COMMISSION
EUROPÉENNE

Bruxelles, le 24.6.2020
COM(2020) 264 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique - deux années d'application du règlement général sur la protection des données

{SWD(2020) 115 final}

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique - deux années d'application du règlement général sur la protection des données

1 LES RÈGLES EN MATIÈRE DE PROTECTION DES DONNÉES: UN PILIER DE L'AUTONOMISATION DES CITOYENS ET DE L'APPROCHE DE L'UNION À L'ÉGARD DE LA TRANSITION NUMÉRIQUE

Le présent rapport est le premier rapport élaboré conformément à l'article 97 du règlement général sur la protection des données[1] (ci-après le «RGPD») concernant l'évaluation et le réexamen de celui-ci, et en particulier l'application et le fonctionnement des règles relatives au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, ainsi que des règles en matière de coopération et de contrôle de la cohérence.

Le RGPD, applicable depuis le 25 mai 2018, constitue l'élément central du cadre de l'UE[2] garantissant le droit fondamental à la protection des données, tel qu'il est inscrit dans la charte des droits fondamentaux de l'Union européenne (article 8) et les traités (article 16 du traité sur le fonctionnement de l'Union européenne, ci-après le «TFUE»). Le RGPD a renforcé les garanties apportées en matière de protection des données. Il confère aux citoyens des droits supplémentaires et renforcés, accroît la transparence et garantit une plus grande responsabilité de l'ensemble des acteurs du traitement des données à caractère personnel qui relèvent de son champ d'application. Il dote les autorités indépendantes chargées de la protection des données de pouvoirs d'exécution plus solides et plus harmonisés et met en place un nouveau système de gouvernance. De même, il crée une égalité des conditions de concurrence pour toutes les entreprises exerçant des activités sur le marché de l'UE, indépendamment de leur lieu d'établissement, et garantit la libre circulation des données dans l'UE, renforçant de la sorte le marché intérieur.

Le RGPD est un élément important d'une approche de la technologie qui soit centrée sur l'être humain. Il sert de fil directeur à l'utilisation de la technologie dans le cadre de la double transition écologique et numérique qui caractérise l'élaboration des politiques de l'UE. Cela a été souligné tout récemment dans le livre blanc sur l'intelligence artificielle[3], ainsi que dans la communication sur la stratégie européenne pour les données[4] (ci-après la «stratégie pour les données») de février 2020.

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119, 4.5.2016, p. 1.

[2] À la suite de son intégration dans l'accord sur l'Espace économique européen (ci-après l'«accord EEE»), le règlement s'applique également à la Norvège, à l'Islande et au Liechtenstein.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

Dans une économie de plus en plus fondée sur le traitement des données, y compris des données à caractère personnel, le RGPD constitue un outil essentiel permettant de garantir aux citoyens un meilleur contrôle de leurs données à caractère personnel, ainsi qu'un traitement légal, équitable et transparent de ces données à des fins légitimes. Le RGPD contribue par ailleurs à favoriser une innovation digne de confiance, notamment par son approche fondée sur les risques et par des principes tels que le respect de la vie privée dès la conception et par défaut. La Commission a proposé de compléter le cadre législatif relatif à la protection des données et à la vie privée[5] par le règlement «vie privée et communications électroniques»[6], qui doit remplacer l'actuelle directive «vie privée et communications électroniques»[7]. Cette proposition est actuellement examinée par les colégislateurs, et il est très important qu'elle soit adoptée rapidement.

Dans le cadre des grandes priorités définies par la Commission en vue d'une «Europe adaptée à l'ère numérique»[8] et du «pacte vert pour l'Europe»[9], de nouvelles initiatives peuvent être élaborées pour permettre aux citoyens de jouer un rôle plus actif dans la transition numérique et pour tirer profit de l'utilisation des outils numériques en vue de parvenir à une société neutre pour le climat et à un développement plus durable. Le RGPD définit un cadre pour ces initiatives et garantit que celles-ci sont conçues de façon à fournir effectivement des moyens d'action aux citoyens.

La stratégie pour les données[10] préconise la création d'un «espace européen commun des données» constituant un véritable marché unique des données, ainsi que d'espaces européens communs des données au niveau sectoriel, pertinents aux fins de la double transition écologique et numérique[11]. Pour toutes ces priorités, un cadre clair et opérationnel est essentiel en vue d'un partage de données sûr et d'une plus grande disponibilité des données. Dans le cadre de sa stratégie pour les données, la Commission a également fait part de son intention d'examiner dans sa législation future les moyens de permettre l'utilisation des données conservées dans des bases de données publiques

[5] Ce cadre législatif comprend également la directive en matière de protection des données dans le domaine répressif (directive 2016/680) et le règlement sur la protection des données pour les institutions, organes et agences de l'UE (règlement 2018/1725).

[6] Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final - 2017/03 (COD).

[7] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 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»), JO L 201 du 31.7.2002, p. 37.

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr

[9] Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions - Le pacte vert pour l'Europe [COM(2019) 640 final].

[10] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «Une stratégie européenne pour les données», COM (2020) 66 final.

[11] Ces dix espaces européens communs des données mis en place au niveau sectoriel ont trait à la santé, à la fabrication industrielle, à l'énergie, à la mobilité, à l'agriculture, aux données financières, à l'administration publique, aux compétences, au pacte vert et à la science ouverte (nuage européen pour la science ouverte).

à des fins de recherche scientifique, dans le respect du RGPD. Les espaces des données doivent être encouragés par la fédération européenne de l'informatique en nuage pour permettre un traitement des données et des services d'infrastructures en nuage conformes au RGPD. Le RGPD garantit un niveau élevé de protection des données à caractère personnel et confère aux individus un rôle central dans tous ces espaces des données, tout en offrant la souplesse nécessaire permettant de concilier des approches différentes.

La nécessité de garantir la confiance et la demande de protection des données à caractère personnel ne se limitent certainement pas à l'UE. Partout dans le monde, les citoyens accordent de plus en plus d'importance à la confidentialité et à la sécurité de leurs données. Ainsi qu'il ressort d'une enquête récente de portée mondiale[12], il s'agit selon eux d'un aspect important, qui influence leurs décisions d'achat et leur comportement en ligne. Un nombre croissant d'entreprises ont répondu à cette demande de protection de la vie privée, notamment en étendant volontairement certains des droits et garanties prévus par le RGPD à leurs clients établis en dehors de l'UE. De nombreuses entreprises promeuvent également le respect des données à caractère personnel en tant qu'atout concurrentiel et argument de vente sur le marché mondial, en offrant des produits et des services innovants assortis de solutions novatrices en matière de protection de la vie privée ou de sécurité des données. En outre, la capacité accrue des acteurs privés et publics de collecter et de traiter des données à grande échelle soulève des questions importantes et complexes, qui placent de plus en plus la protection de la vie privée au centre du débat public dans différentes parties du monde.

L'adoption du RGPD a incité d'autres pays, dans de nombreuses régions du monde, à envisager de suivre la voie de l'UE. Il s'agit d'une tendance véritablement mondiale, qui s'observe du Chili à la Corée du Sud, du Brésil au Japon, du Kenya à l'Inde et de la Californie à l'Indonésie. Le rôle de chef de file joué par l'Union en faveur de la protection des données montre que l'Union peut être une référence à l'échelle mondiale. Il a été salué par des acteurs importants sur la scène internationale, parmi lesquels le secrétaire général des Nations unies, M. António Guterres, qui a souligné combien le RGPD a «*donné l'exemple* [...] *qui a inspiré des mesures similaires ailleurs*» et a «*demand[é] instamment à l'UE et aux États membres de continuer à jouer un rôle moteur en vue de façonner l'ère numérique et d'être à l'avant-garde de l'innovation et de la réglementation dans le domaine technologique*»[13].

