COMMISSION
EUROPÉENNE

Bruxelles, le 25.7.2024
COM(2024) 357 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Deuxième rapport sur l'application du règlement général sur la protection des données

1 INTRODUCTION

Il s'agit du deuxième rapport de la Commission sur l'application du règlement général sur la protection des données (RGPD), adopté conformément à l'article 97 du RGPD. Le premier rapport a été adopté le 24 juin 2020 (ci-après le «rapport de 2020»)[1)].

Le RGPD est l'une des pierres angulaires de l'approche de l'UE à l'égard de la transformation numérique. Ses principes de base - traitement équitable, sûr et transparent des données à caractère personnel, garantissant que les personnes en conservent le contrôle - sous-tendent toutes les politiques de l'UE impliquant le traitement de données à caractère personnel.

Depuis le rapport de 2020, l'UE a adopté une série d'initiatives visant à placer les personnes physiques au centre de la transition numérique. Chaque initiative poursuit un objectif particulier, consistant notamment à créer un environnement plus sûr en ligne, à rendre l'économie numérique plus équitable et plus compétitive, à faciliter la recherche novatrice, à garantir le développement d'une intelligence artificielle (IA) sûre et digne de confiance et à créer un véritable marché unique des données. Chaque fois que des données à caractère personnel sont concernées, ces initiatives s'appuient sur le RGPD. Le RGPD fournit également une base pour les initiatives sectorielles qui ont une incidence sur le traitement des données à caractère personnel, par exemple dans les domaines des services financiers, de la santé, de l'emploi, de la mobilité et des services répressifs.

Il existe un large consensus parmi les parties prenantes, les autorités chargées de la protection des données et les États membres sur le fait que, malgré certaines difficultés, le RGPD a produit des résultats importants pour les particuliers et les entreprises. L'approche fondée sur les risques et neutre sur le plan technologique assure une protection solide des personnes concernées et garantit des obligations proportionnées pour les responsables du traitement et les sous-traitants. Dans le même temps, des progrès supplémentaires devraient être accomplis dans un certain nombre de domaines. En particulier, dans les années à venir, l'accent devrait être mis sur le soutien aux efforts de mise en conformité accomplis par les parties prenantes, en particulier les petites et moyennes entreprises (PME), les petits opérateurs, les chercheurs et les organismes de recherche, sur l'offre d'orientations plus claires et plus pratiques de la part des autorités chargées de la protection des données, et sur une interprétation et une application plus cohérentes du RGPD dans l'ensemble de l'UE.

Conformément à l'article 97 du RGPD, la Commission devrait examiner en particulier l'application et le fonctionnement du transfert international de données à caractère personnel vers des pays tiers (c'est-à-dire des pays ne faisant pas partie de l'UE/EEE) (chapitre V du RGPD) et les mécanismes de coopération et de contrôle de la cohérence entre les autorités nationales chargées de la protection des données (chapitre VII du RGPD). Toutefois, comme pour le rapport de 2020, le présent rapport fournit une évaluation générale de l'application du RGPD allant au-delà de ces deux éléments: il recense également une série d'actions nécessaires pour soutenir l'application effective du RGPD dans des domaines prioritaires clés.

Le présent rapport tient compte des sources suivantes: i) la position et les conclusions du Conseil, adoptées en décembre 2023[2]; ii) les contributions recueillies auprès des parties

---

1 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, 24.6.2020 COM(2020) 264 final.

2 https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/fr/pdf

prenantes, en particulier par l'intermédiaire du groupe multipartite du RGPD[3] et d'un appel public à contributions[4]; et iii) les contributions des autorités chargées de la protection des données [au moyen de la contribution du comité européen de la protection des données[5] (ci-après le «comité») et d'un rapport élaboré par l'Agence des droits fondamentaux (FRA) sur la base d'entretiens menés avec différentes autorités chargées de la protection des données[6] (ci-après le «rapport de la FRA»)]. Le rapport s'appuie également sur le suivi permanent, par la Commission, de l'application du RGPD, incluant des dialogues bilatéraux avec les États membres sur la conformité de la législation nationale, une contribution active aux travaux du comité et des contacts étroits avec un large éventail de parties prenantes sur l'application pratique du règlement.

2 MISE EN ŒUVRE DU RGPD ET FONCTIONNEMENT DES MECANISMES DE COOPERATION ET DE CONTROLE DE LA COHERENCE

Le système de guichet unique du RGPD vise à garantir une interprétation et une application harmonisées par des autorités indépendantes chargées de la protection des données. Il requiert une coopération entre les autorités chargées de la protection des données en cas de traitement transfrontalier, lorsque des personnes concernées dans plusieurs États membres sont sensiblement affectées. Les litiges entre autorités sont résolus par le comité dans le cadre du mécanisme de contrôle de la cohérence du RGPD.

2.1 Rendre le traitement des affaires transfrontières plus efficace: la proposition de règles de procédure

Le rapport de 2020 soulignait la nécessité d'un traitement plus efficace et harmonisé des affaires transfrontières dans l'ensemble de l'UE, en particulier à la lumière des différences majeures entre les procédures administratives nationales et dans l'interprétation des notions dans le mécanisme de coopération du RGPD. Par conséquent, en juillet 2023, la Commission a adopté une proposition de règlement sur les règles de procédure[7], en s'appuyant également sur une liste de questions soumises par le comité à la Commission en octobre 2022[8], ainsi que sur les contributions des parties prenantes[9] et des États membres[10]. La proposition complète le RGPD en établissant des règles détaillées sur les réclamations transfrontières, la participation du plaignant, les droits des parties faisant l'objet d'une enquête à une procédure régulière (responsables du traitement et sous-traitants) et la coopération entre les autorités chargées de la protection des données. L'harmonisation de ces aspects procéduraux contribuera à l'achèvement des enquêtes en

---

3 Un résumé des contributions du groupe d'experts multipartite sur le RGPD est disponible à l'adresse suivante: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Les contributions reçues en réponse à l'appel public à contributions et lors de réunions bilatérales avec les parties prenantes reflètent largement les points de vue exprimés par les membres du groupe d'experts multipartite du RGPD.

4 https://ec.europa.eu/info/law/better-regulation/

5 Contribution du comité européen de la protection des données à l'évaluation du RGPD au titre de l'article 97 | Comité européen de la protection des données (europa.eu)

6 GDPR in practice – Experiences of data protection authorities | (Le RGPD en pratique - expériences des autorités de protection des données) Agence des droits fondamentaux de l'Union européenne (europa.eu)

7 Proposition de règlement du Parlement européen et du Conseil établissant des règles de procédure supplémentaires relatives à l'application du règlement (UE) 2016/679 [COM(2023) 348 final]

8 https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_fr

9 Par l'intermédiaire du groupe d'experts multipartites du RGPD et d'un appel à contributions lancé en février 2023.

10 Notamment par l'intermédiaire du groupe d'experts des États membres sur le RGPD: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=fr&do=groupDetail.groupDetail&groupID=3461

temps utile et à la mise en place de voies de recours rapides pour les particuliers. La proposition fait actuellement l'objet de négociations entre le Parlement européen et le Conseil.

2.2 Renforcement de la coopération entre les autorités chargées de la protection des données et recours au mécanisme de contrôle de la cohérence

Le nombre d'affaires transfrontières a considérablement augmenté ces dernières années. Les autorités chargées de la protection des données ont démontré une volonté accrue d'utiliser les outils de coopération prévus par le RGPD. Toutes les autorités chargées de la protection des données ont eu recours à l'outil d'assistance mutuelle[11] ainsi qu'à des demandes «informelles» de se prêter mutuellement assistance sur une base volontaire. Les autorités chargées de la protection des données privilégient les demandes informelles, qui n'imposent pas de délai ou d'obligation stricte de répondre. Bien que le comité ait adopté des lignes directrices sur les opérations conjointes en 2021[12], les autorités n'ont toujours pas utilisé cet outil[13] de manière significative et citent les différences entre les procédures nationales et le manque de clarté de la procédure comme les principales raisons de son utilisation limitée.

Le RGPD donne aux autorités chargées de la protection des données concernées la possibilité de soulever une objection pertinente et motivée lorsqu'elles ne sont pas d'accord avec un projet de décision de l'autorité de protection des données chef de file dans une affaire transfrontière. Lorsque les autorités chargées de la protection des données ne peuvent parvenir à un consensus sur une objection pertinente et motivée, le RGPD prévoit un règlement des litiges par le comité[14]. Les sujets les plus fréquemment soulevés dans les objections pertinentes et motivées étaient les suivants: i) la base juridique du traitement; ii) les obligations d'information et de transparence; iii) la notification des violations de données; iv) les droits des personnes concernées; v) les dérogations pour les transferts internationaux; vi) le recours à des mesures correctives; et vii) le montant d'une amende administrative.

Le système d'application du RGPD repose sur la prémisse d'une coopération loyale et efficace entre les autorités chargées de la protection des données. Si la procédure de règlement des litiges joue un rôle important dans cette architecture de contrôle de l'application de la législation, elle devrait être utilisée dans l'esprit dans lequel elle a été conçue, à savoir en tenant dûment compte de la répartition des compétences entre les autorités chargées de la protection des données, de la nécessité de respecter les droits à une procédure régulière et de l'intérêt de parvenir à une résolution rapide de l'affaire pour les personnes concernées. Chaque procédure de règlement des litiges nécessite des ressources importantes de la part de l'autorité chef de file, des autorités concernées et du secrétariat du comité, et retarde la mise en place d'un recours pour les personnes concernées.

11 Article 61 du RGPD.
12 internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
13 Article 62 du RGPD.
14 Article 65 du RGPD.

Utilisation accrue des outils de coopération par les autorités chargées de la protection des données

- Près de 2 400 dossiers ont été enregistrés dans le système d'échange d'informations du comité[15].
- Les autorités chargées de la protection des données chefs de file ont élaboré environ 1 500 projets de décision[16], dont 990 ont abouti à des décisions finales constatant une violation du RGPD[17].
- Les autorités chargées de la protection des données ont déclenché près de 1 000 demandes d'assistance mutuelle «formelles»[18] et environ 12 300 demandes «informelles»[19].
- Cinq opérations conjointes ont été lancées, auxquelles ont participé des autorités chargées de la protection des données de sept États membres.
- Les autorités chargées de la protection des données de 18 États membres ont soulevé des objections pertinentes et motivées[20].

Le mécanisme de contrôle de la cohérence du RGPD est de plus en plus utilisé par les autorités chargées de la protection des données. Il comprend trois volets: i) les avis du comité; ii) le règlement des litiges par le comité; et iii) la procédure d'urgence[21].

Le comité aborde de plus en plus de questions importantes d'application générale dans ses avis[22]. Le comité devrait assurer une consultation en temps utile et pertinente avant l'adoption de ces avis. Les cas soumis au mécanisme de règlement des litiges ont porté sur des questions telles que la base juridique du traitement des données à des fins de publicité comportementale sur les médias sociaux et le traitement des données relatives aux enfants en ligne. La plupart des décisions contraignantes ultérieures ont été contestées devant le Tribunal.

La transparence du processus décisionnel du comité est essentielle pour garantir le respect du droit à une bonne administration en vertu de la charte des droits fondamentaux de l'Union européenne. La procédure d'urgence du RGPD permet aux autorités chargées de la protection des données de déroger au mécanisme de coopération et de contrôle de la cohérence afin d'adopter des mesures urgentes lorsque cela est nécessaire pour protéger les droits et libertés des personnes concernées. Par dérogation à la procédure normale de coopération prévue par le RGPD, des outils tels que la procédure d'urgence sont conçus pour être utilisés uniquement dans des circonstances exceptionnelles et lorsque la procédure normale de coopération ne peut protéger les droits et libertés des personnes concernées.

15 Au 3 novembre 2023 (contribution du comité).
16 Au titre de l'article 60, paragraphe 3, du RGPD.
17 Au 3 novembre 2023.
18 Les autorités irlandaises ont formulé le plus grand nombre de demandes formelles (246), tandis que les autorités allemandes ont reçu le plus grand nombre de demandes (516).
19 Les autorités irlandaises ont formulé le plus grand nombre de demandes informelles (4 245), suivies par les autorités allemandes (2 036).
20 Sur les 289 objections pertinentes et motivées communiquées par les autorités, 101 (35 %) ont été soulevées par les autorités allemandes. Le taux de réussite pour parvenir à un consensus sur les objections pertinentes et motivées varie de 15 % (des objections soulevées par les autorités allemandes) à 100 % (des objections soulevées par les autorités polonaises).
21 Respectivement les articles 64, 65 et 66, du RGPD.
22 Avis relevant de l'article 64, paragraphe 2, du RGPD.

Le mécanisme de contrôle de la cohérence

- Le comité a adopté 190 avis relatifs à la cohérence.
- Neuf décisions contraignantes ont été adoptées dans le cadre du règlement des litiges[23]. Toutes ont donné instruction à l'autorité chargée de la protection des données chef de file de modifier son projet de décision et plusieurs ont donné lieu à des amendes importantes.
- Cinq autorités chargées de la protection des données ont adopté des mesures provisoires dans le cadre de la procédure d'urgence (Allemagne, Espagne, Finlande, Italie et Norvège).
- Deux autorités chargées de la protection des données ont demandé une décision contraignante d'urgence du comité[24] et le comité a ordonné des mesures définitives d'urgence dans un cas.

2.3 Renforcement des mesures coercitives

Ces dernières années, les autorités chargées de la protection des données ont renforcé leurs activités coercitives, notamment en infligeant des amendes substantielles dans des affaires marquantes contre de grandes entreprises multinationales technologiques. Des amendes ont, par exemple, été infligées pour: i) la violation de la licéité et de la sécurité du traitement; ii) la violation du traitement de catégories particulières de données à caractère personnel; et iii) le non-respect des droits de particuliers[25]. Cela a conduit des entreprises privées à «prendre au sérieux la protection des données»[26] et contribué à ancrer une culture du respect des règles dans les organisations. Les autorités chargées de la protection des données adoptent des décisions constatant des infractions au RGPD dans des cas fondés sur des réclamations ou des cas décelés d'office. Bien qu'elles ne soient pas disponibles dans tous les États membres, de nombreuses autorités chargées de la protection des données ont fait un usage efficace des procédures de «règlement à l'amiable» pour résoudre rapidement les cas fondés sur des réclamations, à la satisfaction de l'auteur de la réclamation. La proposition relative aux règles de procédure reconnaît la possibilité de régler les réclamations à l'amiable[27].

