COMMISSION
EUROPÉENNE

Bruxelles, le 24.6.2020
SWD(2020) 115 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

[…]

accompagnant le document

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN ET AU CONSEIL

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

{COM(2020) 264 final}

Contents

1 CONTEXTE

Le règlement général sur la protection des données[1] (ci-après le «RGPD») est le résultat de huit années de préparation, de rédaction et de négociations interinstitutionnelles, et est entré en application le 25 mai 2018 à la suite d'une période de transition de deux ans (mai 2016 - mai 2018). L'article 97 du RGPD impose à la Commission de rendre compte de l'évaluation et du réexamen du règlement, en commençant par un premier rapport après deux ans d'application, puis tous les quatre ans.

L'évaluation s'inscrit également dans le cadre d'une approche à multiples facettes que la Commission a déjà suivie avant l'entrée en vigueur du RGPD et qu'elle a continué à poursuivre activement depuis lors. Dans le cadre de cette approche, la Commission a engagé des dialogues bilatéraux qui sont en cours avec les États membres sur la conformité de la législation nationale avec le RGPD, a activement contribué aux travaux du comité européen de la protection des données (ci-après le «comité») en apportant son expérience et son expertise, en soutenant les autorités chargées de la protection des données et en entretenant des contacts étroits avec un large éventail de parties prenantes sur l'application pratique du règlement.

L'évaluation se fonde sur le bilan que la Commission a réalisé au cours de la première année d'application du RGPD et qui a été résumé dans la communication publiée en juillet 2019[2]. Elle fait également suite à la communication sur l'application du RGPD publiée en janvier 2018[3]. La Commission a également adopté les orientations sur l'utilisation des données à caractère personnel dans le contexte électoral, publiées en septembre 2018, ainsi que les orientations sur les applications soutenant la lutte contre la pandémie de COVID-19, publiées en avril 2020.

Bien que l'accent soit placé sur les deux questions mises en exergue à l'article 97, paragraphe 2, du RGPD, à savoir les transferts internationaux et les mécanismes de coopération et de contrôle de la cohérence, cette évaluation adopte une approche plus large afin d'aborder les problématiques soulevées par différents acteurs au cours des deux dernières années.

Afin de préparer l'évaluation, la Commission a pris en considération:

- la contribution du Conseil[4];

---

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

[2] Communication de la Commission au Parlement européen et au Conseil intitulée «Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan», COM(2019) 374 final, 24.7.2019.

[3] Communication de la Commission au Parlement européen et au Conseil intitulée «Une meilleure protection et de nouvelles perspectives – Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018», COM/2018/043 final.

[4] Position et conclusions du Conseil relatives à l'application du règlement général sur la protection des données - 14994/2/19 Rev2, 15.1.2020:
https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/fr/pdf

- la contribution du Parlement européen (commission des libertés civiles, de la justice et des affaires intérieures)[5];
- la contribution du comité[6] et de différentes autorités chargées de la protection des données[7], sur la base d'un questionnaire envoyé par la Commission;
- le retour d'information des membres du groupe d'experts multipartite pour soutenir l'application du RGPD[8], également sur la base d'un questionnaire envoyé par la Commission;
- et les contributions ad hoc reçues des parties prenantes.

2 MISE EN ŒUVRE DU RGPD ET FONCTIONNEMENT DES MÉCANISMES DE COOPÉRATION ET DE CONTRÔLE DE LA COHÉRENCE

Le RGPD a mis en place un système de gouvernance innovant et jeté les fondements d'une véritable culture européenne de la protection des données, qui vise à garantir non seulement une interprétation harmonisée, mais aussi une application et un contrôle harmonisés des règles en matière de protection des données. Ses piliers sont les autorités nationales indépendantes chargées de la protection des données et le nouveau comité.

Étant donné que les autorités chargées de la protection des données sont essentielles au fonctionnement de l'ensemble du système de protection des données de l'UE, la Commission surveille attentivement leur véritable indépendance, notamment en ce qui concerne les ressources financières, humaines et techniques adéquates.

Il est encore trop tôt pour évaluer pleinement le fonctionnement des mécanismes de coopération et de contrôle de la cohérence, compte tenu de la courte expérience acquise jusqu'alors[9]. En outre, les autorités chargées de la protection des données n'ont pas encore utilisé l'ensemble des outils prévus par le RGPD pour renforcer davantage leur coopération.

2.1 Recours à des pouvoirs renforcés par les autorités chargées de la protection des données

Le RGPD établit des autorités indépendantes chargées de la protection des données et leur accorde des pouvoirs d'exécution harmonisés et renforcés. Depuis que le RGPD s'applique, ces autorités utilisent un large éventail de pouvoirs correctifs prévus par le

---

[5] Lettre de la commission LIBE du Parlement européen du 21 février 2020 au commissaire Reynders, réf.: IPOL-COM-LIBE D (2020)6525.

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

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

[8] Le groupe d'experts multipartite sur le RGPD créé par la Commission est composé de représentants de la société civile et d'entreprises, d'universitaires et de professionnels: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537 Le rapport du groupe multipartite est disponible à l'adresse suivante: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

[9] Ce fait est également mis en évidence notamment par le Conseil, dans sa position et ses conclusions sur l'application du RGPD, et par le comité, dans sa contribution à l'évaluation.

RGPD, tels que des amendes administratives (22 autorités UE/EEE)[10], des avertissements et des rappels à l'ordre (23), des injonctions de donner suite aux demandes de la personne concernée (26), des ordres de mise en conformité avec le RGPD (27) et des injonctions de rectifier, d'effacer ou de limiter le traitement (17). Près de la moitié des autorités chargées de la protection des données (13) ont imposé des limitations temporaires ou définitives au traitement, y compris des interdictions. Cela démontre une utilisation consciente de toutes les mesures correctives prévues dans le RGPD; les autorités chargées de la protection des données n'ont pas hésité à imposer des amendes administratives en complément ou au lieu d'autres mesures correctrices, en fonction des circonstances propres à chaque cas.

Amendes administratives:

Entre le 25 mai 2018 et le 30 novembre 2019, 22 autorités de l'UE et de l'EEE chargées de la protection des données ont délivré environ 785 amendes. Seules quelques autorités n'ont pas encore imposé d'amendes administratives, bien que des procédures actuellement en cours puissent conduire à de telles sanctions. La plupart des amendes sont liées à des infractions commises à l'encontre: du principe de licéité; du consentement valable; de la protection des données sensibles; de l'obligation de transparence, des droits des personnes concernées; et des violations des données.

Exemples d'amendes infligées par des autorités de protection des données[11]:

- 200 000 EUR pour non-respect du droit d'opposition à la vente directe en Grèce;
- 220 000 EUR pour une société de courtage de données en Pologne, pour ne pas avoir informé les personnes que leurs données étaient traitées;
- 250 000 EUR pour la ligue de football espagnole LaLiga, pour manque de transparence dans la conception de son application pour smartphone;
- 14 500 000 EUR pour la violation des principes de la protection des données, notamment le stockage illicite, par une entreprise immobilière allemande;
- 18 000 000 EUR pour le traitement illicite de catégories particulières de données à grande échelle par les services postaux autrichiens;
- 50 000 000 EUR pour Google en France, en raison des conditions d'obtention du consentement des utilisateurs.

Le succès du RGPD ne devrait pas être mesuré par le nombre d'amendes infligées, étant donné que le RGPD prévoit un éventail plus large de pouvoirs en ce qui concerne les mesures correctrices. En fonction des circonstances, par exemple, l'effet dissuasif d'une interdiction de traitement ou de la suspension des flux de données peut être beaucoup plus fort.

Questions spécifiques pour le secteur public

Le RGPD autorise les États membres à déterminer si et dans quelle mesure des amendes administratives peuvent être infligées aux autorités et organismes publics.

[10] Les chiffres entre parenthèses indiquent le nombre d'autorités chargées de la protection des données de l'UE/EEE qui ont eu recours aux pouvoirs indiqués entre mai 2018 et fin novembre 2019. Voir la contribution du comité, pages 32 et 33.

[11] Plusieurs décisions infligeant des amendes font toujours l'objet d'un contrôle juridictionnel.

Lorsque les États membres font usage de cette possibilité, cela ne prive pas les autorités chargées de la protection des données d'utiliser tous les autres pouvoirs d'adoption de mesures correctrices à l'égard des autorités et organismes publics[12].

Une autre question spécifique est celle de la surveillance des tribunaux: bien que le RGPD s'applique également aux activités des juridictions, ces dernières sont dispensées de la surveillance par les autorités chargées de la protection des données lorsqu'elles agissent dans l'exercice de leurs fonctions juridictionnelles. Toutefois, la Charte et le TFUE imposent aux États membres de confier à un organisme indépendant, dans le cadre de leurs systèmes judiciaires, la surveillance de ces opérations de traitement[13].

Coopération avec d'autres autorités de réglementation

Comme annoncé dans sa communication de juillet 2019, la Commission soutient l'interaction avec d'autres autorités de réglementation, dans le plein respect des compétences respectives. Les domaines de coopération prometteurs sont notamment la protection des consommateurs et la concurrence. Le comité a indiqué qu'elle était disposée à coopérer avec d'autres autorités de réglementation, en particulier en ce qui concerne la concentration sur les marchés numériques[14]. La Commission a reconnu l'importance de la protection de la vie privée et des données en tant que paramètre qualitatif de la concurrence[15]. Les membres du comité ont participé, avec le réseau de coopération en matière de protection des consommateurs, à des ateliers conjoints consacrés à la coopération en vue d'une meilleure application de la législation de l'UE en matière de protection des consommateurs et des données. Cette approche sera poursuivie afin de favoriser une compréhension commune et de mettre au point des moyens pratiques de résoudre les problèmes concrets rencontrés par les consommateurs, en particulier dans l'économie numérique.