La crise actuelle liée à la pandémie de COVID-19 est une illustration éloquente de cette mondialisation du débat sur la protection de la vie privée, tant durant la crise proprement dite que dans le cadre des efforts déployés dans le monde pour en sortir. Dans l'UE, plusieurs États membres ont pris des mesures d'urgence afin de protéger la santé publique. Le RGPD est clair quant au fait que toute limitation doit respecter le

---

[12] Voir par exemple l'étude sur la vie privée des consommateurs réalisée par Cisco en 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Selon cette étude, menée auprès de 2 600 consommateurs dans le monde, de très nombreux consommateurs ont déjà pris des mesures pour protéger leur vie privée, par exemple en changeant d'entreprise ou de fournisseur en raison de leurs politiques en matière de données ou de leurs pratiques en matière de partage des données.

[13] Discours du secrétaire général des Nations unies devant le Sénat italien, 18 décembre 2019 (disponible à l'adresse suivante: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

contenu essentiel des libertés et droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un intérêt public, tel que la santé publique. Alors que les mesures de confinement sont progressivement levées, les décideurs doivent répondre aux attentes des citoyens, qui veulent des solutions numériques dignes de confiance et respectueuses des droits à la vie privée et à la protection des données à caractère personnel.

Dans de nombreux pays, des mesures intégrées de protection de la vie privée, telles que le consentement volontaire des utilisateurs, la minimisation et la sécurité des données et l'exclusion de la géolocalisation, sont considérées comme essentielles pour garantir la fiabilité et l'acceptation par la société de solutions fondées sur des données qui visent à contrôler et à contenir la propagation du virus, à calibrer les contre-mesures de politique publique, à aider les patients ou à mettre en œuvre des stratégies de sortie. Dans l'Union, le cadre législatif relatif à la protection des données et au respect de la vie privée[14] s'est avéré être un outil suffisamment souple pour permettre l'élaboration de solutions pratiques (comme, par exemple, des applications de traçage) tout en garantissant un niveau élevé de protection des données à caractère personnel. Dans ce contexte, la Commission a publié le 16 avril 2020 des orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données[15].

La protection des données à caractère personnel est également déterminante pour prévenir la manipulation des choix posés par les citoyens, en particulier au moyen d'un microciblage des électeurs sur la base d'un traitement illicite de données à caractère personnel, pour empêcher toute interférence dans les processus démocratiques et pour préserver le débat ouvert, l'équité et la transparence, essentiels dans une démocratie. C'est la raison pour laquelle la Commission a publié en septembre 2018 des orientations relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral[16].

Pour cette évaluation et cet examen, la Commission a tenu compte des contributions du Conseil[17], du Parlement européen[18], du comité européen de la protection des

---

[14] Ce cadre comprend, outre le RGPD, la directive «vie privée et communications électroniques» (directive 2002/58/CE), dont les dispositions régissent notamment l'accès aux informations et le stockage de celles-ci sur les équipements terminaux des utilisateurs.

[15] Communication de la Commission intitulée «Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données», 2020/C 124 I/01 - C/2020/2523, JO C 124I du 17.4.2020, p. 1. Le 16 avril 2020, les États membres de l'UE, avec l'appui de la Commission, ont mis au point une boîte à outils au niveau de l'UE en vue de l'utilisation d'applications mobiles de traçage des contacts et d'alerte pour lutter contre la pandémie de coronavirus. Cela s'inscrit dans le cadre d'une approche coordonnée commune visant à soutenir la levée progressive des mesures de confinement, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Orientations de la Commission relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral - La contribution de la Commission européenne à la réunion des chefs d'État et de gouvernement à Salzbourg les 19 et 20 septembre 2018 - COM/2018/638 final.

[17] Position et conclusions du Conseil relatives à l'application du règlement général sur la protection des données (RGPD):
https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/fr/pdf

[18] Lettre adressée le 21 février 2020 par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen au Commissaire Reynders, réf.: IPOL-COM-LIBE D (2020)6525.

données (ci-après le «comité»)[19] et de différentes autorités de protection des données[20], du groupe d'experts multipartite[21] et d'autres parties prenantes, y compris au moyen des retours d'information sur la feuille de route[22].

De l'avis général, deux ans après son entrée en vigueur, le RGPD a atteint ses objectifs, à savoir renforcer la protection des droits des citoyens en matière de protection des données à caractère personnel et garantir la libre circulation des données à caractère personnel dans l'UE[23]. Toutefois, plusieurs domaines ont également été désignés comme devant faire l'objet d'améliorations à l'avenir. À l'instar de la plupart des parties prenantes et des autorités chargées de la protection des données, la Commission considère qu'il serait prématuré à ce stade de tirer des conclusions définitives sur l'application du RGPD. Il est probable qu'une plus grande expérience de cette application dans les années à venir sera utile pour résoudre la plupart des problèmes mis en évidence par les États membres et les parties prenantes. Néanmoins, le présent rapport met en lumière les difficultés rencontrées à ce jour pour ce qui est de l'application du RGPD et indique des solutions possibles pour y remédier.

Même s'ils mettent l'accent sur les deux aspects soulignés à l'article 97, paragraphe 2, du RGPD, à savoir les transferts internationaux et les mécanismes de coopération et de contrôle de la cohérence, cette évaluation et cet examen adoptent une approche plus large permettant de se pencher également sur des aspects évoqués par divers acteurs au cours des deux dernières années.

2 PRINCIPALES CONSTATATIONS

Mise en œuvre du RGPD et fonctionnement des mécanismes de coopération et de contrôle de la cohérence

Le RGPD a mis en place un système de gouvernance innovant, qui s'appuie sur des autorités indépendantes chargées de la protection des données dans les États membres, ainsi que sur la coopération entre ces autorités dans les situations transfrontières et au sein du comité. De l'avis général, les autorités chargées de la protection des données ont usé de manière équilibrée des pouvoirs renforcés qui leur sont conférés en ce qui concerne l'application de mesures correctrices, telles que des avertissements et des rappels à l'ordre, des amendes et des restrictions temporaires ou définitives en matière de traitement des données[24]. La Commission constate que les autorités ont eu recours à des amendes administratives allant de quelques milliers à plusieurs millions d'euros

[19] Contribution du comité à l'évaluation du RGPD au titre de l'article 97, adoptée le 18 février 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en

[21] Le groupe d'experts multipartite sur le règlement créé par la Commission est composé de représentants de la société civile et d'entreprises, d'universitaires et de professionnels: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Voir, par exemple, la position et les conclusions du Conseil, ainsi que la contribution du comité.

[24] Voir le point 2.1 du document de travail des services de la Commission.

selon la gravité des infractions. D'autres sanctions, telles qu'une interdiction de traitement, peuvent avoir un effet tout aussi dissuasif, sinon plus, que des amendes. L'objectif final du RGPD est de modifier la culture et le comportement de tous les acteurs concernés dans l'intérêt des citoyens. De plus amples informations sur l'utilisation des pouvoirs conférés aux autorités chargées de la protection des données en ce qui concerne l'application de mesures correctrices sont fournies dans le document de travail des services de la Commission qui accompagne le présent rapport.