Les autorités chargées de la protection des données ont largement fait usage de leurs pouvoirs d'adopter des mesures correctrices, bien que le nombre de mesures correctrices imposées varie considérablement d'une autorité à l'autre. Outre les amendes, les mesures correctrices les plus couramment utilisées étaient les avertissements, les blâmes et les injonctions de se conformer au RGPD. Les responsables du traitement et les sous-traitants contestent fréquemment les décisions constatant des violations du RGPD devant les juridictions nationales, le plus souvent pour des motifs procéduraux[28].

Renforcement des mesures coercitives

[23] Au titre de l'article 65, paragraphe 1, point a), du RGPD.
[24] En application de l'article 66, paragraphe 2, du RGPD.
[25] Voir la contribution 5.3.4 du comité.
[26] Rapport de la FRA, p. 36.
[27] Proposition relative aux règles de procédure, article 5.
[28] En Roumanie, les 26 décisions constatant une infraction ont toutes été contestées devant les tribunaux, tandis qu'aux Pays-Bas, le taux de recours était de 23 %. Le taux de réussite des recours était le plus élevé en Belgique (39 %).

- Les autorités chargées de la protection des données ont lancé plus de 20 000 enquêtes de leur propre initiative[29].
- Collectivement, elles reçoivent plus de 100 000 réclamations par an[30].
- Le délai médian pour le traitement des réclamations par les autorités chargées de la protection des données (de la réception à la clôture du dossier) varie de 1 à 12 mois et est inférieur ou égal à 3 mois dans cinq États membres [Danemark (1 mois), Espagne (1,5 mois), Estonie (3 mois), Grèce (3 mois) et Irlande (3 mois)].
- Plus de 20 000 réclamations ont été réglées à l'amiable. Le règlement amiable est le plus couramment utilisé en Autriche, en Hongrie, au Luxembourg et en Irlande.
- En 2022, les autorités allemandes chargées de la protection des données ont adopté le plus grand nombre de décisions imposant une mesure correctrice (3 261), suivies par l'Espagne (774), la Lituanie (308) et l'Estonie (332). Le nombre le plus faible de mesures correctrices a été imposé au Liechtenstein (8), en Tchéquie (8), en Islande (10), aux Pays-Bas (17) et au Luxembourg (22).
- Les autorités chargées de la protection des données ont infligé plus de 6 680 amendes pour un montant d'environ 4,2 milliards d'EUR[31]. L'autorité irlandaise a infligé le montant total d'amendes le plus élevé (2,8 milliards d'EUR), suivie du Luxembourg (746 millions d'EUR), de l'Italie (197 millions d'EUR) et de la France (131 millions d'EUR). Le Liechtenstein (9 600 EUR), l'Estonie (201 000 EUR) et la Lituanie (435 000 EUR) ont infligé les amendes les plus faibles.

Bien que la plupart des autorités chargées de la protection des données considèrent que leurs outils d'enquête sont adéquats, certaines exigent des outils supplémentaires au niveau national, prévoyant notamment des sanctions adéquates lorsque les responsables du traitement ne coopèrent pas ou ne fournissent pas les informations nécessaires[32]. Les autorités chargées de la protection des données considèrent que l'insuffisance des ressources et les lacunes en matière d'expertise technique et juridique constituent le principal facteur affectant leur capacité d'exécution[33].

2.4 Comité européen de la protection des données

Le comité est composé du chef d'une autorité chargée de la protection des données de chaque État membre et du Contrôleur européen de la protection des données, la Commission y participant sans droit de vote. Le comité, soutenu dans ses travaux par son secrétariat, est chargé de veiller à l'application cohérente du RGPD[34]. La plupart des autorités chargées de la protection des données estiment que le comité a joué un rôle positif

29 En Allemagne, les autorités chargées de la protection des données ont lancé le plus grand nombre d'enquêtes d'initiative (7 647), suivies par la Hongrie (3 332), l'Autriche (1 681) et la France (1 571).

30 En 2022, neuf autorités chargées de la protection des données ont reçu plus de 2 000 réclamations. Le plus grand nombre de réclamations a été enregistré par l'Allemagne (32 300), l'Italie (30 880), l'Espagne (15 128), les Pays-Bas (13 133) et la France (12 193), tandis que le plus petit nombre de réclamations a été enregistré par le Liechtenstein (40), l'Islande (140) et la Croatie (271).

31 Toutes les autorités ont infligé des amendes administratives, à l'exception du Danemark, qui ne prévoit pas d'amendes administratives. Le plus grand nombre d'amendes ont été infligées en Allemagne (2 106) et en Espagne (1 596). Le plus faible nombre d'amendes ont été infligées au Liechtenstein (3), en Islande (15) et en Finlande (20).

32 Rapport de la FRA, p. 38.

33 Rapport de la FRA, pages 20 et 23. Voir également la position et les conclusions du Conseil, point 17.

34 Article 70, paragraphe 1, du RGPD.

dans le renforcement de la coopération entre elles[35]. De nombreuses autorités chargées de la protection des données consacrent des ressources importantes aux activités du comité, bien que des autorités plus petites indiquent que leur taille les empêche d'y participer pleinement[36]. Certaines autorités estiment que l'efficacité du fonctionnement du comité devrait être améliorée, notamment en réduisant le nombre de réunions et en accordant moins d'attention aux questions mineures[37]. En fonction de l'issue des négociations sur la proposition relative aux règles de procédure du RGPD, qui vise à réduire le nombre d'affaires soumises au comité en vue du règlement du litige, il pourrait être nécessaire de se pencher sur la question de savoir si le comité a besoin de ressources supplémentaires.

En novembre 2023, le comité avait adopté 35 lignes directrices. Si les parties prenantes et les autorités chargées de la protection des données les ont jugées utiles, elles estiment que les lignes directrices devraient être fournies plus rapidement et que leur qualité devrait être améliorée[38]. Les parties prenantes notent qu'elles sont souvent trop théoriques, trop longues et ne reflètent pas l'approche fondée sur les risques du RGPD[39]. Les autorités chargées de la protection des données et le comité devraient fournir des lignes directrices concises et pratiques qui apportent des réponses à des problèmes concrets et reflètent un équilibre entre la protection des données et d'autres droits fondamentaux. Les lignes directrices devraient également être faciles à comprendre pour les personnes sans formation juridique, par exemple dans les PME et les organisations bénévoles[40]. Un moyen d'y parvenir est de rendre la préparation des lignes directrices plus transparente et de procéder à des consultations à un stade précoce afin de permettre une meilleure compréhension de la dynamique du marché, des pratiques commerciales et de la manière d'appliquer les lignes directrices dans la pratique[41]. Il faut se féliciter que, dans le cadre de sa stratégie 2024-2027, le comité ait mis l'accent sur son objectif de fournir des orientations pratiques accessibles au public concerné[42].

Les parties prenantes soulignent la nécessité de lignes directrices supplémentaires, notamment en ce qui concerne l'anonymisation et la pseudonymisation[43], l'intérêt légitime et la recherche scientifique[44]. Dans son rapport de 2020, la Commission invitait le comité à adopter des lignes directrices sur la recherche scientifique, mais celles-ci n'ont pas encore été adoptées. Compte tenu de l'importance de la recherche scientifique dans la société, en particulier pour surveiller les maladies et mettre au point des traitements, et pour favoriser l'innovation, il est essentiel que les autorités chargées de la protection des données agissent pour clarifier ces questions sans plus tarder[45]. Les pouvoirs publics bénéficieraient également d'orientations pour relever les défis particuliers auxquels ils sont confrontés[46].

---

35 Rapport de la FRA, p. 64.

36 Rapport de la FRA, p. 67. En 2023, les autorités allemandes chargées de la protection des données sont celles qui ont consacré le plus de ressources aux activités du comité [26 équivalents temps plein (ETP)], suivies par l'Irlande (16) et la France (12) (contribution du comité).

37 Rapport de la FRA, p. 67.

38 Rapport de la FRA, p. 67; résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

39 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

40 Voir également la position et les conclusions du Conseil, point 45.

41 Voir également la position et les conclusions du Conseil, point 34.

42 https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf

43 Voir également la position et les conclusions du Conseil, point 31 d).

44 Elles nécessitent des éclaircissements, notamment en ce qui concerne la signification du terme «recherche scientifique», le rôle du consentement au traitement de données à caractère personnel à des fins de recherche, la base juridique pertinente, ainsi que les rôles et responsabilités des acteurs concernés.

45 Voir également la position et les conclusions du Conseil, point 31 b).

46 Position et conclusions du Conseil, points 27 et 28.

2.5 Autorités chargées de la protection des données

2.5.1 Indépendance et ressources

L'indépendance des autorités chargées de la protection des données est inscrite dans la charte des droits fondamentaux de l'Union européenne et dans le traité sur le fonctionnement de l'Union européenne. Le RGPD fixe des exigences visant à garantir l'«indépendance totale» des autorités chargées de la protection des données[47]. Le rapport de la FRA a constaté que la plupart des autorités chargées de la protection des données fonctionnent indépendamment du gouvernement, du parlement ou de tout autre organisme public[48].

Les autorités chargées de la protection des données ont besoin de ressources humaines, techniques et financières suffisantes pour être en mesure d'accomplir efficacement et en toute indépendance leurs missions au titre du RGPD. Dans le rapport de 2020, la Commission a constaté que les ressources allouées aux autorités chargées de la protection des données n'étaient toujours pas satisfaisantes et a régulièrement soulevé cette question avec les États membres. Depuis lors, la situation s'est améliorée.

Augmentation des ressources pour les autorités chargées de la protection des données[49]

- Entre 2020 et 2024, toutes les autorités chargées de la protection des données, sauf deux, ont bénéficié d'une augmentation des effectifs et cette augmentation a dépassé 25 % dans 14 États membres.
- L'autorité irlandaise chargée de la protection des données a enregistré la plus forte augmentation des effectifs (79 %), suivie de l'Estonie, de la Suède (57 % dans les deux cas) et de la Bulgarie (56 %).
- Le personnel de l'autorité a légèrement diminué en Tchéquie (- 1 %), tandis qu'il n'a pas augmenté au Liechtenstein et qu'il a légèrement augmenté à Chypre (4 %) et en Hongrie (8 %).
- Entre 2020 et 2024, toutes les autorités chargées de la protection des données, sauf une, ont vu leur budget augmenter, et cette augmentation a dépassé 50 % dans 13 États membres.
- L'autorité chargée de la protection des données à Chypre a enregistré la plus forte augmentation de budget (130 %), suivie de l'Autriche (107 %), de la Bulgarie (100 %) et de l'Estonie (97 %).
- Le budget de l'autorité grecque chargée de la protection des données a diminué de 15 %, tandis que des augmentations budgétaires mineures ont été enregistrées pour les autorités du Liechtenstein (1 %), de la Slovaquie (6 %) et de la République tchèque (8 %).

Si ces statistiques montrent une tendance générale à l'augmentation des ressources des autorités chargées de la protection des données, les autorités elles-mêmes considèrent qu'elles ne disposent toujours pas de ressources humaines suffisantes[50]. Elles insistent sur

47 Article 52 du RGPD.
48 Rapport de la FRA, p. 31.
49 Voir la section 4.4.1 de la contribution du comité, également pour les chiffres absolus.
50 Cinq autorités chargées de la protection des données seulement estiment qu'elles disposent de ressources humaines adéquates (contribution du comité, p. 33).

la nécessité de disposer de connaissances techniques très spécialisées, notamment en ce qui concerne les technologies nouvelles et émergentes[51], dont le manque affecte la quantité et la qualité de leur travail, et sur les difficultés à concurrencer le secteur privé pour les ressources humaines. Les autorités chargées de la protection des données citent l'insuffisance des connaissances juridiques et le manque de compétences linguistiques comme des facteurs affectant leur performance. La faiblesse de la rémunération, l'incapacité à sélectionner le personnel de manière autonome et la lourde charge de travail sont mises en évidence comme les principaux facteurs qui influent sur la capacité des autorités à recruter et à conserver du personnel[52]. Les autorités chargées de la protection des données soulignent également qu'elles ont besoin de ressources financières pour moderniser et numériser leurs processus et acquérir des équipements techniques[53]. Toutes les autorités chargées de la protection des données accomplissent des tâches allant au-delà de celles qui leur sont confiées par le RGPD[54], par exemple en tant qu'autorités de contrôle de la directive en matière de protection des données dans le domaine répressif et de la directive «vie privée et communications électroniques», tandis que nombre d'entre elles expriment des préoccupations quant à l'exercice de responsabilités supplémentaires au titre de la nouvelle législation numérique[55].

2.5.2 Difficultés à traiter un grand nombre de réclamations

Plusieurs autorités chargées de la protection des données indiquent qu'elles consacrent une trop grande partie de leurs ressources au traitement d'un grand nombre de réclamations, dont la plupart sont, selon elles, insignifiantes et infondées, étant donné que le traitement de chaque réclamation est une obligation en vertu du RGPD qui est soumise à un contrôle juridictionnel[56]. Cela signifie que les autorités chargées de la protection des données ne peuvent allouer des ressources suffisantes à d'autres activités, telles que des enquêtes d'office, des campagnes de sensibilisation du public et le dialogue avec les responsables du traitement[57]. En tant qu'autorités publiques, les autorités chargées de la protection des données ont le pouvoir discrétionnaire d'allouer leurs ressources comme elles l'entendent afin d'accomplir chacune de leurs missions (énumérées à l'article 57, paragraphe 1, du RGPD) dans l'intérêt public. De nombreuses autorités chargées de la protection des données ont adopté des stratégies visant à accroître l'efficacité du traitement des réclamations, telles que l'automatisation[58], le recours à des procédures de règlement à l'amiable[59] et le «regroupement» de réclamations portant sur des questions similaires[60].

2.5.3 Interprétation du RGPD par les autorités nationales chargées de la protection des données

L'un des principaux objectifs du RGPD était de supprimer l'approche fragmentée de la protection des données qui existait dans le cadre de la précédente directive sur la protection

---

51 Rapport de la FRA, p. 20. Certaines autorités chargées de la protection des données externalisent certaines tâches à des contractants externes, telles que le traitement des réclamations, l'analyse juridique et l'analyse judiciaire.

