux de l'évaluation des risques, à la lumière des obligations juridiques énoncées dans le RGPD et le règlement (UE) 2018/1725.

L'évaluation des risques est un élément clé de la prévention et de la lutte contre les violations de données à caractère personnel, qui suscitent de manière inhérente beaucoup d'incertitudes. Contrairement à d'autres méthodologies d'évaluation des risques, dans le cas des violations de données à caractère personnel, l'accent est mis sur le risque pour les droits et les libertés des personnes. Tandis que les différentes parties prenantes, autorités de contrôle et organisations publiques et privées utilisent un large éventail de méthodes d'évaluation, nos lignes directrices sur les violations de données visent à simplifier cet exercice en proposant des exemples pratiques à l'intention des institutions de l'UE.

En plus de cette conférence, nous avons travaillé avec la Commission européenne pour organiser plusieurs ateliers ayant pour thème la violation de données. Nous avons créé du matériel de formation spécifique en coopération avec la Commission et nous avons fourni des conseils quant aux questions clés liées aux violations de données à caractère personnel. Deux ateliers ont été organisés, respectivement le 14 et le 21 juin 2019 ; ces ateliers ont rassemblé plus de 100 participants issus de nombreuses directions générales de la Commission européenne.

@EU_EDPS

#EDPS @enisa_eu kick off now their joint conference towards assessing the risk in personal #databreaches #CyberSecurity #GDPR #DataProtection

Informatique dématérialisée

L'informatique dématérialisée recueille une adhésion croissante auprès des institutions de l'UE, car elle leur permet de réduire les coûts et d'augmenter la productivité. Cependant, elle soulève un grand nombre de questions complexes en ce qui concerne la protection des données. C'est la raison pour laquelle le CEPD aborde ce sujet au cours de ses réunions avec les DPD et qu'il y a consacré des lignes directrices.

En 2016, la Commission européenne a lancé le premier appel d'offres interinstitutionnel concernant la fourniture de services informatiques dématérialisés (Cloud I). Dans le cadre de sa stratégie relative à l'informatique en nuage, la direction générale de l'informatique de la Commission européenne (DG DIGIT) a institué un sous-groupe dans son groupe de travail sur l'informatique dématérialisée (CVTF) en vue d'évaluer la sécurité et les contrôles relatifs à la protection des données offerts par les contractants potentiels. Le CEPD a pris part aux travaux de ce sous-groupe, en mettant, si nécessaire, son expertise et ses conseils à la disposition de ce sous-groupe.

Sur la base des résultats et des enseignements tirés de Cloud I, la DG DIGIT a organisé un deuxième appel d'offres pour les produits et services informatiques dématérialisés. Nous avons suivi de près la préparation de cet appel d'offres et nous avons rendu des avis complémentaires pour veiller à ce que les obligations du RGPD, qui incombent notamment aux sous-traitants, soient prises en considération aux niveaux contractuel et opérationnel. Il reste, cependant, de nombreux défis à relever. Nous allons, par conséquent, continuer d'investir nos efforts dans ce sujet majeur, afin que les données à caractère personnel de tous les agents et citoyens de l'UE soient protégées de façon adéquate.

@EU_EDPS

Need to find new ways for applying data protection principles to the latest technologies #bigdata #IoT #cloud computing #eudatap

Autres initiatives en matière d'informatique au sein des institutions de l'UE

Le CEPD participe à plusieurs initiatives visant à promouvoir la coordination et la coopération entre les institutions de l'UE sur des questions liées à l'informatique et à la sécurité informatique. Citons notamment le comité interinstitutionnel pour l'informatique (CII), pour les responsables informatiques des institutions de l'UE, le comité consultatif des agences de l'UE sur les technologies de l'information et de la communication (ICTAC), le sous-groupe «Sécurité» du CII et l'équipe d'intervention en cas d'urgence informatique pour les organes de l'UE (CERT-UE).

Cette coopération permet au CEPD d'accéder directement à la communauté informatique de l'administration de l'Union européenne. Cela signifie que nous sommes informés des évolutions et tendances pertinentes concernant l'infrastructure informatique utilisée par les institutions de l'UE et que nous sommes en mesure de communiquer les évolutions pertinentes en matière de protection des données aux responsables et aux professionnels de l'informatique travaillant au sein des institutions de l'UE.

Avec le soutien du CII et de l'ICTAC, par exemple, le CEPD a pu consulter la communauté informatique au sein des institutions de l'UE au cours de la préparation de directives ayant trait aux questions informatiques, telles que celles sur les services web, les dispositifs mobiles, les applications mobiles, l'informatique en nuage et la gouvernance et la gestion informatiques (voir illustration 14).

6.3 Faciliter l'élaboration responsable et éclairée de politiques

Presque toutes les propositions politiques de l'UE impliquent désormais, sous une forme ou sous une autre, le traitement de données à caractère personnel. Dans un monde où les législateurs doivent répondre rapidement à des problèmes aigus de sécurité publique et se tenir au courant de l'évolution de l'économie numérique ou du commerce international, il

importe plus que jamais de veiller à ce que les nouvelles propositions de l'Union européenne respectent les droits fondamentaux.

Le CEPD s'est toujours efforcé de soutenir et d'assister le législateur de l'UE. Habituellement, les propositions législatives faisaient l'objet de consultations formelles menées au titre de l'article 28 du règlement (CE) nº 45/2001 ; en vertu d'une procédure convenue avec la Commission en 2009, des consultations informelles pouvaient également être organisées. Depuis décembre 2018, les consultations sont couvertes par l'article 42 du règlement (UE) 2018/1725 et, conformément aux articles 56 et 57 dudit règlement, le CEPD a la possibilité de conseiller les autres institutions et organes de l'UE, à leur demande ou de sa propre initiative.

Prenant acte du nombre croissant d'initiatives stratégiques de l'UE impliquant maintenant le traitement de données à caractère personnel, notre stratégie définit plusieurs étapes en vue d'améliorer la qualité et l'efficacité des avis que nous rendons au législateur. Nous avons, notamment, recensé les domaines dans lesquels assistance et conseils étaient particulièrement nécessaires et nous avons amélioré notre collaboration avec la Commission européenne, le Parlement européen et le Conseil.

6.3.1 Cybersécurité : assurer une protection respectueuse de la vie privée contre les cyberattaques

Une enquête Eurobaromètre publiée en septembre 2017 a révélé que, pour 87 % des personnes interrogées, la cybercriminalité est une menace importante pour la sécurité intérieure de l'Union européenne. D'après cette même enquête, l'utilisation abusive des données à caractère personnel est la préoccupation majeure des utilisateurs de l'internet.

Le 13 septembre 2017, la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont proposé un train de mesures visant à accroître la résilience de l'UE face aux cyberattaques. Ce *paquet cybersécurité* faisait spécifiquement mention de la nécessité d'établir, au niveau de l'UE, un système de cyberdissuasion et de droit pénal qui protégerait mieux les personnes, les entreprises et les institutions publiques dans l'UE. La Commission a détaillé quelques-unes de ces initiatives dans son rapport sur la sécurité de l'Union, publié le 18 octobre 2017. Le 15 décembre 2017, nous lui avons soumis des observations formelles sur le train de mesures envisagé, dans lesquelles nous avons exposé nos préoccupations et nos recommandations.

Une stratégie de cybersécurité adéquate est nécessaire pour protéger la vie privée et les données à caractère personnel. Cependant, la prévention est également importante. Si des poursuites efficaces sont nécessaires, il est préférable d'éviter en premier lieu d'être victime de cyberattaques.

C'est dans cette optique que nous avons salué l'engagement pris par la Commission d'éviter d'affaiblir ou de compromettre la solidité du cryptage. Des capacités de cryptage fiables sont essentielles pour les marchés numériques et les sociétés. Elles protègent les données et inspirent confiance quant aux services en ligne et aux outils de cybersécurité.

Lorsque les mêmes outils peuvent être utilisés pour protéger les données à caractère personnel et pour préserver activement la cybersécurité, les organisations doivent respecter à la fois les règles de cybersécurité et les règles de la protection des données. Il est essentiel que la Commission fournisse des orientations appropriées dans le cadre des politiques de certification et de gestion des incidents pour éviter toute confusion ou contradiction.

Nous avons insisté sur le fait que toute mesure supplémentaire visant à lutter contre les cybercriminels doit être élaborée et appliquée dans le respect total des principes de nécessité et de proportionnalité de la protection des données. Nous avons également rappelé à la Commission, comme nous le lui avions déjà fait remarquer, que, si les outils que nous concevons pour combattre les cyberattaques tombent entre de mauvaises mains, ils pourraient être utilisés contre nous. Par conséquent, nous avons exhorté la Commission à prendre cet aspect en considération dans le cadre de tout travail futur sur le paquet cybersécurité (voir section 6.4.4).

6.3.2 Le portail numérique unique : à l'ère numérique, l'Europe doit protéger ses données

Le 1er août 2017, nous avons publié un avis sur la proposition de règlement de la Commission établissant un portail numérique unique et sur le principe de la transmission unique d'informations. Cette proposition prévoit que l'échange de justificatifs pour certaines procédures transfrontalières particulières, comme une demande de reconnaissance de diplôme, se déroule dans le cadre d'un système technique. Ce système permettrait aux autorités nationales d'échanger directement des données, mais uniquement à la demande expresse de la personne concernée.

Nous nous sommes félicités de la proposition de moderniser les services administratifs de l'UE. Cette modernisation contribuerait à améliorer la disponibilité, la qualité et l'accessibilité des informations dans l'UE, en instaurant un système grâce auquel les citoyens ne devraient soumettre certains documents qu'une seule fois, et dans un seul État membre.

Cependant, nous avons recommandé à la Commission de tenir compte de certaines considérations importantes relatives à la protection des données au moment d'affiner le principe « une fois pour toutes ». Nous lui avons notamment suggéré de clarifier davantage certains principes essentiels de la protection des données, comme la base juridique du traitement des données à caractère personnel, la limitation de la finalité et la minimisation des données.

6.3.3 Contenu numérique : la nécessité de renforcer la protection des données et des consommateurs

La proposition de directive de la Commission européenne concernant certains aspects des contrats de fourniture de contenu numérique avait pour objectif d'étendre la protection des consommateurs au contenu numérique, que celui-ci soit fourni aux consommateurs contre de l'argent ou contre des données. Prenant acte des efforts que nous avons déployés en vue d'améliorer la coopération entre le CEPD et le Conseil, celui-ci a demandé l'avis du CEPD sur la proposition.

Le 14 mars 2017, nous avons publié un avis, dans lequel nous avons exprimé notre appui à l'objectif poursuivi par la Commission, c'est-à-dire renforcer les droits des consommateurs. Cependant, nous avons également souligné le risque de confusion pour les consommateurs et les entreprises, concernant toute nouvelle disposition de la législation de l'UE qui semble traiter les informations personnelles comme une marchandise et non comme un droit fondamental. Conformément à la législation de l'Union européenne, les citoyens disposent des mêmes droits en ligne et hors ligne. Ces droits incluent la consommation de biens et de services, qu'ils soient fournis contre de l'argent ou pas.

Le RGPD réglemente également l'utilisation des données dans l'économie numérique, y compris les conditions strictes dans lesquelles les données à caractère personnel peuvent être traitées dans le cadre d'une relation contractuelle. Nous avons donc exhorté l'UE à éviter de créer une insécurité juridique en interférant par inadvertance avec les règles établies par le RGPD et le futur règlement relatif à la vie privée et aux communications électroniques (voir section 6.1.5).

Bien que nous reconnaissions qu'il est essentiel pour la croissance de l'UE de développer l'économie fondée sur les données, assurer la confiance dans cette économie dépend de la protection des droits fondamentaux. Nous avons soutenu que la proposition relative au contenu numérique devrait être considérée comme une occasion de garantir la compatibilité de l'ensemble des règles prospectives de l'UE sur la protection des données et des consommateurs afin de servir les intérêts des individus.

6.3.4 La santé mobile : Les soins de santé en mouvement

La technologie mobile révolutionne le marché des soins de santé. Partout dans le monde, la population a désormais accès à toute une série d'options répondant à un large éventail de besoins de santé.

Cette convergence entre la technologie et les soins de santé devrait permettre aux personnes de bénéficier d'un meilleur système de soins à moindre coût, de mieux contrôler leurs soins de santé et d'accéder plus facilement et plus rapidement aux informations et soins médicaux en ligne. Cependant, elle pourrait également avoir pour corollaire la collecte, l'achat, la vente et l'analyse de grandes quantités d'informations à caractère personnel, sans que la personne concernée n'en soit informée et n'ait donné son consentement éclairé.

Le 21 mai 2015, nous avons publié un avis sur la santé mobile, dans lequel nous avons invité l'industrie, les gouvernements et les consommateurs à traiter cette question. Un consensus s'est dégagé sur la nécessité de jouer la carte de la transparence concernant la manière dont les données à caractère personnel sont traitées, partagées et réutilisées et à quelles fins. Nous avons mis en garde contre le fait que la non-application de mesures de protection des données entraînerait une lourde perte de confiance. Par conséquent, les opportunités pour les pouvoirs publics et les entreprises seraient restreintes, ce qui entraverait le développement du marché de la santé.

Le RGPD n'étant pas encore entré en vigueur au moment de la publication de cet avis, nous avons insisté sur le fait que les futures politiques de l'UE devraient encourager les prestataires de services et leurs associés à être plus responsables de leurs actes. Nous avons réclamé qu'il soit mis un terme à la collecte systématique de données à caractère personnel et à tout profilage discriminatoire et nous avons encouragé l'application du principe du respect de la vie privée dès la conception et par défaut dans le cadre de l'élaboration de technologies de santé mobile, ainsi que le renforcement des mesures de sécurité. Le respect des choix individuels devrait être au cœur de toutes les nouvelles technologies.

Si les personnes devraient certes être à même d'adopter une démarche volontariste concernant le suivi de leur état de santé, cela ne devrait pas se faire aux dépens d'une perte totale de contrôle de leur vie privée. La transparence, la sensibilisation et le contrôle effectif de nos données à caractère personnel sont indispensables pour que cela reste le cas.

@EU_EDPS

Solutions on #mhealth should serve individuals, respect their choices and be ethically tenable and foster #trust #eudatap

6.3.5 Des politiques intelligentes pour des technologies intelligentes

Dans notre société numérique, les technologies intelligentes sont omniprésentes. Les réseaux intelligents et les systèmes de transports intelligents en sont deux exemples.

Les compteurs intelligents mesurent la consommation d'énergie et transmettent les informations à une chaîne d'acteurs chargés de produire, de distribuer et de fournir le gaz et l'électricité à travers des réseaux intelligents. Ce processus permet aux entreprises de produire et de distribuer de l'énergie de manière plus efficace tout en réduisant les coûts à la fois pour le prestataire de services et le client.