S'il est encore trop tôt pour évaluer pleinement le fonctionnement des nouveaux mécanismes de coopération et de contrôle de la cohérence, les autorités chargées de la protection des données ont étendu leur coopération au moyen du mécanisme de guichet unique[25] et d'un large recours à l'assistance mutuelle[26]. Le mécanisme de guichet unique, qui constitue un élément essentiel du marché intérieur, est utilisé pour trancher dans de nombreuses situations transfrontières[27]. Des décisions importantes présentant une dimension transfrontière et relevant du mécanisme du guichet unique sont actuellement pendantes. Ces décisions, qui ont souvent trait à de grandes multinationales technologiques, auront une incidence considérable sur les droits des citoyens dans de nombreux États membres.

Le développement d'une véritable culture européenne commune en matière de protection des données entre les autorités chargées de la protection des données constitue cependant un processus permanent. Ces autorités n'ont pas encore fait pleinement usage des instruments que leur offre le RGPD, tels que des opérations conjointes susceptibles de déboucher sur des enquêtes conjointes. Il est arrivé que la définition d'une approche commune revienne à opter pour le plus petit dénominateur commun, et des occasions ont ainsi été manquées de renforcer l'harmonisation[28].

De nouvelles avancées doivent être réalisées en vue d'un traitement plus efficace et davantage harmonisé des situations transfrontières dans l'ensemble de l'UE, y compris sur le plan procédural, pour des aspects tels que les procédures de traitement des plaintes, les critères de recevabilité des plaintes, la durée des procédures due à des différences de délais ou à l'absence de délais dans les législations nationales en matière de procédure administrative, le stade de la procédure auquel le droit d'être entendu est accordé, ainsi que la participation des plaignants au cours de la procédure. Le processus de réflexion lancé en la matière par le comité a reçu un accueil favorable, et la Commission participe aux discussions[29].

Les activités et les orientations du comité revêtent une importance cruciale en vue d'un renforcement cohérent des échanges entre ledit comité et les parties prenantes[30].

---

[25] Si une entreprise traite des données à caractère personnel, l'autorité compétente en matière de protection des données est celle de l'État membre dans lequel se trouve le siège principal de cette entreprise.

[26] Voir le point 2.2 du document de travail des services de la Commission.

[27] Entre le 25 mai 2018 et le 31 décembre 2019, 141 projets de décision ont été soumis dans le cadre de la procédure de guichet unique, et 79 d'entre eux ont abouti à une décision définitive.

[28] Les listes nationales des types de traitement requérant une analyse d'impact relative à la protection des données conformément à l'article 35 du RGPD, par exemple, auraient pu faire l'objet d'une plus grande harmonisation.

[29] Voir le point 2.2 du document de travail des services de la Commission.

[30] En particulier les représentants des entreprises et de la société civile. Voir le point 2.3 du document de travail des services de la Commission.

Fin 2019, le comité avait adopté 67 documents, dont 10 nouvelles lignes directrices[31] et 43 avis[32]. Les parties prenantes saluent généralement les lignes directrices élaborées par le comité et en sollicitent d'autres sur des aspects clés du RGPD, mais soulignent également certaines incohérences entre les orientations données à l'échelle nationale et ces lignes directrices. Elles soulignent la nécessité de conseils plus pratiques, et en particulier d'exemples plus concrets, et indiquent que les autorités chargées de la protection des données doivent se doter des ressources humaines, techniques et financières nécessaires pour mener à bien leurs tâches.

La Commission a toujours insisté sur l'obligation pour les États membres d'allouer des ressources humaines, financières et techniques suffisantes aux autorités nationales chargées de la protection des données[33]. La plupart de ces autorités ont vu leurs effectifs et leur budget augmenter entre 2016 et 2019[34], mais c'est en Irlande, aux Pays-Bas, en Islande, au Luxembourg et en Finlande qu'elles ont bénéficié des augmentations relatives d'effectifs les plus importantes. Les plus grandes multinationales technologiques étant établies en Irlande et au Luxembourg, les autorités chargées de la protection des données dans ces pays agissent en tant qu'autorités compétentes principales dans de nombreuses situations transfrontières de premier plan et peuvent avoir besoin de ressources plus grandes que ce que leur population ne laisserait supposer. La situation reste toutefois inégale d'un État membre à l'autre et n'est pas encore globalement satisfaisante. Les autorités chargées de la protection des données jouent un rôle essentiel pour garantir la mise en œuvre du RGPD au niveau national et un fonctionnement efficace des mécanismes de coopération et de contrôle de la cohérence au sein du comité, y compris, en particulier, le mécanisme de guichet unique pour les situations transfrontières. Les États membres sont donc invités à leur fournir les ressources nécessaires, ainsi que le prévoit le RGPD[35].

Des règles harmonisées, mais encore un certain niveau de fragmentation et des approches divergentes

La Commission surveille la transposition du RGPD en droit national. Au moment de la rédaction du présent rapport, à l'exception de la Slovénie, tous les États membres ont adopté une nouvelle législation ou ont adapté leur législation nationale en matière

[31] Celles-ci viennent s'ajouter aux 10 lignes directrices adoptées par le groupe de travail «article 29» dans la perspective de l'entrée en vigueur du règlement et approuvées par le comité. Ce dernier a également adopté quatre lignes directrices supplémentaires entre le mois de janvier et la fin du mois de mai 2020 et a actualisé des lignes directrices existantes.

[32] Parmi ces avis, 42 ont été adoptés en application de l'article 64 du RGPD et un avis portant sur la décision relative à l'adéquation du niveau de protection des données à l'égard du Japon a été adopté en application de l'article 70, paragraphe 1, point s), du RGPD.

[33] Communication de la Commission au Parlement européen et au Conseil intitulée «Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan»:

[34] Globalement, les effectifs des autorités nationales chargées de la protection des données, considérées conjointement, ont augmenté de 42 % entre 2016 et 2019, tandis que leur budget a augmenté de 49 %.

[35] Voir le point 2.4 du document de travail des services de la Commission.

de protection des données. La Slovénie[36] a été invitée à fournir des éclaircissements à la Commission sur l'achèvement de ce processus[37].

Le RGPD prévoit une approche cohérente en ce qui concerne les règles en matière de protection des données dans l'ensemble de l'UE. Toutefois, il exige des États membres qu'ils légifèrent dans certains domaines[38], et leur donne la possibilité d'apporter des précisions quant à l'application du RGPD dans d'autres[39]. En conséquence, il subsiste un certain niveau de fragmentation qui est dû, notamment, à un recours intensif à des clauses de spécification facultatives. Par exemple, les différences entre les États membres au sujet de l'âge de consentement des enfants en ce qui concerne les services de la société de l'information créent une incertitude pour les enfants et leurs parents quant à l'application de leurs droits en matière de protection des données dans le marché unique. Cette fragmentation crée aussi des difficultés en ce qui concerne l'exercice d'activités internationales dans l'UE, l'innovation, en particulier les nouvelles évolutions technologiques, et les solutions en matière de cybersécurité. Pour garantir le bon fonctionnement du marché intérieur et éviter qu'une charge inutile pèse sur les entreprises, il est également essentiel que la législation nationale n'aille pas au-delà des marges fixées par le RGPD et n'introduise pas d'exigences supplémentaires lorsqu'aucune marge n'a été fixée.