52 Rapport de la FRA, p. 24.

53 Rapport de la FRA, p. 22.

54 Voir la section 4.4.5 de la contribution du comité.

55 Contribution du comité, p. 32.

56 Rapport de la FRA, p. 48.

57 Rapport de la FRA, p. 45. Les autorités chargées de la protection des données considèrent les enquêtes d'office comme particulièrement importantes, étant donné que les auteurs des réclamations peuvent ne pas avoir connaissance de nombreuses violations du RGPD.

58 Rapport de la FRA, p. 8.

59 Rapport de la FRA, p. 39.

60 Rapport de la FRA, p. 41.

des données (directive 95/46/CE)[61]. Toutefois, les autorités chargées de la protection des données continuent d'adopter des interprétations divergentes sur les concepts clés de la protection des données[62]. Les parties prenantes considèrent qu'il s'agit du principal obstacle à l'application cohérente du RGPD dans l'UE. La persistance d'interprétations divergentes crée une insécurité juridique et augmente les coûts pour les entreprises (par exemple en exigeant des documents différents pour plusieurs États membres), ce qui perturbe la libre circulation des données à caractère personnel dans l'UE, entrave les activités transfrontières ainsi que la recherche et l'innovation face à des défis sociétaux urgents.

Parmi les questions spécifiques soulevées par les parties prenantes figurent: i) le fait que les autorités chargées de la protection des données dans trois États membres adoptent chacune un point de vue différent quant à la base juridique appropriée pour le traitement des données à caractère personnel lors de la conduite d'un essai clinique; ii) il existe souvent des divergences de vues sur la question de savoir si une entité est responsable du traitement ou sous-traitant; et iii) dans certains cas, les autorités chargées de la protection des données ne suivent pas les lignes directrices du comité ou publient des lignes directrices au niveau national qui sont contraires à celles du comité[63]. Ces problèmes sont aggravés lorsque plusieurs autorités chargées de la protection des données au sein d'un seul État membre adoptent des interprétations contradictoires.

Certaines parties prenantes estiment également que certaines autorités chargées de la protection des données et le comité adoptent des interprétations qui s'écartent de l'approche fondée sur les risques du RGPD, ce qui constitue un défi pour le développement de l'économie numérique[64] ainsi que pour la liberté et la pluralité des médias. Elles mentionnent comme sujets de préoccupation: i) l'interprétation de l'anonymisation; ii) la base juridique de l'intérêt légitime et du consentement[65]; et iii) les exceptions à l'interdiction de la prise de décision individuelle automatisée[66]. Il convient de rappeler que les autorités chargées de la protection des données et le comité sont chargés d'assurer à la fois la protection des personnes physiques en ce qui concerne le traitement de leurs données à caractère personnel et le libre flux des données à caractère personnel au sein de l'UE. Comme il ressort du RGPD[67], le droit à la protection des données à caractère personnel doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité.

2.5.4 Dialogue avec les responsables du traitement et les sous-traitants

Les parties prenantes soulignent l'intérêt d'avoir la possibilité d'engager un dialogue constructif avec les autorités chargées de la protection des données afin de veiller à ce qu'elles respectent le RGPD dès le départ, en particulier en ce qui concerne les technologies émergentes. Les parties prenantes notent que certaines autorités chargées de la protection des données dialoguent activement avec les responsables du traitement, tandis que d'autres sont lentes à réagir, donnent des réponses vagues ou ne répondent pas du tout[68].

---

61 Considérant 9 du RGPD.
62 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.
63 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.
64 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.
65 Respectivement l'article 6, paragraphe 1, point f) et l'article 6, paragraphe 1, point a), du RGPD.
66 Article 22, paragraphe 2, du RGPD.
67 Considérant 4
68 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

3 MISE EN ŒUVRE DU RGPD PAR LES ÉTATS MEMBRES

3.1 Fragmentation de l'application au niveau national

Si le RGPD, en tant que règlement, est directement applicable, il impose aux États membres de légiférer dans certains domaines et leur donne la possibilité de préciser davantage son application dans un nombre limité de domaines[69]. Lorsqu'ils légifèrent au niveau national, les États membres doivent le faire dans les conditions et dans les limites fixées par le RGPD. Comme en 2020, les parties prenantes signalent avoir rencontré des difficultés en raison de la fragmentation des règles nationales lorsque les États membres ont la possibilité de préciser le RGPD, notamment en ce qui concerne:

- l'âge minimum du consentement d'un enfant en ce qui concerne l'offre de services de la société de l'information à cet enfant[70];
- l'introduction par les États membres de conditions supplémentaires concernant le traitement des données génétiques, des données biométriques ou des données relatives à la santé[71];
- le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions[72], ce qui crée des difficultés dans certains secteurs réglementés.

Dans le même temps, il est important de noter que de nombreuses parties prenantes signalent que les problèmes de fragmentation découlent principalement d'interprétations divergentes du RGPD par les autorités chargées de la protection des données, plutôt que de l'utilisation de clauses de spécification facultatives par les États membres.

Les États membres estiment qu'un degré limité de fragmentation pourrait être acceptable et que les clauses de spécification prévues par le RGPD restent bénéfiques, en particulier pour le traitement par les autorités publiques[73]. Le RGPD impose aux États membres de consulter leur autorité nationale chargée de la protection des données lors de l'élaboration de la législation relative au traitement des données à caractère personnel[74]. Le rapport de la FRA a constaté que certains gouvernements fixent des délais très serrés pour ces autorités et, dans certains cas, ne les consultent pas du tout[75].

3.2 Suivi par la Commission

La Commission suit en permanence la mise en œuvre du RGPD. La Commission a engagé des procédures d'infraction à l'encontre des États membres sur des questions telles que l'indépendance des autorités chargées de la protection des données (y compris le fait de rester libre de toute influence extérieure et la disponibilité d'un recours juridictionnel en cas de licenciement)[76] et le droit à un recours juridictionnel effectif pour les personnes concernées lorsque l'autorité de protection des données ne traite pas une réclamation[77]. Dans le cadre de son suivi, la Commission demande également que les autorités chargées de la protection des données fournissent, sur une base strictement confidentielle, des

69 Par exemple, l'âge minimal du consentement de l'enfant en ce qui concerne les services de la société de l'information (article 8, paragraphe 1, du RGPD).
70 Article 8, paragraphe 1, du RGPD.
71 Une possibilité prévue à l'article 9, paragraphe 4, du RGPD.
72 Article 10 du RGPD.
73 Position et conclusions du Conseil, point 30.
74 Article 36 du RGPD.
75 Rapport de la FRA, p. 11.
76 Belgique (2021/4045) et Belgique (2022/2160).
77 Finlande (2022/4010) et Suède (2022/2022).

informations régulières[78] sur des affaires transfrontières à grande échelle en cours, notamment celles concernant les grandes multinationales technologiques.

La Commission communique régulièrement avec les États membres sur la mise en œuvre du RGPD. Comme elle l'a indiqué dans le rapport de 2020, la Commission a continué de recourir au groupe d'experts des États membres sur le RGPD[79] pour faciliter les discussions et le partage d'expériences sur la mise en œuvre effective du RGPD. Le groupe d'experts a tenu des discussions spécifiques sur: i) le contrôle des juridictions agissant dans l'exercice de leur fonction juridictionnelle (article 55 du RGPD; article 8 de la Charte); ii) la conciliation entre le droit à la protection des données et le droit à la liberté d'expression (article 85 du RGPD); et iii) le droit à un recours juridictionnel effectif contre une autorité de contrôle (article 78 du RGPD). À la suite de ces discussions, la Commission a compilé un aperçu des approches adoptées pour la mise en œuvre de ces dispositions dans les États membres[80]. La Commission a également eu recours à ce groupe pour procéder à des échanges de vues avec les États membres lors de l'élaboration de la proposition relative aux règles de procédure.

La conformité de la législation et des pratiques nationales avec les règles en matière de protection des données énoncées dans le corpus législatif de l'UE relatif à l'espace Schengen est également examinée dans le cadre des évaluations Schengen menées conjointement par les États membres et la Commission. Au moins cinq évaluations de la protection des données sont réalisées sur place chaque année, actuellement axées sur les systèmes d'information à grande échelle et le système d'information Schengen, le système d'information sur les visas, ainsi que sur le rôle de surveillance de ces systèmes exercé par les autorités nationales chargées de la protection des données.

La Commission contribue activement au grand nombre d'affaires portées devant la Cour de justice (avec environ 30 décisions préjudicielles par an ces dernières années), qui jouent un rôle central dans l'interprétation cohérente des concepts clés du RGPD. Une jurisprudence de plus en plus abondante de la Cour a apporté plusieurs précisions, notamment en ce qui concerne la définition des données à caractère personnel[81], les catégories particulières de données à caractère personnel[82], le responsable du traitement[83], le consentement[84], l'intérêt légitime[85], le droit d'accès[86], le droit à l'effacement[87], le droit à réparation[88], la prise de décision individuelle automatisée[89], les amendes administratives[90], les délégués à la protection des données[91], la publication de données à

---

78 Avec des informations sur la référence de l'affaire, le type d'enquête (d'office ou fondée sur une réclamation), un résumé du champ de l'enquête, les autorités chargées de la protection des données concernées, les principales étapes et dates de la procédure, l'enquête ou toute autre mesure prise et les dates.

79 https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=fr&do=groupDetail.groupDetail&groupID=3461

80 https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=fr&meetingId=31754&fromExpertGroups=3461

81 Affaire C-319/22, EU:C:2023:837.

82 Affaires C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.

83 Affaires C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.

84 Affaire C-61/19, ECLI:EU:C:2020:901.

85 Affaires C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.

86 Affaires C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.

87 Affaire C-460/20, ECLI:EU:C:2022:962.

88 Affaire C-300/21, ECLI:EU:C:2023:370; affaire C-687/21, ECLI:EU:C:2024:72; affaire C-667/21, ECLI:EU:C:2023:1022.

89 Affaires jointes C-26/22 et C-64/22, ECLI:EU:C:2023:958.

90 Affaires C-807/21, ECLI:EU:C:2023:950; affaire C-683/21, ECLI:EU:C:2023:949.

91 Affaire C-453/21, ECLI:EU:C:2023:79.

caractère personnel dans des registres[92] et l'application du RGPD aux activités des parlements[93].

4 DROITS DES PERSONNES CONCERNEES

Sensibilisation des particuliers au RGPD et aux autorités chargées de la protection des données (Eurobaromètre 549 de 2024 sur la justice, les droits et les valeurs)

- 72 % des répondants dans l'ensemble de l'UE indiquent avoir entendu parler du RGPD, parmi lesquels 40 % savent ce que c'est.
- Dans 19 États membres, plus de 70 % des répondants indiquent avoir connaissance du RGPD, les répondants en Suède (92 %) étant les plus informés, suivis par les Pays-Bas (88 %), Malte et le Danemark (84 %), tandis que les répondants en Bulgarie (59 %) sont les moins informés, suivis par la Lituanie (63 %) et la France (64 %).
- 68 % des répondants dans l'ensemble de l'UE indiquent avoir entendu parler d'une autorité nationale chargée de protéger leurs droits en matière de protection des données, 24 % de l'ensemble des répondants indiquant qu'ils savent également quelle autorité publique est responsable.
- Dans tous les États membres, au moins la moitié des répondants ont entendu parler d'une telle autorité nationale, avec les niveaux les plus élevés aux Pays-Bas (82 %), en Tchéquie, en Slovénie et en Pologne (75 % tous) et au Portugal (74 %). Les répondants en Autriche (56 %) et en Espagne (58 %) sont les moins informés de l'existence de cette autorité.

Les personnes sont de plus en plus familiarisées avec les droits que leur confère le RGPD et les exercent activement[94]. Les autorités chargées de la protection des données allouent des ressources substantielles à la sensibilisation du grand public aux droits et obligations en matière de protection des données, par exemple au moyen de campagnes de médias sociaux et de campagnes télévisées, de lignes d'assistance téléphonique, de bulletins d'information et de présentations dans des établissements d'enseignement[95]. Bon nombre de ces initiatives ont bénéficié d'un financement de l'UE[96]. L'Agence des droits fondamentaux note que si la sensibilisation du grand public à la protection des données a augmenté, la compréhension de la protection des données fait toujours défaut, comme en témoignent un grand nombre de réclamations insignifiantes ou infondées[97]. Plusieurs outils numériques conviviaux ont été mis au point pour permettre aux personnes concernées d'exercer plus facilement leurs droits[98]. Les actes législatifs, en particulier le règlement sur la gouvernance des données[99], devraient conduire à la création de moyens supplémentaires permettant aux personnes concernées d'exercer leurs droits à l'avenir. Les entreprises notent que le droit à l'effacement est de plus en plus utilisé, alors que c'est rarement le cas du droit de rectification et du droit d'opposition.

92 Affaires C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
93 Affaires C-33/22, ECLI:EU:C:2024:46; C-272/19, ECLI:EU:C:2020:535.
94 Position et conclusions du Conseil, point 13.
95 Contribution du comité, section 6.
96 https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=fr
97 Rapport de la FRA, pages 9 et 48.
98 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.
99 Article 10 du règlement (UE) 2022/868 (règlement sur la gouvernance des données), (JO L 152 du 3.6.2022, p. 1).

4.1 Droit d'accès

Les responsables du traitement indiquent que le droit d'accès (article 15 du RGPD) est le droit le plus fréquemment invoqué par les personnes concernées. Alors que le comité a adopté des lignes directrices sur ce droit en 2022, les responsables du traitement continuent de signaler des difficultés, par exemple lorsqu'ils interprètent la notion de «demandes infondées ou excessives»[100], lorsqu'ils répondent à un grand nombre de demandes et lorsqu'ils traitent des demandes qui sont formulées à des fins étrangères à la protection des données, par exemple pour recueillir des preuves dans le cadre de procédures judiciaires[101]. Les organisations de la société civile notent que les réponses aux demandes d'accès sont souvent retardées ou incomplètes, tandis que les données reçues ne sont pas toujours dans un format lisible[102]. Les pouvoirs publics citent des difficultés dans l'interaction entre le droit d'accès et les règles relatives à l'accès du public aux documents[103]. Il est donc bienvenu que le comité ait lancé une action conjointe sur le droit d'accès dans le cadre d'application coordonné en février 2024[104].