Afin de garantir une approche cohérente de la protection de la vie privée et des données, et dans l'attente de l'adoption du règlement «vie privée et communications électroniques», une coopération étroite avec les autorités compétentes pour l'application de la directive «vie privée et communications électroniques»[16], la lex specialis dans le domaine des communications électroniques, est indispensable. Une coopération plus étroite avec les autorités compétentes au titre de la directive sur la SRI[17] et avec le groupe de coopération SRI s'exercerait au bénéfice mutuel de ces autorités et des autorités chargées de la protection des données.

---

12 Article 83, paragraphe 7, du RGPD.

13 Article 8, paragraphe 3, de la Charte; article 16, paragraphe 2, du TFUE; considérant 20 du RGPD.

14 Voir la déclaration du comité sur les incidences de la concentration économique sur la protection des données, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_fr.pdf.

15 Voir l'affaire COMP M. 8124 Microsoft/LinkedIn.

16 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (JO L 201 du 31.7.2002, p. 37).

17 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

2.2 Les mécanismes de coopération et de contrôle de la cohérence

Le RGPD a créé le mécanisme de coopération (système de guichet unique pour les opérateurs, les opérations conjointes et l'assistance mutuelle entre les autorités chargées de la protection des données) et le mécanisme de contrôle de la cohérence afin de favoriser une application uniforme des règles en matière de protection des données, grâce à une interprétation cohérente et à la résolution d'un éventuel désaccord entre les autorités par le comité.

Le comité, qui réunit toutes les autorités chargées de la protection des données, a été créé en tant qu'organe de l'UE doté de la personnalité juridique et est pleinement opérationnel, avec l'appui d'un secrétariat[18]. Il est essentiel au fonctionnement des deux mécanismes susmentionnés. Fin 2019, le comité avait adopté 67 documents, dont 10 nouvelles lignes directrices[19] et 43 avis[20] [21].

Le rôle important du comité est apparu lorsqu'il a été nécessaire de fournir rapidement une interprétation cohérente du RGPD et de trouver des solutions immédiatement applicables au niveau de l'UE. Par exemple, dans le contexte de l'épidémie de COVID-19, le comité a adopté en mars 2020 une déclaration sur le traitement des données à caractère personnel, qui porte, entre autres, sur la licéité du traitement et l'utilisation des données de localisation mobile dans ce contexte[22], et en avril 2020 des lignes directrices sur le traitement des données relatives à la santé aux fins de la recherche scientifique dans le cadre de la pandémie de COVID-19 [23] et des lignes directrices relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19[24]. Le comité a également contribué de manière significative à la conception de l'approche de l'UE en matière d'applications de traçage par la Commission et les États membres.

La coopération au quotidien entre les autorités chargées de la protection des données, qu'elles agissent en leur nom propre ou en tant que membres du comité, est fondée sur les échanges d'informations et les notifications de dossiers ouverts par les autorités. Afin de faciliter la communication entre elles, la Commission a apporté aux autorités un soutien important en leur fournissant un système d'échange d'informations[25]. La plupart des autorités estiment qu'il est adapté aux besoins des mécanismes de

---

[18] Voir les informations détaillées sur les activités du secrétariat fournies par le comité dans sa contribution, pages 24 à 26.

[19] En plus des 10 lignes directrices adoptées par le groupe de travail «article 29» à l'approche de l'entrée en vigueur du RGPD et approuvées par le comité. En outre, le comité a adopté 4 lignes directrices supplémentaires entre janvier et fin mai 2020 et mis à jour une ligne directrice existante.

[20] 42 de ces avis ont été adoptés en vertu de l'article 64 du RGPD et un avis, qui concernait la décision d'adéquation relative au Japon, a été adopté en vertu de l'article 70, paragraphe 1, point s), du RGPD.

[21] Voir la contribution du comité, pages 18 à 23, pour un aperçu complet des activités du comité.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_fr.

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_fr.pdf.

[25] Système d'information du marché intérieur («IMI»).

coopération et de contrôle de la cohérence, quand bien même il pourrait être encore affiné, par exemple en le rendant plus convivial.

Bien qu'il soit encore fort tôt, un certain nombre de réalisations et de défis peuvent déjà être recensés et présentés ci-dessous. Ils montrent que, jusqu'à présent, les autorités chargées de la protection des données ont fait un usage efficace des outils de coopération, avec une préférence pour des solutions plus flexibles.

Le guichet unique

En règle générale, dans les affaires transfrontières, l'autorité de protection des données d'un État membre peut participer soit i) en tant qu'autorité chef de file lorsque l'établissement principal de l'opérateur est situé dans cet État membre, soit ii) en tant qu'autorité concernée lorsque l'opérateur dispose d'un établissement sur le territoire de cet État membre, lorsque des personnes dans cet État membre sont substantiellement touchées, ou lorsqu'une plainte a été déposée auprès d'elle.

Cette étroite coopération est devenue une pratique quotidienne: depuis la date d'application du RGPD, les autorités chargées de la protection des données dans tous les États membres ont, à un moment ou un autre, été recensées en tant qu'autorités chefs de file ou autorités concernées dans les affaires transfrontières, bien que dans une autre mesure.

Entre mai 2018 et la fin de l'année 2019, l'autorité irlandaise chargée de la protection des données a fait office de chef de file dans le plus grand nombre d'affaires transfrontières (127), suivie de l'Allemagne (92), du Luxembourg (87), de la France (64) et des Pays-Bas (45). Ce classement reflète notamment la situation spécifique de l'Irlande et du Luxembourg, qui accueillent plusieurs grandes entreprises technologiques multinationales.

Le classement est différent en ce qui concerne la participation en tant qu'autorités chargées de la protection des données, les autorités allemandes étant celles qui sont intervenues dans le plus grand nombre d'affaires (435), suivies de l'Espagne (337), du Danemark (327), de la France (332) et de l'Italie (306)[26].

Entre le 25 mai 2018 et le 31 décembre 2019, 141 projets de décisions ont été soumis dans le cadre de la procédure de guichet unique, dont 79 ont donné lieu à des décisions finales. À la date de publication du présent rapport, plusieurs décisions importantes ayant une dimension transfrontière et soumises au mécanisme de guichet unique sont en cours. Parmi ces décisions, certaines concernent de grandes entreprises technologiques multinationales[27]. Elles devraient fournir des éclaircissements et contribuer à une plus grande harmonisation dans l'interprétation du RGPD.

Assistance mutuelle

[26] Voir la contribution du comité, page 8.

[27] Par exemple, le 22 mai 2020, l'autorité irlandaise de protection des données a soumis un projet de décision à d'autres autorités concernées, conformément à l'article 60 du règlement, concernant une enquête sur Twitter International Company portant sur la notification d'une violation de données. Le même jour, l'autorité irlandaise chargée de la protection des données a également annoncé qu'un projet de décision sur WhatsApp Ireland Limited pour soumission au titre de l'article 60 était en préparation. Ce projet de décision portait sur la transparence, y compris la transparence quant aux informations partagées avec Facebook.

Les autorités chargées de la protection des données ont largement eu recours à l'outil d'assistance mutuelle.

À la fin de l'année 2019, on dénombrait 115 procédures d'assistance mutuelle[28] en vue, notamment, de la réalisation d'enquêtes, la plupart d'entre elles par les autorités chargées de la protection des données en Espagne (26), en Allemagne (20), au Danemark (13), en Pologne (12) et en République tchèque (10). En revanche, l'Irlande (19), la France (11), l'Autriche (10), l'Allemagne (10) et le Luxembourg (9) avaient reçu le plus de demandes [29].

La grande majorité des autorités considèrent l'assistance mutuelle comme un outil de coopération très utile et n'ont rencontré aucun obstacle particulier à l'application de la procédure d'assistance mutuelle. L'échange volontaire d'assistance mutuelle, qui n'est pas soumis à un délai légal ni à une obligation de réponse stricte, a été utilisé plus fréquemment, dans 2 427 procédures. L'autorité irlandaise chargée de la protection des données a envoyé et reçu le plus grand nombre de demandes d'assistance mutuelle (527 envoyées et 359 reçues), suivies par les autorités allemandes (260 envoyées et 356 reçues).

Par ailleurs, les opérations conjointes[30], qui permettraient aux autorités chargées de la protection des données de plusieurs États membres de participer déjà au niveau des enquêtes sur des affaires transfrontières, n'ont pas encore été menées. Une réflexion est en cours au sein du comité sur la mise en œuvre pratique de cet outil et sur la manière de promouvoir son utilisation.

Mécanisme de contrôle de la cohérence

Jusqu'à présent, seule la première partie du mécanisme de contrôle de la cohérence a été utilisée, à savoir l'adoption des avis du comité[31]. Par ailleurs, aucun règlement des différends au niveau du comité[32] ni aucune procédure d'urgence[33] n'a encore été lancé(e).

Entre le 25 mai 2018 et le 31 décembre 2019, le comité a émis 36 avis dans le cadre de l'adoption de mesures par l'un de ses membres[34]. La plupart de ces avis (31) concernaient l'adoption de listes nationales d'opérations de traitement nécessitant une analyse d'impact relative à la protection des données. Deux avis concernaient des règles d'entreprise contraignantes, deux autres concernaient des projets d'exigences en matière d'accréditation pour un organisme de contrôle du code de conduite, et un dernier concernait des clauses contractuelles types[35].

En outre, le comité a adopté, sur demande, six avis[36]. Trois de ces avis concernaient des listes nationales identifiant un traitement qui ne nécessite pas d'analyse d'impact relative à la protection des données. Les autres concernaient respectivement un

[28] Article 61 du RGPD.
[29] Voir la contribution du comité, pages 12 à 14.
[30] Article 62 du RGPD.
[31] Sur la base de l'article 64 du RGPD.
[32] Article 65 du RGPD.
[33] Article 66 du RGPD.
[34] Au titre de l'article 64, paragraphe 1, du RGPD.
[35] Article 28, paragraphe 8, du RGPD.
[36] Au titre de l'article 64, paragraphe 2, du RGPD.

arrangement administratif pour le transfert de données à caractère personnel entre les autorités de surveillance financière établies dans l'EEE et hors de l'EEE, l'interaction entre la directive «vie privée et communications électroniques» et le RGPD, et la compétence d'une autorité de contrôle en cas de changement de circonstances concernant l'établissement principal ou unique[37].