L'une des difficultés pour la législation nationale est de concilier le droit à la protection des données à caractère personnel avec la liberté d'expression et d'information et de garantir un juste équilibre entre ces droits. Certaines législations nationales posent le principe de la primauté de la liberté d'expression, tandis que d'autres font primer la protection des données à caractère personnel: elles ne dispensent de l'application des règles en matière de protection des données que dans des cas spécifiques, par exemple lorsqu'une personne ayant un statut public est concernée. Enfin, d'autres États membres laissent une certaine marge de manœuvre au législateur et/ou permettent une appréciation au cas par cas en ce qui concerne les dérogations à certaines dispositions du RGPD.

La Commission poursuivra son évaluation de la législation nationale. La conciliation doit être prévue par la loi, respecter le contenu essentiel de ces droits fondamentaux, respecter le principe de proportionnalité et être nécessaire[40]. Les règles en matière de protection des données (ainsi que leur interprétation et leur application) ne devraient pas avoir d'incidence sur l'exercice de la liberté d'expression et d'information, par exemple en créant un effet dissuasif ou en exerçant une pression sur des journalistes pour qu'ils divulguent leurs sources. La conciliation de ces deux droits par les législations nationales devrait être régie par la jurisprudence de la Cour de justice et/ou de la Cour européenne des droits de l'homme[41].

---

[36] Tout récemment, par une lettre du commissaire Reynders en mars 2020.

[37] Il convient de noter que l'autorité nationale chargée de la protection des données en Slovénie est établie sur la base de la législation nationale en vigueur en matière de protection des données et supervise l'application du RGPD dans cet État membre.

[38] Voir le point 3.1 du document de travail des services de la Commission.

[39] Voir le point 3.2 du document de travail des services de la Commission.

[40] Article 52, paragraphe 1, de la charte des droits fondamentaux.

[41] Voir le point 3.1 du document de travail des services de la Commission: concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.

La législation des États membres suit des approches différentes lorsqu'il s'agit de mettre en œuvre des dérogations à l'interdiction générale de traiter des catégories particulières de données à caractère personnel, en ce qui concerne le niveau de précision et les garanties, y compris en matière de santé et à des fins de recherche. Pour remédier à cette situation, la Commission, dans un premier temps, recense les différentes approches des États membres[42] et, dans un deuxième temps, elle soutiendra la mise en place d'un ou plusieurs codes de conduite qui contribueraient à une approche plus cohérente dans ce domaine et faciliteraient le traitement transfrontière des données à caractère personnel[43]. En outre, les orientations futures du comité sur l'utilisation des données à caractère personnel dans le domaine de la recherche scientifique contribueront à garantir une approche harmonisée. La Commission apportera sa contribution au comité, notamment en ce qui concerne la recherche dans le domaine de la santé, y compris sous la forme de questions concrètes et d'analyses de scénarios spécifiques qu'elle a reçus du monde de la recherche.

[42] La Commission a lancé une étude sur l'«évaluation des règles des États membres en ce qui concerne les données en matière de santé à la lumière du RGPD», Chafea/2018/Health/03, contrat spécifique n° 2019 70 01.

[43] Voir les mesures annoncées dans la stratégie européenne pour les données, page 30.

Donner aux personnes les moyens de contrôler leurs données

Selon une enquête sur les droits fondamentaux[44], 69 % de la population de l'UE âgée de plus de 16 ans ont entendu parler du RGPD et 71 % des citoyens de l'UE connaissent leur autorité nationale chargée de la protection des données.

Les particuliers connaissent de mieux en mieux leurs droits: droit d'accès, droit de rectification, droit à l'effacement, portabilité des données à caractère personnel, droit de s'opposer au traitement des données à caractère personnel, et transparence renforcée. Le RGPD a renforcé les droits procéduraux, qui englobent le droit d'introduire une réclamation auprès d'une autorité chargée de la protection des données, y compris au moyen d'actions représentatives, et le droit à un recours juridictionnel. Les personnes exercent de plus en plus ces droits, mais il est nécessaire de faciliter leur exercice et de veiller à ce qu'ils soient pleinement respectés. Les réflexions menées par le comité clarifieront et faciliteront encore l'exercice des droits individuels, tandis que la proposition de directive sur les actions représentatives[45], une fois adoptée, devrait permettre aux particuliers d'intenter des actions collectives dans tous les États membres et réduira les coûts des actions transfrontières.

Il est incontestable que le droit à la portabilité des données, qui n'est pas encore pleinement exploité, a la capacité de placer les personnes au centre de l'économie fondée sur les données, leur permettant de passer d'un prestataire de services à un autre, de combiner différents services, d'utiliser d'autres services innovants et de choisir les services les plus à même de protéger leurs données. Indirectement, il favorisera la concurrence et soutiendra l'innovation. Tirer parti de ce potentiel est l'une des priorités de la Commission, en particulier dans la mesure où, en raison de l'utilisation croissante des dispositifs de «l'internet des objets», de plus en plus de données sont générées par les consommateurs, qui risquent d'être exposés à des pratiques déloyales et à des effets de verrouillage technologique. La portabilité pourrait procurer des avantages considérables en ce qui concerne la santé et le bien-être, la réduction de l'empreinte environnementale et l'accès aux services publics et privés, l'augmentation de la productivité dans l'industrie manufacturière et l'amélioration de la qualité et de la sécurité des produits.

La stratégie pour les données a souligné la nécessité de remédier aux difficultés telles que l'absence de normes permettant la fourniture de données dans un format lisible par machine et d'accroître l'utilisation effective du droit à la portabilité des données, qui est actuellement limitée à quelques secteurs (comme les services bancaires et les télécommunications). La conception d'outils appropriés et de formats et d'interfaces standard pourrait y contribuer[46]. Cette utilisation accrue pourrait également être obtenue en rendant obligatoires les interfaces techniques et les formats lisibles par machine permettant la portabilité des données en temps réel. Grâce à une utilisation

[44] Agence des droits fondamentaux de l'Union européenne (FRA), 2020: enquête sur les droits fondamentaux 2019. Protection des données et technologies: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Une fois adoptée, la proposition de directive relative aux actions représentatives dans le domaine de la protection des intérêts collectifs des consommateurs [COM/2018/0184 final - 2018/089 (COD)] devrait renforcer le cadre des actions représentatives également dans le domaine de la protection des données.

[46] Ces outils peuvent comprendre des «outils de gestion du consentement» et des applications de gestion des informations à caractère personnel.

accrue du droit à la portabilité, il serait notamment plus facile pour les particuliers d'autoriser l'utilisation de leurs données dans l'intérêt public (par exemple pour favoriser la recherche dans le secteur de la santé), s'ils le souhaitent («altruisme en matière de données»). En vue de l'élaboration du paquet relatif aux services numériques[47], la Commission étudiera de manière plus approfondie le rôle des données et des pratiques liées aux données dans l'écosystème des plateformes.