En tant que membre du GT29, le CEPD a pris part à un projet lancé par la Commission européenne pour garantir la sécurité et la protection des données à caractère personnel dans ce processus depuis 2012. Nous avons notamment fourni des conseils concernant le modèle d'analyse d'impact sur la protection des données dans les réseaux intelligents.

En janvier 2016, plusieurs grandes entreprises européennes de services publics ont fait part de leur expérience concernant l'utilisation de ce modèle lors d'un atelier organisé auprès de la direction générale de l'énergie de la Commission (DG ENER). En sa qualité de contrôleur adjoint, Wojciech Wiewiórowski a précisé que cet exercice était extrêmement utile, avant la mise en œuvre du RGPD, qui rend obligatoires les analyses d'impact relatives à la protection des données si le traitement des données à caractère personnel semble présenter un risque élevé pour les individus. La Commission européenne a publié

la version définitive du modèle en octobre 2018, en tenant compte des dispositions finales du RGPD et des orientations proposées par le comité européen de la protection des données.

Les systèmes de transport intelligent coopératif (C-ITS) constituent un groupe de technologies et d'applications qui permettent aux véhicules de se connecter les uns aux autres ainsi qu'à d'autres éléments du système de transport, tels que les systèmes de contrôle de la circulation ou de péage. Ils ont pour but d'éviter les collisions, de contribuer à la sécurité routière et d'améliorer la circulation.

Les considérations relatives à la protection de la vie privée sont primordiales dans le déploiement des C-ITS, la technologie utilisée pouvant permettre de collecter d'énormes quantités de données qui pourraient servir à profiler ou à tracer les utilisateurs.

En novembre 2014, la Commission européenne a lancé sa plate-forme C-ITS. En tant que membre du sous-groupe sur la protection des données, nous avons suivi de près son évolution tout au long du mandat. Nous avons notamment attiré l'attention sur les difficultés potentiellement inhérentes à la préservation de la qualité et de la sécurité des données et à la promotion de la responsabilisation et de la limitation de la finalité. Nous avons également souligné la nécessité de garantir la transparence et la protection des données à caractère personnel et nous avons recommandé d'accorder une attention particulière à la promotion du respect de la vie privée dès la conception, en définissant les rôles et les responsabilités, en recensant les problèmes de sécurité et en informant les utilisateurs à propos de la collecte, du stockage et de l'utilisation de leurs données à caractère personnel.

6.4 Promouvoir un dialogue constructif sur la sécurité et le respect de la vie privée

La sécurité publique, la lutte contre la criminalité et le terrorisme ont toujours été des dossiers importants pour l'Union européenne. Au cours du mandat, la nécessité urgente de traiter ces questions s'est accrue, principalement du fait de plusieurs événements tragiques hautement médiatisés. Cependant, alors que les menaces qui pèsent sur la sécurité des individus et de la société sont bien réelles, nous devons faire en sorte que nos interventions soient à la fois nécessaires et proportionnées. Toute intervention interférant excessivement avec nos droits fondamentaux ne fera qu'entamer la confiance du public à l'égard des gouvernements, compromettant ainsi les efforts déployés pour faire face aux préoccupations communes de sécurité.

Nous sommes fermement convaincus que la sécurité peut être renforcée sans restreindre de manière excessive les droits relatifs à la protection des données. C'est la raison pour laquelle nous nous sommes engagés à promouvoir un dialogue constructif sur la sécurité et le respect de la vie privée. Ce dialogue met l'accent sur la recherche de solutions technologiques et juridiques innovantes, qui assurent un équilibre satisfaisant entre la protection des droits fondamentaux et la nécessité de renforcer les mesures de sécurité. Il importe de souligner, dans ce contexte, que l'article 6 de la Charte, qui couvre le droit à la liberté et à la sûreté, vise à protéger la liberté et la sûreté individuelles contre l'État, et non pas à les garantir à travers l'État.

Des discussions dans ce domaine sont en cours. Étant donné qu'il est peu probable que les menaces pesant sur la sécurité de l'UE diminuent dans l'immédiat, il est essentiel de garantir la poursuite de ce dialogue aux plus hauts niveaux. Par conséquent, le CEPD continuera d'intervenir directement auprès des institutions et des organes de l'UE actifs dans ces domaines et de fournir aux responsables politiques les outils nécessaires à l'élaboration de solutions adéquates.

6.4.1 Faciliter l'élaboration de politiques respectueuses de la vie privée

Afin de respecter les règles de l'UE en matière de protection des données, toute mesure proposée par le législateur de l'UE qui implique une restriction des droits relatifs à la protection des données doit être à la fois nécessaire et proportionnelle. Cette question concerne en particulier les politiques relatives à la sécurité de l'UE. Cependant, il n'est pas facile pour les

décideurs politiques de l'UE d'évaluer la nécessité et la proportionnalité des mesures proposées, en particulier lorsqu'ils travaillent sous la pression de l'urgence. C'est la raison pour laquelle le CEPD a élaboré une boîte à outils pour l'évaluation de la nécessité et des lignes directrices visant à déterminer la proportionnalité.

À l'aide d'une approche fondée sur des données factuelles, les décideurs politiques doivent être en mesure de démontrer que tout projet de limitation des droits fondamentaux en matière de protection des données et de respect de la vie privée est strictement nécessaire pour atteindre un objectif d'intérêt général ou pour protéger les droits et libertés d'autrui. Cela s'applique également à la limitation de tout autre droit susceptible d'être affecté par le traitement de données à caractère personnel.

Pour aider les décideurs politiques dans l'exécution de cette tâche, nous avons publié un guide pour l'évaluation de la nécessité le 11 avril 2017. Ce guide fournit aux responsables politiques une liste de contrôle pratique, qui indique point par point les différents aspects à prendre en considération lors de l'évaluation de la nécessité d'une nouvelle législation et qui fournit des exemples pour illustrer chaque étape. À cela s'ajoute une analyse juridique des principaux concepts en jeu, tels que la limitation du droit à la protection des données à caractère personnel, l'objectif d'intérêt général ainsi que la nécessité et la proportionnalité d'un projet de mesure législative.

Tout comme ils doivent être en mesure de démontrer l'absolue nécessité d'une mesure qui limiterait des droits fondamentaux, les décideurs politiques doivent également pouvoir démontrer la proportionnalité des mesures proposées, en tenant compte des objectifs de la politique et de la finalité du traitement des données. Pour les aider dans cette tâche, nous avons élaboré des lignes directrices sur la façon d'évaluer la proportionnalité. Ces lignes directrices ont fait l'objet d'une consultation publique le 25 février 2019.

Elles proposent un test constitué de quatre critères par rapport auxquels les responsables politiques peuvent évaluer la proportionnalité de toute nouvelle mesure et ainsi ajuster leur proposition en conséquence. Elles contiennent également des exemples visant à démontrer l'incidence négative qu'une limitation injustifiée du droit à la protection des données peut avoir sur les autres libertés et droits fondamentaux. Cela montre que les mesures ayant une incidence sur la vie privée et la protection des données ont non seulement des répercussions pour les personnes directement concernées, mais aussi pour la société dans son ensemble.

À l'instar du guide pour l'évaluation de la nécessité des mesures, les lignes directrices visant à déterminer la proportionnalité tiennent compte des recommandations de la Commission et du Conseil sur la façon de vérifier la compatibilité des nouvelles législations de l'UE avec la charte de l'UE. Tant la boîte à outils que les lignes directrices font référence à la jurisprudence européenne existante, aux récents avis législatifs et aux observations formelles du CEPD.

Étant donné que presque toutes les propositions politiques de l'UE impliquent désormais, sous une forme ou sous une autre, un traitement de données à caractère personnel, il importe au plus haut point de veiller à ce que les responsables politiques soient bien équipés pour évaluer de façon adéquate la nécessité et la proportionnalité d'une mesure proposée. Le guide pour l'évaluation de la nécessité des mesures et les lignes directrices sur la proportionnalité du CEPD encouragent les responsables politiques à tenir compte de ces dimensions essentielles dès le début du processus législatif, facilitant ainsi une élaboration des politiques responsable et éclairée.

@EU_EDPS

#EDPS publishes necessity toolkit as part of commitment to facilitating responsible & informed policymaking
http://europa.eu/!Yu63VB

6.4.2 Débat sur l'avenir du partage d'informations dans l'UE : l'interopérabilité des systèmes d'information à grande échelle

Pour relever les défis en matière de sécurité et de gestion des frontières, l'UE doit adopter une approche plus intelligente en ce qui concerne

le partage d'informations. Un outil pouvant s'avérer utile à cet égard est l'interopérabilité. Cependant, l'interopérabilité est également susceptible d'avoir de profondes conséquences juridiques et sociétales, qu'il convient d'évaluer et d'examiner soigneusement avant de la mettre en pratique.

Comme indiqué en novembre 2017 dans notre document de synthèse sur le sujet, bien que l'interopérabilité des systèmes d'information soit souvent considérée comme un simple concept technique, elle ne saurait être dissociée de la question de savoir si elle est nécessaire, politiquement souhaitable ou juridiquement envisageable.

Le 16 avril 2018, faisant suite à notre document de synthèse, nous avons publié un avis sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE dans les domaines de la migration, de l'asile, de la gestion des frontières, de la police et de la coopération judiciaire. L'interopérabilité permettrait à ces bases de données à grande échelle de l'UE de communiquer et d'échanger des informations.

Les propositions prévoient la possibilité d'utiliser les systèmes plus largement, au-delà des finalités spécifiques pour lesquelles ils ont été établis. En particulier, les données stockées dans les différents systèmes seront rassemblées pour lutter contre la fraude à l'identité, mais aussi pour faciliter et permettre les contrôles d'identité sur le territoire des États membres. Ils simplifieraient également l'accès des autorités répressives aux systèmes d'information à finalité non répressive.

Le CEPD s'inquiète, en particulier, de la proposition de création d'une base de données centralisée de l'UE, qui contiendrait des informations sur des millions de ressortissants de pays tiers, y compris leurs données biométriques. En raison de l'ampleur de cette base de données et de la nature des données à stocker dans celle-ci, les conséquences d'une violation de données pourraient porter gravement atteinte à un nombre potentiellement très élevé d'individus. Pour évaluer la nécessité d'une telle base de données, il convient de démontrer clairement l'ampleur du problème de la fraude à l'identité parmi les ressortissants de pays tiers. Par ailleurs, l'identification d'une personne n'étant pas une fin en soi, mais devant être mise au service d'un objectif spécifique, la finalité des contrôles d'identité sur le territoire des États membres devrait être formulée de manière plus précise.

Il est nécessaire que les autorités répressives aient à leur disposition les meilleurs outils possibles pour lutter contre le terrorisme et d'autres délits graves. Cependant, faciliter l'accès des autorités répressives aux informations obtenues pour des finalités autres que répressives est loin d'être anodin du point de vue de la protection des droits fondamentaux. Des garanties juridiques, techniques et organisationnelles strictes et appropriées doivent, par conséquent, être mises en place dans l'ensemble des bases de données de l'UE et une attention particulière doit être accordée à la définition de la finalité de cet accès et aux conditions d'accès à ces données.

Tenant compte de l'incidence de l'interopérabilité sur les droits fondamentaux, nous avons appelé à un débat plus large sur l'avenir de l'échange d'informations au sein de l'UE, sur la gouvernance des systèmes d'information de l'UE et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte. En 2019, pour favoriser cette discussion, nous avons organisé une réunion-débat sur le sujet lors de la conférence « Computers, Privacy and Data Protection » (CPDP). Cette réunion-débat devait permettre d'échanger des points de vue sur la réponse apportée par l'UE à la crise migratoire et aux enjeux liés à la sécurité, qui s'appuie dans une large mesure sur l'interopérabilité des systèmes d'information à grande échelle de l'UE. Nous avons également organisé un atelier sur les systèmes d'information interopérables dans l'espace de liberté, de sécurité et de justice de l'UE, en collaboration avec la faculté de droit et le Centre européen des politiques migratoires de l'Institut universitaire européen (IUE) et le Centre d'études de la politique européenne (CEPS).

6.4.3 Contrôle d'Europol

Une Europe ouverte et sûre impose d'améliorer l'efficacité opérationnelle de la lutte contre les formes graves de criminalité et le terrorisme, mais elle suppose également un engagement

en faveur de la protection des libertés et droits fondamentaux des personnes.

Europol est l'organe de l'UE qui soutient les autorités répressives des États membres dans la lutte contre la grande criminalité internationale et le terrorisme. Il incombe au CEPD de veiller à ce qu'Europol agisse conformément aux règles en matière de protection des données (voir chapitre 1).

@EU_EDPS

New Regulation boosts the roles of #EDPS and @Europol

Le CEPD et Europol

En sa qualité d'autorité de contrôle d'Europol, le CEPD est le gardien des libertés et droits fondamentaux dans le domaine répressif. Par conséquent, le CEPD mène un dialogue constructif avec Europol afin de garantir le respect de la vie privée lors du traitement de données à des fins répressives.

Les résultats de ce dialogue ont souvent des répercussions sur les autorités répressives au sens large. Étant donné sa nature même, Europol s'acquitte de ses fonctions en interagissant constamment avec les autorités compétentes des États membres ainsi qu'avec ses partenaires du monde entier. Cela signifie que la mise en œuvre d'un système de protection des données par Europol a des répercussions qui dépassent le cadre d'Europol. Les données échangées avec les partenaires d'Europol sont non seulement protégées de façon appropriée par le solide système de protection des données de l'agence, mais le cadre de protection des données mis en place par Europol peut également encourager ses partenaires à évaluer et améliorer leurs propres normes. L'organisation par Europol de nombreuses réunions et conférences, auxquelles le CEPD participe autant que possible, permet à Europol de partager constamment son expertise en matière de protection des données.

Nous sommes pleinement conscients du contexte général dans lequel Europol opère et nous en tenons compte dans le cadre de notre collaboration. Notre coopération avec les autres APD, à travers le comité de coopération d'Europol, permet de garantir l'application d'une approche commune partout en Europe en ce qui concerne la protection des données (voir section 5.3.1)

Le contrôle des activités de traitement des données dans le domaine répressif comporte de nombreux enjeux. Tout d'abord, il s'agit d'un domaine dans lequel les droits des personnes sont limités, ce qui justifie des régimes dérogatoires. Par ailleurs, l'incidence de ces activités de traitement des données sur les libertés et les droits individuels est élevée. Les données à caractère personnel sont collectées et traitées pour permettre aux pouvoirs publics de prendre des décisions, qui peuvent avoir une incidence non négligeable sur les droits des personnes, d'autant plus qu'une grande partie des personnes concernées appartient à des groupes vulnérables. Enfin, ces activités de traitement des données sont opaques. Il est difficile pour les personnes concernées de savoir qui traite leurs données et à quelles fins. En ce qui concerne Europol, le contrôle de ces activités de traitement des données est d'autant plus ardu que les systèmes d'information d'Europol sont complexes et qu'ils traitent un volume important de données à caractère personnel. Europol œuvre dans plusieurs domaines de criminalité, qui ont tous des contraintes et des impératifs spécifiques.