Problèmes à résoudre

Bien que les autorités chargées de la protection des données collaborent très activement au sein du comité et utilisent déjà intensivement l'outil de coopération de l'assistance mutuelle, la création d'une véritable culture commune en matière de protection des données est toujours en cours.

En particulier, le traitement des affaires transfrontières requiert une approche plus efficiente et harmonisée ainsi que l'utilisation efficace de tous les outils de coopération prévus par le RGPD. Il existe un très large consensus sur ce point, étant donné qu'il a été soulevé de différentes manières par le Parlement européen, le Conseil, le contrôleur européen de la protection des données, les parties prenantes (au sein du groupe multipartite et au-delà) et les autorités chargées de la protection des données.

Les principales questions à aborder dans ce contexte sont les suivantes:

- les procédures administratives nationales, notamment en ce qui concerne: les procédures de traitement des plaintes, les critères de recevabilité des plaintes, la durée des procédures en raison des délais différents ou de l'absence de délais, le moment de l'octroi du droit d'être entendu au cours de la procédure, l'information et la participation des plaignants au cours de la procédure;
- les interprétations des notions relatives au mécanisme de coopération, telles que les informations pertinentes, la notion de «sans délai», la «plainte», le document qui est défini comme étant le «projet de décision» de l'autorité de protection des données chef de file, le règlement à l'amiable (en particulier la procédure conduisant à un règlement à l'amiable et la forme juridique du règlement); et
- l'approche adoptée pour lancer la procédure de coopération, permettre aux autorités chargées de la protection des données concernées de participer à celle-ci et leur communiquer des informations. Les plaignants manquent également de clarté quant à la manière dont leurs affaires sont traitées dans des situations transfrontières, comme l'ont souligné plusieurs membres du groupe multipartite. En outre, les entreprises indiquent que, dans certains cas, les autorités nationales chargées de la protection des données n'ont pas soumis ces affaires à l'autorité chargée de la protection des données chef de file, mais les ont traitées comme des affaires locales.

La Commission se félicite de l'annonce du comité selon laquelle il a entamé une réflexion sur la manière de répondre à ces préoccupations. En particulier, le comité a indiqué qu'il clarifiera les étapes de la procédure de coopération entre l'autorité chef de file et les autorités concernées chargées de la protection des données, analysera les lois de procédure administrative nationales, œuvrera à l'interprétation commune de

[37] Voir la contribution du comité, page 15.

notions clés et renforcera la communication et la coopération (y compris les opérations conjointes). La réflexion et l'analyse du comité devraient déboucher sur l'élaboration de modalités de travail plus efficaces dans les affaires transfrontières[38], notamment en s'appuyant sur l'expertise de ses membres et en renforçant la participation de son secrétariat. En outre, il convient de noter que la responsabilité du comité dans la garantie d'une interprétation cohérente du RGPD ne peut être assumée par la simple constatation du plus petit dénominateur commun.

Enfin, en tant qu'organe de l'UE, le comité doit également appliquer le droit administratif de l'UE et garantir la transparence du processus décisionnel.

2.3 Conseils et lignes directrices

Sensibilisation et conseil des autorités chargées de la protection des données

Plusieurs autorités chargées de la protection des données ont créé de nouveaux outils, tels que des lignes d'assistance pour les particuliers et les entreprises, et des boîtes à outils pour les entreprises[39]. De nombreux opérateurs se félicitent du pragmatisme dont ont fait preuve ces autorités en aidant à l'application du RGPD. En particulier, plusieurs d'entre elles ont activement et étroitement collaboré et communiqué avec les délégués à la protection des données, y compris par l'intermédiaire des associations de délégués à la protection des données. De nombreuses autorités ont également publié des lignes directrices portant sur le rôle des délégués à la protection des données et les obligations de soutien aux délégués à la protection des données au cours de leurs activités quotidiennes et ont organisé des séminaires spécialement conçus pour eux. Toutefois, ce n'est pas le cas de toutes les autorités chargées de la protection des données.

Les réactions des parties prenantes indiquent également un certain nombre de points relatifs à l'orientation et au conseil:

- l'absence d'approche et d'orientations cohérentes entre les autorités nationales chargées de la protection des données sur certaines questions (par exemple, sur les cookies[40], l'application de l'intérêt légitime, les notifications des violations de données ou les analyses d'impact relatives à la protection des données) ou encore entre les autorités chargées de la protection des données au sein des mêmes États membres (comme c'est le cas par exemple en Allemagne en ce qui concerne les notions de responsable du traitement et de sous-traitant);
- l'incohérence entre les lignes directrices adoptées au niveau national et celles adoptées par le comité;

---

38 Ainsi qu'il ressort également de la position et des conclusions du Conseil.

39 Voir le point 7 ci-après.

40 Dans l'attente de l'adoption du règlement «vie privée et communications électroniques», il est nécessaire d'établir une coopération étroite avec les autorités compétentes chargées de l'application de la directive «vie privée et communications électroniques» dans les États membres. Conformément à cette directive, dans certains États membres, les autorités compétentes pour faire appliquer l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» (qui définit les conditions selon lesquelles les «cookies» peuvent être paramétrés et accessibles sur l'équipement terminal d'un utilisateur) ne sont pas les mêmes que les autorités de contrôle du RGPD.

- l'absence de consultations publiques sur certaines lignes directrices adoptées au niveau national;
- différents niveaux d'engagement auprès des parties prenantes parmi les autorités chargées de la protection des données;
- des retards dans la réception des réponses aux demandes d'information;
- des difficultés à obtenir des conseils pratiques et utiles de la part des autorités chargées de la protection des données;
- la nécessité d'accroître le niveau d'expertise sectorielle au sein de certaines autorités chargées de la protection des données (par exemple dans le secteur sanitaire et pharmaceutique).

Plusieurs de ces questions sont également liées au manque de ressources au sein de plusieurs autorités chargées de la protection des données (voir ci-dessous).

Pratiques divergentes en ce qui concerne la notification des violations de données[41]

Bien que le Conseil mette l'accent sur la charge découlant de ces notifications, il existe des divergences importantes en ce qui concerne les notifications entre les États membres: si, de mai 2018 à fin novembre 2019, le nombre total de notifications de violations des données était inférieur à 2 000 dans la plupart des États membres et compris entre 2 000 et 10 000 dans sept États membres, les autorités de protection des données néerlandaises et allemandes ont établi respectivement 37 400 et 45 600 notifications[42].

Cela pourrait indiquer un manque de cohérence dans l'interprétation et la mise en œuvre, malgré l'existence de lignes directrices au niveau de l'UE sur les notifications de violations des données.

Lignes directrices du comité européen de la protection des données

À ce jour, le comité a adopté plus de 20 lignes directrices couvrant des aspects essentiels du RGPD[43]. Les lignes directrices constituent un outil essentiel pour l'application cohérente du RGPD et ont donc été, dans une large mesure, accueillies favorablement par les parties prenantes, qui ont salué la consultation publique systématique (de 6 à 8 semaines). Toutefois, elles demandent davantage de dialogue avec le comité. Dans ce contexte, la pratique consistant à organiser des ateliers sur des sujets ciblés avant de rédiger des lignes directrices devrait être poursuivie et amplifiée afin de garantir la transparence, l'inclusion et la pertinence des travaux du comité. Les parties prenantes demandent également que l'interprétation des questions les plus controversées soit abordée dans les lignes directrices, étant donné qu'elles font l'objet d'une consultation publique, et non dans les avis visés à l'article 64, paragraphe 2, du RGPD. Certaines parties prenantes demandent également des lignes directrices plus

41 Article 33 du RGPD.

42 Voir la contribution du comité, page 35.

43 Les travaux sur les lignes directrices ont déjà commencé avant l'entrée en vigueur du RGPD le 25 mai 2018 dans le cadre du groupe de travail «article 29». Voir la liste complète des lignes directrices à l'adresse suivante: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_fr

pratiques, qui détaillent l'application des notions et des dispositions du RGPD[44]. Les membres du groupe multipartite soulignent qu'il est nécessaire de donner des exemples plus concrets afin de réduire autant que possible les possibilités d'interprétations divergentes entre les autorités chargées de la protection des données. Dans le même temps, les demandes visant à clarifier les modalités d'application du RGPD et à garantir la sécurité juridique ne devraient pas entraîner d'exigences supplémentaires ni réduire les avantages de l'approche fondée sur les risques et du principe de responsabilité.

Les sujets sur lesquels les parties prenantes souhaiteraient des lignes directrices supplémentaires de la part du comité comprennent: le champ d'application des droits des personnes concernées (y compris dans le contexte professionnel); des mises à jour de l'avis sur le traitement fondé sur l'intérêt légitime; les notions de responsable du traitement, de responsable conjoint du traitement et de sous-traitant, ainsi que les arrangements nécessaires entre les parties[45]; l'application du RGPD aux nouvelles technologies (telles que les chaînes de blocs et l'intelligence artificielle); le traitement dans le cadre de la recherche scientifique (y compris dans le cadre de la collaboration internationale); le traitement des données relatives aux enfants; la pseudonymisation et l'anonymisation; et le traitement des données relatives à la santé.

Le comité a déjà indiqué qu'il publiera des lignes directrices sur bon nombre de ces sujets et que les travaux ont déjà commencé pour plusieurs d'entre eux (par exemple, en ce qui concerne l'application de l'intérêt légitime comme base juridique du traitement).

Les parties prenantes demandent au comité de mettre à jour et de réviser, le cas échéant, les lignes directrices existantes, en tenant compte de l'expérience acquise depuis leur publication et en saisissant le cas échéant l'occasion d'entrer davantage dans le détail.

2.4 Ressources des autorités chargées de la protection des données

Doter chaque autorité de protection des données des ressources humaines, techniques et financières, des locaux et des infrastructures nécessaires est une condition préalable à la bonne exécution de leurs missions et à l'exercice de leurs pouvoirs, et donc une condition essentielle de leur indépendance[46].