[47] https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_962

Perspectives et défis pour les organisations, en particulier les petites et moyennes entreprises

Le RGPD et le règlement relatif au libre flux des données à caractère non personnel[48] offrent des perspectives aux entreprises en favorisant la concurrence et l'innovation, en garantissant le libre flux des données au sein de l'UE et en créant une égalité des conditions de concurrence avec les entreprises établies en dehors de l'UE[49]. Le droit à la portabilité, associé au nombre toujours plus grand de personnes à la recherche de solutions plus respectueuses de la vie privée, est susceptible d'abaisser les barrières à l'entrée pour les entreprises et d'offrir des perspectives de croissance fondées sur la confiance et l'innovation. Certaines parties prenantes indiquent que l'application du RGPD est compliquée, en particulier pour les petites et moyennes entreprises (PME). Selon une approche fondée sur les risques, il ne serait pas approprié de prévoir des dérogations fondées sur la taille des opérateurs, étant donné que la taille de ces derniers ne constitue pas, en soi, un indicateur des risques que peut supposer, pour les particuliers, le traitement des données à caractère personnel qu'ils effectuent. Plusieurs autorités chargées de la protection des données ont fourni des outils pratiques pour faciliter la mise en œuvre du RGPD par les PME dont les activités de traitement des données impliquent peu de risques. Ces efforts devraient être intensifiés et élargis, de préférence dans le cadre d'une approche européenne commune afin de ne pas créer d'obstacles sur le marché unique.

Les autorités chargées de la protection des données ont pris un certain nombre de mesures pour aider les PME à satisfaire au RGPD, par exemple en fournissant des modèles de contrats de traitement et des registres des activités de traitement, des lignes directes de consultation, ou en organisant des séminaires. Plusieurs de ces initiatives ont bénéficié d'un financement de l'UE[50]. Il conviendrait de prévoir d'autres mesures visant à faciliter l'application du RGPD par les PME.

Le RGPD met à la disposition de tous les types d'entreprises et d'organisations une boîte à outils pour les aider à démontrer qu'ils satisfont au RGPD, tels que les codes de conduite, les mécanismes de certification et la clause contractuelle type. Il convient d'exploiter toutes les possibilités offertes par cette boîte à outils. Les PME soulignent notamment l'importance et l'utilité des codes de conduite adaptés à leur situation et qui n'entraînent pas de coûts disproportionnés. En ce qui concerne les mécanismes de certification, la sécurité (y compris la cybersécurité) et la protection des données dès la conception sont des éléments essentiels à prendre en considération dans le cadre du

[48] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (JO L 303 du 28.11.2018, p. 59).

[49] Voir le point 5 du document de travail des services de la Commission. Voir également le document COM(2019)250 final, «Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne», expliquant les règles régissant le traitement d'ensembles de données mixtes, composés à la fois de données à caractère personnel et de données à caractère non personnel, ce qui facilite les choses pour les entreprises, y compris les PME.

[50] La Commission a apporté un soutien financier au moyen de trois séries de subventions, pour un montant total de 5 millions d'euros, les deux plus récentes ayant spécifiquement pour objectif de soutenir les autorités nationales chargées de la protection des données dans leurs efforts pour toucher les particuliers et les petites et moyennes entreprises: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_fr. Un montant supplémentaire d'un million d'euros sera alloué en 2020.

RGPD et qui gagneraient à bénéficier d'une approche commune et ambitieuse dans l'ensemble de l'UE. La Commission travaille actuellement à l'élaboration de clauses contractuelles types entre les responsables du traitement et les sous-traitants[51], en s'appuyant sur les travaux en cours sur la modernisation des clauses contractuelles types pour les transferts de données au niveau international[52].

Application du RGPD aux nouvelles technologies

Le RGPD, qui a été élaboré de manière neutre du point de vue des technologies, repose sur des principes et, dès lors, vise à couvrir les nouvelles technologies au fur et à mesure de leur développement.

Il est considéré comme un outil essentiel et flexible dont l'objectif est de veiller au développement des nouvelles technologies dans le respect des droits fondamentaux. L'importance et la souplesse du cadre législatif relatif à la protection des données et au respect de la vie privée ont été démontrées lors de la crise du COVID-19, notamment en ce qui concerne la conception des applications de traçage et d'autres solutions technologiques destinées à lutter contre la pandémie. Parmi les nouveaux défis qui s'annoncent, il conviendra de préciser comment il faudra appliquer les principes bien établis à des technologies spécifiques telles que l'intelligence artificielle, les chaînes de blocs, l'internet des objets ou la reconnaissance faciale, qui nécessitent une surveillance continue. Le livre blanc de la Commission sur l'intelligence artificielle[53], par exemple, a suscité un débat public sur les circonstances particulières éventuelles qui pourraient justifier l'utilisation de l'intelligence artificielle à des fins d'identification biométrique à distance (comme la reconnaissance faciale) dans les lieux publics, ainsi que sur la nécessité de garanties communes. À cet égard, les autorités chargées de la protection des données devraient être prêtes à accompagner les processus de conception technique à un stade précoce.

En outre, l'application stricte et effective du RGPD à l'égard des grandes plateformes numériques et des entreprises intégrées, y compris dans des domaines tels que la publicité en ligne et le microciblage, est un élément essentiel en matière de protection des personnes.

Mise au point d'une boîte à outils moderne pour les transferts internationaux de données

Le RGPD propose une boîte à outils modernisée pour faciliter les transferts de données à caractère personnel de l'UE vers un pays tiers ou une organisation internationale, tout en garantissant que les données continuent à bénéficier d'un niveau élevé de protection. Au cours des deux dernières années, la Commission a redoublé d'efforts pour exploiter tout le potentiel des outils disponibles au titre du RGPD.

Ainsi, elle a notamment maintenu activement un dialogue avec des partenaires clés en vue de parvenir à une «décision d'adéquation». Une telle décision permet un flux libre et sécurisé des données à caractère personnel vers le pays tiers sans que l'exportateur

[51] Article 28 du RGPD.
[52] Article 46 du RGPD.
[53] Livre blanc intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance» [COM(2020) 65 final].

des données n'ait à fournir de garanties supplémentaires ni à obtenir une quelconque autorisation. Ainsi, les décisions d'adéquation mutuelle entre l'UE et le Japon, qui sont entrées en vigueur en février 2019, ont créé le plus grand espace de flux libres et sécurisés au monde. En outre, le processus d'adéquation avec la République de Corée a atteint un stade avancé et des entretiens préliminaires sont en cours avec d'autres partenaires importants en Asie et en Amérique latine.

L'adéquation joue aussi un rôle important dans le contexte des relations futures avec le Royaume-Uni, sous réserve du respect des conditions applicables. Elle constitue un facteur favorisant les échanges, y compris le commerce numérique, et constitue une condition préalable essentielle à une coopération étroite et ambitieuse dans le domaine répressif et dans celui de la sécurité. De plus, il est important de parvenir à un degré élevé de convergence dans le domaine de la protection des données pour garantir une égalité des conditions de concurrence entre deux économies si étroitement intégrées. Conformément à la déclaration politique concernant les relations futures entre l'UE et le Royaume-Uni, la Commission procède actuellement à une évaluation de l'adéquation au regard du RGPD et de la directive en matière de protection des données dans le domaine répressif[54].