Le CEPD a, par conséquent, un rôle spécifique à jouer, à savoir garantir la protection effective des droits individuels, les personnes n'ayant pas le pouvoir d'exercer ce contrôle dans la même mesure que dans d'autres domaines.

Préparatifs en vue de notre nouveau rôle

En 2015, nous avons fourni des conseils aux législateurs concernant des questions spécifiques liées à la protection des données dans le règlement Europol. En décembre 2015, les législateurs se sont mis d'accord sur un texte final. Le nouveau règlement attribue au CEPD la majorité des tâches précédemment remplies par l'autorité de contrôle commune d'Europol (ACC), notamment le contrôle du traitement des données à caractère personnel relatives aux activités opérationnelles d'Europol. Le règlement a été approuvé le 11 mai 2016 et est en vigueur depuis le 1er mai 2017.

Dans le cadre des préparatifs menés en vue de notre nouveau rôle, un groupe de travail interne spécifique réunissant l'ensemble des unités et des secteurs du CEPD a été créé. Des membres du personnel du CEPD ont suivi des sessions de formation internes et externes en rapport avec la supervision d'Europol et nous avons établi des contacts réguliers avec l'équipe d'Europol chargée des activités liées à la protection des données afin de favoriser une compréhension mutuelle et d'établir des canaux de communication efficaces. En 2016, des réunions de haut niveau ont également eu lieu entre Giovanni Buttarelli, le contrôleur européen de la protection des données, et Rob Wainwright, alors directeur d'Europol.

Les 15 et 16 mai 2017, juste après avoir endossé nos nouvelles responsabilités, nous avons procédé à une visite opérationnelle chez Europol, qui nous a permis de nous familiariser avec les pratiques et les procédures de l'agence.

Pour saisir pleinement les questions actuellement en jeu dans la supervision d'Europol et pour préparer la coopération avec les États membres, nous avons également demandé à avoir un aperçu des principales recommandations adressées à Europol par l'ACC après ses inspections les plus récentes ainsi qu'un rapport actualisé des mesures prises par Europol pour faire suite à ces recommandations.

Depuis que nous avons pris nos nouvelles fonctions le 1er mai 2017, nous avons mis en place un système structuré de contrôle visant à promouvoir la coopération et à garantir la responsabilisation.

Coopération avec Europol

Nous travaillons en étroite collaboration avec l'équipe du DPD d'Europol et avec d'autres membres du personnel opérationnel, auxquels nous prodiguons, le cas échéant, des conseils informels notamment au cours de réunions bimestrielles. Cela nous aide à anticiper les consultations et d'autres questions sur le traitement des données ainsi qu'à définir et planifier nos futures activités, telles que les inspections ou les enquêtes.

La coopération au sommet de la hiérarchie est tout aussi importante et des réunions entre les dirigeants du CEPD et d'Europol ont lieu régulièrement.

Coopération avec d'autres autorités de contrôle

Étant donné que la plupart des données traitées par Europol proviennent des États membres, la supervision d'Europol suppose également une coopération étroite avec les autorités de contrôle compétentes dans les États membres. Tandis qu'il nous incombe de superviser le traitement par Europol des données à caractère personnel, les APD nationales ont pour mission de surveiller le traitement des données à caractère personnel par leurs autorités répressives nationales respectives. Pour que nous puissions nous acquitter de nos fonctions concernant Europol, il est, par conséquent, essentiel que nous puissions coopérer efficacement avec les APD nationales.

C'est la raison pour laquelle le règlement Europol prévoit la création d'un comité de coopération, composé de représentants des APD nationales et du CEPD. Le comité fait office d'organe consultatif pour les questions impliquant le traitement par Europol de données à caractère personnel qui proviennent des États membres. Le CEPD assure le secrétariat de ce comité, qui se réunit au moins deux fois par an (voir section 5.3.1).

La coopération est assurée essentiellement par l'intermédiaire du comité de coordination, mais nous coopérons également avec des représentants des APD pour réaliser des inspections.

Au moins une fois par an, le CEPD rend compte au groupe de contrôle parlementaire conjoint, qui surveille Europol, pour discuter du respect par Europol des règles et principes relatifs à la protection des données à caractère personnel.

Activités de contrôle

Afin de garantir un contrôle efficace, le CEPD surveille activement le respect effectif des règles en matière de protection des données, de sa propre initiative ou à la suite d'une réclamation.

Le règlement Europol autorise le traitement de données à caractère personnel aux fins d'une analyse opérationnelle, à l'appui d'enquêtes judiciaires et d'opérations de renseignement en matière pénale menées par les autorités répressives dans les États membres. Cependant, les autorités répressives ne peuvent agir de la sorte que dans la cadre de *projets d'analyse opérationnelle* (PAO). Pour chaque PAO, Europol est tenu de communiquer au CEPD la finalité du projet, les catégories de données, les individus concernés, les participants, le délai de conservation des données, les conditions d'accès et toute proposition de transfert ou d'utilisation des données concernées.

Nous fournissons des conseils sur toutes les questions liées au traitement par Europol des données à caractère personnel, sous la forme d'avis. Par ailleurs, chaque fois qu'Europol planifie une nouvelle activité de traitement de données impliquant le traitement de données sensibles ou la possibilité d'un risque significatif pour une personne, il doit en informer le CEPD et lui fournir une description générale des opérations de traitement envisagées, une évaluation des risques pour les libertés individuelles et les mesures envisagées pour contrer ces risques. Nous examinons les propositions d'Europol et nous adressons des recommandations (voir illustration 15). Jusqu'à présent, nous avons reçu six consultations préalables et avons rendu un nombre équivalent d'avis.

Nous menons également des inspections générales et thématiques au sein d'Europol. Ces inspections sont la pierre angulaire de nos activités de contrôle et, depuis mai 2017, nous avons effectué trois inspections générales. La première a eu lieu en décembre 2017, la deuxième et la troisième ont été réalisées respectivement en mai 2018 et en juin 2019. Au cours de chaque inspection, nous avons minutieusement vérifié certains aspects juridiques et techniques du traitement des données. Nos inspections incluent également un contrôle du respect de la sécurité des données selon les normes internationales. Lors de ces inspections, nous avons tenu compte des recommandations critiques émises par l'ACC lors de sa dernière inspection. Nous avons

Europol: Consultation préalable

Lorsque Europol prévoit un nouveau type d'activité de traitement supposant le traitement de données sensibles ou pouvant entraîner un certain risque pour les particuliers, ces opérations doivent être notifiées au CEPD. Nous examinons les propositions et nous donnons notre avis à leur sujet. À ce jour, le CEPD a reçu sept notifications et a émis un avis sur les six opérations de traitement suivantes:

QUEST (Querying Europol Systems): Interface automatique destinée à faciliter la vérification croisée des données dans les bases de données nationales et dans la base de données d'Europol concernant les suspects. Grâce à son mécanisme de recherche simplifié, QUEST offre aux États membres de nouvelles capacités d'enquête. Cela permet aux policiers autorisés dans les États membres d'effectuer des recherches simultanées dans le système d'information d'Europol et dans d'autres bases de données nationales et internationales depuis leur propre environnement de travail, en interrogeant leurs bases de données nationales.

ETS (European Tracking Solution): Outil permettant à des unités spécialisées, principalement basées dans les États membres, d'échanger des données de géolocalisation quasiment en temps réel. Il est utilisé pour localiser et suivre des objets et des personnes.

IRMa (Internet Referral Management application): Outil logiciel utilisé par l'unité chargée du signalement des contenus sur l'internet (IRU) d'Europol pour contribuer à automatiser le *processus de signalement*, qui consiste à repérer les contenus terroristes en ligne et à notifier aux fournisseurs de services en ligne la nécessité de les supprimer. Europol a mis au point cet outil et souhaite le mettre à la disposition des États membres pour qu'ils en fassent le même usage.

SIENA 4.0: Mise à jour du système d'échange de messages sécurisé d'Europol. Ce système est utilisé pour gérer l'échange d'informations opérationnelles et stratégiques relatives à la criminalité entre les États membres, Europol et ses autres partenaires.

Portail web sur les cryptomonnaies: Une plateforme qu'Europol a l'intention de créer et qui aderas les forces de l'ordre à interroger les systèmes de cryptomonnaie et à surveiller les activités correspondant à des adresses particulières. Faute d'informations suffisantes, notamment en ce qui concerne les risques recensés et les mesures d'atténuation, nous avons considéré que nous n'étions pas en mesure d'émettre un avis favorable sur le portail.

Accès aux données des dossiers passagers: Europol a mis au point une procédure permettant de demander des informations sur les dossiers passagers (Passenger Name Record – PNR) à des unités spécialisées des États membres, désignées sous le nom d'unités d'informations passagers ou UIP, conformément à la directive PNR. Les données des dossiers passagers sont des informations fournies par les passagers lors de la réservation des billets et de l'enregistrement sur les vols, qui sont aussi collectées par les compagnies aériennes pour leur propre usage commercial.

Illustration 15. Consultations préalables d'Europol

notamment procédé au contrôle du traitement des données à caractère personnel dans le cadre des PAO, de la procédure en cas de violation de données et du système d'information Europol (SIE).

Nous invitons des experts provenant des APD nationales à participer à nos inspections générales. Les États membres étant les principaux fournisseurs d'informations d'Europol, la participation d'experts nationaux au processus d'inspection contribue à attirer l'attention sur des problèmes survenant au niveau d'Europol, qui trouvent peut-être l'origine au niveau national. Ces problèmes peuvent être liés à la qualité des données ou à une justification insuffisante concernant le traitement de données sensibles ou de données sur des catégories particulières de personnes, telles que les mineurs. De retour dans leur pays, les experts peuvent réfléchir à la façon d'aborder ces problèmes dans le cadre de leurs propres activités de contrôle, ce qui permet de renforcer la coordination entre les activités de contrôle menées aux niveaux de l'UE et national.

Les 5 et 6 février 2019, nous avons également effectué un contrôle ciblé du rôle de vérificateur joué par Europol dans le cadre de la mise en œuvre de l'accord sur le programme de surveillance du financement du terrorisme (TFTP) entre l'UE et les États-Unis.

Après avoir mené nos activités sur place, nous exposons une série de recommandations visant à obtenir des améliorations, dans un rapport d'inspection que nous envoyons au directeur exécutif d'Europol ainsi qu'au comité de coopération. Nous assurons un suivi étroit de ces recommandations pour nous assurer qu'Europol les met en pratique. Nos conclusions offrent l'occasion d'entreprendre des activités visant à renforcer le niveau de protection des données et l'efficacité des activités opérationnelles d'Europol.

Outre des inspections, nous menons des enquêtes de notre propre initiative sur des questions portées à notre attention au cours des autres activités de contrôle. Nous traitons également les réclamations des personnes physiques relatives au traitement par Europol de leurs données à caractère personnel.

Europol a l'obligation de nous informer, dans les plus brefs délais, de toute violation de données à caractère personnel. En pareil cas, Europol a également l'obligation d'évaluer l'incidence négative de la violation de données sur les droits et les libertés des personnes concernées et de les en informer si cette incidence est significative. Depuis le début, nous contrôlons, dans le cadre de nos réunions bimestrielles, la procédure interne mise en place par Europol pour traiter ce genre de cas et nous transmettons nos observations.

Communication

S'appuyant sur les connaissances acquises en procédant au contrôle d'Europol, le CEPD contribue au débat public sur la sécurité et le respect de la vie privée par l'ensemble des autorités répressives.

Par exemple, le 22 novembre 2018, Wojciech Wiewiórowski, le contrôleur adjoint, a prononcé le discours d'ouverture d'une conférence sur la liberté et la sécurité, organisée conjointement par le réseau d'experts en protection de données d'Europol (EDEN) et l'Académie de droit européen (ERA). Par ailleurs, plusieurs membres du personnel du CEPD prennent régulièrement part à des conférences et des événements portant sur la protection des données et la surveillance, en qualité de participants et d'intervenants.

L'avenir

Nous procédons au contrôle d'Europol depuis deux ans. Nous avons établi des liens solides avec l'agence et avons acquis une bonne connaissance des problèmes auxquels elle est confrontée dans le cadre de la mise en œuvre de la protection des données. Les nouveaux défis nécessiteront un contrôle spécifique de la part du CEPD. Parmi ceux-ci, citons notamment l'émergence d'échanges structurels de données entre les organes de la justice et des affaires intérieures des institutions de l'UE, entre les autorités nationales et les agences de l'UE, ainsi que l'utilisation de nouvelles technologies, telles que les données massives et l'intelligence artificielle.

6.4.4 Technologies de surveillance intrusive

Le 15 décembre 2015, nous avons publié un avis sur les technologies de surveillance intrusive.

En juillet 2015, les courriers électroniques internes, les détails commerciaux et la documentation technique d'une entreprise vendant des outils de surveillance à des administrations publiques, à l'intérieur et à l'extérieur de l'UE, ont été divulgués au public. Ces documents décrivaient en détail les capacités de ces outils, qui étaient utilisés par des pouvoirs publics et des autorités répressives pour enquêter sur la vie des individus.

Dans notre avis, nous avons attiré l'attention sur les risques qu'un marché en expansion et non réglementé pose pour la vente, la distribution et l'utilisation de tels outils. Nous avons insisté sur le fait que des efforts supplémentaires doivent être fournis pour contrôler ce marché et nous avons invité les législateurs à envisager des mesures de protection qui intègrent le respect de la vie privée dès la conception et qui garantissent la préservation de la vie privée.

Les pouvoirs publics affirment que l'utilisation légitime et réglementée d'outils de surveillance par les autorités répressives est nécessaire. Cependant, il convient de reconnaître que ces outils peuvent aussi être utilisés à des fins de contournement des mesures de sécurité entourant les communications électroniques et le traitement des données, compromettant ainsi l'intégrité des bases de données, des systèmes et des réseaux.