La plupart des autorités chargées de la protection des données ont bénéficié d'une augmentation de leur personnel et de leurs ressources depuis l'entrée en vigueur du RGPD en 2016[47]. Toutefois, nombre d'entre elles continuent de déclarer qu'elles ne disposent pas de ressources suffisantes[48].

Nombre de personnes travaillant pour les autorités nationales chargées de la protection des données

---

44 Le Parlement européen et le Conseil ont également mis l'accent sur ce point.

45 Des lignes directrices du comité sur les responsables du traitement et les sous-traitants sont actuellement en préparation.

46 Voir l'article 52, paragraphe 4, du RGPD.

47 Le règlement est entré en vigueur en mai 2016 puis est entré en application en mai 2018, à la suite d'une période de transition de deux ans.

48 Voir la contribution du comité, pages 26 à 30.

Le nombre total d'agents travaillant au sein des autorités chargées de la protection des données dans l'EEE a augmenté de 42 % entre 2016 et 2019 (de 62 % si l'on considère les prévisions de 2020).

Le nombre d'agents a augmenté au sein de la plupart des autorités durant cette période, la plus forte augmentation (en pourcentage) étant enregistrée pour les autorités en Irlande (+ 169 %), aux Pays-Bas (+ 145 %), en Islande (+ 143 %), au Luxembourg (+ 126 %) et en Finlande (+ 114 %). Par ailleurs, le nombre d'agents a diminué au sein de plusieurs autorités chargées de la protection des données, les plus fortes baisses ayant été observées en Grèce (-15 %), en Bulgarie (-14 %), en Estonie (-11 %), en Lettonie (-10 %) et en Lituanie (-8 %). Au sein de certaines autorités, la diminution du personnel est également due au départ d'experts de la protection des données vers le secteur privé, qui offre des conditions plus attrayantes.

D'une manière générale, les prévisions pour 2020 prévoient une augmentation du personnel par rapport à 2019, sauf pour les autorités autrichiennes, bulgares, italiennes, suédoises et islandaises (dont les effectifs devraient rester stables), chypriotes et danoises (dont les effectifs devraient diminuer).

Les autorités allemandes chargées de la protection des données[49] comptent, conjointement, le plus grand nombre d'agents (888 en 2019/1 002 selon les prévisions de 2020), suivies par les autorités polonaises (238/260), françaises (215/225), espagnoles (170/220), néerlandaises (179/188), italiennes (170/170) et irlandaises (140/176).

Les autorités chargées de la protection des données qui comptent le nombre d'agents le plus faible sont les autorités chypriotes (24/22), lettonnes (19/31), islandaises (17/17), estoniennes (16/18) et maltaises (13/15).

Budget des autorités chargées de la protection des données

Le budget total des autorités de l'EEE chargées de la protection des données a augmenté de 49 % entre 2016 et 2019 (de 64 % si l'on considère les prévisions pour 2020).

Le budget de la plupart des autorités a augmenté au cours de cette période, la plus forte augmentation (en pourcentage) étant enregistrée pour les autorités irlandaises (+ 223 %), islandaises (+ 167 %), luxembourgeoises (+ 165 %), néerlandaises (+ 130 %) et chypriotes (+ 114 %). Par ailleurs, certaines autorités n'ont connu qu'une légère augmentation budgétaire, les plus faibles augmentations étant enregistrées pour les autorités de protection des données estoniennes (7 %), lettones (4 %), roumaines (3 %) et belges (1 %), tandis que les autorités françaises ont enregistré une diminution (-2 %).

D'une manière générale, les prévisions pour 2020 prévoient une augmentation du budget par rapport à 2019, à l'exception des autorités autrichiennes, bulgares, estoniennes et néerlandaises (dont les budgets devraient rester stables).

Les autorités chargées de la protection des données ayant le budget le plus élevé sont

[49] L'Allemagne compte 18 autorités, dont une autorité fédérale et 17 autorités régionales (dont deux en Bavière).

celles de l'Allemagne (76,6 millions d'EUR en 2019/85,8 millions d'EUR selon les prévisions de 2020), de l'Italie (29,1/30,1), des Pays-Bas (18,6/18,6), de la France (18,5/20,1) et de l'Irlande (15,2/16,9).

Les autorités dont le budget est le plus faible sont celles de la Croatie (1,2 million d'EUR en 2019/1,4 million d'EUR selon les prévisions de 2020), de la Roumanie (1,1/1,3), de la Lettonie (0,6/1,2), de Chypre (0,5/0,5) et de Malte (0,5/0,6).

Le tableau figurant à l'annexe II présente un aperçu des ressources humaines et budgétaires des autorités nationales chargées de la protection des données.

Outre son incidence sur leur capacité à faire appliquer les règles au niveau national, le manque de ressources limite également la capacité des autorités chargées de la protection des données à participer et à contribuer aux mécanismes de coopération et de contrôle de la cohérence, ainsi qu'aux travaux menés au sein du comité. Comme l'a souligné le comité, le succès du mécanisme de guichet unique dépend du temps et de l'effort que les autorités chargées de la protection des données peuvent consacrer au traitement et à la coopération dans les affaires transfrontières individuelles. La question des ressources est aggravée par le rôle accru des autorités dans la surveillance des systèmes informatiques à grande échelle qui sont en cours d'élaboration. En outre, les autorités chargées de la protection des données en Irlande et au Luxembourg ont des besoins en ressources spécifiques, compte tenu de leur rôle de chef de file dans la mise en œuvre du RGPD par rapport aux grandes entreprises technologiques, qui sont principalement situées dans ces États membres.

Si le Conseil souligne l'incidence du mécanisme de coopération et de ses délais sur les travaux des autorités chargées de la protection des données[50], le RGPD impose aux États membres de fournir à leurs autorités nationales de protection des données des ressources humaines, financières et techniques adéquates[51].

Le secrétariat du comité, qui est assuré par le contrôleur européen de la protection des données[52], est actuellement composé de 20 personnes, dont des experts juridiques, informatiques et en communication. Il convient d'évaluer si ce chiffre doit évoluer à l'avenir compte tenu de la satisfaction effective de sa fonction d'appui analytique, administratif et logistique au comité et à ses sous-groupes, y compris par la gestion du système d'échange d'informations.

3 DES RÈGLES HARMONISÉES, MAIS UN CERTAIN DEGRÉ DE FRAGMENTATION ET DES APPROCHES DIVERGENTES

Le RGPD prévoit une approche cohérente des règles en matière de protection des données dans l'ensemble de l'UE, en remplacement des différents régimes nationaux existant dans le cadre de la directive de 1995 sur la protection des données.

3.1 Mise en œuvre du RGPD par les États membres

[50] Article 60 du RGPD.
[51] Article 52, paragraphe 4, du RGPD.
[52] Article 75 du RGPD.

Le RGPD est directement applicable dans tous les États membres depuis le 25 mai 2018. Il a obligé les États membres à légiférer, notamment pour mettre en place des autorités nationales de protection des données et les conditions générales de leurs membres, afin de garantir que chaque autorité agit en toute indépendance dans l'accomplissement de ses missions et dans l'exercice de ses pouvoirs conformément au RGPD. Les obligations légales et les missions de service public ne peuvent constituer un fondement juridique pour le traitement de données à caractère personnel que si elles sont énoncées dans le droit (de l'Union ou) national. En outre, les États membres doivent fixer des règles en matière de sanctions notamment pour les infractions qui ne sont pas passibles d'amendes administratives et doivent concilier le droit à la protection des données à caractère personnel ainsi que le droit à la liberté d'expression et d'information. La législation nationale peut également prévoir une base juridique pour l'exemption de l'interdiction générale de traiter des catégories particulières de données à caractère personnel, par exemple pour des raisons d'intérêt public important dans le domaine de la santé publique, y compris la protection contre les menaces transfrontières graves pour la santé. En outre, les États membres doivent veiller à l'accréditation des organismes de certification.

La Commission surveille la mise en œuvre du RGPD dans la législation nationale. Au moment de la rédaction du présent rapport, tous les États membres, à l'exception de la Slovénie, ont adopté une nouvelle législation en matière de protection des données ou adapté leur législation dans ce domaine. La Commission a donc demandé à la Slovénie de fournir des éclaircissements sur les progrès accomplis à ce jour et l'a invitée à finaliser ce processus[53].

En outre, la conformité de la législation nationale aux règles de protection des données pour ce qui concerne l'acquis de Schengen est également évaluée dans le cadre du mécanisme d'évaluation de Schengen coordonné par la Commission. La Commission et les États membres évaluent conjointement la manière dont les pays mettent en œuvre et appliquent l'acquis de Schengen dans un certain nombre de domaines; pour ce qui est de la protection des données, cela porte sur des systèmes informatiques à grande échelle tels que le système d'information Schengen et le système d'information Via Information, et inclut le rôle des autorités chargées de la protection des données dans la supervision du traitement des données à caractère personnel au sein de ces systèmes.

Les travaux relatifs à l'adaptation des actes législatifs sectoriels sont toujours en cours au niveau national. À la suite de l'intégration du RGPD dans l'accord sur l'Espace économique européen, son application a été étendue à la Norvège, à l'Islande et au Liechtenstein. Ces pays ont également adopté leur législation nationale en matière de protection des données.

La Commission utilisera tous les outils à sa disposition, y compris les procédures d'infraction, pour veiller à ce que les États membres respectent le RGPD.