4.2 Le droit à la portabilité

Dans le rapport de 2020, la Commission s'est engagée à étudier les moyens pratiques de faciliter une utilisation accrue du droit à la portabilité (article 20 du RGPD) par les particuliers, conformément à la stratégie en matière de données. Depuis lors, la Commission a adopté un certain nombre d'initiatives qui complètent ce droit. Ces initiatives facilitent le passage d'un service à l'autre, créant ainsi un plus grand choix pour les particuliers, soutenant la concurrence et l'innovation et permettant aux particuliers de tirer parti de l'utilisation de leurs données. Le règlement sur les données confère aux utilisateurs de dispositifs intelligents un droit renforcé à la portabilité des données générées par ces dispositifs - et prévoit que la conception du produit ou d'un serveur dorsal du fabricant ou du détenteur de données rend cette portabilité techniquement possible. Le règlement sur les marchés numériques exige des fournisseurs de services de plateforme essentiels désignés comme «contrôleurs d'accès» qu'ils assurent la portabilité effective des données des utilisateurs, y compris un accès continu et en temps réel à ces données. Plusieurs autres initiatives de la Commission en cours de négociation ou sur lesquelles un accord politique a été conclu prévoient un renforcement des droits à la portabilité dans des domaines spécifiques, notamment la directive sur le travail via une plateforme[105], l'espace européen des données de santé[106] et le cadre pour l'accès aux données financières[107].

4.3 Le droit d'introduire une réclamation

Comme en témoigne le grand nombre de réclamations, le droit d'introduire une réclamation auprès d'une autorité chargée de la protection des données est largement connu. Les organisations de la société civile soulignent les différences injustifiées entre les pratiques nationales en matière de traitement des réclamations, question qui est abordée

---

100 Article 12, paragraphe 5, du RGPD.

101 Toutefois, la Cour de justice a précisé que la personne concernée n'est pas tenue de motiver sa demande d'accès à des données à caractère personnel: affaire C-307/22, ECLI:EU:C:2023:811, point 38.

102 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

103 Position et conclusions du Conseil, points 27 et 28.

104 https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_en.

105 Travailleurs des plateformes: Le Conseil confirme l'accord sur de nouvelles règles visant à améliorer leurs conditions de travail - Consilium (europa.eu)

106 Proposition de règlement relatif à l'espace européen des données de santé (COM/2022/197 final).

107 Proposition de règlement relatif à un cadre pour l'accès aux données financières et modifiant les règlements (UE) nº 1093/2010, (UE) nº 1094/2010, (UE) nº 1095/2010 et (UE) 2022/2554 (COM/2023/360 final).

dans la proposition de la Commission relative aux règles de procédure. Peu d'États membres ont fait usage de la faculté prévue par le RGPD de donner à un organisme à but non lucratif le droit de prendre des mesures indépendamment du mandat d'une personne concernée (article 80, paragraphe 2). Toutefois, la directive relative aux actions représentatives[108], adoptée en 2020, conduira à une plus grande harmonisation à cet égard en facilitant les actions collectives des particuliers pour violation du RGPD. Les mesures nationales de transposition de la directive sont entrées en vigueur en juin 2023.

4.4 La protection des données à caractère personnel des enfants

Les enfants ont besoin d'une protection spécifique lors du traitement de leurs données à caractère personnel[109]. Le RGPD fait partie d'un cadre juridique complet qui garantit que les enfants sont protégés aussi bien hors ligne qu'en ligne[110]. Compte tenu de la présence accrue d'enfants en ligne, un certain nombre de mesures ont été prises au niveau de l'UE et au niveau national ces dernières années pour soutenir la protection des enfants en ligne. Les autorités chargées de la protection des données ont infligé des amendes importantes à des entreprises de médias sociaux pour violation du RGPD lors du traitement de données d'enfants. Elles coopèrent également avec d'autres autorités pour demander une meilleure protection des enfants dans le domaine de la publicité. Dans le rapport de 2020, la Commission a invité le comité à adopter des lignes directrices sur le traitement des données relatives aux enfants et les travaux sont en cours à cette fin[111]. Le règlement sur les services numériques comprend des dispositions spécifiques visant à garantir un niveau élevé de respect de la vie privée, de sûreté et de sécurité aux enfants utilisant les plateformes en ligne.

Certaines parties prenantes signalent des difficultés liées à l'exercice des droits des personnes concernées, lorsque ces personnes sont des enfants. En particulier, elles indiquent que les enfants ne comprennent pas pleinement leurs droits, manquent de compétences en matière d'habileté numérique et peuvent faire l'objet d'une influence indue[112]. La Commission a financé plusieurs initiatives au niveau national sur la protection des données relatives aux enfants et sur la promotion de la sensibilisation des enfants à la protection des données[113]. Dans le cadre de la stratégie pour un internet mieux adapté aux enfants (BIK+), la Commission fournit des ressources de sensibilisation et des formations aux enfants sur leurs droits numériques, y compris la protection des données (par exemple, le consentement numérique)[114]. L'accent est de plus en plus mis sur la nécessité de disposer d'outils de vérification de l'âge efficaces et respectueux de la vie privée. Début 2024, la Commission a mis en place un groupe de travail sur la vérification de l'âge avec les États membres, le comité et le groupe des régulateurs européens pour les services de médias audiovisuels, dans le but de discuter et de soutenir l'élaboration d'une approche de la vérification de l'âge à l'échelle de l'UE. Ces travaux vont à présent se poursuivre sous l'égide du comité du règlement sur les services numériques, au sein du groupe de travail

---

108 Directive (UE) 2020/1828 du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

109 Considérant 38 du RGPD.

110 Recommandation relative au développement et au renforcement de systèmes intégrés de protection de l'enfance dans l'intérêt supérieur de l'enfant: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_fr.

111 Voir également la position et les conclusions du Conseil, point 31 a).

112 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

113 https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=fr

114 https://digital-strategy.ec.europa.eu/fr/policies/strategy-better-internet-kids

chargé de la protection des mineurs. Dans le contexte du règlement concernant un cadre européen relatif à une identité numérique[115], qui est entré en vigueur en mai 2024, la Commission s'emploie à faire en sorte que le portefeuille européen d'identité numérique soit accessible à tous les citoyens et résidents de l'UE en 2026, y compris à des fins de vérification de l'âge. Entre-temps, avant que l'écosystème du portefeuille devienne pleinement opérationnel, une solution à court terme concernant la vérification de l'âge sera mise en place et disponible dans l'ensemble de l'UE.

5 OPPORTUNITES ET DEFIS POUR LES ORGANISATIONS, EN PARTICULIER LES PME

Le RGPD a créé des conditions de concurrence équitables pour les entreprises opérant sur le marché intérieur, et son approche technologiquement neutre et propice à l'innovation permet aux entreprises de réduire les formalités administratives et de bénéficier d'une plus grande confiance des consommateurs[116]. De nombreuses entreprises ont développé une culture interne de la protection des données et considèrent la vie privée et la protection des données comme des paramètres essentiels de la concurrence. Les entreprises estiment que l'approche fondée sur les risques du RGPD constitue un principe directeur permettant la flexibilité et l'évolutivité de leurs obligations[117].

5.1 Boîte à outils pour les entreprises

Le RGPD fournit une panoplie d'instruments permettant aux organisations de gérer et de démontrer avec souplesse leur conformité, y compris des codes de conduite, des mécanismes de certification et des clauses contractuelles types. Comme annoncé dans le rapport de 2020, la Commission a adopté des clauses contractuelles types sur la relation entre responsable du traitement et sous-traitant en 2021[118]. Ces clauses contractuelles types fournissent un outil de mise en conformité volontaire prêt à l'emploi et facile à mettre en œuvre, ce qui est particulièrement utile pour les PME ou les organisations qui ne disposent peut-être pas des ressources nécessaires pour négocier des contrats individuels avec leurs partenaires commerciaux. Les entreprises font état d'un retour d'information mitigé sur l'utilisation des clauses contractuelles types, en ce sens que certaines entreprises (principalement des PME) les utilisent entièrement ou partiellement, tandis que d'autres (principalement les grandes entreprises) ont tendance à ne pas les utiliser parce qu'elles préfèrent utiliser leurs propres clauses.

Les entreprises soulignent que les codes de conduite recèlent un potentiel important en tant qu'outil de mise en conformité sectoriel et rentable[119]. Toutefois, l'élaboration de codes de conduite a été limitée[120]. Selon les informations disponibles à ce jour, seuls deux codes à l'échelle de l'UE ont été approuvés (tous deux dans le secteur de l'informatique en nuage),

---

115 Règlement (UE) 2024/1183 modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique (JO L 2024/1183 du 30.4.2024).

116 Comme le reconnaît le rapport de la plateforme «Prêts pour l'avenir», un groupe d'experts de haut niveau mis en place pour aider la Commission dans ses efforts visant à simplifier la législation de l'UE et à réduire les coûts inutiles qui y sont liés: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_fr. Voir également le résumé du retour d'information du groupe d'experts multipartite sur le RGPD et la position et les conclusions du Conseil, point 12.

117 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

118 Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du RGPD et de l'article 29, paragraphe 7, du RGPD (C/2021/3701) - (JO L 199 du 7.6.2021, p. 18).

119 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

120 Position et conclusions du Conseil, point 25.

tandis que six codes l'ont été au niveau national[121]. Les parties prenantes signalent la lourdeur des exigences (notamment la nécessité de mettre en place un organisme de contrôle accrédité), le manque d'engagement des autorités chargées de la protection des données et la longueur du processus d'approbation en tant que principaux facteurs limitant l'adoption des codes de conduite[122].

Il est nécessaire d'accroître la transparence du processus et de fixer des délais d'approbation clairs. Les autorités chargées de la protection des données, et dans le cas de codes à l'échelle de l'UE, le comité, devraient encourager plus activement l'élaboration des codes de conduite en collaborant avec les associations qui les conçoivent. Cela contribuera à résoudre les divergences d'interprétation et à accélérer le processus d'approbation. Les parties prenantes regrettent les longs retards dans l'adoption des codes de conduite, dus à des questions débattues en parallèle dans le cadre des travaux sur les lignes directrices. De même, les entreprises déclarent que la certification n'est pas largement utilisée parce que le processus de développement est lent et complexe. Comme pour les codes de conduite, les autorités chargées de la protection des données devraient prévoir des délais plus clairs pour l'examen et l'approbation des certifications.

Dans sa stratégie 2024-2027, le comité s'est engagé à continuer de soutenir les mesures de conformité telles que la certification et les codes de conduite, notamment en dialoguant avec des groupes clés de parties prenantes afin d'expliquer comment les outils peuvent être utilisés[123].

5.2 Défis spécifiques pour les PME et les petits opérateurs

Dans son rapport de 2020, la Commission demandait que les efforts visant à soutenir le respect du RGPD par les PME soient intensifiés. Ces dernières années, les autorités chargées de la protection des données et le comité ont continué à mettre au point des outils de mise en conformité pour les PME, soutenus en partie par des financements de la Commission[124]. En avril 2023, le comité a lancé un guide de la protection des données à l'intention des petites entreprises[125], qui fournit des informations pratiques aux PME dans un format accessible et aisément compréhensible.

Dans de nombreux États membres, les PME soulignent les avantages d'un soutien sur mesure de la part de leurs autorités locales chargées de la protection des données. Toutefois, les approches divergentes des autorités chargées de la protection des données en matière de sensibilisation et d'orientation font que les PME de certains États membres considèrent que le respect des règles est complexe et craignent des mesures répressives[126]. Les autorités chargées de la protection des données devraient redoubler d'efforts pour relever ces défis, notamment en dialoguant de manière proactive avec les PME afin de dissiper tout problème de conformité infondé. Les autorités chargées de la protection des données devraient s'attacher à fournir un soutien sur mesure et des outils pratiques, tels que des modèles (par exemple pour la réalisation d'analyses d'impact relatives à la protection des données), des lignes d'assistance téléphonique, des exemples illustratifs, des listes de contrôle et des orientations sur des opérations de traitement spécifiques (facturation ou lettres d'information, par exemple) et des mesures techniques et organisationnelles. Étant donné que la plupart des PME ne disposent pas d'une expertise interne en matière de

121 https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational

122 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

123 https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf

124 https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en

125 https://edpb.europa.eu/sme-data-protection-guide/home_fr

126 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

protection des données, toute orientation destinée aux PME devrait être facilement comprise par des personnes qui ne disposent pas d'une formation juridique[127].

Conformément à l'approche fondée sur les risques du RGPD, les PME qui mènent des activités de traitement à faible risque ne supportent pas une charge de mise en conformité substantielle. Bien que la dérogation relative à la tenue de registres des activités de traitement[128] s'applique dans des circonstances limitées[129], les PME effectuant un traitement à faible risque peuvent se conformer en conservant des registres simplifiés fondés sur des modèles fournis par les autorités chargées de la protection des données. En outre, ces registres devraient être considérés comme un outil utile pour permettre aux PME de faire le point sur leurs activités de traitement.

5.3 Délégués à la protection des données

Les délégués à la protection des données jouent un rôle important pour garantir le respect du RGPD dans les organisations dans lesquelles ils travaillent. En général, les délégués à la protection des données exerçant leurs activités dans l'UE disposent des connaissances et des compétences nécessaires pour accomplir leurs tâches au titre du RGPD, et leur indépendance est respectée[130]. Toutefois, plusieurs défis restent à relever, notamment: i) des difficultés à nommer des délégués à la protection des données possédant l'expertise requise; ii) l'absence de normes à l'échelle de l'UE en matière d'éducation et de formation; iii) l'absence d'intégration adéquate des délégués à la protection des données dans les processus organisationnels; iv) le manque de ressources; v) des tâches supplémentaires en dehors de la protection des données; et vi) une ancienneté insuffisante[131]. Le comité a noté qu'il était nécessaire que les autorités chargées de la protection des données intensifient leurs activités de sensibilisation, ainsi que leurs actions d'information et de contrôle de l'application des règles afin de veiller à ce que les délégués à la protection des données puissent remplir leur rôle au titre du RGPD[132].