Dans le cadre de la première évaluation du RGPD, la Commission est également tenue de réexaminer les décisions d'adéquation adoptées au titre des règles précédentes[55]. Les services de la Commission ont engagé un dialogue approfondi avec chacun des 11 pays et territoires tiers concernés[56] afin d'évaluer la manière dont leurs systèmes de protection des données ont évolué depuis l'adoption de la décision d'adéquation et de déterminer s'ils satisfont à la norme fixée par le RGPD. La nécessité de veiller à la continuité de ces décisions, en tant qu'instrument essentiel du commerce et de la coopération internationale, est l'un des facteurs qui ont amené plusieurs de ces pays et territoires à moderniser et à renforcer leur législation en matière de protection de la vie privée. Des garanties supplémentaires sont en cours de discussion avec certains de ces pays et territoires pour faire face aux différences significatives en matière de protection. Toutefois, étant donné que la Cour de justice de l'Union européenne pourrait apporter des éclaircissements dans un arrêt qui sera rendu le 16 juillet, qui pourraient présenter un intérêt pour certains éléments du principe d'adéquation, la Commission établira un rapport distinct sur les décisions d'adéquation existantes, après que la Cour aura rendu son arrêt dans cette affaire[57].

---

[54] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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 (JO L 119 du 4.5.2016, p. 89).

[55] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[56] Ces pays et territoires sont l'Andorre, l'Argentine, le Canada, Guernesey, l'Île de Man, les Îles Féroé, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay.

[57] Voir l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems (ci-après «Schrems II»), qui porte sur un renvoi préjudiciel relatif aux «clauses contractuelles types». Cependant, il est possible que certains éléments du principe d'adéquation soient encore précisés par la Cour.

Parallèlement aux mesures qu'elle prend en ce qui concerne l'adéquation, la Commission s'emploie à moderniser en profondeur les clauses contractuelles types, afin de les actualiser à la lumière des nouvelles exigences introduites par le RGPD. L'objectif est de mieux prendre en considération les réalités des opérations de traitement dans l'économie numérique moderne et de réfléchir à la nécessité éventuelle, notamment à la lumière de la jurisprudence à venir de la Cour de justice[58], de clarifier davantage certaines garanties. Ces clauses constituent, de loin, le mécanisme le plus largement utilisé pour les transferts de données; des milliers d'entreprises de l'UE y ont recours pour fournir un large éventail de services à leurs clients, fournisseurs, partenaires et employés.

Le comité a également joué un rôle actif en ce qui concerne les aspects internationaux du RGPD. Il s'agit notamment de mettre à jour les orientations sur les mécanismes existants pour le transfert de données, tels que les règles d'entreprise contraignantes et les «dérogations», ainsi que de développer l'infrastructure juridique pour l'utilisation de nouveaux instruments introduits par le RGPD, à savoir les codes de conduite et les mécanismes de certification.

Pour permettre aux parties prenantes d'utiliser pleinement la boîte à outils du RGPD pour les transferts de données, il est important que le comité intensifie ses travaux en cours sur les différents mécanismes pour les transferts de données, notamment en rationalisant davantage le processus d'approbation des règles d'entreprise contraignantes, en parachevant les orientations sur les codes de conduite et les mécanismes de certification en tant qu'instruments pour les transferts de données, et en clarifiant l'interaction entre les règles relatives aux transferts internationaux de données (chapitre V) et le champ d'application territorial du RGPD (article 3).

Un autre aspect important de la dimension internationale des règles de l'UE en matière de protection des données est le champ d'application territorial élargi du RGPD, qui couvre également les activités de traitement des opérateurs étrangers actifs sur le marché de l'UE. Pour garantir le respect effectif du RGPD et une vraie égalité des conditions de concurrence, il est essentiel que cet élargissement soit dûment pris en compte par les autorités chargées de la protection des données lorsqu'elles veillent au respect du RGPD. Elles doivent notamment s'adresser aussi, si nécessaire, au représentant du responsable du traitement ou du sous-traitant dans l'UE, en plus ou au lieu de s'adresser à la société établie en dehors de l'UE. Il convient de suivre cette approche de manière plus rigoureuse afin d'envoyer un message clair soulignant que l'absence d'établissement dans l'UE ne décharge pas les opérateurs étrangers de leurs responsabilités au titre du RGPD.

Encourager la convergence et la coopération internationale dans le domaine de la protection des données

Le RGPD est désormais un point de référence essentiel au niveau international, et il a déjà joué un rôle de catalyseur dans de nombreux pays du monde, les incitant à envisager l'introduction de règles modernes en matière de protection de la vie privée. Cette tendance à une convergence au niveau mondial est une évolution très positive

[58] Voir l'affaire «Schrems II».

qui ouvre de nouvelles possibilités pour mieux protéger les personnes dans l'UE lors du transfert de leurs données vers l'étranger, tout en facilitant les flux de données.

Poursuivant cette tendance, la Commission a intensifié son dialogue dans un certain nombre d'enceintes bilatérales, régionales et multilatérales afin de promouvoir une culture mondiale du respect de la vie privée et d'instaurer des éléments de convergence entre les différents systèmes de protection de la vie privée. À cette fin, la Commission a pu compter sur le soutien actif du Service européen pour l'action extérieure et du réseau des délégations de l'UE dans les pays tiers et des missions auprès d'organisations internationales, et elle continuera à s'appuyer sur eux. Cela a également permis de renforcer la cohérence et la complémentarité entre les différents aspects de la dimension extérieure des politiques de l'UE, du commerce au nouveau partenariat UE-Afrique. Le G20 et le G7 ont également reconnu récemment que la protection des données contribue à la confiance placée dans l'économie numérique et dans les flux de données, en particulier grâce à la notion de «Libre flux de données en toute confiance» («Data Free Flow with Trust»), initiative lancée par la présidence japonaise du G20[59]. La stratégie pour les données montre que la Commission entend continuer à encourager l'échange de données avec des partenaires de confiance, tout en luttant contre les abus tels que l'accès disproportionné des autorités publiques (étrangères) aux données à caractère personnel.

Tout en encourageant la convergence des normes de protection des données au niveau international, comme moyen de faciliter les flux de données et, partant, le commerce, la Commission est également déterminée à s'attaquer au protectionnisme numérique, comme elle l'a récemment souligné dans la stratégie européenne pour les données[60]. À cette fin, elle a élaboré des dispositions spécifiques sur les flux de données et la protection des données dans les accords commerciaux[61], qu'elle inclut systématiquement dans ses négociations bilatérales (tout récemment avec l'Australie, la Nouvelle-Zélande et le Royaume-Uni) et multilatérales, comme les pourparlers actuels sur le commerce électronique avec l'OMC[62]. Ces dispositions horizontales excluent les restrictions injustifiées, telles que des exigences relatives à la localisation forcée des données, tout en préservant l'autonomie réglementaire des parties pour protéger le droit fondamental à la protection des données.

Il convient donc d'étudier plus avant les synergies possibles entre le commerce et les instruments de protection des données afin de garantir des flux de données internationaux libres et sûrs; ceux-ci sont essentiels pour les activités commerciales, la compétitivité et la croissance des entreprises européennes, y compris les PME, dans une économie de plus en plus numérisée.

---

[59] Voir, par exemple, le texte de la déclaration d'Osaka des dirigeants du G20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Stratégie pour les données, p. 23.