Principaux problèmes liés à la mise en œuvre au niveau national

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

Les principaux problèmes recensés à ce jour dans le cadre de l'évaluation en cours de la législation nationale et des échanges bilatéraux avec les États membres sont notamment les suivants:

- restrictions à l'application du RGPD: certains États membres, par exemple, excluent complètement les activités du parlement national;
- les différences dans l'applicabilité de la législation nationale en matière de spécification. Certains États membres subordonnent l'applicabilité de leur législation nationale à l'endroit où les biens ou les services sont offerts, alors que d'autres la font dépendre du lieu d'établissement du responsable du traitement ou du sous-traitant. Cela va à l'encontre de l'objectif d'harmonisation poursuivi par le RGPD;
- les lois nationales qui soulèvent des questions sur la proportionnalité de l'ingérence dans le droit à la protection des données. Par exemple, la Commission a lancé une procédure d'infraction à l'encontre d'un État membre qui avait adopté une législation obligeant les juges à divulguer des informations spécifiques sur leurs activités non professionnelles, ce qui est incompatible avec le droit au respect de la vie privée et le droit à la protection des données à caractère personnel[54];
- l'absence d'organisme indépendant pour la surveillance du traitement des données par les juridictions agissant dans l'exercice de leurs fonctions juridictionnelles[55];
- La législation dans les domaines entièrement réglementés par le RGPD au-delà de la marge prévue pour les spécifications ou les restrictions. Tel est notamment le cas lorsque des dispositions nationales déterminent les conditions d'un traitement fondé sur un intérêt légitime, en prévoyant la mise en balance des intérêts respectifs du responsable du traitement et des personnes concernées, tandis que le RGPD oblige chaque responsable du traitement à procéder à une telle mise en balance individuelle et à se prévaloir de cette base juridique.
- les spécifications et autres exigences que le traitement pour le respect d'une obligation légale ou l'exécution d'une mission de service public (par exemple, pour la vidéosurveillance dans le secteur privé ou pour la vente directe);, ainsi que pour les notions employées dans le RGPD (par exemple, «grande échelle» ou «effacement»).

Certaines de ces questions peuvent être clarifiées par la Cour de justice dans des affaires encore pendantes[56].

Rapprochement du droit à la protection des données à caractère personnel et de la liberté d'expression et d'information

---

[54] Cette procédure d'infraction a trait à la loi polonaise relative au système judiciaire du 20 décembre 2019, qui porte atteinte à l'indépendance des juges et concerne, entre autres, la divulgation de la participation des juges à des activités non professionnelles. https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_772.

[55] Voir l'article 8, paragraphe 3, de la Charte; Article 16 du TFUE; considérant 20 du RGPD.

[56] Par exemple, l'exemption de l'application du RGPD par une commission parlementaire fait actuellement l'objet d'une procédure préjudicielle (C-272/19).

Une question spécifique concerne la mise en œuvre de l'obligation pour les États membres de concilier, par la loi, le droit à la protection des données à caractère personnel avec la liberté d'expression et d'information[57]. Cette question est très complexe, étant donné qu'une évaluation de l'équilibre entre ces droits fondamentaux doit également tenir compte des dispositions et des garanties prévues par la législation relative aux médias et à la presse.

L'évaluation de la législation des États membres montre différentes approches pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information:

- Certains États membres fixent le principe de primauté de la liberté d'expression ou exemptent en principe l'application de chapitres entiers mentionnés à l'article 85, paragraphe 2, du RGPD si le traitement à des fins journalistiques et d'expression académique, artistique et littéraire est en jeu. Dans une certaine mesure, les lois sur les médias prévoient certaines garanties en ce qui concerne les droits des personnes concernées.
- Certains États membres prévoient la primauté de la protection des données à caractère personnel et ne dispensent de l'application des règles en matière de protection des données que dans des situations spécifiques, par exemple lorsqu'une personne ayant un statut public est concernée.
- D'autres États membres prévoient une certaine mise en balance par le législateur et/ou une évaluation au cas par cas en ce qui concerne les dérogations à certaines dispositions du RGPD.

La Commission poursuivra son évaluation de la législation nationale sur la base des exigences de la Charte. Le rapprochement doit être prévu par la loi, respecter le contenu essentiel de ces droits fondamentaux et être proportionnel et nécessaire (article 52, paragraphe 1, de la Charte). Les règles en matière de protection des données ne devraient pas avoir d'incidence sur l'exercice de la liberté d'expression et d'information, notamment en créant un effet dissuasif ou en étant interprétées comme un moyen de faire pression sur les journalistes pour qu'ils divulguent leurs sources.

[57] Article 85 du RGPD.

3.2 Les clauses de spécification facultatives et leurs limites

Le RGPD donne aux États membres la possibilité de préciser davantage son application dans un nombre limité de domaines. Cette marge pour la législation nationale doit être distinguée de l'obligation de mettre en œuvre certaines autres dispositions du RGPD comme indiqué ci-dessus. Les clauses relatives aux spécifications facultatives figurent à l'annexe I.

Les marges pour la législation des États membres sont soumises aux conditions et aux limites fixées par le RGPD et ne permettent pas de mettre en place un régime national parallèle de protection des données[58]. Les États membres sont tenus de modifier ou d'abroger les législations nationales en matière de protection des données, y compris la législation sectorielle présentant des aspects liés à la protection des données.

En outre, la législation relative aux États membres ne doit pas comporter de dispositions qui pourraient créer une certaine confusion en ce qui concerne l'application directe du RGPD. Par conséquent, lorsque le RGPD prévoit des spécifications ou des restrictions de ses règles par la législation d'un État membre, les États membres peuvent intégrer des éléments du RGPD dans leur droit national, dans la mesure nécessaire pour garantir la cohérence et rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent[59].

Les parties prenantes estiment que les États membres devraient s'abstenir de recourir à des clauses de spécification facultatives ou limiter un tel recours, étant donné qu'elles ne contribuent pas à l'harmonisation. Les divergences nationales tant dans la mise en œuvre des lois que dans leur interprétation par les autorités chargées de la protection des données augmentent considérablement le coût du respect de la législation dans l'ensemble de l'UE.

Fragmentation liée à l'utilisation de clauses de spécification facultatives

- Limite d'âge pour le consentement des enfants pour les services de la société de l'information

Un certain nombre d'États membres ont fait usage de la possibilité de prévoir un âge inférieur à 16 ans pour le consentement en ce qui concerne les services de la société de l'information (article 8, paragraphe 1, du RGPD). Alors que neuf États membres appliquent la limite d'âge de 16 ans, huit États membres ont opté pour une limite de 13 ans, six pour une limite de 14 ans et trois pour une limite de 15 ans[60].

Par conséquent, une entreprise fournissant des services de la société de l'information aux mineurs dans toute l'UE doit faire la distinction entre les âges des utilisateurs potentiels, en fonction de l'État membre dans lequel ils résident. Cela est contraire à

---

[58] La notion largement utilisée de «clauses d'ouverture» pour désigner les clauses de spécification est trompeuse, car elle pourrait donner l'impression que les États membres disposent d'une marge de manœuvre au-delà des dispositions du règlement.

[59] Considérant 8 du RGPD.

[60] 13 ans en Belgique, au Danemark, en Estonie, en Finlande, en Lettonie, à Malte, au Portugal et en Suède; 14 ans en Autriche, en Bulgarie, à Chypre, en Espagne, en Italie et en Lituanie; 15 ans en République tchèque, en Grèce et en France; 16 ans en Allemagne, en Croatie, en Hongrie, en Irlande, au Luxembourg, aux Pays-Bas, en Pologne, en Roumanie et en Slovaquie.

l'objectif clé du RGPD, qui est de garantir un niveau égal de protection des personnes et des débouchés commerciaux dans tous les États membres.

Ces différences entraînent des situations dans lesquelles l'État membre dans lequel le responsable du traitement est établi prévoit une autre limite d'âge que celle appliquée dans les États membres dans lesquels les personnes concernées résident.

- Santé et recherche

Lorsqu'elle met en œuvre des dérogations à l'interdiction générale de traiter des catégories particulières de données à caractère personnel[61], la législation des États membres suit différentes approches en ce qui concerne le niveau de spécification et les garanties, y compris à des fins de santé et de recherche. La plupart des États membres ont introduit ou maintenu des conditions supplémentaires pour le traitement des données génétiques, des données biométriques ou des données relatives à la santé. C'est également le cas pour les dérogations relatives aux droits des personnes concernées à des fins de recherche[62], tant en ce qui concerne l'étendue des dérogations que les garanties qui s'y rapportent.

Les futures lignes directrices du comité sur l'utilisation des données à caractère personnel dans le domaine de la recherche scientifique contribueront à une approche harmonisée dans ce domaine. La Commission apportera sa contribution au comité, en particulier en ce qui concerne la recherche dans le domaine de la santé, y compris sous la forme de questions concrètes et d'analyses de scénarios concrets qu'elle a reçus de la part de la communauté des chercheurs. Il serait utile que ces lignes directrices puissent être adoptées avant le lancement du programme-cadre «Horizon Europe» en vue d'harmoniser les pratiques en matière de protection des données et de faciliter le partage des données pour les progrès de la recherche. Des lignes directrices du comité sur le traitement des données à caractère personnel dans le domaine de la santé pourraient également être utiles.

Le RGPD fournit un cadre solide pour la législation nationale dans le domaine de la santé publique et inclut explicitement les menaces transfrontières pour la santé et la surveillance des épidémies et de leur propagation[63], ce qui était pertinent dans le cadre de la lutte contre la pandémie de COVID-19.

Au niveau de l'UE, la Commission a adopté, le 8 avril 2020, une recommandation relative à la boîte à outils pour l'utilisation des technologies et des données dans ce contexte, y compris les applications mobiles et l'utilisation de données de mobilité rendues anonymes[64], et, le 16 avril 2020, des orientations sur les applications soutenant la lutte contre la pandémie en matière de protection des données[65]. Le 19 mars 2020, le comité a publié une déclaration sur le traitement des données dans ce contexte[66], suivie, le 21 avril 2020, de lignes directrices sur le traitement des données à des fins de recherche et sur l'utilisation de données de localisation et d'outils de

---

61 Article 9 du RGPD.

62 Article 89, paragraphe 2, du RGPD.

63 Voir l'article 9, paragraphe 2, point i), du RGPD et le considérant 46.

64 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

65 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417 (08) & from = EN.