6 LE RGPD, PIERRE ANGULAIRE DE LA POLITIQUE DE L'UE DANS LE DOMAINE NUMERIQUE

6.1 Une politique numérique fondée sur le RGPD

Dans son rapport de 2020, la Commission s'engageait à soutenir l'application cohérente du cadre de protection des données aux nouvelles technologies, afin de soutenir l'innovation et les évolutions technologiques. Depuis, l'UE a adopté une série d'initiatives, dont certaines complètent le RGPD ou précisent comment il devrait être appliqué dans des

---

127 Voir position et conclusions du Conseil, point 24; résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

128 Article 30, paragraphe 5, du RGPD.

129 Lorsque l'organisation emploie moins de 250 personnes, à moins que le traitement qu'elle effectue ne soit susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, le traitement n'est pas occasionnel, ou le traitement comprend des catégories particulières de données visées à l'article 9, paragraphe 1, du RGPD ou des données à caractère personnel relatives aux condamnations pénales et aux infractions visées à l'article 10 du RGPD.

130 Position et conclusions du Conseil, point 26; Comité européen de la protection des données (EDPB 2023), Coordinated Enforcement Action Designation and Position of Data Protection Officers (Action coordonnée en matière d'application de la législation, désignation et position des délégués à la protection des données): https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf

131 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD

132 Voir les recommandations figurant dans le document «Coordinated Enforcement Action» du comité européen de la protection des données.

domaines spécifiques, afin de poursuivre des objectifs particuliers, comme indiqué ci-dessous.

- Le règlement sur les services numériques[133], qui vise à fournir aux particuliers et aux entreprises un environnement en ligne sûr, interdit aux plateformes en ligne de présenter de la publicité qui repose sur du profilage en utilisant les «catégories particulières de données à caractère personnel» définies dans le RGPD.
- Afin de rendre les marchés numériques plus équitables et plus contestables, le règlement sur les marchés numériques[134] interdit aux opérateurs désignés comme «contrôleurs d'accès» de «combiner» et d'«utiliser de manière croisée» des données à caractère personnel entre leurs services de plateforme essentiels et d'autres services, à moins que l'utilisateur ait donné son consentement au sens du RGPD.
- Le règlement sur l'intelligence artificielle[135] précise les règles de l'UE en matière de protection des données dans des domaines spécifiques où l'intelligence artificielle (IA) est utilisée, par exemple dans les systèmes d'identification biométrique à distance, le traitement de catégories particulières de données pour détecter les biais et le traitement ultérieur des données à caractère personnel dans des bacs à sable réglementaires.
- La directive relative au travail via une plateforme[136] complète le RGPD dans le domaine de l'emploi en établissant des règles relatives aux systèmes de surveillance et de prise de décision automatisés utilisés par les plateformes de travail numériques, et en particulier les limitations concernant le traitement des données à caractère personnel, la transparence, la supervision humaine et le réexamen par l'homme, et la portabilité.
- Le règlement sur la publicité à caractère politique[137] interdit l'utilisation de catégories particulières de données à caractère personnel dans la publicité à caractère politique et exige une plus grande transparence en ce qui concerne les techniques de ciblage et d'amplification utilisées.
- Le règlement concernant un cadre européen relatif à une identité numérique permet la création d'un portefeuille européen d'identité numérique universel, fiable et sécurisé. Cela permettra aux particuliers de fournir la preuve d'attributs personnels tels que l'âge, le permis de conduire, le diplôme et les comptes bancaires, en contrôlant pleinement leurs données à caractère personnel et sans partage inutile de données.

La proposition de règlement «vie privée et communications électroniques»[138] visant à remplacer l'actuelle directive «vie privée et communications électroniques»[139] et à compléter le cadre législatif en matière de protection de la vie privée et des données est en négociation depuis plusieurs années. Une réflexion est nécessaire sur les prochaines étapes de cette initiative, y compris sur sa relation avec le RGPD.

---

133 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

134 Règlement (UE) 2022/1925 (règlement sur les marchés numériques) (JO L 265 du 12.10.2022, p. 1).

135 Règlement (UE) 2024/1689 (règlement sur l'intelligence artificielle) (JO L 2024/1689 du 12.7.2024).

136 Travailleurs des plateformes: le Conseil confirme l'accord sur de nouvelles règles visant à améliorer leurs conditions de travail - Consilium (europa.eu)

137 Règlement (UE) 2024/900 relatif à la transparence et au ciblage de la publicité à caractère politique (JO L 2024/900 du 20.3.2024).

138 Proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques [COM(2017) 10 final].

139 Directive 2002/58/CE (directive «vie privée et communications électroniques») (JO L 201 du 31.7.2002, p. 37).

Le règlement pour une Europe interopérable[140] vise à rendre les services publics numériques interopérables dans l'ensemble de l'UE. Il soutient la coopération entre les autorités chargées de la protection des données, notamment au moyen de «bacs à sable» réglementaires en matière d'interopérabilité.

Plusieurs initiatives de l'UE fournissent une base juridique pour le traitement de données à caractère personnel par des entités privées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Toute législation de ce type doit être soigneusement ciblée afin de réduire au minimum les ingérences dans le droit à la protection des données à caractère personnel et doit être proportionnée à l'objectif poursuivi[141]. La Charte, le RGPD et la jurisprudence de la Cour de justice fournissent un cadre au regard duquel il convient de mesurer ces initiatives. La proposition de nouveau train de mesures anti-blanchiment de capitaux[142] contient des garanties substantielles pour la protection des données à caractère personnel, sans compromettre l'objectif consistant à atténuer les risques de blanchiment de capitaux et de financement du terrorisme et à détecter efficacement les tentatives criminelles d'utilisation abusive du système financier de l'UE.

Dans ce contexte, le Conseil a souligné que toute nouvelle législation de l'UE contenant des dispositions relatives au traitement des données à caractère personnel devrait être conforme au RGPD et à la jurisprudence de la Cour de justice.

6.2 Un cadre juridique pour améliorer le partage des données

La stratégie européenne pour les données vise à créer un marché unique des données, dans lequel les données circulent librement au sein de l'UE et entre les secteurs, dans l'intérêt des entreprises, des chercheurs et des administrations publiques. L'un des principaux objectifs de cette stratégie est la création d'espaces européens communs des données qui facilitent la mise en commun, l'accès et le partage des données. En ce qui concerne les données à caractère personnel, le RGPD fournit le cadre de toutes les initiatives visant à renforcer la libre circulation des données dans l'UE, qui constitue elle-même un objectif du RGPD. Pour ce qui est des données à caractère personnel, les protections prévues par le RGPD ne sont pas affectées.

Le règlement sur la gouvernance des données[143] et le règlement sur les données[144] sont des piliers de la stratégie pour les données. Le règlement sur la gouvernance des données établit des règles concrètes dans le contexte de la réutilisation des données du secteur public contenant des données à caractère personnel et établit un cadre législatif pour les services d'intermédiation de données, y compris les services de gestion des informations à caractère personnel (PIMS) ou les nuages de données à caractère personnel proposés afin de donner aux personnes concernées les moyens d'exercer leurs droits au titre du RGPD. Il définit également les conditions d'utilisation des données à des fins altruistes. Le règlement sur les données renforce le contrôle des personnes concernées sur les données qu'elles génèrent grâce à l'utilisation d'objets intelligents qu'elles possèdent, louent ou détiennent en crédit-bail, en imposant des exigences techniques en matière d'accès aux données et de portabilité.

---

140 Règlement (UE) 2024/903 (règlement pour une Europe interopérable) (JO L 2024/903 du 22.3.2024).
141 Voir la position et les conclusions du Conseil, point 31 f).
142 https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_fr
143 Règlement (UE) 2022/868 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).
144 Règlement (UE) 2023/2854 (règlement sur les données) (JO L 2023/2854 du 22.12.2023).

Le règlement relatif à l'espace européen des données de santé (EHDS)[145] prend en compte les besoins spécifiques recensés dans le secteur des données de santé, tout en s'appuyant également sur le RGPD. Il permet aux particuliers d'accéder facilement à leurs données de santé sous forme électronique et de les partager avec des professionnels de la santé, y compris dans d'autres États membres, améliorant ainsi la prestation de soins de santé et renforçant le contrôle des patients sur leurs données. Il met également en place un cadre juridique commun pour la réutilisation des données de santé à des fins telles que la recherche, l'innovation et la santé publique, sur la base d'une autorisation délivrée par un organisme responsable de l'accès aux données de santé. Afin de garantir la protection des données à caractère personnel, le règlement relatif à l'EHDS fournira un cadre fiable pour un accès sécurisé aux données de santé et leur traitement. La Commission continue de soutenir les travaux sur le développement d'espaces européens communs des données dans 14 secteurs en mettant en œuvre le nouveau cadre législatif et en finançant des initiatives sectorielles.

6.3 Gouvernance des nouvelles règles numériques

L'élaboration de réglementations numériques rend nécessaire une coopération étroite dans tous les domaines réglementaires[146]. Une telle coopération est d'autant plus nécessaire que les questions de protection des données se recoupent de plus en plus avec des questions telles que le droit de la concurrence, le droit des consommateurs, les règles relatives aux marchés numériques, la réglementation des communications électroniques et la cybersécurité. C'est par exemple le cas lors de l'appréciation de la compatibilité des modèles «consentir ou payer» avec le droit de l'Union.

Dans certains cas, les autorités chargées de la protection des données sont chargées de faire appliquer les dispositions spécifiques de la nouvelle législation numérique de l'UE[147]. De nouvelles réglementations numériques créent également des structures sur mesure qui réunissent les autorités de réglementation compétentes afin d'assurer une application cohérente, telles que le groupe de haut niveau pour le règlement sur les marchés numériques, le comité européen de l'innovation dans le domaine des données (créé en vertu du règlement sur la gouvernance des données) et le comité européen des services numériques (créé en vertu du règlement sur les services numériques). La directive SRI 2[148] fixe des règles plus détaillées concernant la coopération entre les autorités de réglementation et les autorités chargées de la protection des données en ce qui concerne le traitement des incidents de sécurité qui constituent des violations de données à caractère personnel.

En dehors de ces structures formelles, les autorités chargées de la protection des données prennent des mesures pour veiller à ce que leurs actions soient complémentaires et cohérentes avec d'autres domaines réglementaires. En juillet 2020, les autorités chargées de la protection des consommateurs et des données ont mis en place un «groupe de volontaires» afin de déterminer les meilleures pratiques et de partager les expériences en matière d'application de la législation. Les autorités chargées de la protection des données continuent de participer à des ateliers conjoints avec le réseau de coopération en matière de protection des consommateurs. En 2023, le comité a mis en place un groupe de travail

145 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_FR.html

146 Voir position et conclusions du Conseil, points 40 et 41; Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

147 Voir, par exemple, l'article 37, paragraphe 3, du règlement sur les données.

148 Directive (UE) 2022/2555 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

sur l'interaction entre la protection des données, la concurrence et la protection des consommateurs.

Si ces évolutions sont positives, il est nécessaire de disposer de moyens de coopération plus structurés et plus efficaces, en particulier pour faire face à des situations qui touchent un grand nombre de personnes dans l'UE et demandent l'intervention de plusieurs autorités de réglementation[149]. Ces structures devraient veiller à ce que les autorités restent à tout moment responsables de toutes les questions relatives au respect des règles dans leurs domaines de compétence. Les États membres devraient également veiller à une coopération appropriée au niveau national[150].

7 TRANSFERTS INTERNATIONAUX ET COOPERATION MONDIALE

7.1 La boîte à outils du RGPD pour les transferts

Les flux de données font désormais partie intégrante de la transformation numérique de la société et de la mondialisation de l'économie. Plus que jamais auparavant, le respect de la vie privée est une condition préalable à la stabilité, à la sécurité et à la compétitivité des flux commerciaux, ainsi qu'un catalyseur de nombreuses formes de coopération internationale. La boîte à outils du RGPD pour les transferts, visée en son chapitre V, offre divers instruments pour traiter différents scénarios de transfert, tout en veillant à ce que les données continuent de bénéficier d'un niveau élevé de protection lorsqu'elles quittent l'UE.

Depuis le rapport de 2020, les exigences en matière de transferts de données énoncées dans la législation de l'UE en matière de protection des données ont été clarifiées et la boîte à outils pour les transferts a continué d'évoluer. Une clarification importante concerne la notion de «transfert international», qui a été définie par le comité[151] comme englobant toute divulgation de données à caractère personnel par un responsable du traitement ou un sous-traitant et dont le traitement est soumis au RGPD à un autre responsable du traitement ou sous-traitant dans un pays tiers, que le traitement effectué par ce dernier soit ou non soumis au RGPD[152]. Ces orientations du comité étaient particulièrement importantes pour apporter une sécurité juridique aux responsables du traitement et aux sous-traitants européens en ce qui concerne les scénarios dans lesquels un outil de transfert au titre du chapitre V du RGPD est nécessaire.

D'autres précisions ont également été apportées par la Cour de justice dans son arrêt dans l'affaire *Schrems II*[153] sur la protection qui doit être assurée par différents instruments de transfert afin de garantir que le niveau de protection garanti par le RGPD n'est pas compromis[154]. En particulier, ces instruments doivent assurer que les personnes dont les données à caractère personnel sont transférées en dehors de l'UE bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE[155]. Il incombe à

149 Voir la position et les conclusions du Conseil, points 18 et 40 à 41, ainsi que le résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

150 L'Allemagne a mis en place un «pôle numérique», qui rassemble des autorités de réglementation de différents domaines, dans le but d'étendre leur coopération à tous les aspects de la numérisation et de partager les connaissances et les bonnes pratiques: https:// www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn

151 Lignes directrices 05/2021 du comité européen de la protection des données.

152 Section 2 des lignes directrices 05/2021 du comité européen de la protection des données.

153 Arrêt dans l'affaire C-311/18, EU:C:2020:559 (*arrêt Schrems II*).

154 *Arrêt Schrems II*, point 93.

155 *Arrêt Schrems II*, points 96 et 105.

l'exportateur de données de l'UE de déterminer si tel est le cas, en tenant compte des circonstances particulières de ses transferts[156].

Pour évaluer le niveau de protection, les exportateurs de données doivent tenir compte à la fois des garanties en matière de protection des données énoncées dans l'instrument de transfert conclu avec un importateur de données de pays tiers (par exemple, un contrat), ainsi que des éléments pertinents du système juridique du pays dans lequel l'importateur de données est établi, en particulier en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données[157]. Ce dernier doit être évalué à la lumière des critères d'évaluation de l'adéquation énoncés à l'article 45 du RGPD. La Cour a également développé ces critères, notamment en ce qui concerne les règles relatives à l'accès des autorités publiques aux données à caractère personnel à des fins répressives et de sécurité nationale.