[61] Voir le texte des dispositions horizontales relatives aux flux de données transfrontières et à la protection des données à caractère personnel (dans les accords de l'UE en matière de commerce et d'investissement): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 membres de l'OMC sont désormais engagés dans des négociations multilatérales sur le commerce électronique, à la suite d'une initiative de déclaration conjointe adoptée par les ministres le 25 janvier 2019 à Davos. Dans le cadre de ce processus, l'UE a présenté, le 3 mai 2019, sa proposition relative aux futures règles et obligations en matière de commerce électronique. La proposition comporte des dispositions horizontales relatives aux flux de données et à la protection des données à caractère personnel: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

De même, il est important de veiller à ce que, lorsque des entreprises actives sur le marché européen sont appelées, sur la base d'une demande légitime, à partager des données à des fins répressives, elles puissent le faire sans devoir faire face à des conflits de lois, et dans le plein respect des droits fondamentaux de l'UE. Afin d'améliorer ces transferts, la Commission est déterminée à mettre en place avec ses partenaires internationaux les cadres juridiques qui s'imposent afin d'éviter les conflits de lois et de soutenir des formes de coopération efficaces, notamment en prévoyant les garanties nécessaires en matière de protection des données, et de contribuer ainsi à une lutte plus efficace contre la criminalité.

Enfin, alors que des problèmes relatifs au respect de la vie privée ou des incidents liés à la sécurité des données peuvent affecter un grand nombre de personnes, simultanément et dans plusieurs juridictions, la coopération «sur le terrain» devrait être encore renforcée entre les régulateurs européens et internationaux. À cette fin, il est nécessaire, entre autres, de mettre au point des instruments juridiques appropriés pour les formes plus étroites de coopération et d'assistance mutuelle, notamment en permettant les échanges d'informations qui s'imposent dans le cadre des enquêtes. C'est également dans cet esprit que la Commission met en place une «académie pour la protection des données», une plateforme où les autorités européennes et étrangères chargées de la protection des données pourraient partager leurs connaissances, expériences et meilleures pratiques afin de faciliter et de soutenir la coopération entre les autorités chargées de veiller à la protection de la vie privée.

3 LA VOIE À SUIVRE

Pour réaliser tout le potentiel du RGPD, il importe de créer une approche harmonisée et une culture européenne commune en matière de protection des données et de favoriser un traitement plus efficace et plus harmonisé des situations transfrontières. C'est ce qu'attendent les citoyens et les entreprises, et c'est un objectif essentiel de la réforme des règles de l'UE en matière de protection des données. Il est tout aussi important de veiller à ce que tous les outils disponibles dans le cadre du RGPD soient pleinement mis à profit pour garantir une application efficace aux particuliers et aux entreprises.

La Commission poursuivra ses échanges bilatéraux avec les États membres sur la mise en œuvre du RGPD et, au besoin, continuera de faire usage de tous les outils à sa disposition pour favoriser le respect, par les États membres, des obligations qui leur incombent en application du RGPD.

Étant donné que l'évaluation des législations nationales est en cours, que l'expérience pratique acquise depuis l'entrée en application du RGPD est brève et que la législation sectorielle est encore en cours de réexamen dans de nombreux États membres, il est encore trop tôt pour tirer des conclusions définitives sur le niveau actuel de fragmentation. Pour ce qui est des éventuels conflits de lois résultant de la mise en œuvre de clauses de spécification par les États membres, il est nécessaire, au préalable, de mieux comprendre les conséquences pour les responsables du traitement et les sous-traitants[63].

[63] Cf. la position et les conclusions du Conseil relatives à l'application du RGPD.

En s'attachant à ces questions, la jurisprudence pertinente des juridictions nationales et de la Cour de justice contribue à mettre en place une interprétation cohérente des règles en matière de protection des données. Des juridictions nationales ont récemment rendu des jugements invalidant des dispositions nationales s'écartant du RGPD[64].

En ce qui concerne la dimension internationale, la Commission continuera de centrer ses efforts sur la promotion de la convergence des règles en matière de protection des données comme moyen de garantir la sécurité des flux de données. Cela inclut différents types de travaux «en amont», par exemple dans le contexte des réformes en cours visant à renouveler ou à actualiser la législation en matière de protection des données, ou de la défense de la notion de «libre flux de données en toute confiance» dans les enceintes multilatérales. Cela comprend également la conduite de dialogues d'adéquation divers et le fait de moderniser et d'étendre nos instruments de transfert en mettant à jour les clauses contractuelles types et en jetant les fondements de mécanismes de certification. Ces travaux incluent également des négociations internationales, notamment en ce qui concerne la coopération en matière de répression pénale, par exemple dans le domaine de l'accès transfrontière aux preuves électroniques, le but étant de veiller à ce que les transferts de données soient assortis de garanties adéquates en matière de protection des données. Enfin, en engageant des négociations sur la coopération internationale et l'assistance mutuelle entre instances chargées de veiller à la protection des données, la Commission s'emploiera à faire passer la convergence de la théorie à la pratique.

Sur la base de cette évaluation de l'application du RGPD depuis mai 2018, les actions énumérées ci-après ont été jugées nécessaires pour soutenir cette application. La Commission suivra leur mise en œuvre et ce, également dans la perspective du rapport d'évaluation prévu pour 2024.

Mettre en œuvre et compléter le cadre juridique

Les États membres devraient:

- achever l'alignement de leurs législations sectorielles sur le RGPD;
- envisager de limiter le recours à des clauses de spécification susceptibles d'engendrer une fragmentation et de mettre en danger la libre circulation des données dans l'UE;
- déterminer si la législation nationale transposant le RGPD respecte dans tous les cas de figure la latitude permise pour la législation nationale.

La Commission entend:

- mener des échanges bilatéraux avec les États membres sur la conformité de la législation nationale avec le RGPD, y compris en ce qui concerne l'indépendance et les ressources des autorités nationales chargées de la protection des données; faire usage de tous les outils à sa disposition, y

[64] Il en a été ainsi en Allemagne et en Espagne, ou encore en Autriche, ce qui a permis de combler une lacune dans la législation nationale.

compris les procédures d'infraction, pour faire en sorte que les États membres respectent le RGPD;

- appuyer la poursuite d'échanges de vues et de pratiques nationales entre États membres dans des domaines susceptibles de faire l'objet de spécifications supplémentaires au niveau national afin de réduire le niveau de fragmentation du marché unique, tels que le traitement de données à caractère personnel concernant la santé et la recherche, ou dans lesquels un équilibre doit être trouvé avec d'autres droits tels que la liberté d'expression;
- favoriser une application cohérente du cadre en matière de protection des données en lien avec les nouvelles technologies afin de soutenir l'innovation et les évolutions technologiques;
- faire appel au groupe d'experts des États membres sur le RGPD (créé lors de la phase transitoire avant l'entrée en application du RGPD) afin de faciliter les discussions et le partage d'expériences entre les États membres et avec la Commission;
- examiner, à la lumière de l'expérience et de la jurisprudence pertinente supplémentaires, l'opportunité de proposer l'adoption future d'éventuelles modifications ciblées portant sur certaines dispositions du RGPD, notamment en ce qui concerne le registre des activités de traitement effectuées par des PME dont l'activité principale ne consiste pas à traiter des données (faible risque)[65], et l'harmonisation éventuelle de l'âge de consentement des enfants pour les services de la société de l'information.

Faire en sorte que le nouveau système de gouvernance réalise tout son potentiel

Le comité et les autorités chargées de la protection des données sont invités:

- à mettre en place des dispositifs efficaces entre les autorités chargées de la protection des données en ce qui concerne le fonctionnement des mécanismes de coopération et de contrôle de la cohérence, y compris pour les aspects procéduraux, en s'appuyant sur l'expertise des membres du comité et en renforçant la participation de son secrétariat;
- à favoriser l'harmonisation pour ce qui est d'appliquer et de faire respecter le RGPD et ce, par tous les moyens à sa disposition, y compris en clarifiant davantage les notions clés du RGPD et en veillant à ce que les orientations nationales soient pleinement conformes aux lignes directrices adoptées par le comité;
- à encourager l'utilisation de tous les outils prévus par le RGPD visant à en garantir l'application cohérente;
- à intensifier la coopération entre les autorités chargées de la protection des données, par exemple en menant des enquêtes conjointes.