66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en.

recherche de contacts dans ce contexte[67]. Ces recommandations et lignes directrices précisent comment les principes et les règles en matière de protection des données à caractère personnel s'appliquent dans le cadre de la lutte contre la pandémie.

- Restrictions étendues des droits des personnes concernées

La plupart des législations nationales en matière de protection des données qui restreignent les droits de la personne concernée ne précisent pas les objectifs d'intérêt général garantis par ces restrictions et/ou ne satisfont pas suffisamment aux conditions et aux garanties prévues à l'article 23, paragraphe 2, du RGPD[68]. Plusieurs États membres ne laissent pas de place à l'évaluation de la proportionnalité ou étendent les restrictions même au-delà du champ d'application de l'article 23, paragraphe 1, du RGPD. Par exemple, certaines législations nationales refusent le droit d'accès, pour des raisons d'effort disproportionné de la part du responsable du traitement, en ce qui concerne les données à caractère personnel stockées sur la base d'une obligation de conservation ou liées à l'exécution de missions de service public, sans limiter cette restriction aux objectifs d'intérêt public général.

- Exigences supplémentaires pour les entreprises

Bien que l'exigence d'un délégué à la protection des données obligatoire repose sur l'approche fondée sur les risques[69], un État membre[70] l'a étendue à un critère quantitatif, en obligeant les entreprises dans lesquelles 20 salariés ou plus prennent part de manière permanente au traitement automatisé de données à caractère personnel à désigner un délégué à la protection des données, indépendamment des risques liés aux activités de traitement[71]. Cette obligation a entraîné des charges supplémentaires.

4 DONNER AUX PERSONNES LES MOYENS DE CONTRÔLER LEURS DONNÉES

Le RGPD confère des droits fondamentaux, en particulier le droit à la protection des données à caractère personnel, mais aussi les autres droits fondamentaux reconnus par la Charte, notamment le respect de la vie privée et familiale, la liberté d'expression et d'information, la non-discrimination, la liberté de pensée, de conscience et de religion, la liberté d'entreprise et le droit à un recours effectif. Ces droits doivent être mis en balance les uns avec les autres, dans le respect du principe de proportionnalité[72].

Le RGPD fournit aux personnes physiques des droits exécutoires, tels que le droit d'accès, de rectification, d'effacement, d'opposition, de portabilité et une transparence accrue. Il confère également aux particuliers le droit d'introduire une

---

67 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

68 Par exemple parce qu'elles se contentent de répéter le libellé de l'article 23, paragraphe 1, du RGPD.

69 Article 37, paragraphe 1, du RGPD.

70 Allemagne.

71 Utilisation de la clause relative à la spécification figurant à l'article 37, paragraphe 4, du RGPD.

72 Voir le considérant 4 du RGPD.

réclamation auprès d'une autorité chargée de la protection des données, y compris par des actions représentatives, et de former un recours juridictionnel.

Les particuliers sont de plus en plus conscients de leurs droits, comme le montrent les résultats de l'enquête Eurobaromètre de juillet 2019[73] et l'enquête menée par l'Agence des droits fondamentaux[74].

Selon l'enquête sur les droits fondamentaux réalisée par l'Agence des droits fondamentaux:

- 69 % de la population âgée de 16 ans et plus dans l'UE a entendu parler du RGPD;
- 71 % des personnes interrogées dans l'UE ont entendu parler de leur autorité nationale de protection des données; ce chiffre est compris entre 90 % pour la République tchèque et 44 % pour la Belgique;
- 60 % des personnes interrogées dans l'UE ont connaissance d'une loi qui leur permet d'accéder à leurs données à caractère personnel détenues par l'administration publique; toutefois, ce pourcentage diminue pour s'établir à 51 % pour les entreprises privées;
- plus d'une personne interrogée sur cinq (23 %) dans l'UE ne souhaite pas partager de données à caractère personnel (comme l'adresse, la nationalité ou la date de naissance) avec l'administration publique, et 41 % ne souhaitent pas partager ces données avec des entreprises privées.

Les particuliers utilisent de plus en plus leur droit de porter plainte auprès des autorités chargées de la protection des données, soit individuellement, soit par des actions représentatives[75]. Seuls quelques États membres ont autorisé les organisations non gouvernementales à lancer des actions sans mandat, conformément à la possibilité offerte par le RGPD. Une fois adoptée, la directive sur les actions représentatives dans le domaine de la protection des intérêts collectifs des consommateurs[76] qui est proposée devrait renforcer également le cadre des actions représentatives dans le domaine de la protection des données.

Plaintes

Le nombre total de plaintes entre mai 2018 et fin novembre 2019, tel qu'il a été signalé par le comité, est d'environ 275 000[77]. Toutefois, ce chiffre devrait être considéré avec beaucoup de prudence, étant donné que la définition d'une plainte n'est pas identique parmi les autorités. Le nombre absolu de plaintes reçues par les autorités chargées de la protection des données[78] est très différent d'un État membre à l'autre. Le plus grand nombre de plaintes a été enregistré en Allemagne (67 000), aux Pays-Bas (37 000), en Espagne et en France (18 000 chacun), en Italie (14 000), en

[73] https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_2956.
[74] Agence des droits fondamentaux de l'Union européenne (FRA) (2020): Enquête sur les droits fondamentaux 2019. Protection des données et technologie. https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.
[75] Article 80 du RGPD.
[76] COM/2018/0184 final - 2018/089 (COD).
[77] Au titre des articles 77 et 80 du RGPD.
[78] Voir la contribution du comité, pages 31 et 32.

Pologne et en Irlande (12 000 chacun). Deux tiers des autorités ont signalé un nombre de plaintes compris entre 600 et 8 000. Les nombres de plaintes les plus faibles ont été enregistrés en Estonie et en Belgique (environ 500), à Malte et en Islande (moins de 200 chacun).

Le nombre de plaintes n'est pas nécessairement corrélé à la taille de la population ou au PIB; il y a, par exemple, près de deux fois plus de plaintes en Allemagne qu'aux Pays-Bas, et quatre fois plus qu'en Espagne et en France.

Les réactions du groupe multipartite montrent que les organisations ont adopté toute une série de mesures pour faciliter l'exercice des droits des personnes concernées, y compris des processus de mise en œuvre qui garantissent l'examen individuel des demandes et une réponse du responsable du traitement, l'utilisation de plusieurs canaux (courrier, adresse électronique spécialisée, site web, etc.), des procédures et des politiques internes mises à jour concernant le traitement interne des demandes en temps voulu, ainsi que la formation du personnel. Certaines entreprises ont mis en place des portails numériques accessibles par l'intermédiaire du site internet de l'entreprise (ou de l'intranet de l'entreprise pour les salariés) afin de faciliter l'exercice des droits par les personnes concernées.

Toutefois, des progrès supplémentaires sont nécessaires en ce qui concerne les points suivants:

- Tous les responsables du traitement ne respectent pas leur obligation de faciliter l'exercice des droits des personnes concernées[79]. Ils doivent veiller à ce que les personnes concernées disposent d'un point de contact effectif auquel elles peuvent expliquer leurs problèmes. Il peut s'agir du délégué à la protection des données, dont les coordonnées doivent être fournies de manière proactive à la personne concernée[80]. Les modalités de contact ne doivent pas se limiter aux courriers électroniques, mais doivent également permettre à la personne concernée de s'adresser au responsable du traitement par d'autres moyens.
- Les particuliers rencontrent toujours des difficultés lorsqu'ils demandent à accéder à leurs données, par exemple auprès de plateformes, de courtiers de données et d'entreprises AdTech.
- Le droit à la portabilité des données n'est pas pleinement exploité. La stratégie européenne pour les données (ci-après dénommée «stratégie en matière de données»)[81], adoptée par la Commission le 19 février 2020, a souligné la nécessité de faciliter toutes les utilisations possibles de ce droit [par exemple en rendant obligatoires les interfaces techniques et les formats lisibles par machine permettant la portabilité des données en temps (quasi) réel]. Les opérateurs font observer qu'il est parfois difficile de fournir les données dans un format structuré, couramment utilisé par machine (en raison de l'absence de norme). Seules les organisations issues de secteurs particuliers, comme le secteur bancaire et les secteurs des télécommunications et des compteurs d'eau et de chauffage, indiquent avoir mis en œuvre les interfaces nécessaires[82]. De nouveaux outils

[79] Article 12, paragraphe 2, du RGPD.
[80] Article 13, paragraphe 1, point b), et article 14, paragraphe 1, point b), du RGPD.
[81] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
[82] Voir le rapport du groupe multipartite.

technologiques ont été mis au point pour faciliter l'exercice, par les particuliers, de leurs droits au titre du RGPD, qui ne se limitent pas à la portabilité des données (par exemple, les espaces de données à caractère personnel et les services de gestion de l'information personnelle).

- Droits des enfants: plusieurs membres du groupe multipartite soulignent la nécessité de fournir des informations aux enfants et le fait que de nombreuses organisations ignorent que les enfants peuvent être concernés par le traitement de leurs données. Le Conseil a souligné qu'une attention particulière pouvait être accordée à la protection des enfants lors de l'élaboration de codes de conduite. La protection des enfants est également une priorité pour les autorités chargées de la protection des données[83].
- Droit à l'information: certaines entreprises adoptent une approche très légaliste en considérant les avis de protection des données comme un exercice juridique, les informations étant relativement complexes, difficiles à comprendre ou incomplètes, alors que le RGPD exige que toute information soit concise et fasse l'objet d'un langage clair et simple[84]. Il semble que certaines entreprises ne suivent pas les recommandations du comité, par exemple en ce qui concerne la liste des noms des entités avec lesquelles elles partagent des données.
- Plusieurs États membres ont largement restreint les droits des personnes concernées en vertu du droit national, et, pour certains, même au-delà des marges de l'article 23 du RGPD.
- L'exercice des droits des personnes est parfois entravé par les pratiques de quelques grands acteurs numériques qui empêchent les particuliers de choisir les paramètres qui protègent le mieux leur vie privée (en violation de l'exigence de protection des données dès la conception et par défaut[85])[86].