Cette interprétation a également été prise en compte dans les orientations du comité, qui ont mis à jour ses «critères de référence pour l'adéquation»[158] (qui fournissaient des orientations sur les éléments dont la Commission doit tenir compte lorsqu'elle procède à une évaluation de l'adéquation). Le comité a également adopté de nouvelles orientations fournissant des précisions supplémentaires sur: i) les éléments à prendre en compte par les exportateurs de données individuels lors de l'évaluation du niveau de protection; ii) une vue d'ensemble des sources potentielles qui peuvent être utilisées; et iii) des exemples de mesures supplémentaires possibles (par exemple, des garanties contractuelles et techniques)[159]. Ces orientations soulignent spécifiquement que chaque évaluation effectuée par les exportateurs de données est unique et qu'il convient donc de tenir compte des caractéristiques spécifiques de chaque transfert, qui peuvent varier en fonction de la finalité du transfert de données, des types d'entités concernées, du secteur dans lequel le transfert a lieu, des catégories de données à caractère personnel transférées, etc. [160].

Compte tenu de ces différentes clarifications sur les exigences applicables aux transferts internationaux de données, des mesures importantes ont été prises ces dernières années pour poursuivre le développement et la mise en œuvre de la boîte à outils du RGPD pour les transferts.

7.1.1 Décisions d'adéquation

Comme le montrent également les retours d'information reçus des parties prenantes, les décisions d'adéquation continuent de jouer un rôle clé dans la boîte à outils du RGPD pour les transferts[161], en fournissant une solution simple et complète pour les transferts de données sans que l'exportateur de données ait besoin de fournir des garanties supplémentaires ou d'obtenir une autorisation. En permettant le libre flux des données à caractère personnel, ces décisions ont ouvert des canaux commerciaux aux opérateurs de l'UE, notamment en complétant et en amplifiant les avantages des accords commerciaux, et facilité la coopération avec des partenaires étrangers dans un grand nombre de domaines, de la coopération en matière réglementaire à la recherche.

---

156 *Arrêt Schrems II*, point 131.

157 *Arrêt Schrems II*, point 105.

158 Recommandations 02/2020 du comité européen de la protection des données et critères d'adéquation, WP 254 rév. 01.

159 Recommandations 01/2020 du comité européen de la protection des données, complétées par les recommandations 02/2020.

160 Voir par exemple les points 8 à 13 et 32 et 33 des recommandations 01/2020 du comité européen de la protection des données.

161 Voir la contribution du comité, pages 7 et 8; position et conclusions du Conseil, point 36; Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

Depuis le rapport de 2020, le nombre de pays qui ont adopté des lois modernes en matière de protection des données - prévoyant, entre autres, des principes essentiels en matière de protection des données, des droits individuels et une application effective par des autorités de réglementation indépendantes - n'a cessé d'augmenter. Cette tendance[162] a également permis à la Commission d'intensifier son travail d'adéquation. Cela concerne notamment l'adoption d'une décision d'adéquation pour le Royaume-Uni[163], qui est essentielle pour garantir le bon fonctionnement des différents accords conclus avec le Royaume-Uni à la suite du Brexit. Afin de garantir qu'elle résiste au temps, la décision d'adéquation comprend une «clause de caducité» qui expire en 2025, après quoi elle peut être renouvelée si le niveau de protection reste adéquat. La Commission a également adopté une décision d'adéquation pour la République de Corée[164], qui complète l'accord de libre-échange UE-Corée sur les flux de données à caractère personnel et facilite la coopération en matière réglementaire. Un premier réexamen de la décision d'adéquation est prévu vers la fin de 2024.

En outre, à la suite de l'invalidation de la décision d'adéquation relative au bouclier de protection des données UE-États-Unis, la Commission a entamé des discussions avec le gouvernement des États-Unis en vue d'élaborer un accord qui lui succéderait conformément aux exigences précisées par la Cour[165]. Le président des États-Unis a adopté un nouveau décret présidentiel intitulé «Enhancing Safeguards for United States Signals Intelligence Activities» (renforcement des garanties applicables aux activités de renseignement d'origine électromagnétique menées par les États-Unis), qui a introduit de nouvelles garanties contraignantes et exécutoires afin de garantir que l'accès aux données à des fins de sécurité nationale n'est possible que dans la mesure nécessaire et proportionnée, et que les Européens disposent de voies de recours efficaces. Sur cette base, la Commission a adopté sa décision d'adéquation relative au cadre de protection des données (CPD) UE-États-Unis[166], qui permet aux données à caractère personnel de circuler librement de l'UE vers les entreprises américaines adhérant au CPD. Étant donné que les garanties mises en place par le gouvernement américain dans le domaine de la sécurité nationale s'appliquent à tous les transferts de données vers des entreprises aux États-Unis, quel que soit le mécanisme de transfert du RGPD utilisé, l'utilisation d'autres outils, tels que des clauses contractuelles types et des règles d'entreprise contraignantes, a été considérablement facilitée. Un premier examen du fonctionnement du CPD aura lieu à l'été 2024 afin de vérifier que tous les éléments pertinents ont été pleinement mis en œuvre dans le cadre juridique américain et fonctionnent efficacement dans la pratique.

Des négociations sur l'adéquation sont en cours avec le Brésil et le Kenya et, pour la première fois, avec plusieurs organisations internationales (ainsi, les pourparlers sur l'adéquation sont à un stade avancé avec l'Organisation européenne des brevets)[167]. Conformément également aux appels lancés par différentes parties prenantes[168], la Commission a participé activement à des discussions exploratoires avec des pays de différentes régions du monde.

---

162 Communication de la Commission intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», 10.1.2017 [COM(2017) 7 final].

163 Décision d'exécution (UE) 2021/1772 de la Commission (JO L 360 du 11.10.2021, p. 1).

164 Décision d'exécution (UE) 2022/254 de la Commission (JO L 44 du 24.2.2022, p. 1).

165 https://commission.europa.eu/news/joint-press-statement-commissioner-didier-reynders-and-us-secretary-commerce-gina-raimondo-first-2024-07-19_en?prefLang=fr

166 Décision d'exécution (UE) 2023/1795 de la Commission (JO L 231 du 20.9.2023, p. 118).

167 L'Organisation européenne des brevets est une organisation intergouvernementale créée sur la base de la Convention sur le brevet européen. Sa mission principale consiste à délivrer des brevets européens. Dans ce contexte, elle coopère étroitement avec les entreprises et les pouvoirs publics des États membres de l'UE, ainsi qu'avec différents organes et institutions de l'UE.

168 Contribution du comité, pages 7 à 8.

La Commission suit également en permanence l'évolution de la situation dans les pays qui bénéficient déjà de constats d'adéquation et réexamine périodiquement les décisions existantes, conformément aux obligations qui lui incombent en vertu du RGPD[169]. En avril 2023, la Commission a adopté son rapport sur le premier examen périodique de la décision d'adéquation pour le Japon[170], dans lequel elle concluait que le Japon continuait d'assurer un niveau de protection adéquat[171]. Cet examen a montré que les cadres de l'UE et du Japon en matière de protection des données étaient encore convergents depuis l'adoption des décisions d'adéquation mutuelle.

En outre, conformément à l'article 97 du RGPD, le premier examen des onze décisions d'adéquation[172] adoptées au titre de l'ancien cadre de l'Union en matière de protection des données (la directive sur la protection des données) a été entamé dans le cadre de l'évaluation de 2020 de l'application et du fonctionnement du RGPD. La conclusion de cet aspect de l'examen a été reportée, notamment pour tenir compte de l'arrêt rendu par la Cour de justice dans l'affaire *Schrems II* et de son interprétation ultérieure par le comité. Les éclaircissements susmentionnés de la Cour sur les éléments clés de la norme d'adéquation ont donné lieu à des échanges approfondis avec les pays et territoires concernés sur les aspects pertinents de leur cadre juridique, ainsi que sur les mécanismes de surveillance et d'application.

Le 15 janvier 2024, la Commission a publié son rapport sur ces onze décisions, ainsi que des rapports détaillés par pays décrivant l'évolution de la situation dans chacun des pays et territoires depuis l'adoption des décisions d'adéquation, ainsi que les règles applicables à l'accès des autorités publiques aux données, en particulier à des fins répressives et de sécurité nationale[173]. La Commission conclut que les onze pays et territoires continuent d'assurer un niveau adéquat de protection des données à caractère personnel transférées depuis l'UE. Cela montre que tous les pays et territoires concernés ont modernisé et renforcé de différentes manières leur cadre juridique en matière de protection de la vie privée. En outre, afin de remédier aux différences importantes de niveau de protection, des garanties supplémentaires concernant les données à caractère personnel transférées depuis l'Europe ont été négociées et convenues avec certains d'entre eux lorsque cela était nécessaire pour assurer la continuité de la décision d'adéquation.

Ces examens montrent également que les décisions d'adéquation, au lieu d'être un «point final», ont jeté les bases d'une coopération plus étroite et d'une convergence réglementaire accrue entre l'UE et ces partenaires partageant les mêmes valeurs. Par exemple, le rapport sur le premier réexamen de la décision d'adéquation pour le Japon reconnaît que le renforcement du cadre japonais en matière de protection des données peut ouvrir la voie à une extension de la décision d'adéquation au-delà des échanges commerciaux, afin de couvrir les transferts actuellement exclus de son champ d'application, par exemple dans le domaine de la coopération réglementaire et de la recherche. Des discussions sont en cours en vue d'étudier cette possibilité d'extension. De manière générale, les décisions d'adéquation sont devenues une composante stratégique de la relation globale de l'UE avec

---

169 Article 45, paragraphes 4 et 5, du RGPD. Voir également l'arrêt *Schrems I*, point 76.

170 Décision d'exécution (UE) 2019/419 de la Commission (JO L 76 du 19.3.2019, p. 1). Voir également https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_421. Cette décision constituait la première décision d'adéquation adoptée en vertu du RGPD et le premier accord d'adéquation réciproque.

171 Rapport de la Commission sur le premier examen du fonctionnement de la décision d'adéquation pour le Japon, 3.4.2023, COM(2023) 275 final [et SWD(2023) 75 final].

172 L'Andorre, l'Argentine, le Canada (pour les opérateurs commerciaux), les Îles Féroé, Guernesey, l'Île de Man, Israël, Jersey, la Nouvelle-Zélande, la Suisse et l'Uruguay.

173 Rapport de la Commission sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE du 15.1.2024, COM(2024) 7 final [et SWD(2024) 3 final].

ces partenaires étrangers et sont reconnues comme un catalyseur majeur de l'approfondissement de la coopération dans un large éventail de domaines.

Outre qu'il constitue une base solide pour renforcer la coopération bilatérale, le réseau croissant de pays et de territoires pour lesquels l'UE a adopté une décision d'adéquation offre de nouvelles possibilités de maximiser les avantages d'un flux sûr et libre de données et de coopérer plus étroitement entre partenaires partageant les mêmes valeurs en ce qui concerne l'application des règles en matière de protection des données. C'est ainsi qu'en mars 2024, la Commission a accueilli la toute première réunion de haut niveau sur la sécurité des flux de données, qui a réuni les ministres compétents et les chefs des autorités chargées de la protection des données de 15 pays et territoires pour lesquels l'UE a adopté une décision d'adéquation, ainsi que la présidente du comité européen de la protection des données[174]. Plusieurs points d'action concrets ont été déterminés lors de la réunion, lesquels font l'objet de travaux de suivi au sein de ce groupe.

De manière plus générale, grâce à leur «effet de réseau», les décisions d'adéquation adoptées par la Commission européenne revêtent une importance croissante, même en dehors de l'UE, car elles permettent non seulement la libre circulation des données avec les 30 économies de l'EEE, mais également avec de nombreux autres pays ou territoires dans le monde, qui reconnaissent les pays pour lesquels il existe une décision d'adéquation de l'UE comme des «destinations sûres» selon leurs propres règles de protection des données[175].

7.1.2 Instruments prévoyant des garanties appropriées

Depuis le rapport de 2020, des outils supplémentaires prévoyant des garanties appropriées ont été mis au point et des orientations pratiques ont été publiées pour faciliter leur utilisation.

Comme annoncé dans le rapport de 2020, la Commission a adopté des clauses contractuelles types (CCT) modernisées[176], qu'elle a élaborées en s'appuyant largement sur les retours d'information de diverses parties prenantes[177]. Les nouvelles CCT ont remplacé les trois séries de CCT qui avaient été adoptées en vertu de la directive sur la protection des données. Les principales innovations sont les suivantes: i) des garanties actualisées conformément au RGPD; ii) une approche modulaire offrant un point d'entrée unique couvrant un large éventail de scénarios de transfert; iii) une flexibilité accrue en cas d'utilisation des CCT par plusieurs parties; et iv) une boîte à outils pratique pour se conformer à l'arrêt *Schrems II*.

Les CCT modernisées ont été accueillies favorablement par les parties prenantes et les retours d'information reçus confirment que les CCT restent de loin l'outil le plus utilisé pour les transferts par les exportateurs de données de l'UE[178]. Afin d'aider les exportateurs de données dans leurs efforts de mise en conformité, la Commission a créé une foire aux questions (FAQ) fournissant des orientations supplémentaires sur l'utilisation des clauses[179], qui seront mises à jour si de nouvelles questions se posent, notamment à la lumière des retours d'information reçus dans le cadre de la présente évaluation.

---

174 https:// ec.europa.eu/commission/presscorner/detail/en/mex_24_1307#11

175 Tels que l'Argentine, la Colombie, Israël, le Maroc, la Suisse et l'Uruguay.

176 Décision d'exécution (UE) 2021/914 de la Commission (JO L 199 du 7.6.2021, p. 31).

177 Il s'agissait, par exemple, de l'avis conjoint 2/2021 du comité européen de la protection des données et du Contrôleur européen de la protection des données dans le cadre de la procédure d'adoption des CCT.