Nos existences numériques étant de plus en plus connectées, les risques ne feront qu'augmenter. Une approche coordonnée de lutte contre ces risques, y compris une meilleure réglementation de la commercialisation et de l'utilisation des logiciels de surveillance, est, par conséquent, nécessaire pour protéger de façon adéquate la vie privée de toutes les personnes dans l'UE, tant au niveau national qu'à l'étranger. Le RGPD vient en quelque sorte combler ces lacunes, en incluant expressément le principe de la protection des données dès la conception ; par exemple, dans le cas présent, cela signifie que les capacités techniques des outils destinés aux activités répressives ne peuvent pas être supérieures à celles qui sont autorisées par la législation. Cependant, il reste encore beaucoup à faire.

7. COMMUNICATION ET GESTION DES RESSOURCES

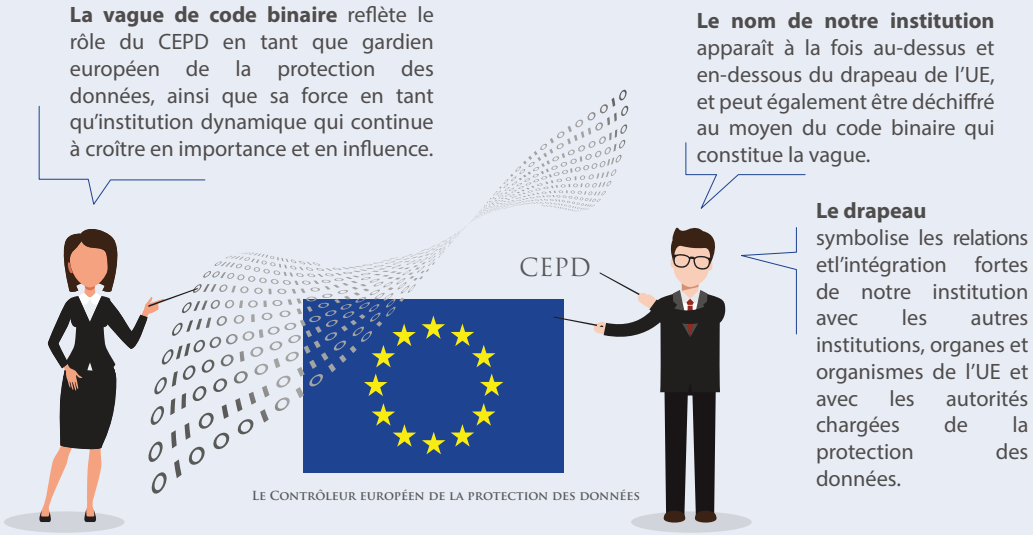
7.1 Information et communication

Le nouveau mandat a entraîné l'adoption d'une nouvelle approche concernant les activités de communication du CEPD. L'image a été renouvelée, ainsi que les outils de communication, tandis que la stratégie de communication a subi une refonte générale. Nous nous positionnons comme chef de file mondial, ce qui suppose que l'important travail accompli par le CEPD doit atteindre le public visé.

La protection des données doit être compréhensible et accessible. Tout le monde doit être en mesure de comprendre ses droits et ses obligations ; pourtant, nous sommes pleinement conscients du fait que de nombreuses personnes considèrent la protection des données comme étant technique et obscure. Les enjeux sont nombreux et importants ; nous ne pouvons pas prendre le risque que nos messages ne soient pas entendus. Nous nous sommes, par conséquent, efforcés de communiquer de manière claire, concise et transparente à travers l'ensemble de nos canaux de communication.

La création d'une nouvelle identité visuelle, le lancement de nouvelles initiatives et l'amélioration de la manière dont nous utilisons les canaux de communication existants ont été essentiels au positionnement du CEPD en tant que chef de file mondial sur les questions de protection des données et de la vie privée, que nous nous adressions aux experts de

LE LOGO DU CEPD



la protection des données ou aux citoyens ordinaires de l'UE.

7.1.1 Une nouvelle identité visuelle

En mai 2015, nous avons inauguré le nouveau logo du CEPD. Ce dernier s'inscrivait dans un processus visant à doter le CEPD d'une nouvelle identité visuelle reflétant une ère nouvelle dans l'histoire de l'institution, qui se positionne en tant que chef de file mondial en matière de protection des données et de la vie privée. Il s'agissait de la première étape d'un projet visant à donner une nouvelle image au CEPD, qui a été déployé durant la première moitié du mandat.

Une fois le logo dévoilé, nous avons concentré notre attention sur la refonte de notre site web. Nous voulions qu'il soit plus convivial, plus clair et plus transparent.

La première étape de ce processus de refonte a pris fin en novembre 2015, lorsque nous avons mis en ligne la nouvelle mouture de notre site web, auquel nous avons intégré une série de nouvelles fonctions destinées à renforcer l'accessibilité et la transparence du site. En voici quelques exemples :

- un programme ;
- une conception adaptée aux téléphones intelligents et aux tablettes ;
- une nouvelle mise en page pour la page d'accueil.

Les travaux portant sur le site web du CEPD se sont poursuivis en 2016 ; nous avions pour objectif de mettre en service un site web flambant neuf au début de 2017. Nous avons notamment conçu une nouvelle mise en page, migré le contenu de l'ancien site web vers le nouveau et opéré une transition vers un nouveau système de gestion des contenus (SGC), EC Drupal.

En mars 2017, nous avons lancé le nouveau site web du CEPD. La nouvelle mise en page permet d'accéder facilement aux travaux du CEPD, qui sont organisés par thèmes, ainsi qu'aux réseaux sociaux, à travers un mur Twitter. Nous avons enrichi la page d'accueil de nouveaux contenus (par exemple, l'histoire du CEPD, nos derniers blogs et nos dernières vidéos) et nous avons intégré un puissant moteur de recherche qui permet aux utilisateurs de trouver facilement les informations qu'ils recherchent.

Depuis 2017, nous avons apporté plusieurs améliorations et modifications au site web, afin de répondre aux préoccupations soulevées tant par les membres du personnel du CEPD que par les utilisateurs externes. Nous avons notamment ajouté une section *Quicklinks* sur la page d'accueil du site web, qui permet aux utilisateurs d'accéder rapidement à certaines des pages les plus fréquemment consultées. Nous avons, dans la mesure du possible, commencé à publier nos documents au format HTML et non plus au format PDF, améliorant ainsi l'expérience des utilisateurs de téléphones mobiles et de tablettes.

Afin que notre site web reste aussi respectueux de la protection des données que possible, nous avons également abandonné, au début de l'année 2019, la possibilité pour les utilisateurs de s'opposer au traitement de leurs données (*opt out*) au profit d'un consentement préalable des utilisateurs pour le traitement de leur données (*opt in*). Cela signifie que nous pouvons suivre les visiteurs de notre site web uniquement si ceux-ci nous donnent leur consentement explicite.

Le bulletin d'information du CEDP a également subi une cure de rajeunissement. Le nombre d'abonnés à notre bulletin d'information augmente d'année en année ; il s'agit donc d'un outil précieux qui nous permet de fournir des informations sur nos activités les plus récentes et les plus importantes. Nous avons adopté un nouveau format en ligne pouvant être visualisé facilement sur les appareils portables afin de rendre le bulletin d'information plus accessible et plus convivial, quel que soit le support utilisé pour le lire.

Nous envoyons le bulletin d'information aux utilisateurs dont le nom figure sur la liste de distribution et nous le publions sur notre site web. Bien que le contenu du bulletin d'information reste globalement le même, nous avons opté pour une publication plus fréquente afin que nos lecteurs soient mieux informés des activités que nous menons et des évolutions dans le domaine de la protection des données.

Le premier numéro de la nouvelle version de notre bulletin d'information a été publié en juin 2017 ; dix numéros sont désormais publiés chaque année. D'après une enquête menée en mai 2019 auprès des abonnés à notre bulletin d'information, nos lecteurs sont généralement satisfaits du nouveau format.

@EU_EDPS

EDPS' new logo - new era in the history of our organisation

7.1.2 Nouvelles initiatives

En juillet 2015, nous avons lancé une application mobile, qui permettait aux utilisateurs de comparer les recommandations du CEPD sur le RGPD et les textes de la Commission européenne, du Parlement et du Conseil. L'application a été mise à jour en 2016 pour permettre aux utilisateurs de consulter le texte final du RGPD ainsi que la proposition législative initiale de la Commission, les recommandations fournies par le CEPD et les règles définies dans la directive 95/46/CE sur la protection des données. L'application fournit également un historique du processus de réforme (voir section 6.1.1).

L'application était un moyen innovant pour le CEPD d'encourager le législateur à mettre en œuvre des solutions pragmatiques, en le tenant pour responsable de ses décisions, et de contribuer à la transparence et à la responsabilisation du processus législatif.

Une autre initiative, le blog du CEPD, a été lancée en avril 2016. Le blog fournit des informations plus détaillées sur les travaux du CEPD et, notamment, des Contrôleurs. Il permet à ceux-ci d'échanger de façon plus personnelle sur leurs idées, leurs avis et leurs activités ainsi que sur les travaux de l'institution. Nous souhaitions rendre nos travaux, et la protection des données en général, plus accessibles et mieux compréhensibles et, ainsi, atteindre de nouveaux publics.

Le blog du CEPD fait désormais partie intégrante de nos activités de communication. Nous y publions régulièrement de nouveaux billets sur un large éventail de sujets, notamment sur des préoccupations actuelles et des initiatives indépendantes lancées par le CEPD. Nous relayons l'ensemble des billets publiés sur le blog sur les réseaux sociaux et distribuons certains d'entre eux à notre réseau de journalistes et d'autres parties intéressées. Tous les billets publiés sur le blog sont facilement accessibles depuis la page d'accueil de notre site web.

7.1.3 Réseaux sociaux

Les réseaux sociaux sont devenus un outil de communication indispensable pour le CEPD. Tout au long du mandat, nous avons renforcé notre présence sur trois réseaux sociaux influents, qui nous permettent d'atteindre facilement et rapidement un public mondial.

Bien que Twitter reste notre outil le plus influent, notre présence sur LinkedIn a enregistré l'une des hausses les plus considérables au cours des cinq dernières années ; nous sommes passés de 877 abonnées fin 2015 à 16 344 abonnés le 30 septembre 2019. Le nombre d'abonnements à notre chaîne YouTube a également augmenté, en grande partie grâce à nos efforts de communication lors de la conférence internationale 2018 des commissaires à la protection des données et à la vie privée.

Notre croissance continue sur les réseaux sociaux témoigne à la fois de l'expansion de notre influence mondiale en tant qu'organisation et des efforts que nous déployons pour mettre en œuvre une stratégie efficace sur les réseaux sociaux.

7.1.4 Le RGPD pour l'UE : la campagne de communication

Les nouvelles règles en matière de protection des données pour les institutions de l'UE sont devenues pleinement applicables le 11 décembre 2018. Pour compléter nos actions de sensibilisation (voir section 6.2.1), nous avons lancé une campagne de communication. Si cette campagne visait principalement les membres du personnel des institutions de l'UE, nous avons également souhaité sensibiliser les personnes externes aux institutions de l'UE à l'incidence

que les nouvelles règles peuvent avoir sur leur vie et leurs droits.

Nous avons assemblé un kit de communication contenant des informations utiles et pertinentes pour l'ensemble des membres du personnel de l'UE. Ce kit, qui a été distribué à tous les délégués à la protection des données (DPD) des institutions de l'UE avant le 11 décembre 2018, a été conçu pour aider les DPD à conscientiser les membres du personnel de leur institution respective.

Il comprend une vidéo sur la responsabilité, une affiche que les DPD peuvent imprimer et apposer dans leur bâtiment, des illustrations destinées à leur intranet et aux réseaux sociaux et des caches webcam qu'ils peuvent distribuer à certains membres du personnel de l'UE. Nous avons également créé trois fiches d'information portant respectivement sur les droits à la protection des données au titre des nouvelles règles, sur les conséquences des nouvelles règles pour les salariés de l'UE et sur la manière de garantir l'obligation de rendre compte ; des copies de ces fiches étaient disponibles dans le kit et sur notre site web.

Par ailleurs, des copies individuelles du nouveau règlement ont été préparées et distribuées aux DPD lors de la réunion CEPD-DPD, qui a eu lieu le 12 décembre 2018 (voir section 6.2.2).

En complément de notre coopération avec les DPD, nous avons également lancé une campagne dans les médias et sur les réseaux sociaux pour sensibiliser à la question en dehors des institutions de l'UE. Nous avons utilisé Twitter et LinkedIn pour fournir des informations sur les nouvelles règles, leurs implications, mais aussi le rôle et les activités du CEPD. Par ailleurs, nous avons publié un communiqué de presse et contacté directement plusieurs organes de presse pour essayer d'assurer une couverture suffisante. Un message publicitaire présentant une bande dessinée accrocheuse a été publié dans *Politico* le 13 décembre 2018 en vue de soutenir la campagne. Nous nous sommes également efforcés d'actualiser notre site web et la page Wikipedia pour qu'ils reflètent les modifications de la législation.

7.1.5 Préparations en vue du comité européen de la protection des données – communication

En tant que nouvel organe de l'UE, le comité européen de la protection des données devait être doté d'une identité visuelle propre (voir section 6.1.3). En 2017, nous avons présenté plusieurs modèles de logo aux membres du groupe de travail « article 29 » (GT29), qui en ont sélectionné un. Nous avons ensuite créé une identité institutionnelle sur la base de ce logo, en précisant de quelle manière il pourrait être utilisé.

Le Comité devait également disposer d'un site web ; la transition vers le nouveau site web du CEPD a servi de point de départ à sa création. La migration du site web du CEPD vers un nouveau SGC, EC Drupal (voir section 7.1.1), s'inscrit dans un cadre stratégique qui ouvre la voie à une flexibilité accrue, tant en ce qui concerne la manière dont nous présentons nos travaux sur notre propre site web, qu'en ce qui concerne la création de sites web supplémentaires, y compris le site web du comité européen de la protection des données. Nous avons commencé à développer le site web du Comité en 2017 et l'avons achevé à temps pour qu'il soit mis en ligne le 25 mai 2018, le jour où le RGPD est devenu pleinement applicable.

Bien que le secrétariat du comité européen de la protection des données possède sa propre équipe de communication, nous avons continué de lui fournir un appui en fonction des exigences, pour les publications, les vidéos ou l'organisation de manifestations. Nous travaillons en étroite collaboration avec l'ensemble des membres du comité européen de la protection des données dans le cadre du réseau de communication du Comité, en vue de mieux coordonner les actions de communication des autorités chargées de la protection des données (APD) dans l'UE et de nous soutenir mutuellement.