Les lignes directrices du comité sur les droits des personnes concernées sont très attendues par les parties prenantes.

---

83 Voir les résultats d'une consultation publique sur les droits de l'enfant en matière de protection des données réalisée par l'autorité irlandaise chargée de la protection des données: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. L'autorité française chargée de la protection des données a également lancé une consultation publique en avril 2020: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique.

84 Article 12, paragraphe 1, du RGPD.

85 Article 25 du RGPD.

86 Voir le rapport du Conseil norvégien de la consommation, «Deceived by Design» (*trompé par la conception*), qui a mis en évidence les «tendances sombres», les paramètres par défaut et les autres caractéristiques et techniques utilisées par les entreprises pour orienter les utilisateurs vers des options intrusives:
https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.
Voir également les recherches publiées en décembre 2019 par le Dialogue transatlantique des consommateurs et la Fondation Heinrich-Böll-Stiftung, qui analysent les pratiques de trois grandes plateformes mondiales:
https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms.

5 OPPORTUNITÉS ET DÉFIS POUR LES ORGANISATIONS, EN PARTICULIER LES PETITES ET MOYENNES ENTREPRISES

Possibilités pour les organisations

Le RGPD encourage la concurrence et l'innovation. Avec le règlement relatif au libre flux des données à caractère non personnel[87], il garantit la libre circulation des données au sein de l'UE et crée des conditions de concurrence équitables avec les entreprises non établies dans l'UE. En créant un cadre harmonisé pour la protection des données à caractère personnel, le RGPD garantit que tous les acteurs du marché intérieur sont liés par les mêmes règles et bénéficient des mêmes possibilités, où qu'ils soient établis et où que le traitement ait lieu. La neutralité technologique du RGPD prévoit le cadre de la protection des données pour les nouvelles évolutions technologiques. Les principes de la protection des données dès la conception et par défaut encouragent l'adoption de solutions innovantes, lesquelles incluent des considérations relatives à la protection des données dès le début de la procédure et peuvent réduire le coût du respect des règles en matière de protection des données.

En outre, le respect de la vie privée devient un paramètre concurrentiel important que les particuliers prennent de plus en plus en considération lors du choix de leurs services. Ceux qui sont mieux informés et sensibles aux considérations relatives à la protection des données recherchent des produits et des services qui garantissent une protection efficace des données à caractère personnel. La mise en œuvre du droit à la portabilité des données est susceptible de réduire les barrières à l'entrée pour les entreprises offrant des services innovants et adaptés à la protection des données. Il convient de surveiller les effets d'une utilisation potentiellement plus large de ce droit sur le marché dans différents secteurs. Le respect des règles en matière de protection des données et leur application transparente permettront de renforcer la confiance à l'égard de l'utilisation des données à caractère personnel de la population et, partant, de proposer de nouvelles possibilités pour les entreprises.

Comme tous les règlements, les règles en matière de protection des données comportent des coûts de mise en conformité inhérents aux entreprises. Toutefois, ces coûts sont contrebalancés par les possibilités et les avantages d'une confiance renforcée dans l'innovation numérique et par les avantages que présente pour les sociétés le respect d'un droit fondamental. En garantissant des conditions de concurrence équitables et en dotant les autorités chargées de la protection des données de ce dont elles ont besoin pour faire appliquer les règles de manière efficace, le RGPD empêche les entreprises non conformes de parasiter la confiance instillée par ceux qui suivent les règles.

Défis spécifiques pour les petites et moyennes entreprises (PME)

Il existe une perception générale par les parties prenantes, mais aussi par le Parlement européen, le Conseil et les autorités chargées de la protection des données, du fait que l'application du RGPD est particulièrement difficile pour les micro, petites et moyennes entreprises, ainsi que pour les petites organisations bénévoles et caritatives.

---

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

Selon une approche fondée sur les risques, il ne serait pas approprié de prévoir des dérogations fondées sur la taille des opérateurs, étant donné que la taille de ces derniers ne constitue pas, en soi, un indicateur des risques que peut supposer, pour les particuliers, le traitement des données à caractère personnel qu'ils effectuent. L'approche fondée sur les risques allie flexibilité et protection effective. Elle tient compte des besoins des PME pour lesquelles le traitement des données ne relève pas de leur activité principale, et calibre leurs obligations notamment en fonction de la probabilité et de la gravité des risques liés au traitement spécifique qu'elles effectuent[88].

Le traitement occasionnel à faible risque ne devrait pas être traité de la même manière qu'un traitement à haut risque et fréquent, indépendamment de la taille de la société qui l'entreprend. Par conséquent, conformément aux conclusions du comité, «en tout état de cause, l'approche fondée sur les risques préconisée par le législateur dans le texte devrait être maintenue, étant donné que les risques pour les personnes concernées ne dépendent pas de la taille des responsables du traitement»[89]. Les autorités chargées de la protection des données devraient pleinement tenir compte de ce principe lors de l'application du RGPD, de préférence dans le cadre d'une approche européenne commune afin de ne pas créer d'obstacles sur le marché unique.

Les autorités chargées de la protection des données ont mis au point plusieurs outils et ont souligné leur intention de les améliorer encore. Certaines autorités ont lancé des campagnes de sensibilisation et organiseront même gratuitement des «cours de RGPD» pour les PME.

Exemples d'orientations et d'outils fournis spécifiquement aux PME par les autorités chargées de la protection des données:

- publication d'informations destinées aux PME;
- séminaires destinés aux délégués à la protection des données et aux manifestations pour les PME qui n'ont pas besoin de désigner un délégué à la protection des données;
- guides interactifs pour aider les PME;
- lignes téléphoniques directes pour les consultations;
- modèles pour le traitement des contrats et les enregistrements relatifs aux activités de traitement.

Le comité fournit dans sa contribution une description des activités menées par les autorités chargées de la protection des données[90].

Plusieurs des actions qui soutiennent spécifiquement les PME ont bénéficié d'un financement de l'UE. La Commission a fourni un soutien financier au moyen de trois vagues de subventions, pour un montant total de 5 millions d'EUR, les deux plus récentes ayant spécifiquement pour objectif de soutenir les autorités nationales chargées de la protection des données dans leurs efforts pour atteindre les particuliers et les PME. En conséquence, en 2018, 2 millions d'EUR ont été alloués à

[88] Article 24, paragraphe 1, du RGPD.
[89] Voir la contribution du comité, p. 35.
[90] Voir la contribution du comité, pages 35 à 45.

neuf autorités chargées de la protection des données pour des activités réalisées en 2018-2019 (la Belgique, la Bulgarie, le Danemark, la Hongrie, la Lituanie, la Lettonie, les Pays-Bas, la Slovénie et l'Islande)[91] et, en 2019, 1 million d'EUR a été alloué à quatre autorités chargées de la protection des données pour des activités menées en 2020 (la Belgique, Malte, la Slovénie et la Croatie en partenariat avec l'Irlande)92. Un million d'EUR supplémentaire sera alloué en 2020.

En dépit de ces initiatives, les PME et les jeunes entreprises déclarent souvent qu'elles ont du mal à appliquer le principe de responsabilité énoncé dans le RGPD[93]. Elles indiquent notamment qu'elles ne reçoivent pas toujours suffisamment d'orientations et de conseils pratiques de la part des autorités nationales chargées de la protection des données ou que le temps nécessaire pour obtenir des orientations et des conseils est trop long. Il y a également eu des cas où les autorités étaient peu enclines à s'engager dans des questions juridiques. Lorsqu'elles sont confrontées à de telles situations, les PME se tournent souvent vers des conseillers et avocats externes pour traiter de la mise en œuvre du principe de responsabilité et de l'approche fondée sur les risques (y compris les exigences en matière de transparence, les dossiers de traitement et les notifications des violations de données). Cela peut également entraîner des coûts supplémentaires pour ces entreprises.

Une question spécifique concerne l'enregistrement des activités de traitement, considéré par les PME et les petites associations comme une lourde charge administrative. L'exemption de cette obligation prévue à l'article 30, paragraphe 5, du RGPD est en effet très réduite. Toutefois, les efforts connexes pour satisfaire à cette obligation ne devraient pas être surestimés. Lorsque les activités principales des PME n'impliquent pas le traitement de données à caractère personnel, ces enregistrements peuvent être simples et non contraignants. Il en va de même pour les associations bénévoles et les autres associations. Ces enregistrements simplifiés seraient facilités par des enregistrements modèles, comme cela est déjà le cas pour certaines autorités chargées de la protection des données. En tout état de cause, quiconque procède au traitement de données à caractère personnel devrait considérer globalement ce traitement comme une exigence fondamentale du principe de responsabilité.

La mise au point par le comité, au niveau de l'UE, d'outils pratiques, tels que des formulaires harmonisés pour les violations de données et des comptes rendus simplifiés des activités de traitement, peut aider les PME et les petites associations[94] dont les activités principales ne sont pas axées sur le traitement des données à caractère personnel à s'acquitter de leurs obligations.

Diverses associations sectorielles ont déployé des efforts pour sensibiliser et informer leurs membres, par exemple au moyen de conférences et de séminaires, en fournissant aux entreprises des informations sur les orientations disponibles ou en élaborant un service d'assistance à la protection de la vie privée pour les membres. Elles font également état d'un nombre croissant de séminaires, de réunions et d'événements

---

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en

93 Voir le rapport du groupe multipartite.

94 Voir la contribution du Conseil.

organisés par des groupes de réflexion et des associations de PME sur des questions liées au RGPD.

Afin de renforcer la libre circulation de toutes les données au sein de l'UE et de mettre en place une application cohérente du RGPD et du règlement sur le libre flux des données à caractère non personnel, la Commission a également publié des orientations pratiques sur les règles régissant le traitement des séries de données mixtes, composées à la fois de données à caractère personnel et de données à caractère non personnel, et ciblant en particulier les PME[95].