178 Position et conclusions du Conseil, point 37, contribution du comité, page 9, résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

179 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en?prefLang=fr

De nombreux exportateurs de données font état de difficultés à réaliser les «évaluations de l'incidence des transferts» requises par l'arrêt *Schrems II*, en se référant notamment à leur complexité, ainsi qu'aux coûts et au temps nécessaires à leur réalisation[180]. Tout en se félicitant des orientations du comité et des CCT, ils demandent des orientations supplémentaires (par exemple, sur les responsabilités des parties concernées et le niveau de détail requis dans les évaluations des incidences des transferts) et des outils supplémentaires pour faciliter la réalisation de ces évaluations (modèles, évaluations générales par pays, catalogues des risques, par exemple). Bien que les parties prenantes aient principalement fourni un tel retour d'information sur les CCT, les mêmes évaluations sont également requises pour d'autres instruments de transfert (comme les règles d'entreprise contraignantes). Il importe donc que le comité - s'appuyant sur l'expérience acquise ces dernières années dans l'application des exigences de *Schrems II*, y compris dans le cadre des activités de contrôle de l'application des autorités nationales de protection des données - envisage d'étudier les moyens/outils permettant d'aider davantage les exportateurs de données dans leurs efforts de mise en conformité dans ce contexte.

Afin de compléter les CCT existantes, la Commission élabore actuellement des ensembles de clauses supplémentaires afin de fournir aux exportateurs de données de l'UE un ensemble complet et cohérent. Il s'agira notamment des CCT relevant du règlement (UE) 2018/1725 pour les transferts de données par les institutions et organes de l'UE à des opérateurs commerciaux dans des pays tiers[181] et des CCT pour les transferts de données vers des importateurs de données de pays tiers dont les opérations de traitement sont directement soumises au RGPD. Ces dernières répondent à la demande des parties prenantes de couvrir spécifiquement les scénarios dans lesquels l'importateur de données relève du champ d'application territorial du RGPD (par exemple parce que le traitement en question cible le marché de l'Union conformément à l'article 3, paragraphe 2, du RGPD)[182]. Comme l'a précisé le comité, un outil de transfert relevant du chapitre V du RGPD est également requis dans ce cas, en raison des risques accrus pour les données à caractère personnel traitées en dehors de l'UE, par exemple en raison d'un éventuel conflit entre les législations nationales ou d'un accès disproportionné des pouvoirs publics dans le pays tiers[183]. Les nouvelles CCT élaborées par la Commission aborderont spécifiquement ce scénario et tiendront pleinement compte des exigences qui s'appliquent déjà directement à ces responsables du traitement et sous-traitants en vertu du RGPD[184].

Comme le reconnaissent également différents types de parties prenantes[185], les clauses types jouent un rôle toujours plus central dans la facilitation des flux de données dans le monde entier. Plusieurs juridictions ont fait leurs les CCT de l'UE en tant que mécanisme de transfert en vertu de leur propre législation en matière de protection des données, avec des ajustements formels limités de leur ordre juridique interne[186]. Un certain nombre d'autres pays ont adopté leurs propres clauses types, qui partagent d'importantes

---

180 Voir, par exemple, le résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

181 Conformément aux dispositions de l'article 48, paragraphe 2, point b), du règlement (CE) nº 2018/1725.

182 Position et conclusions du Conseil, point 37, contribution du comité, page 9, résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

183 Lignes directrices 05/2021 du comité européen de la protection des données, p. 3.

184 Comme indiqué également dans les lignes directrices 05/2021 du comité européen de la protection des données, section 4.

185 Contribution du comité, page 9, résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

186 Par exemple, le Royaume-Uni (https:// ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) et la Suisse (https:// www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html) .

caractéristiques communes avec les CCT de l'UE[187]. Un exemple particulièrement pertinent est la création de clauses types par d'autres organisations ou réseaux internationaux/régionaux, tels que le comité consultatif de la Convention 108 du Conseil de l'Europe, le réseau ibéro-américain de protection des données et l'Association des nations de l'Asie du Sud-Est (ASEAN)[188]. Cela ouvre de nouvelles perspectives pour faciliter les flux de données entre les différentes régions du monde sur la base de clauses types. Un exemple concret est le guide UE-ASEAN sur les CCT de l'UE et les clauses types de l'ASEAN, qui, ayant dûment tenu compte des contributions des entreprises, aide celles-ci dans leurs efforts de mise en conformité au titre des deux ensembles de clauses[189].

Outre les CCT, les règles d'entreprise contraignantes (REC) continuent d'être largement utilisées pour les flux de données entre les membres de groupes d'entreprises ou entre entreprises exerçant une activité économique conjointe. Depuis l'entrée en vigueur du RGPD, le comité a adopté 80 avis positifs sur les décisions nationales approuvant les REC[190]. Le comité a également publié des orientations sur les éléments à inclure dans les REC à l'intention des responsables du traitement (et sur les informations à fournir dans le cadre d'une demande de REC), qui ont été mises à jour pour tenir compte des exigences du RGPD et de l'arrêt *Schrems II*[191]. Des orientations actualisées sur les REC à l'intention des sous-traitants sont également en cours d'élaboration[192]. Étant donné que les REC visent à mettre en place des politiques/programmes contraignants en matière de protection des données dans les entreprises, de nombreuses parties prenantes les considèrent comme un outil de conformité particulièrement utile et un instrument de transfert fiable[193]. Dans le même temps, les parties prenantes continuent de signaler que la longueur et la complexité du processus d'approbation par les autorités nationales chargées de la protection des données empêchent une adoption plus large des REC. Il importe donc que les autorités continuent d'œuvrer à la rationalisation et au raccourcissement du processus d'approbation.

Depuis le rapport de 2020, des mesures ont également été prises pour faciliter l'utilisation de la certification et des codes de conduite en tant qu'outils de transfert, par exemple par l'adoption de lignes directrices spécifiques sur ces deux outils par le comité[194]. Dans le même temps, les parties prenantes font état des mêmes difficultés concernant le calendrier et la complexité du processus d'approbation que celles mentionnées ci-dessus en ce qui concerne la certification et les codes de conduite en tant qu'outils de responsabilisation.

Enfin, le RGPD prévoit également des instruments spécifiques - accords internationaux et arrangements administratifs approuvés par les autorités chargées de la protection des données - que les autorités publiques peuvent utiliser pour transférer des données à caractère personnel à leurs homologues dans des pays tiers ou à des organisations internationales. Le comité a adopté des lignes directrices sur les garanties qui devraient

---

187 Par exemple, la Nouvelle-Zélande (https:// privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) et l'Argentine (https:// servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).

188 Voir https:// rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https:// www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf et https:// asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

189 https:// commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf

190 Contribution du comité, p. 9.

191 Recommandations 1/2022 du comité européen de la protection des données.

192 Contribution du comité, p. 9.

193 Résumé du retour d'information du groupe d'experts multipartite sur le RGPD.

194 Lignes directrices 07/2022 et lignes directrices 04/2021 du comité européen de la protection des données.

être incluses dans ces instruments[195], car elles sont susceptibles de contribuer à la négociation de tels accords et arrangements.

7.1.3 Assurer la complémentarité avec d'autres politiques

Étant donné que les flux de données sont devenus essentiels pour bon nombre d'activités, il est essentiel de veiller à ce que les politiques de protection des données et les autres politiques se complètent mutuellement. L'inclusion de garanties en matière de protection des données dans les instruments internationaux est non seulement souvent une condition préalable aux flux de données, mais également un catalyseur important d'une coopération stable et fiable.

Par exemple, les accords internationaux prévoyant les garanties nécessaires en matière de protection des données, notamment en assurant la continuité de la protection de la part d'une autorité requérante, sont essentiels pour garantir la courtoisie et faciliter l'accès transfrontière des services répressifs aux preuves électroniques détenues par les entreprises et, partant, une lutte plus efficace contre la criminalité. Cette approche se reflète dans le deuxième protocole additionnel à la convention sur la cybercriminalité[196], qui renforce les règles existantes pour obtenir un accès transfrontière aux preuves électroniques dans le cadre des enquêtes pénales, tout en garantissant des garanties appropriées en matière de protection des données. Ce protocole a entre-temps été signé par plusieurs États membres de l'UE. De même, des négociations bilatérales progressent entre l'UE et les États-Unis en vue d'un accord sur l'accès transfrontière aux preuves électroniques aux fins de la coopération en matière pénale[197].

L'échange de données des dossiers passagers (PNR) est un autre domaine de la politique de sécurité de l'UE qui a bénéficié de la mise en place de garanties solides en matière de protection des données. En 2023, les négociations entre l'UE et le Canada ont abouti à un nouvel accord PNR, conformément aux exigences énoncées par la Cour de justice dans son avis 1/15[198]. Des garanties similaires ont été introduites dans le chapitre PNR de l'accord de commerce et de coopération entre l'UE et le Royaume-Uni. L'inclusion de protections renforcées en matière de respect de la vie privée dans ces accords, qui peuvent servir de modèle pour de futurs accords avec d'autres partenaires, apporte une sécurité juridique aux transporteurs aériens tout en garantissant la stabilité des échanges importants d'informations aux fins de la lutte contre le terrorisme et d'autres formes graves de criminalité transnationale.

La Commission est également favorable à des dispositions fortes visant à protéger la vie privée et à stimuler le commerce numérique au sein de l'Organisation mondiale du commerce dans le cadre des négociations en cours sur l'initiative de déclaration conjointe sur le commerce électronique. Des dispositions similaires sur la lutte contre les obstacles injustifiés au commerce numérique, tout en protégeant l'espace nécessaire aux parties dans le domaine de la protection des données, ont été systématiquement incluses dans les accords de libre-échange conclus par l'UE à la suite de l'entrée en application du RGPD, notamment dans l'accord de commerce et de coopération UE-Royaume-Uni et dans les accords avec le Chili, le Japon et la Nouvelle-Zélande. Les dispositions relatives à la

---

195 Lignes directrices 2/2020 du comité européen de la protection des données.

196 Deuxième protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE nº 224).

197 https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en?prefLang=fr

198 Proposition de décision du Conseil relative à la signature, au nom de l'Union européenne, d'un accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (données PNR) [COM(2024) 94 final].

protection de la vie privée et aux flux de données sont également examinées dans le cadre des négociations en cours sur le commerce numérique avec Singapour et la Corée du Sud.

7.2 Coopération internationale en matière de protection des données

7.2.1 La dimension bilatérale

La Commission a continué d'engager un dialogue avec les pays et les organisations internationales sur l'élaboration, la réforme et la mise en œuvre des règles en matière de protection de la vie privée, notamment en soumettant à des consultations publiques des projets de loi ou des mesures réglementaires dans le domaine de la protection de la vie privée[199], en témoignant devant les organes parlementaires compétents[200] et en participant à des réunions spécifiques avec des représentants de pouvoirs publics, des délégations parlementaires et des autorités de réglementation de nombreuses régions du monde[201]. Un certain nombre de ces activités ont été menées dans le cadre du projet «Enhanced Data Protection and Data Flows» (Protection renforcée des données et flux de données) financé par l'UE, qui soutient les pays ayant l'intention de mettre en place des cadres modernes de protection des données ou de renforcer les capacités de leurs autorités de réglementation, par la formation, le partage des connaissances, le renforcement des capacités et l'échange de bonnes pratiques. La Commission a également contribué à d'autres initiatives, telles que l'alliance numérique UE-CELAC.

La protection des données continuera également de jouer un rôle clé dans les travaux de la Commission liés à l'élargissement. La législation de l'UE en matière de protection des données est un élément important des efforts globaux déployés par les pays visés par l'élargissement pour aligner leurs cadres juridiques sur ceux de l'UE (d'autant plus que le traitement et l'échange de données à caractère personnel sont au cœur d'un très grand nombre de politiques). En outre, l'indépendance et le bon fonctionnement d'une autorité chargée de la protection des données constituent un élément essentiel de l'équilibre global des pouvoirs et de l'état de droit, et ils gagneront sans cesse en importance à mesure que l'UE intégrera progressivement les pays visés par l'élargissement dans le marché unique (comme le prévoient des initiatives telles que le plan de croissance pour les Balkans occidentaux).

Un aspect de plus en plus important du dialogue de l'UE avec les pays tiers réside dans les échanges entre les autorités de réglementation. Comme annoncé dans le rapport de 2020, la Commission a créé une «Académie pour la protection des données», afin de favoriser les échanges entre les autorités chargées de la protection des données de l'UE et des pays tiers et, de cette manière, de contribuer au renforcement des capacités et d'améliorer la coopération «sur le terrain». L'Académie propose des formations sur mesure à la demande des autorités de pays tiers et rassemble l'expertise de représentants des services répressifs, du monde universitaire, du secteur privé et des institutions européennes. La valeur ajoutée des formations réside dans l'adaptation de ses différentes composantes aux intérêts et aux besoins de l'autorité requérante. En outre, ces formations permettent aux autorités chargées de la protection des données de l'UE et des pays tiers d'établir des contacts, de partager des connaissances, d'échanger des expériences et des bonnes pratiques et de recenser les domaines de coopération potentiels. Jusqu'à présent, l'Académie a dispensé des formations aux autorités chargées de la protection des données d'Indonésie, du Brésil, du

[199] Il s'agissait de consultations organisées, par exemple, par l'Australie, la Chine, le Rwanda, l'Argentine, le Brésil, l'Éthiopie, l'Indonésie, le Pérou, la Malaisie et la Thaïlande.

[200] Par exemple, devant les organes parlementaires du Chili, de l'Équateur et du Paraguay.

[201] Il s'agissait également d'organiser des séminaires et des visites d'étude, par exemple avec le Kenya, l'Indonésie et Singapour.

Kenya, du Nigeria et du Rwanda, et elle prépare actuellement des formations pour plusieurs autres pays.

Au-delà de l'importance de maintenir un dialogue entre les autorités de réglementation, la nécessité devient pressante, comme le reconnaissent également les retours d'information reçus du Conseil et du comité[202], de mettre au point des instruments juridiques appropriés pour des formes plus étroites de coopération et d'assistance mutuelle, y compris en permettant l'échange nécessaire d'informations dans le cadre des enquêtes. En effet, étant donné que les violations de la vie privée produisent de plus en plus d'effets transfrontières, elles ne peuvent souvent faire l'objet d'enquêtes et de mesures efficaces que dans le cadre d'une coopération entre les autorités de réglementation de l'UE et de pays tiers. La Commission demandera donc l'autorisation d'ouvrir des négociations en vue de conclure des accords de coopération en matière d'application de la législation avec les pays tiers concernés (comme le prévoit également l'article 50 du RGPD). À cet égard, la Commission prend note de la demande du comité de considérer spécifiquement les pays avec le plus grand nombre d'opérateurs directement soumis au RGPD comme des contreparties potentielles, en particulier les pays du G7 et/ou les pays qui bénéficient de décisions d'adéquation[203].