7.1.6 La conférence internationale 2018 – communication

Le coup d'envoi des actions de communication relatives à l'édition 2018 de la conférence

internationale, co-organisée à Bruxelles par le comité européen de la protection des données (voir section 5.2.1), a été donné lors de l'édition 2017 de la conférence, qui a eu lieu à Hong Kong. Nous avons fait la promotion de l'édition 2018 de la conférence à l'aide d'un vidéogramme, dans lequel nous avons présenté le thème principal de la conférence et les questions que nous souhaitions aborder au cours de celle-ci. Nous avons également distribué des dépliants d'information sur la conférence.

Au milieu de l'année 2017, nous avons investi des ressources pour développer le logo de la conférence. Soucieux de faire la promotion de la conférence, nous avons encouragé les concepteurs du monde entier à nous soumettre des propositions. Le logo a été intégré au matériel promotionnel et aux documents de la conférence, parallèlement à d'autres idées provenant des propositions que nous avons reçues.

Nous avons commencé à travailler sur le site web de la conférence en 2017 également. Comme nous l'avions fait pour le site web du comité européen de la protection des données, nous avons utilisé à notre avantage la migration vers EC Drupal pour créer le site web de la conférence. Nous avons lancé le site web le 19 mars 2018. Il contenait l'ensemble des informations pertinentes sur le thème, le programme, les intervenants et les lieux de la conférence et il a également servi de portail pour l'inscription à la conférence. Par ailleurs, les participants à la session fermée de la conférence ont pu consulter l'ensemble des documents de la réunion sur le site web, grâce à leurs données de connexion et à leur mot de passe. Nous avons actualisé le site web tout au long de la conférence en y téléchargeant immédiatement les documents, les vidéos et les informations dès qu'ils nous étaient transmis.

Pour encourager les participants à prendre part au débat en ligne, nous avons créé, en 2017, un compte Twitter consacré à l'événement. En 2018, nous avons renforcé notre présence sur les réseaux sociaux en créant un compte Instagram. Nous avons utilisé ces deux canaux tout au long de la conférence, en y postant régulièrement des mises à jour, des informations et des données sur la conférence. Nous avons soutenu nos actions en utilisant les comptes du CEPD sur les réseaux sociaux.

Par ailleurs, en 2017, nous nous sommes lancés dans la création d'une application mobile destinée à promouvoir la participation du public à la conférence. L'application a été lancée quelques semaines avant la conférence et tous les délégués ont été invités à la télécharger pour l'utiliser au cours de la session publique. Elle reflétait et complétait le contenu du site web de la conférence. Les participants ont pu l'utiliser pour prendre des notes, répondre à des sondages, échanger des points de vue et envoyer des questions aux organisateurs de la conférence, auxquelles les intervenants répondaient sur scène.

Toutes ces actions ont été accompagnées d'une campagne médiatique destinée aux médias internationaux. Le premier jour de la session publique, une conférence de presse a été organisée et un communiqué de presse publié. L'excellente couverture médiatique dont l'événement a bénéficié aux quatre coins du monde a reflété l'intérêt que les sujets de discussion et les orateurs ont suscité.

7.2 Administration, budget et personnel

L'unité «Ressources humaines, budget et administration» (HRBA) du CEPD soutient le conseil d'administration et les équipes opérationnelles du CEPD, en veillant à ce qu'ils disposent des outils et des ressources nécessaires pour atteindre les objectifs établis dans la stratégie du CEPD pour la période 2015-2019.

Elle a notamment recruté, géré, formé et renforcé le personnel du CEPD pour élargir ses connaissances et ses compétences et pour veiller à ce qu'il se démarque du point de vue de la responsabilisation en matière de protection des données, en montrant l'exemple à d'autres.

En outre, au cours du mandat, elle a pris part à deux projets importants du CEPD : la création du secrétariat du comité européen de la protection des données et les préparatifs en vue de la conférence internationale 2018 des commissaires à la protection des données et de la vie privée.

7.2.1 Une organisation en pleine expansion

Le CEPD a connu une croissance importante entre 2015 et 2019. La nécessité d'engager plus d'experts de la protection des données, pour que le CEPD puisse endosser une série de nouveaux rôles et remplir ses nouvelles fonctions de façon compétente et efficace, en est l'une des principales causes. Le CEPD a notamment assuré le secrétariat du comité européen de la protection des données, assumé la responsabilité de la supervision d'Europol et veillé à ce que nous ayons le personnel et les connaissances nécessaires pour accomplir les tâches qui nous ont été assignées au titre du nouveau règlement (UE) 2018/1725. Nous avons également dû faire face à une rotation inhabituelle du personnel.

En outre, les scandales liés à la protection des données, les nouvelles technologies et le nouveau cadre de protection des données de l'UE ont davantage sensibilisé le public aux droits et obligations en matière de protection des données. Les services des APD, y compris ceux du CEPD, sont plus sollicités que jamais. Nous devons nous assurer d'être en mesure de répondre à cette demande afin de garantir la protection des droits des individus.

Fin 2014, tenant compte de la nécessité d'étoffer notre personnel, nous avons demandé à l'Office européen de sélection du personnel (EPSO) d'organiser un concours pour les spécialistes de la protection des données. Une liste de réserve destinée à pourvoir les postes vacants a été établie; nous y avons puisé les nouveaux membres du personnel à partir de 2015.

Cette liste de réserve ayant été épuisée en l'espace de trois ans, nous avons lancé, au cours de l'été 2018, un nouveau concours public pour 30 administrateurs dans le domaine de la protection des données. Une liste a été finalisée au milieu de l'année 2019, nous fournissant une nouvelle réserve d'experts à partir de laquelle nous allons recruter des membres du personnel. Nous pourrons ainsi faire face à la croissance du secrétariat du comité européen de la protection des données et accomplir les nouvelles tâches qui nous ont été confiées par le législateur, comme le contrôle d'Eurojust et du Parquet européen. Depuis la fin de 2018, le CEPD se prépare à reprendre la responsabilité de la supervision d'Eurojust à compter du 12 décembre 2019; il est régulièrement en contact avec ses homologues d'Eurojust, avec lesquels il échange des connaissances, mène des actions de sensibilisation et recense les priorités pour les premiers mois de la supervision.

En plus d'organiser ces concours, nous avons également adopté une politique de maintien des effectifs en 2016, que nous avons révisée en 2017, en tenant compte des résultats de l'enquête que nous avons menée auprès du personnel en 2016. Cette politique vise à garantir le maintien des membres du personnel talentueux, compétents et créatifs que nous recrutons, en leur offrant des conditions de travail plus flexibles et de meilleures perspectives d'évolution personnelle et professionnelle, mais aussi à encourager les

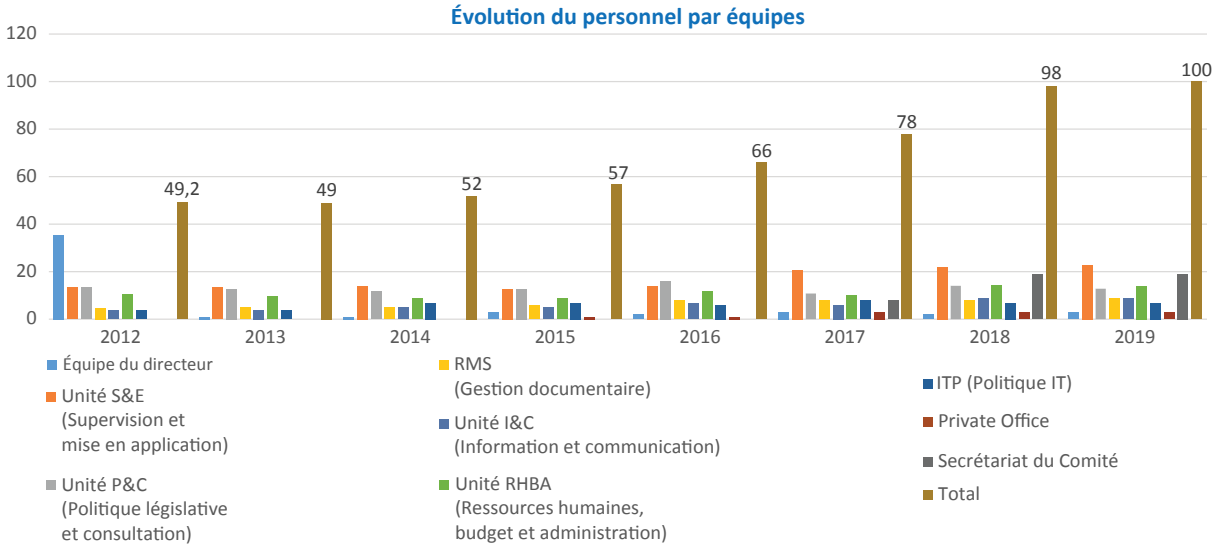


Illustration 16. Évolution du personnel par équipes (jusqu'au 30 juin 2019)

cadres et à leur rappeler qu'ils doivent entretenir la motivation de leur personnel en leur fournissant des témoignages de reconnaissance et des commentaires constructifs.

Après avoir adopté ce nouveau plan de recrutement, un défi s'est posé à nous, celui d'accueillir un nombre croissant de membres du personnel. Nous avons lancé un projet, encore en cours, axé sur la maximisation des espaces de bureau dont nous disposions déjà et l'acquisition de nouveaux locaux. Le secrétariat du comité européen de la protection des données occupe le premier étage de notre bâtiment actuel ; il existe donc une séparation claire entre le secrétariat et le CEPD. Un programme de réorganisation et de rénovation des bureaux a également été lancé pour accueillir les nouveaux employés du CEPD. Nous nous efforçons de trouver une solution pour accueillir tous les membres du personnel ; des progrès supplémentaires sur ce plan sont attendus dans les prochains mois.

7.2.2 Apprentissage et perfectionnement

En juillet 2015, nous avons adopté une nouvelle stratégie en matière d'apprentissage et de perfectionnement (L&D) visant à promouvoir le perfectionnement du personnel et le renforcement de ses compétences. En vertu de la nouvelle stratégie, chaque année, tous les membres du personnel du CEPD élaborent leur propre plan de L&D, ce qui nous permet d'adopter une vision à long terme en ce qui concerne les besoins en matière d'apprentissage et de perfectionnement de notre personnel

Nous avons également lancé un programme de sessions de formation sur mesure, organisées en interne et adaptées aux besoins spécifiques des membres du personnel du CEPD. Au cours du mandat, les thèmes abordés au cours de ces sessions de formation ont inclus, entre autres, la prise de parole en public et la formation aux médias, les indicateurs clés de performance (ICP) et les analyses d'impact, les outils et procédures utilisés par le CEPD et le Comité, les nouvelles règles en matière de protection des données pour les institutions de l'UE et le règlement général sur la protection des données (RGPD), la sensibilisation aux préjugés inconscients, l'épuisement professionnel et d'autres problématiques.

À cela s'ajoute le grand projet que nous avons lancé en 2017, au titre duquel nous proposons des conseils d'orientation professionnelle à l'ensemble du personnel du CEPD. Cet exercice nous a permis de recenser les membres du personnel désireux de travailler pour le secrétariat du comité européen de la protection des données, mais il a aussi donné l'occasion aux employés du CEPD de réfléchir à leur évolution professionnelle. Tous les membres du personnel, à l'exception des cadres, ont pu bénéficier, sur une base volontaire, de sessions d'orientation professionnelle confidentielles et individuelles. Des sessions et des mesures de suivi ont été mises en place, le cas échéant.

En 2019, nous avons lancé une initiative d'encadrement interne. Cet encadrement a pour but d'améliorer les performances professionnelles de chaque employé en gérant les performances et les talents, la résilience et le perfectionnement ainsi que les relations de travail. Il met l'accent sur le renforcement des points forts et sur l'introduction des changements requis et contribue à la recherche de solutions spécifiques adaptées aux enjeux professionnels. Les sessions d'encadrement sont organisées par notre coach interne.

7.2.3 Création du secrétariat du comité européen de la protection des données – préparatifs administratifs

La création d'un secrétariat indépendant pour le comité européen de la protection des données (voir section 6.1.3) a représenté un véritable défi du point de vue logistique et organisationnel. Il nous a fallu garantir la confidentialité et la séparation des fonctions tout en préservant la coopération administrative et le rapport coût-avantages.

Les préparatifs administratifs en vue de la création du Comité ont débuté en 2013, en coopération avec nos collègues du GT29. Fin 2015, une fois que le Parlement européen et le Conseil sont parvenus à un accord politique sur le texte du RGPD, nous avons intensifié nos

efforts, en mettant sur pied un petit groupe de travail interne au CEPD et en contribuant aux travaux d'un groupe de travail du GT29. À ce stade, nous avions pour objectif d'évaluer la tâche qui nous attendait et de déterminer avec précision les mesures à prendre pour que le conseil d'administration puisse être opérationnel dès le premier jour.

En tant qu'autorité assurant le secrétariat du comité européen de la protection des données, nous devions veiller à ce que l'autorité budgétaire alloue au nouvel organisme des moyens humains et financiers suffisants et à ce que la structure administrative nécessaire à son fonctionnement soit bien en place. En 2016, nous avons, par conséquent, mis en œuvre un ambitieux plan de recrutement des ressources humaines nécessaires pour pourvoir les postes du futur Comité. Nous avons également rédigé quatre fiches d'information portant sur la création du Comité, dans lesquelles nous avons présenté notre vision. Ces fiches avaient pour thème les premiers préparatifs, les ressources humaines, les ressources financières et budgétaires et les accords sur le niveau de service signés par le CEPD. Notre objectif était d'aider les membres du GT29 à mieux comprendre notre vision et l'énergie que nous investissions dans la création du comité européen de la protection des données.

Tout en ayant à l'esprit l'établissement du Comité, nous avons également participé à la mise en œuvre du projet AGM de la Commission européenne visant à améliorer l'organisation des réunions et l'échange des documents de réunion. En septembre 2016, nous avons été désignés comme l'une des organisations pilotes de ce projet.

AGM est une application informatique conçue pour faciliter la gestion des groupes et des comités d'experts. À ce titre, cet outil s'avère particulièrement utile pour le CEPD et le secrétariat du Comité, puisqu'il leur permet de traiter automatiquement une série de tâches chronophages qui, autrement, nécessiteraient de mobiliser plusieurs membres du personnel.

Nous utilisons ce système depuis décembre 2016 pour organiser les réunions du CEPD, les réunions plénières du Comité, les réunions des sous-groupes et d'autres réunions ponctuelles. Il nous permet de gérer électroniquement les procédures d'invitation et de remboursement des experts gouvernementaux. L'illustration 17 contient des statistiques relatives au nombre de dossiers de remboursement par an jusqu'au 30 juin 2019.