[65] Article 30, paragraphe 5, du RGPD.

La Commission entend:

- continuer à suivre de près l'indépendance effective et totale des autorités nationales chargées de la protection des données;
- encourager la coopération entre les autorités de réglementation (notamment dans des domaines tels que la concurrence, les communications électroniques, la sécurité des réseaux et des systèmes d'information et la politique des consommateurs);
- appuyer la réflexion menée au sein du comité au sujet des procédures appliquées par les autorités nationales chargées de la protection des données afin d'améliorer la coopération dans les situations transfrontières.

Les États membres:

- allouent des ressources suffisantes aux autorités chargées de la protection des données pour leur permettre d'accomplir leurs tâches.

Soutenir les parties prenantes

Le comité et les autorités chargées de la protection des données sont invités:

- à adopter des lignes directrices pragmatiques et faciles à comprendre, qui apportent des réponses claires et sans ambiguïté aux questions relatives à l'application du RGPD, par exemple en ce qui concerne le traitement des données des enfants et les droits des personnes concernées, y compris l'exercice du droit d'accès et du droit à l'effacement, en consultant les parties prenantes au cours de ce processus;
- à réexaminer les lignes directrices lorsque des précisions supplémentaires sont nécessaires au regard de l'expérience et des évolutions, y compris la jurisprudence de la Cour de justice;
- à élaborer des outils pratiques, tels que des formulaires harmonisés pour les violations de données et les registres simplifiés des activités de traitement, pour aider les PME à faible risque à remplir leurs obligations.

La Commission entend:

- fournir des clauses contractuelles type pour les transferts internationaux et les relations entre responsables du traitement et sous-traitants;
- prévoir des outils de clarification/soutien à l'application des règles en matière de protection des données aux enfants[66];
- conformément à la stratégie pour les données, étudier les moyens pratiques permettant de favoriser un exercice accru du droit à la portabilité par les particuliers, par exemple en leur accordant davantage de contrôle sur les

[66] Projet de la Commission relatif aux outils de détermination de l'âge – projet pilote en vue de la démonstration d'une infrastructure technique interopérable pour la protection des enfants, y compris la vérification de l'âge et le consentement parental. Cela devrait appuyer la mise en œuvre des mécanismes de protection des enfants fondés sur la législation existante de l'UE pertinente pour la protection des enfants en ligne.

personnes pouvant accéder aux données générées par des machines et les utiliser;

- appuyer la normalisation/certification, notamment en ce qui concerne les aspects liés à la cybersécurité, grâce à la coopération entre l'Agence de l'Union européenne pour la cybersécurité (ENISA), les autorités chargées de la protection des données et le comité;
- le cas échéant, faire usage de son habilitation à charger le comité d'élaborer des lignes directrices et des avis sur des questions spécifiques qui revêtent de l'importance pour les parties prenantes;
- si nécessaire, fournir des orientations, tout en respectant pleinement le rôle du comité;
- soutenir les activités menées par les autorités chargées de la protection des données pour faciliter la mise en œuvre, par les PME, de leurs obligations au titre du RGPD, au moyen d'un soutien financier, notamment en faveur de l'élaboration d'orientations pratiques et d'outils numériques susceptibles d'être réemployés dans d'autres États membres.

Encourager l'innovation

La Commission entend:

- surveiller l'application du RGPD aux nouvelles technologies, en tenant également compte des éventuelles initiatives futures dans le domaine de l'intelligence artificielle et dans le cadre de la stratégie pour les données;
- encourager, y compris par un soutien financier, l'élaboration de codes de conduite de l'UE dans le domaine de la santé et de la recherche;
- suivre de près le développement et l'utilisation d'applications dans le contexte de la pandémie de COVID-19.

Le comité est invité:

- à émettre des lignes directrices sur l'application du RGPD dans le domaine de la recherche scientifique, de l'intelligence artificielle, des chaînes de blocs et d'autres évolutions technologiques éventuelles;
- à réexaminer les lignes directrices en vue d'apporter des clarifications supplémentaires si les évolutions technologiques l'imposent.

Poursuivre l'élaboration de la boîte à outils pour les transferts de données

La Commission entend:

- poursuivre les dialogues d'adéquation avec les pays tiers intéressés, conformément à la stratégie définie dans sa communication de 2017 intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», y compris, si possible, en englobant les transferts de données vers les autorités répressives en matière pénale (au titre de la directive en matière de protection des données dans le domaine répressif) et vers d'autres

autorités publiques; cela inclut la conclusion du processus d'adéquation avec la République de Corée dans les meilleurs délais;

- mener à bonne fin l'évaluation en cours des décisions d'adéquation existantes et faire rapport au Parlement européen et au Conseil;
- mener à bonne fin les travaux de modernisation des clauses contractuelles type, afin de les mettre à jour en tenant compte du RGPD, de manière à couvrir tous les cas de figure de transfert et à mieux refléter les pratiques commerciales modernes.

Le comité est invité:

- à clarifier davantage la manière dont s'articulent les règles relatives aux transferts internationaux de données (chapitre V) avec le champ d'application territorial du RGPD (article 3);
- à veiller à la mise en œuvre effective des dispositions à l'égard des opérateurs établis dans des pays tiers qui relèvent du champ d'application territorial du RGPD, y compris, le cas échéant, en ce qui concerne la désignation d'un représentant (article 27);
- à rationaliser l'évaluation et l'approbation éventuelle des règles d'entreprises contraignantes afin d'accélérer le processus;
- à achever les travaux concernant l'architecture, les procédures et les critères d'évaluation relatifs aux codes de conduite et aux mécanismes de certification en tant qu'instruments pour les transferts de données.

Promouvoir la convergence et développer la coopération internationale

La Commission entend:

- appuyer les processus de réforme en cours dans des pays tiers visant à renouveler ou à moderniser les règles en matière de protection des données, grâce au partage d'expériences et de bonnes pratiques;
- dialoguer avec les partenaires africains afin de promouvoir la convergence réglementaire et de soutenir le renforcement des capacités des autorités de surveillance dans le cadre du chapitre numérique du nouveau partenariat UE-Afrique;
- évaluer la manière dont la coopération entre les opérateurs privés et les autorités répressives pourrait être facilitée, y compris en négociant des cadres bilatéraux et multilatéraux pour les transferts de données dans le contexte de l'accès des autorités répressives étrangères en matière pénale aux preuves électroniques, afin d'éviter les conflits de lois tout en offrant des garanties adéquates en matière de protection des données;
- dialoguer avec des organisations internationales et régionales telles que l'OCDE, l'ASEAN ou le G20 pour promouvoir des flux de données fiables fondés sur des normes élevées en matière de protection des données, y compris dans le contexte de l'initiative «Libre flux de données en toute confiance»;

- mettre en place une «académie pour la protection des données» afin de faciliter et de soutenir les échanges entre les autorités de réglementation européennes et internationales;
- promouvoir la coopération internationale en matière répressive entre les autorités de surveillance, y compris grâce à la négociation d'accords de coopération et d'assistance mutuelle.