La mise en place de tels accords de coopération et d'assistance mutuelle en matière de contrôle de l'application de la législation contribuerait également à garantir le respect et l'application effective des règles par les opérateurs étrangers soumis au RGPD, par exemple parce qu'ils ciblent spécifiquement le marché de l'Union en proposant des biens ou des services. Le Conseil note qu'il importe de faire respecter le RGPD dans de tels cas et fait part de ses inquiétudes concernant l'égalité des conditions de concurrence avec les entités établies dans l'UE et l'efficacité de la protection des droits des personnes physiques[204]. La Commission rejoint le Conseil sur sa suggestion d'étudier différentes manières de faciliter l'application de la législation dans ce scénario. S'il est certain que des formes plus formelles de coopération avec les autorités de réglementation des pays tiers pourraient jouer un rôle important, le recours à d'autres voies, déjà existantes, devrait également gagner en vigueur. Il s'agit notamment de tirer pleinement parti de la panoplie d'outils de mise en œuvre prévue à l'article 58 du RGPD et d'associer les représentants d'entreprises étrangères dans l'UE (désignés conformément à l'article 27 du RGPD).

7.2.2 La dimension multilatérale

La Commission continue également de jouer un rôle actif dans un certain nombre d'enceintes internationales afin de promouvoir des valeurs communes et de renforcer la convergence aux niveaux régional et mondial.

Par exemple, elle contribue activement aux travaux du comité consultatif sur la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), seul instrument multilatéral juridiquement contraignant dans le domaine de la protection des données à caractère personnel. À ce jour, 31 États ont ratifié le protocole d'amendement visant à moderniser la Convention 108[205], dont de nombreux États membres de l'UE, ainsi que certains pays non membres du Conseil de l'Europe (Argentine, Maurice et Uruguay). Parmi les États membres de l'UE, seule la signature d'un État membre est toujours en suspens[206], tandis que huit États membres[207] l'ont signée à ce

202 Contribution du comité, p. 8; position et conclusions du Conseil, point 38.
203 Contribution du comité, p. 8.
204 Position et conclusions du Conseil, point 39.
205 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE nº 223).
206 Le Danemark.
207 La Belgique, la Tchéquie, la Grèce, l'Irlande, la Lettonie, le Luxembourg, les Pays-Bas et la Suède.

jour, mais n'ont pas ratifié la Convention modernisée. La Commission demande instamment à l'État membre restant de signer la convention modernisée, et aux autres de procéder rapidement à la ratification, afin de permettre son entrée en vigueur dans un avenir proche. Par ailleurs, elle continue à encourager de manière proactive l'adhésion de pays tiers.

Au niveau du G20 et du G7, les discussions sur la protection de la vie privée et les flux de données se sont concentrées sur la mise en œuvre du concept de «libre circulation des données en toute confiance» (data free flow with trust, DFFT), proposé à l'origine par le Japon, qui reconnaît que la protection et la sécurité des données peuvent contribuer à la confiance dans l'économie numérique et faciliter les flux de données[208]. L'OCDE joue un rôle particulièrement important dans ce contexte, en fournissant un forum pour une communauté d'experts du DFFT, qui réunit un large éventail de parties prenantes (gouvernements, autorités de réglementation, industrie, société civile, universités) invitées à apporter leur contribution sur des projets et des questions spécifiques liés au DFFT. En outre, l'adoption par l'OCDE d'une déclaration sur l'accès des pouvoirs publics aux données à caractère personnel détenues par les entités du secteur privé, premier instrument international dans ce domaine, est un résultat important de l'initiative DFFT, à laquelle la Commission a contribué de manière significative. Elle contient une série d'exigences communes visant à protéger la vie privée lors de l'accès aux données à caractère personnel à des fins répressives et de sécurité nationale. Dans un contexte de reconnaissance croissante, à l'échelle mondiale, du fait que la confiance dans les transferts de données est affectée par un accès disproportionné des pouvoirs publics aux données, cette déclaration contribue dans une importante mesure à faciliter des flux de données fiables. La Commission continuera d'encourager les pays à adhérer à cette déclaration, qui est également ouverte aux pays non membres de l'OCDE.

La Commission collabore également avec différentes organisations régionales et différents réseaux régionaux qui définissent des garanties communes en matière de protection des données. Il s'agit par exemple de l'ASEAN, de l'Union africaine, du forum Asie-Pacifique des autorités de protection de la vie privée, du réseau ibéro-américain de protection des données et du réseau des autorités africaines de protection des données (NADPA – RADPD). L'élaboration du guide UE-ASEAN sur les clauses types, évoqué précédemment, est un exemple concret de cette coopération fructueuse.

Enfin, la Commission dialogue avec différentes organisations internationales, notamment pour étudier les moyens de faciliter encore les flux de données entre l'UE et ces organisations. Étant donné que de nombreuses organisations ont procédé à la modernisation de leurs cadres de protection des données ces dernières années, ou y procèdent actuellement, de nouvelles possibilités se présentent également pour échanger expériences et meilleures pratiques. À cet égard, les ateliers annuels organisés par le Contrôleur européen de la protection des données avec des organisations internationales et un groupe de travail spécial sur les transferts internationaux de données se sont révélés particulièrement utiles pour échanger et explorer des instruments concrets de coopération, y compris l'échange de données à caractère personnel[209].

---

[208] Voir, par exemple, https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1

[209] https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en

8 CONCLUSION

Au cours des six années qui ont suivi sa mise en application, le RGPD a donné aux personnes les moyens d'exercer un contrôle sur leurs données. Il a également contribué à créer des conditions de concurrence équitables pour les entreprises et a servi de pierre angulaire pour la panoplie d'initiatives qui contribuent à conduire la transition numérique dans l'UE.

Pour atteindre pleinement le double objectif du RGPD, à savoir assurer une protection solide pour les personnes physiques tout en garantissant le libre flux des données à caractère personnel au sein de l'UE et des flux de données sûrs en dehors de l'UE, il convient de se concentrer sur les points suivants:

- une application rigoureuse du RGPD, à commencer par l'adoption rapide de la proposition de la Commission relative aux règles de procédure afin d'offrir des voies de recours rapides et la sécurité juridique dans les affaires concernant des personnes dans l'ensemble de l'Union;
- une assistance proactive des autorités chargées de la protection des données à l'intention des parties prenantes pour les soutenir dans leurs efforts de mise en conformité, en particulier les PME et les petits opérateurs;
- une interprétation et une application cohérentes du RGPD dans l'ensemble de l'Union;
- une coopération efficace entre les autorités de réglementation, tant au niveau national qu'au niveau de l'UE, afin de garantir l'application uniforme et cohérente du corpus croissant de règles numériques de l'UE;
- poursuivre la mise en œuvre de la stratégie internationale de la Commission en matière de protection des données.

Pour soutenir l'application effective du RGPD et contribuer à de nouvelles réflexions sur la protection des données, plusieurs actions recensées ici s'imposent. La Commission soutiendra et surveillera leur mise en œuvre également dans la perspective du prochain rapport en 2028.

Mettre en place des structures de coopération efficaces

Le Parlement européen et le Conseil sont invités à adopter rapidement la proposition de règles de procédure relatives à l'application du RGPD.

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

- à établir une coopération régulière avec d'autres autorités de réglementation sectorielles sur les questions ayant une incidence sur la protection des données, en particulier celles qui ont été mises en place en vertu de la nouvelle législation numérique de l'UE, et participer activement aux structures au niveau de l'Union destinées à faciliter la coopération entre les autorités de réglementation;
- à faire un usage plus exhaustif des outils de coopération fournis par le RGPD, de sorte que le règlement des litiges ne soit qu'une solution de dernier ressort.
- à mettre en œuvre des modalités de travail plus efficaces et plus ciblées pour les lignes directrices, les avis et les décisions et à hiérarchiser les questions clés afin de réduire la charge pesant sur les autorités chargées de la protection des données et de réagir plus rapidement à l'évolution du marché.

Les États membres devraient

- continuer à suivre de près l'indépendance effective et totale des autorités nationales chargées de la protection des données;

- allouer des ressources suffisantes aux autorités chargées de la protection des données pour leur permettre de s'acquitter de leurs tâches, notamment en leur fournissant les ressources techniques et l'expertise nécessaires pour faire face aux technologies émergentes et assumer de nouvelles responsabilités au titre de la législation numérique;
- doter les autorités chargées de la protection des données des outils d'enquête qui leur sont nécessaires pour utiliser efficacement les pouvoirs d'exécution prévus par le RGPD;
- soutenir le dialogue entre les autorités chargées de la protection des données et les autres autorités de réglementation nationales, en particulier celles qui ont été établies en vertu de la nouvelle législation numérique.

La Commission entend:

- soutenir activement l'adoption rapide de la proposition de règles de procédure relatives à l'application du RGPD par les colégislateurs;
- continuer à suivre de près l'indépendance effective et totale des autorités nationales chargées de la protection des données;
- créer des synergies et une cohérence entre le RGPD et l'ensemble de la législation relative au traitement des données à caractère personnel sur la base de l'expérience acquise et, si nécessaire, prendre les mesures appropriées pour assurer la sécurité juridique;
- réfléchir aux moyens d'aborder au mieux la nécessité d'une coopération entre les autorités de réglementation structurée et efficiente afin de garantir l'application efficace, logique et cohérente des règles numériques de l'UE, tout en respectant la compétence des autorités chargées de la protection des données pour toutes les questions relatives au traitement des données à caractère personnel.

Mettre en œuvre et compléter le cadre juridique

Les États membres devraient:

- veiller à ce que les autorités chargées de la protection des données soient consultées en temps utile avant l'adoption de la législation sur le traitement des données à caractère personnel.

La Commission entend:

- continuer à utiliser tous les outils à sa disposition, y compris les procédures d'infraction, pour veiller à ce que les États membres respectent le RGPD;
- continuer à soutenir les échanges de vues et les pratiques nationales entre les États membres, y compris par l'intermédiaire du groupe d'experts des États membres sur le RGPD;
- mener des actions visant à garantir que les enfants sont protégés, autonomisés et respectés en ligne;
- réfléchir aux prochaines étapes possibles concernant la proposition de règlement «vie privée et communications électroniques», y compris sa relation avec le RGPD.

Soutenir les parties prenantes

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

- à engager un dialogue constructif avec les responsables du traitement et les sous-traitants sur le respect du RGPD;

- à intensifier encore les efforts visant à soutenir le respect des règles par les PME, en proposant des orientations et des outils sur mesure, en répondant à toute inquiétude infondée concernant la conformité des PME dont l'activité principale ne consiste pas à traiter des données à caractère personnel, et en les accompagnant dans leurs efforts de mise en conformité;
- à soutenir la mise en œuvre de mesures efficaces de mise en conformité par les entreprises, telles que la certification et les codes de conduite (y compris en tant qu'outils de transfert), en dialoguant avec les parties prenantes au cours du processus d'approbation, en fournissant des calendriers clairs pour les approbations et, comme annoncé dans la stratégie 2024-2027 du comité, en expliquant aux groupes clés de parties prenantes comment ces outils peuvent être utilisés;
- à veiller à ce que les lignes directrices nationales et l'application du RGPD au niveau national soient conformes aux lignes directrices du comité et à la jurisprudence de la Cour de justice;
- à résoudre les divergences d'interprétation du RGPD entre autorités chargées de la protection des données, y compris entre les autorités d'un même État membre;
- à fournir des lignes directrices concises, pratiques et accessibles au public concerné, comme annoncé dans la stratégie 2024-2027 du comité;
- à organiser une consultation plus précoce et plus utile sur les lignes directrices et les avis, afin de mieux comprendre la dynamique du marché et les pratiques commerciales, à tenir dûment compte des retours d'information reçus et à tenir compte de l'application concrète des interprétations adoptées;
- à achever en priorité les travaux en cours sur les lignes directrices consacrées aux données relatives aux enfants, à la recherche scientifique, à l'anonymisation, à la pseudonymisation et à l'intérêt légitime;
- à intensifier les activités de sensibilisation, les actions d'information et de contrôle de l'application des règles afin de veiller à ce que les délégués à la protection des données puissent s'acquitter de la mission qui leur incombe au titre du RGPD.

La Commission entend:

- continuer à apporter un soutien financier aux autorités chargées de la protection des données pour toutes les activités qui facilitent la mise en œuvre des obligations du RGPD par les PME;
- utiliser tous les moyens dont elle dispose pour apporter des éclaircissements opportuns sur des questions importantes pour les parties prenantes, y compris les PME, notamment en demandant l'avis du comité.

Étoffer la boîte à outils pour les transferts de données et la coopération internationale

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

- à achever les travaux visant à rationaliser et à raccourcir le processus d'approbation des règles d'entreprise contraignantes, ainsi qu'à mettre à jour les orientations sur les éléments figurant dans les règles d'entreprise contraignantes applicables aux sous-traitants;
- à étudier les moyens/outils permettant d'aider davantage les exportateurs de données dans leurs efforts de mise en conformité avec les exigences de Schrems II;

- à explorer d'autres manières de 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.

Les États membres devraient:

- veiller à ce que la convention modernisée 108+ du Conseil de l'Europe soit signée et ratifiée dans les meilleurs délais, en vue de permettre son entrée en vigueur.

La Commission entend:

- réaliser de nouveaux progrès dans les pourparlers en cours sur l'adéquation, se pencher sur la question de savoir s'il est opportun de développer plus avant les constats d'adéquation existants et engager de nouveaux dialogues sur l'adéquation avec les partenaires intéressés;
- soutenir une coopération accrue au sein du réseau des pays bénéficiant de décisions d'adéquation;
- parachever les travaux sur des clauses contractuelles types supplémentaires, en particulier pour les transferts de données à des importateurs de données dont le traitement est directement soumis au RGPD et les transferts au titre du règlement (UE) 2018/1725 pour les transferts de données par les institutions et organes de l'Union;
- coopérer avec des partenaires internationaux pour faciliter les flux de données sur la base de clauses contractuelles types;
- 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 des organisations internationales et régionales telles que l'OCDE et le G7 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 de libre circulation des données en toute confiance;
- faciliter et soutenir les échanges entre autorités de réglementation européennes et les autorités de réglementation internationales, y compris par l'intermédiaire de son Académie pour la protection des données;
- contribuer à faciliter 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.