En novembre 2017, nous avons créé un service chargé des questions relatives au comité européen de la protection des données. Plusieurs membres du personnel du CEPD ont été affectés à ce nouveau service pour mener à bien les tâches qui allaient permettre au Comité d'entrer en fonction en mai 2018. En mars 2018, ces employés ont emménagé dans les bureaux situés au premier étage du bâtiment du CEPD.

Nous devions veiller à ce que tous les membres du personnel du CEPD affectés au comité européen de la protection des données, ainsi que tout nouvel employé du Comité, bénéficient des mêmes droits et soient soumis aux mêmes règles que les employés du CEPD. Nous avons, par conséquent, passé en revue l'ensemble des décisions, lignes directrices et manuels existants et le directeur du CEPD a signé une décision générale. Si certaines décisions spécifiques devaient encore être mises à jour après le 25 mai 2018 pour tenir compte des spécificités du secrétariat du Comité, la majeure partie du travail a été achevée dans les délais impartis.

Nous avons également dû actualiser nos accords sur le niveau de service (ANS) avec

Opérations AGM jusqu'au 30/06/2019					
	2016	**2017**	**2018**	**2019**	**Total général**
nombre d'opérations	16	83	733	776	1608

Illustration 17. Nombre d'opérations AGM (jusqu'au 30 juin 2019)

les prestataires externes. Tandis que les ANS couvrant les membres du personnel du CEPD se sont appliqués automatiquement aux membres du personnel du secrétariat du Comité, les ANS relatifs à la fourniture de service ont dû être actualisés pour que les membres du personnel du Comité puissent utiliser ces services. Au début de l'année 2018, plusieurs ANS ont dès lors été mis à jour pour inclure le Comité. Dans les autres cas, de nouveaux ANS ont été signés directement entre le secrétariat du Comité et le prestataire de service. De cette manière, nous avons pu assurer la continuité des activités et un démarrage en souplesse du secrétariat du comité européen de la protection des données.

Une fois que le Comité a été opérationnel, nous avons lancé un programme pilote de détachement en 2019. Conformément au RGPD, le Comité et d'autres organismes sont chargés de promouvoir l'échange d'informations, de pratiques et de programmes de formation communs, mais aussi de faciliter l'échange de personnel entre les autorités de contrôle. L'unité HRBA du CEPD possédant une solide expérience en la matière, nous avons proposé d'engager un processus prévoyant l'échange de membres du personnel entre les APD ou avec le secrétariat du comité européen de la protection des données. Le projet de programme a été examiné en septembre 2018 lors d'une réunion entre les représentants des ressources humaines et du L&D des APD et la première édition du programme devrait avoir lieu en 2020.

@EU_EDPS

#GDPR rulebook will apply from 25 May 2018: let's prepare for it to strengthen rights of online generation #EUDataP

7.2.4 La conférence internationale 2018 – financement et marchés publics

En plus d'avoir choisi un thème atypique pour la conférence internationale 2018 (voir section 5.2.1), le CEPD a opté pour un mode de financement de la conférence assez inhabituel. En tant qu'autorité de contrôle indépendante, nous avons pris la décision de ne pas recourir au parrainage pour organiser la session fermée et la session publique de la conférence à Bruxelles, mais plutôt de les financer au moyen des frais d'inscription à la conférence.

Le CEPD est une institution de l'UE et, à ce titre, il doit respecter les procédures strictes de passation des marchés établies dans le règlement financier de l'UE. Étant donné que l'organisation de la conférence comprend des tâches chronophages et complexes, telles que le recensement, la sélection et l'embauche de prestataires externes, nous avons décidé de louer les services d'une entreprise spécialisée dans l'organisation d'événements pour aider et soutenir l'équipe financière du CEPD. Nous avons mis au point une procédure financière spécifique pour la conférence, qui a facilité les opérations entre le CEPD, l'organisateur de l'événement et les prestataires externes.

Pour soutenir les membres du personnel et les contrôleurs dans le cadre de leurs préparatifs en vue de la conférence, nous avons également organisé plusieurs cours de formation en communication tout au long de l'année 2018.

7.2.5 Préparer le CEPD aux nouvelles règles en matière de protection des données

En tant qu'institution de l'UE, le CEPD est non seulement chargé de la supervision et de la mise en application des nouvelles règles en matière de protection des données au sein des autres institutions et organes de l'UE, mais il doit aussi les appliquer à ses propres activités et essayer de montrer l'exemple aux autres institutions.

De nombreuses décisions relatives aux ressources humaines et aux finances étant soumises au règlement (UE) 2018/1725, nous avons entamé une révision complète de nos activités de traitement des données relatives aux ressources humaines. Dès le début de l'année 2017, nous avons participé aux travaux du groupe de travail interne sur le projet «Transition vers le nouveau règlement 45» et travaillé en étroite collaboration avec le DPD du CEPD, le DPD adjoint et l'unité «Supervision et mise en application des règles» pour établir des

registres relatifs à la protection des données. Nous avons également révisé nos avis sur la protection des données. Cet exercice nous a permis d'être pleinement préparés lorsque le nouveau règlement est entré en vigueur.

Par ailleurs, nous avons été étroitement associés aux discussions internes sur la création d'un outil de responsabilisation pour le CEPD. En 2015, le CEPD a lancé un projet visant à élaborer un cadre renforçant le principe de responsabilisation dans le domaine du traitement des données, que nous avons appliqué au CEPD à titre de test au cours de l'année 2016.

Cet outil, qui comprenait une série de questions destinées au contrôleur, au directeur, au DPD et aux membres du personnel chargés de gérer les opérations de traitement, avait pour but de veiller à ce que l'institution ait le contrôle des informations personnelles et de leur traitement licite. L'unité HRBA a fourni des commentaires au DPD du CEPD sur les questions relatives à notre domaine d'activité. Après que l'outil a été finalisé en mai 2016, l'agent responsable de la conformité au sein du CEPD a établi une feuille de route pour répondre aux questions, fournir des indications et élaborer un plan d'action interne pour l'unité HRBA.

Nous avons continué d'utiliser cet outil en 2017 et avons actualisé le questionnaire, ce qui nous a permis de démontrer la conformité au principe de responsabilisation de l'unité et, en particulier, notre volonté de garantir le respect des obligations en matière de protection des données et de produire les documents le démontrant.

ANNEXE A – CADRE JURIDIQUE

La fonction de Contrôleur européen de la protection des données a été instituée par le règlement (CE) 45/2001 du Parlement européen et du Conseil 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. Ledit règlement était fondé sur l'article 286 du traité instituant la Communauté européenne, désormais remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne. (TFUE). Il a fixé des règles appropriées pour les institutions et les organes de l'UE conformes à la législation de l'UE sur la protection des données en vigueur à l'époque. Ce règlement est entré en vigueur en 2001. Une version révisée du règlement, le règlement (UE) nº 2018/1725, est entrée en vigueur le 11 décembre 2018.

Depuis l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, l'article 16 du TFUE constitue le fondement juridique du CEPD. L'article 16 souligne l'importance de la protection des données à caractère personnel d'une manière plus générale. Tant l'article 16 du TFUE que l'article 8 de la charte des droits fondamentaux de l'Union européenne prévoient que le respect des règles en matière de protection des données doit être soumis au contrôle d'une autorité indépendante. Au niveau de l'Union européenne, ce pouvoir est délégué au CEPD.

Les autres actes pertinents de l'UE concernant la protection des données sont :

- La directive 95/46/CE, qui a été remplacée par le règlement 2016/679, le règlement général sur la protection des données (RGPD), le 25 mai 2018. Le RGPD définit le cadre général de la législation des États membres en matière de protection des données.
- La directive 2002/58/CE relative à la vie privée et aux communications électroniques (telle que modifiée par la directive 2009/136). Un nouveau règlement sur la vie privée et les communications électroniques est en cours de négociation.
- La directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

Contexte

L'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales consacre le droit au respect de la vie privée et familiale et définit les conditions dans lesquelles ce droit peut faire l'objet de limitations. Cependant, en 1981, il est apparu nécessaire d'adopter une convention distincte en matière de protection des données, afin d'élaborer une approche positive et structurelle de la protection des droits fondamentaux et des libertés fondamentales, qui peut être affectée par le traitement des données à caractère personnel dans une société moderne. Cette convention, également appelée « Convention 108 », a été ratifiée par près de quarante pays membres du Conseil de l'Europe, dont l'ensemble des États membres de l'UE. La convention 108 sera modifiée par son protocole (STCE nº 223) dès son entrée en vigueur.

La directive 95/46/CE, qui a précédé le RGPD, a repris les principes de la convention 108, en les précisant et en les développant de diverses manières. L'objectif était d'assurer un niveau élevé de protection et de permettre la libre

circulation des données à caractère personnel au sein de l'UE. Quand la Commission a présenté la proposition de directive au début des années 1990, elle a indiqué qu'il faudrait prévoir pour les institutions et organes communautaires des garanties juridiques similaires, afin de leur permettre de participer à la libre circulation des données à caractère personnel moyennant des règles de protection équivalentes. Cependant, jusqu'à l'adoption de l'article 286 du traité instituant la Communauté européenne, il n'existait pas de base juridique pour un tel instrument.

Le 6 avril 2016, l'UE a convenu de réformer en profondeur son cadre de protection des données, en remplaçant l'ancienne directive par le RGPD. Le RGPD est une étape essentielle dans le renforcement des droits fondamentaux des citoyens à l'ère numérique. Il est axé sur le renforcement des droits des personnes, l'approfondissement du marché intérieur européen, un contrôle plus strict du respect des règles, la rationalisation des transferts internationaux de données à caractère personnel et l'établissement de normes globales de protection de données.

En outre, le RGPD élargit le champ d'application territorial des règles de l'UE en matière de protection des données, prévoit l'application de sanctions administratives, renforce les conditions du consentement et permet aux citoyens de mieux contrôler leurs données à caractère personnel, notamment en y facilitant l'accès.

Le traité de Lisbonne renforce la protection des droits fondamentaux de différentes façons. Le respect de la vie privée et familiale et la protection des données à caractère personnel sont traités comme des droits fondamentaux distincts dans les articles 7 et 8 de la Charte. Ils sont juridiquement contraignants, tant pour les institutions et les organes de l'UE que pour les États membres, lorsqu'ils appliquent le droit de l'Union. La protection des données est également traitée comme un sujet horizontal dans l'article 16 du TFUE. Il ne fait, dès lors, aucun doute que la protection des données est considérée comme étant une composante clé de la *bonne gouvernance*. Un contrôle indépendant est un élément essentiel de cette protection.

Règlement (CE) nº 45/2001

En examinant de plus près le règlement (CE) nº 45/2001, il convient de noter dans un premier temps que, conformément à l'article 3, paragraphe 1, il s'applique au *traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire*. Cependant, depuis l'entrée en vigueur du traité de Lisbonne et l'abolition de la structure en piliers, qui ont rendu obsolètes les références aux *institutions communautaires* et au *droit communautaire*, le règlement couvre en principe l'ensemble des institutions et des organes de l'UE, sauf dans les cas où d'autres actes de l'UE en disposent autrement.

Les définitions et la teneur du règlement s'inspirent très largement des principes de la directive 95/46/CE. On pourrait dire que le règlement (CE) 45/2001 constitue la mise en œuvre de cette directive au niveau des institutions de l'Union. Cela signifie que le règlement traite des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, les catégories particulières de données sensibles, l'information de la personne concernée, les droits de la personne concernée, les obligations des responsables du traitement (en tenant compte, le cas échéant, des circonstances propres au niveau de l'UE) ainsi que du contrôle, de l'exécution et des recours. Un chapitre particulier est consacré à la protection des données à caractère personnel et de la vie privée dans le cadre des réseaux internes de télécommunications. Ce chapitre constitue la mise en œuvre au niveau de l'Union de l'ancienne directive 97/66/CE sur la vie privée et les communications.

Règlement (UE) nº 2018/1725

Conformément à l'article 2, paragraphe 1, ce règlement s'applique *au traitement de données à caractère personnel par toutes les institutions et tous les organes de l'Union à compter du 11 décembre 2018*. Cependant, il ne s'appliquera au traitement des données à caractère personnel par Eurojust qu'à compter du 12 décembre 2019

et il ne s'applique pas au traitement par Europol et par le Parquet européen de données opérationnelles à caractère personnel, ni au traitement de données à caractère personnel dans le cadre des activités visées à l'article 42, paragraphe 1, et aux articles 43 et 44 du traité UE, telles que les activités menées dans le cadre de la politique de sécurité et de défense commune. En outre, seuls l'article 3 et le chapitre IX du règlement s'appliquent au traitement des données opérationnelles à caractère personnel par les organes, organismes et agences de l'Union dans l'exercice d'activités qui relèvent de la coopération judiciaire en matière pénale ou de la coopération policière.

Les définitions et la teneur du règlement s'inspirent très largement des principes du RGPD. On pourrait dire que le règlement (UE) 2018/1725 constitue la mise en œuvre du RGPD au niveau des institutions de l'Union. La structure du règlement (UE) 2018/1725 devrait être considérée comme le pendant de la structure du RGPD et, lorsque les dispositions dudit règlement font suite au RGPD, elles devraient être interprétées de façon homogène. Cela signifie que le règlement traite des principes généraux tels que le traitement loyal et licite, la proportionnalité et la compatibilité d'utilisation, le consentement, y compris les conditions particulières concernant les enfants, les catégories particulières des données sensibles, ainsi que la transparence, l'information et l'accès aux données à caractère personnel et les droits de la personne concernée. Il traite des obligations qui incombent aux responsables du traitement, aux responsables conjoints du traitement et aux sous-traitants, du contrôle, de l'exécution, des recours, des responsabilités et des sanctions. Une section particulière est consacrée à la protection des données à caractère personnel et de la vie privée dans le cadre des communications électroniques. Cette section constitue la mise en œuvre pour les institutions et organes de l'UE de la directive 2002/58/CE sur la vie privée et les communications électroniques.

Le règlement (CE) 45/2001 a introduit l'obligation pour les institutions et organes de l'UE de désigner au moins une personne au poste de délégué à la protection des données (DPD) ; cette obligation a été réaffirmée dans le règlement (UE) 2018/1725. Ces délégués ont pour mission de garantir l'application interne des dispositions du règlement de manière indépendante, notamment la notification des opérations de traitement. Toutes les institutions et la plupart des organes ont désormais un délégué qui, dans certains cas, exerce ses fonctions depuis plusieurs années. Ces délégués sont souvent mieux placés pour fournir des conseils ou pour intervenir à un stade précoce, et pour contribuer à la mise en place de bonnes pratiques. Les délégués à la protection des données ayant l'obligation formelle de coopérer avec le CEPD, il s'est formé un réseau très important et fort apprécié, qu'il convient de développer encore (voir section 6.2.1).

Missions et compétences du CEPD

Les missions et les compétences du CEPD étaient clairement énoncées au chapitre V, en particulier aux articles 41, 46 et 47, du règlement (CE) 45/2001. Ces dispositions ont été remplacées par le chapitre VI et les articles 52, 57 et 58 du règlement (UE) 2018/1725 (voir l'annexe B), à la fois en termes généraux et spécifiques. L'article 41 du règlement (CE) 45/2001 [article 52 du règlement (UE) 2018/1725] définit la mission principale du CEPD, qui consiste à veiller à ce que les libertés et les droits fondamentaux des personnes physiques, notamment leur droit à la protection des données, en ce qui concerne le traitement des données à caractère personnel, soient respectés par les institutions et organes de l'UE. Il fixe aussi dans leurs grandes lignes certains aspects de cette mission. Ces responsabilités générales sont développées et précisées aux articles 46 et 47 du règlement (CE) 45/2001 et aux articles 57 et 58 du règlement (UE) 2018/1725, lesquels comportent une énumération détaillée des missions et des compétences.

Cette présentation des attributions, fonctions et compétences suit, pour l'essentiel, le même schéma que pour les autorités nationales de contrôle : entendre et examiner les réclamations, effectuer des enquêtes, informer le responsable du traitement et les personnes concernées et effectuer des contrôles préalables lorsque les opérations de traitement présentent des risques particuliers. Le règlement habilite le CEPD à

obtenir l'accès à toutes les informations utiles et aux locaux pertinents lorsque cela est nécessaire pour ses enquêtes. Le CEPD peut aussi imposer des sanctions, lesquelles incluent désormais des sanctions administratives, et saisir la Cour de justice.

Certaines tâches revêtent une nature particulière. La tâche consistant à conseiller la Commission et les autres institutions de l'UE à propos des nouvelles dispositions législatives [confirmée à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 et à l'article 42 du règlement (UE) 2018/1725, par l'obligation formelle qui est faite à la Commission de consulter le CEPD lorsqu'elle adopte une proposition législative relative à la protection des données à caractère personnel)] concerne aussi les projets d'actes délégués ou d'exécution et les mesures relatives aux accords internationaux. Il s'agit d'une fonction stratégique qui permet au CEPD de se pencher, très tôt, sur les implications possibles au regard de la protection de la vie privée et d'envisager différentes approches possibles. Par ailleurs, conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725, la Commission européenne peut consulter le comité européen de la protection des données, qui a été institué pour conseiller la Commission européenne et élaborer des politiques harmonisées au titre du RGPD, lorsqu'une proposition *revêt une importance particulière pour la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel*. Dans ce cas, le CEPD et le comité européen de la protection des données *coordonnent leurs travaux en vue de formuler un avis conjoint*.

Le CEPD a également pour mission importante d'intervenir dans le cadre des recours directs introduits devant la Cour de justice et de répondre aux invitations de la Cour à répondre à des questions ou, dans d'autres cas, à fournir des informations sur la base de l'article 24 du statut de la Cour. Les plaidoiries du CEPD sont généralement disponibles sur notre site web. Depuis décembre 2015, le CEPD a pris part à plusieurs affaires très médiatisées, notamment :

- Affaire C-615/13P Client Earth et Pan Europe contre Autorité européenne de sécurité des aliments (EFSA)
- Affaire C-362/14 Maximillian Schrems contre Data Protection Commissioner (voir section 5.2.3)
- Avis 1/15 Projet d'accord entre le Canada et l'Union européenne – Transfert des données des dossiers passagers aériens depuis l'Union vers le Canada (section 5.2.4)
- Audition commune dans l'affaire C-623/17 (Privacy International) avec les affaires conjointes C-511/18 et C-512/18 (La Quadrature du Net e.a.) et l'affaire C-520/18 (Ordre des barreaux francophone et germanophone e.a.)

La coopération avec les autorités nationales de contrôle et la coopération avec les organes de contrôle relevant de l'ancien *troisième pilier* revêtent également une importance stratégique. La coopération avec les organes de contrôle relevant de l'ancien *troisième pilier* permet au CEPD d'observer les faits nouveaux qui surviennent dans ce contexte et de contribuer à l'élaboration d'un cadre plus cohérent et homogène pour la protection des données à caractère personnel, quel que soit le *pilier* ou le contexte particulier concerné. Le cadre juridique précédent ne prévoyait pas de modèle cohérent de contrôle coordonné. L'article 62 du règlement (UE) 2018/1725 autorise désormais la mise en œuvre d'un modèle unique de contrôle coordonné des systèmes d'information à grande échelle et des organes et organismes de l'Union par le CEPD et les autorités de contrôle nationales.

ANNEXE B – EXTRAIT DU RÈGLEMENT (EU) 2018/1725

Article 41 – Information et consultation

1. Les institutions et organes de l'Union informent le Contrôleur européen de la protection des données lorsqu'ils élaborent des mesures administratives et des règles internes relatives au traitement de données à caractère personnel par une institution ou un organe de l'Union, que ce soit seuls ou conjointement avec d'autres.
2. Les institutions et organes de l'Union consultent le Contrôleur européen de la protection des données lorsqu'ils élaborent les règles internes visées à l'article 25.

Article 42 – Consultation législative

1. À la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel.
2. Lorsqu'un acte visé au paragraphe 1 revêt une importance particulière pour la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel, la Commission peut également consulter le comité européen de la protection des données. Dans ce cas, le Contrôleur européen de la protection des données et le comité européen de la protection des données coordonnent leurs travaux en vue de formuler un avis conjoint.
3. Les avis visés aux paragraphes 1 et 2 sont communiqués par écrit dans un délai maximal de huit semaines à compter de la réception de la demande de consultation prévue aux paragraphes 1 et 2. En cas d'urgence ou s'il y a autrement lieu, la Commission peut réduire ce délai.
4. Le présent article ne s'applique pas lorsque le règlement (UE) 2016/679 fait obligation à la Commission de consulter le comité européen de la protection des données.

Article 52 – Contrôleur européen de la protection des données

1. La fonction de Contrôleur européen de la protection des données est instituée.
2. En ce qui concerne le traitement de données à caractère personnel, le Contrôleur européen de la protection des données est chargé de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union.
3. Le Contrôleur européen de la protection des données est chargé de contrôler et d'assurer l'application des dispositions du présent règlement et de tout autre acte de l'Union concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe de l'Union, ainsi que de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel. À ces fins, le Contrôleur européen de la protection des données remplit les missions prévues à l'article 57 et exerce les pouvoirs qui lui sont conférés à l'article 58.
4. Le règlement (CE) 1049/2001 s'applique aux documents détenus par le Contrôleur

européen de la protection des données. Le Contrôleur européen de la protection des données adopte des modalités d'application du règlement (CE) 1049/2001 en ce qui concerne ces documents.

Article 57 – Missions

1. Sans préjudice des autres missions prévues par le présent règlement, le Contrôleur européen de la protection des données :
   a. contrôle et assure l'application du présent règlement par une institution ou un organe de l'Union, à l'exclusion du traitement de données à caractère personnel par la Cour dans l'exercice de ses fonctions juridictionnelles ;
   b. favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement. Les activités destinées spécifiquement aux enfants font l'objet d'une attention particulière ;
   c. encourage la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du présent règlement ;
   d. fournit, sur demande, à toute personne concernée des informations sur l'exercice des droits que lui confère le présent règlement et, si nécessaire, coopère, à cette fin, avec les autorités de contrôle nationales ;
   e. traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 67, examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ;
   f. effectue des enquêtes sur l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique ;
   g. conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel ;
   h. suit les évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et des communications ;
   i. adopte les clauses contractuelles types visées à l'article 29, paragraphe 8, et à l'article 48, paragraphe 2, point c) ;
   j. établit et tient à jour une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 39, paragraphe 4 ;
   k. participe aux activités du comité européen de la protection des données ;
   l. assure le secrétariat du comité européen de la protection des données, conformément à l'article 75 du règlement (UE) 2016/679 ;
   m. fournit des conseils concernant le traitement visé à l'article 40, paragraphe 2 ;
   n. autorise les clauses contractuelles et les dispositions visées à l'article 48, paragraphe 3 ;
   o. tient des registres internes des violations du présent règlement et des mesures prises conformément à l'article 58, paragraphe 2 ;
   p. s'acquitte de toute autre mission relative à la protection des données à caractère personnel ; et
   q. établit son règlement intérieur.
2. Le Contrôleur européen de la protection des données facilite l'introduction des réclamations visées au paragraphe 1, point e), par la mise à disposition d'un formulaire de réclamation qui peut aussi être rempli par voie électronique, sans que d'autres moyens de communication ne soient exclus.
3. L'accomplissement des missions du Contrôleur européen de la protection des données est gratuit pour la personne concernée.

4. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, le Contrôleur européen de la protection des données peut refuser d'y donner suite. Il incombe au Contrôleur européen de la protection des données de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 58 – Pouvoirs

1. Le Contrôleur européen de la protection des données dispose des pouvoirs d'enquête suivants :
   a. ordonner au responsable du traitement et au sous-traitant de lui communiquer toute information dont il a besoin pour l'accomplissement de ses missions ;
   b. mener des enquêtes sous la forme d'audits sur la protection des données ;
   c. notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement ;
   d. obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions ;
   e. obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation de traitement et à tout moyen de traitement, conformément au droit de l'Union.
2. Le Contrôleur européen de la protection des données dispose du pouvoir d'adopter les mesures correctrices suivantes :
   a. avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement ;
   b. rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement ;
   c. saisir le responsable du traitement ou le sous-traitant concerné et, si nécessaire, le Parlement européen, le Conseil et la Commission ;
   d. ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement ;
   e. ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ;
   f. ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel ;
   g. imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;
   h. ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en vertu des articles 18, 19 et 20 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 19, paragraphe 2, et de l'article 21 ;
   i. imposer une amende administrative, en application de l'article 66, dans le cas où une institution ou un organe de l'Union ne se conformerait pas à l'une des mesures visées aux points d) à h) et j) du présent paragraphe, en fonction des circonstances propres à chaque cas ;
   j. ordonner la suspension des flux de données adressés à un destinataire situé dans un État membre ou un pays tiers ou à une organisation internationale.
3. Le Contrôleur européen de la protection des données dispose des pouvoirs d'autorisation et des pouvoirs consultatifs suivants :
   a. conseiller les personnes concernées sur l'exercice de leurs droits ;
   b. conseiller le responsable du traitement conformément à la procédure de consultation préalable visée à l'article 40, et conformément à l'article 41, paragraphe 2 ;
   c. émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public, sur toute question relative

à la protection des données à caractère personnel ;
d. adopter les clauses types de protection des données visées à l'article 29, paragraphe 8, et à l'article 48, paragraphe 2, point c) ;
e. autoriser les clauses contractuelles visées à l'article 48, paragraphe 3, point a) ;
f. autoriser les arrangements administratifs visés à l'article 48, paragraphe 3, point b) ;
g. autoriser des opérations de traitement en vertu d'actes d'exécution adoptés au titre de l'article 40, paragraphe 4.

4. Le Contrôleur européen de la protection des données a le pouvoir de saisir la Cour dans les conditions prévues par les traités et d'intervenir dans les affaires portées devant la Cour.
5. L'exercice des pouvoirs conférés au Contrôleur européen de la protection des données en vertu du présent article est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévu par le droit de l'Union.

ANNEXE C – LE RÔLE DU CEPD

Surveillance et contrôle de l'application des règles

Le CEPD est chargé de s'assurer non seulement que les institutions de l'UE sont conscientes des obligations qui leur incombent en matière de protection des données, mais aussi qu'elles peuvent être tenues responsables du respect de ces règles. Nous disposons de plusieurs outils, qui visent tous à encourager le développement d'une culture de la protection des données au sein des institutions de l'UE

- **Contrôles préalables/consultations préalables :** en vertu du règlement (CE) nº 45/2001, les institutions et organes de l'UE devaient informer le CEPD de toute procédure qu'ils envisageaient de mener et qui était susceptible de porter atteinte à la protection des données à caractère personnel. Nous avons examiné les propositions et avons formulé des recommandations sur la manière de gérer ces risques. Conformément au nouveau règlement, les contrôles préalables n'existent plus sous cette forme. Cependant, dans certains cas, les institutions et organes de l'UE doivent consulter le CEPD après avoir réalisé une analyse d'impact sur la protection des données d'une procédure envisagée qui comporte des risques.
- **Réclamations :** nous traitons les réclamations des personnes physiques concernant le traitement de leurs données à caractère personnel par les institutions de l'UE. Nous examinons ces réclamations et envisageons la meilleure manière de les traiter.
- **Contrôle de la conformité :** le CEPD a pour mission de veiller à ce que l'ensemble des institutions et des organes de l'UE respecte les règles en matière de protection des données. Nous contrôlons le respect de ces règles de plusieurs façons, notamment au moyen de visites et d'inspections.
- **Consultations relatives aux mesures administratives :** nous publions des avis sur les mesures administratives relatives au traitement des données à caractère personnel, en réponse à une demande spécifique émanant d'une institution de l'Union ou de notre propre initiative.
- **Lignes directrices :** nous publions des lignes directrices pour les institutions de l'UE afin de les aider à mieux mettre en œuvre les principes de la protection des données et de respecter les règles en matière de protection des données.
- **Collaboration avec les délégués à la protection des données :** chaque institution et organe de l'UE doit désigner un DPD, qui a pour mission de veiller à ce que son institution respecte les règles en matière de protection des données. Nous collaborons étroitement avec les DPD ; nous les formons et leur offrons un soutien afin qu'ils puissent s'acquitter efficacement de leur tâche.
- **Formation des institutions et organes de l'UE :** nous offrons des sessions de formation aux cadres et aux membres du personnel des institutions et organes de l'UE. Ces sessions de formation contribuent à garantir le respect des règles en matière de protection des données et le respect des droits et libertés des personnes physiques, mais aussi à promouvoir le développement d'une culture de la protection des données au sein de chaque institution. Elles ont pour but d'aider les institutions à aller au-delà du respect des règles et à faire preuve de responsabilisation.

Politique et consultation

Le CEPD fournit des conseils au législateur de l'Union sur les questions de protection des

données. Nous entendons faire en sorte que les exigences en matière de protection des données soient intégrées à toute nouvelle législation/initiative stratégique et à tout nouvel accord international. Pour ce faire, nous fournissons des conseils sur les propositions législatives à la Commission européenne, en tant que détentrice du droit d'initiative législative, et au Parlement européen et au Conseil, en tant que colégislateurs. Nous disposons de plusieurs outils pour nous aider dans cette tâche :

- **Observations informelles** : conformément à la pratique établie, la Commission est encouragée à consulter le CEPD de manière informelle avant d'adopter une proposition ayant des conséquences en matière de protection des données [considérant 60 du règlement (UE) 2018/1725]. Cette pratique nous permet de nourrir la réflexion de la Commission à un stade précoce du processus législatif, généralement au moyen d'observations informelles, qui ne sont pas publiées.
- **Avis :** nos avis officiels sont disponibles sur notre site web et des résumés dans toutes les langues officielles sont publiés au *Journal officiel de l'Union européenne*. Nous rédigeons des avis pour mettre en évidence nos principales préoccupations et recommandations en matière de protection des données concernant des propositions législatives ou d'autres mesures. Nous publions des avis de notre propre initiative ou sur demande, que nous adressons aux trois institutions de l'UE mobilisées dans le processus législatif.
- **Observations formelles :** à l'instar de nos avis, nos observations formelles portent sur les conséquences des propositions législatives pour la protection des données. Cependant, elles sont généralement plus succinctes et plus techniques, ou ne portent que sur certains aspects d'une proposition. Nous publions les observations formelles sur notre site web.
- **Affaires traitées devant la Cour :** nous pouvons intervenir et mettre notre expertise en matière de protection des données au service des juridictions de l'Union, en intervenant pour soutenir une des parties dans une affaire, ou à l'invitation des juridictions (voir l'annexe A).
- **Coopération internationale, y compris avec les APD nationales :** nous coopérons avec les APD nationales par l'intermédiaire du comité européen de la protection des données. Nous collaborons également avec les APD nationales pour garantir l'application d'une approche cohérente et coordonnée en ce qui concerne le contrôle de plusieurs bases de données de l'UE. Nous coopérons avec des organisations internationales pour promouvoir une culture de la protection des données et nous suivons de près les évolutions pertinentes au sein de l'OCDE, du Conseil de l'Europe et d'autres instances. Le CEPD est un membre actif de l'ICDPPC.

Suivi des évolutions technologiques

Le CEPD suit les évolutions technologiques et leur incidence sur la protection des données et le respect de la vie privée. Nos connaissances et notre expertise dans ce domaine nous permettent de remplir efficacement nos obligations en matière de contrôle et de consultation. Cette capacité et ces compétences continueront à prendre de l'importance, en raison des changements introduits par le RGPD, la directive relative à la protection des données par les secteurs de la police et de la justice et le règlement (UE) 2018/1725 destiné aux institutions et organes de l'UE. Nos activités sont les suivantes :

- **Suivre les avancées technologiques et y faire face :** nous suivons les avancées, les événements et les incidents technologiques et évaluons leur incidence sur la protection des données. Cela nous permet de fournir des conseils sur des questions techniques, notamment en lien avec les missions de contrôle et de consultation du CEPD.
- **Promouvoir l'ingénierie de la vie privée :** en 2014, nous avons lancé le réseau d'ingénierie de la vie privée sur l'internet (IPEN) en collaboration avec les APD nationales, des développeurs et des chercheurs de l'industrie, du monde académique et des représentants de la société civile. Cette initiative vise à la fois à développer des pratiques d'ingénierie qui tiennent compte des préoccupations relatives au respect de

la vie privée et à encourager les ingénieurs à intégrer des mécanismes de protection de la vie privée dans les normes, services et applications utilisés sur l'internet.

- **Définir l'état des connaissances actuelles dans le domaine de la protection des données dès la conception :** le RGPD et le règlement (UE) 2018/1725 étant désormais pleinement applicables, tous les responsables du traitement ont l'obligation légale de tenir compte de l'état actuel des connaissances quant aux technologies respectueuses de la protection des données lorsqu'ils conçoivent, entretiennent et exploitent des systèmes informatiques de traitement des données à caractère personnel. Pour garantir l'application cohérente de cette règle dans l'ensemble de l'UE, les APD doivent coopérer pour parvenir à une compréhension commune des connaissances actuelles et de leur évolution.

ANNEXE D – LISTE DES AVIS ET DES OBSERVATIONS FORMELLES SUR LES PROPOSITIONS LÉGISLATIVES

L'ensemble des avis, des observations formelles et des autres documents publiés par le CEPD entre le 1er janvier 2015 et le 30 septembre 2019 est repris ci-dessous. Veuillez vous reporter au site web du CEPD pour les traductions et les résumés de ces documents.

2019

Avis

- Signification ou notification des actes et obtention des preuves en matière civile ou commerciale 2018 (13 septembre 2019)
- Avis conjoint du comité européen de la protection des données et du CEPD concernant le traitement des données des patients et le rôle de la Commission européenne dans l'infrastructure de services numériques dans le domaine de la santé en ligne (eHDSI) (9 juillet 2019)
- Accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques (2 avril 2019)
- Convention de Budapest sur la cybercriminalité (2 avril 2019)
- Lutte contre la fraude à la TVA (14 mars 2019)

Observations formelles

- Propositions concernant les règlements visant à établir les conditions d'accès à d'autres systèmes d'information de l'UE aux fins d'ETIAS (15 mars 2019)
- Proposition de la Commission relative à la prévention de la diffusion de contenus à caractère terroriste en ligne (13 février 2019)
- Les gestionnaires de crédit, les acheteurs de crédit et le recouvrement de garantie (25 janvier 2019)
- Proposition de refonte de la directive relative au retour (10 janvier 2019)

2018

Avis

- Paquet de mesures de la Commission concernant des élections européennes libres et équitables (18 décembre 2018)
- Amélioration du système d'information sur les visas (13 décembre 2018)
- Une nouvelle donne pour les consommateurs (5 octobre 2018)
- Sécurité des cartes d'identité et des documents de résidence des citoyens de l'UE et des membres de leur famille (10 août 2018)
- Utilisation d'outils et de processus numériques en droit des sociétés (26 juillet 2018)
- Directive concernant la réutilisation des informations du secteur public (ISP) (10 juillet 2018)
- Respect de la vie privée dès la conception (31 mai 2018)
- Interopérabilité des systèmes d'information à grande échelle de l'UE (16 avril 2018)
- Manipulation en ligne et données à caractère personnel (19 mars 2018)
- Échange de données entre Europol et des pays tiers (14 mars 2018)
- Proposition de règlement du Conseil relatif à la compétence, la reconnaissance et l'exécution des décisions en matière matrimoniale et en matière de responsabilité parentale, ainsi qu'à l'enlèvement international d'enfants) (refonte du règlement Bruxelles II bis) (15 février 2018)

Observations formelles

- Corps européen de gardes-frontières et de garde-côtes (30 novembre 2018)
- Obligations garanties et surveillance publique des obligations garanties (12 octobre 2018)
- Faciliter l'utilisation d'informations financières et d'autre nature aux fins de la prévention et de la détection de certaines infractions pénales, et des enquêtes et des poursuites en la matière (10 septembre 2018)
- Assurance de la responsabilité civile résultant de la circulation de véhicules automoteurs (26 juillet 2018)
- Révision du règlement OLAF (24 juillet 2018)
- Migration et protection internationale (18 juillet 2018)
- Contrôle des pêches (18 juillet 2018)
- Le droit d'auteur dans le marché unique numérique (3 juillet 2018)
- La libre circulation des données à caractère non personnel dans l'Union européenne (8 juin 2018)
- Autorité européenne du travail (30 mai 2018)
- Filtrage des investissements directs étrangers dans l'Union européenne (12 avril 2018)
- Fraude dans le domaine de la TVA et coopération administrative (8 mars 2018)
- Élargissement du champ d'application du système d'information sur les visas (VIS) pour y inclure des données concernant les visas de long séjour et les documents de séjour (9 février 2018)

2017

Avis

- Avis sur le système ECRIS-TCN (12 décembre 2017)
- Proposition de règlement concernant les statistiques intégrées sur les exploitations agricoles (20 novembre 2017)
- Proposition de règlement relatif à l'eu-LISA (9 octobre 2017)
- Recommandations du CEPD au stade actuel du processus législatif au sujet du règlement relatif à la vie privée et aux communications électroniques (5 octobre 2017)
- Proposition de la Commission d'un règlement du Parlement européen et du Conseil établissant un portail numérique unique (1er août 2017)
- Paquet de mesures législatives abrogeant la base juridique actuelle du système d'information Schengen (SIS) (3 mars 2017)
- Proposition de règlement relatif à la vie privée et aux communications électroniques (24 avril 2017)
- Règlement (CE) nº 45/2001 (15 mars 2017)
- Contenu numérique (14 mars 2017)
- ETIAS (6 mars 2017)
- Proposition d'un cadre commun pour des statistiques européennes relatives aux personnes et aux ménages (1er mars 2017)
- Proposition modifiant la directive (UE) 2015/849 et la directive 2009/101/CE, accès aux informations sur les bénéficiaires effectifs et conséquences sur la protection des données (lutte contre le blanchiment de capitaux) (2 février 2017)

Observations formelles

- Proposition de règlement relatif à l'initiative citoyenne européenne (19 décembre 2017)
- Le paquet cybersécurité (15 décembre 2017)
- Consultation publique sur l'abaissement de l'âge pour le relevé des empreintes digitales dans le cadre de la procédure de visa (19 novembre 2017)
- Règlement délégué de la Commission complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne «la mise à disposition, dans l'ensemble de l'Union, de services d'informations sur les déplacements multimodaux» (22 août 2017)
- Proposition à l'examen visant à modifier le règlement (CE) nº 883/2004 du Parlement européen et du Conseil du 29 avril 2004 sur la coordination des systèmes de sécurité sociale (le «règlement de base») et son règlement d'application, le règlement (CE) nº 987/2009 (le «règlement d'exécution») (8 mai 2017)
- Proposition de règlement du Parlement européen et du Conseil relatif aux contrôles d'argent liquide entrant dans l'Union ou sortant de l'Union et abrogeant le règlement (CE) nº 1889/2005 (21 février 2017)

Autres documents

- Document de synthèse sur l'interopérabilité des systèmes d'information au sein de l'espace de liberté, de sécurité et de justice (17 novembre 2017)
- Évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel (11 avril 2017)

2016

Avis

- Systèmes de gestion des informations personnelles (20 octobre 2016)
- Application cohérente des droits fondamentaux à l'ère des données massives (Big Data) (23 septembre 2016)
- Le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin) (21 septembre 2016)
- Le deuxième train de mesures «Frontières intelligentes» de l'Union européenne (21 septembre 2016)
- Vie privée et communications électroniques (22 juillet 2016)
- Le «bouclier vie privée UE-États-Unis» (Privacy Shield) – Projet de décision d'adéquation (30 mai 2016)
- Échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS) (13 avril 2016)
- Corps européen de gardes-frontières et de gardes-côtes (18 mars 2016)
- Accord-cadre UE-États-Unis (12 février 2016)

Observations formelles

- Règlement d'exécution de la Commission fixant des règles détaillées relatives à l'application de la politique d'utilisation raisonnable, à la méthode pour évaluer la viabilité de la suppression des frais d'itinérance supplémentaires au détail et aux informations que le fournisseur de services d'itinérance doit transmettre aux fins de cette évaluation (14 décembre 2016)
- Proposition modifiant la directive 98/41 relative à l'enregistrement des personnes voyageant à bord de navires à passagers (9 décembre 2016)

2015

Avis

- Diffusion et utilisation de technologies de surveillance intrusive (15 décembre 2015)
- Relever les défis des données massives (19 novembre 2015)
- Recommandations sur la directive pour la protection des données dans les secteurs police et justice (28 octobre 2015) Tableau comparatif mis à jour (7 décembre 2015)
- L'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (24 septembre 2015)
- Vers une nouvelle éthique numérique: données, dignité et technologie (11 septembre 2015)
- Recommandations relatives aux options de l'UE en matière de réforme de la protection des données (27 juillet 2015)
- Accord entre l'UE et la Suisse sur l'échange automatique d'informations fiscales (8 juillet 2015)
- La santé mobile: concilier innovation technologique et protection des données (21 mai 2015)

Observations formelles

- Consultation publique de la Commission européenne sur les plates-formes en ligne (16 décembre 2015)
- Consultation publique de la Commission européenne sur les frontières intelligentes (3 novembre 2015)
- Stratégie du réseau des agences des médicaments de l'UE à l'horizon 2020 – Collaborer pour améliorer la santé (25 mars 2015)
- L'échange d'informations dans le domaine fiscal (17 juin 2015)
- Services d'informations en temps réel sur la circulation dans l'ensemble de l'Union (21 janvier 2015 et 17 juin 2015)

Comment prendre contact avec l'Union européenne?

En personne

Dans toute l'Union européenne, des centaines de centres d'information Europe Direct sont à votre disposition. Pour connaître l'adresse du centre le plus proche, visitez la page suivante : https://europa.eu/european-union/contact_fr

Par téléphone ou courrier électronique

Europe Direct est un service qui répond à vos questions sur l'Union européenne. Vous pouvez prendre contact avec ce service:
– par téléphone: via un numéro gratuit: 00 800 6 7 8 9 10 11 (certains opérateurs facturent cependant ces appels),
– au numéro de standard suivant: +32 22999696;
– par courrier électronique via la page : https://europa.eu/european-union/contact_fr

Comment trouver des informations sur l'Union européenne?

En ligne

Des informations sur l'Union européenne sont disponibles, dans toutes les langues officielles de l'UE, sur le site internet Europa à l'adresse : https://europa.eu/european-union/index_fr

Publications de l'Union européenne

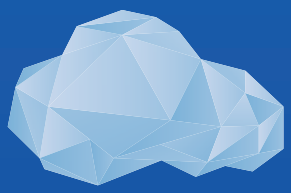
Vous pouvez télécharger ou commander des publications gratuites et payantes à l'adresse : https://publications.europa.eu/fr/publications. Vous pouvez obtenir plusieurs exemplaires de publications gratuites en contactant Europe Direct ou votre centre d'information local (https://europa.eu/european-union/contact_fr).

Droit de l'Union européenne et documents connexes

Pour accéder aux informations juridiques de l'Union, y compris à l'ensemble du droit de l'UE depuis 1952 dans toutes les versions linguistiques officielles, consultez EUR-Lex à l'adresse suivante : http://eur-lex.europa.eu

Données ouvertes de l'Union européenne

Le portail des données ouvertes de l'Union européenne (http://data.europa.eu/euodp/fr) donne accès à des ensembles de données provenant de l'UE. Les données peuvent être téléchargées et réutilisées gratuitement, à des fins commerciales ou non commerciales.



www.edps.europa.eu 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1

@EU_EDPS
EDPS
European Data Protection Supervisor

Office des publications
de l'Union européenne