Boîte à outils pour les entreprises

Le RGPD prévoit des outils qui contribuent à démontrer la conformité, tels que les codes de conduite, les mécanismes de certification et les clauses contractuelles types.

- Codes de conduite

Le comité a publié des lignes directrices[96] pour aider les «propriétaires de codes» et simplifier la rédaction, la modification ou l'extension des codes, ainsi que pour fournir des orientations pratiques et une assistance dans l'interprétation. Ces lignes directrices précisent également les procédures de soumission, d'approbation et de publication des codes tant au niveau national qu'au niveau de l'UE, en définissant les critères minimaux requis.

Les parties prenantes considèrent les codes de conduite comme des outils très utiles. Bien que de nombreux codes soient mis en œuvre au niveau national, un certain nombre de codes de conduite à l'échelle de l'UE sont actuellement en préparation (par exemple sur les applications de santé mobiles et dans les domaines de la recherche en génomique, de l'informatique en nuage, de la vente directe, de l'assurance et du traitement par des services de prévention et de conseil concernant les enfants)[97]. Les opérateurs estiment que les codes de conduite à l'échelle de l'UE devraient être davantage mis en avant dans la mesure où ils favorisent l'application cohérente du RGPD dans tous les États membres.

Toutefois, les codes de conduite requièrent également du temps et des investissements de la part des opérateurs, tant pour leur développement que pour la mise en place des organes de contrôle indépendants requis. Les représentants des PME soulignent l'importance et l'utilité de codes de conduite adaptés à leur situation et n'entraînant pas de coûts disproportionnés.

Par conséquent, les associations d'entreprises de plusieurs secteurs ont mis en œuvre d'autres types d'instruments d'autorégulation, tels que des codes de bonnes pratiques ou des orientations. Si ces outils peuvent fournir des informations utiles, ils ne sont pas approuvés par les autorités chargées de la protection des données et ne peuvent pas contribuer à démontrer le respect du RGPD.

---

[95] Communication de la Commission au Parlement européen et au Conseil intitulée «Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne», COM/2019/250 final.

[96] https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en.

[97] Voir le rapport du groupe multipartite.

Le Conseil souligne que les codes de conduite doivent accorder une attention particulière au traitement des données relatives aux enfants et des données relatives à la santé. La Commission soutient le ou les codes de conduite qui harmoniseraient l'approche en matière de santé et de recherche et faciliteraient le traitement transfrontière des données à caractère personnel[98]. Le comité est en train d'approuver les projets d'exigences d'agréments pour les organes de contrôle des codes de conduite présentés par plusieurs autorités chargées de la protection des données[99]. Une fois que des codes de conduite transnationaux ou au niveau de l'UE sont prêts à être soumis à l'approbation des autorités chargées de la protection des données, ils font l'objet d'une consultation auprès du comité. La mise en place rapide de codes de conduite transnationaux est particulièrement importante pour les domaines nécessitant le traitement d'importants volumes de données (par exemple, l'informatique en nuage) ou le traitement de données sensibles (par exemple, la santé ou la recherche).

- Certification

La certification peut être un instrument utile pour démontrer le respect des exigences spécifiques du RGPD. Elle peut renforcer la sécurité juridique pour les entreprises et promouvoir le RGPD au niveau mondial.

Comme indiqué dans l'étude sur la certification publiée en avril 2019[100], l'objectif devrait être de faciliter l'adoption des systèmes concernés. L'élaboration de systèmes de certification dans l'UE sera soutenue par les lignes directrices émises par le comité en ce qui concerne les critères de certification[101] et l'accréditation des organismes de certification[102].

La sécurité et la protection des données dès la conception sont des éléments essentiels à prendre en considération dans les systèmes de certification au titre du RGPD. Elles bénéficieraient d'une approche commune et ambitieuse dans l'ensemble de l'UE. La Commission continuera à soutenir les contacts actuels entre l'Agence de l'Union européenne pour la cybersécurité (ENISA), les autorités chargées de la protection des données et le comité.

En ce qui concerne la cybersécurité, à la suite de l'adoption du règlement sur la cybersécurité, la Commission a demandé à l'ENISA d'élaborer deux systèmes de certification comprenant un système pour les services en nuage[103]. D'autres mécanismes portant sur la cybersécurité des services et des produits pour les consommateurs sont à l'étude. Bien que ces systèmes de certification établis en vertu du règlement sur la cybersécurité ne traitent pas explicitement de la protection des données et de la vie privée, ils contribuent à accroître la confiance des consommateurs

---

98 Voir les actions annoncées dans la stratégie européenne pour les données, page 30.

99 Au titre de l'article 41, paragraphe 3, du RGPD. Voir les avis du comité à l'adresse: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_fr.

100 https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en.

101 https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-12018-certification-and-identifying-certification_en.

102 https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en. Plusieurs autorités de contrôle ont déjà soumis leurs exigences d'agrément au comité, tant pour les organes de contrôle des codes de conduite que pour les organismes de certification. Voir l'aperçu fourni à l'adresse suivante: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

103 https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe.

dans les services et produits numériques. Ces systèmes peuvent fournir la preuve du respect des principes de sécurité dès la conception ainsi que de la mise en œuvre des mesures techniques et organisationnelles appropriées liées à la sécurité du traitement des données à caractère personnel.

- Clauses contractuelles types

La Commission travaille actuellement sur des clauses contractuelles types entre les responsables du traitement et les sous-traitants[104], notamment à la lumière de la modernisation des clauses contractuelles types pour les transferts internationaux (voir la section 7.2). Un acte de l'Union, adopté par la Commission, produira des effets contraignants à l'échelle de l'UE, ce qui garantira une harmonisation totale et une sécurité juridique.

6 L'APPLICATION DU RGPD AUX NOUVELLES TECHNOLOGIES

Un cadre technologiquement neutre ouvert aux nouvelles technologies

Le RGPD est technologiquement neutre, crée un climat de confiance et repose sur des principes[105]. Ces principes, notamment le traitement licite et transparent, la limitation des finalités et la minimisation des données, offrent une base solide à la protection des données à caractère personnel, quelles que soient les opérations et techniques de traitement appliquées.

Les membres du groupe multipartite indiquent que, dans l'ensemble, le RGPD a une incidence positive sur le développement de nouvelles technologies et constitue une bonne base pour l'innovation. Le RGPD est considéré comme un outil essentiel et flexible pour garantir le développement de nouvelles technologies dans le respect des droits fondamentaux. La mise en œuvre de ses principes fondamentaux est particulièrement cruciale pour le traitement intensif des données. L'approche fondée sur les risques et la neutralité technologique du RGPD confère un niveau de protection des données adéquat pour faire face aux risques du traitement, y compris par les technologies émergentes.

Plus particulièrement, les parties prenantes indiquent que les principes du RGPD relatifs à la limitation des finalités et à d'autres traitements compatibles, la minimisation des données, la limitation du stockage, la transparence, la responsabilité et les conditions dans lesquelles les processus de prise de décision automatisés[106] peuvent être légalement déployés répondent dans une large mesure aux préoccupations liées à l'utilisation de l'intelligence artificielle.

L'approche adaptée aux besoins futurs et fondée sur les risques prévue par le RGPD sera également appliquée dans l'éventuel futur cadre relatif à l'intelligence artificielle et lors de la mise en œuvre de la stratégie en matière de données. Cette dernière vise à favoriser la disponibilité des données et à créer des espaces européens communs de données, avec le soutien des services fédérés d'infrastructure en nuage. En ce qui

[104] Article 28, paragraphe 7, du RGPD.
[105] Comme rappelé par le Conseil, le Parlement européen et le comité dans leurs contributions à l'évaluation.
[106] Toutefois, ces parties prenantes relèvent que tous les processus décisionnels automatisés dans un contexte d'intelligence artificielle ne relèvent pas de l'article 22 du RGPD.

concerne les données à caractère personnel, le RGPD constitue le cadre juridique principal, dans lequel des solutions efficaces peuvent être élaborées au cas par cas en fonction de la nature et du contenu de chaque espace de données.

Le RGPD accroît la sensibilisation à la protection des données à caractère personnel tant à l'intérieur qu'à l'extérieur de l'UE et a incité les entreprises à adapter leurs pratiques afin de tenir compte des principes de la protection des données lorsqu'elles innovent. Toutefois, les organisations de la société civile notent que, bien que l'incidence du RGPD sur le développement de nouvelles technologies semble positive, les pratiques des principaux acteurs du numérique n'ont pas encore fondamentalement évolué vers un traitement plus respectueux de la vie privée.

La Commission analyse les questions plus vastes liées aux comportements des grands acteurs du numérique sur le marché dans le cadre du paquet relatif aux services numériques[107]. En ce qui concerne la recherche dans le domaine des médias sociaux, la Commission rappelle que le RGPD ne peut être utilisé comme excuse par les plateformes de médias sociaux pour limiter l'accès des chercheurs et des vérificateurs de faits aux données à caractère non personnel, telles que des statistiques sur les types de publicités ciblées adressées à des catégories de personnes données, les critères de ciblage utilisés à cette fin, des informations sur les faux comptes, etc.

L'approche adaptée aux besoins futurs et technologiquement neutre du RGPD a été mise à l'épreuve au cours de la pandémie de COVID-19 et s'est révélée efficace. Ses règles fondées sur les principes ont soutenu la mise au point d'outils destinés à lutter contre la propagation du virus et à en assurer le suivi.

Défis à relever

Le développement et l'application de nouvelles technologies ne remettent pas ces principes en question. Les défis à relever consistent à préciser comment appliquer les principes avérés à l'utilisation de technologies spécifiques telles que l'intelligence artificielle, la chaîne de blocs, l'internet des objets, la reconnaissance faciale ou l'informatique quantique.

Dans ce contexte, le Parlement européen et le Conseil ont souligné la nécessité d'un suivi continu afin de faire le point sur l'application du RGPD aux nouvelles technologies et aux grandes entreprises technologiques. En outre, s'agissant de la question de savoir si le RGPD reste adapté à sa finalité, les parties prenantes attirent l'attention sur le fait que l'évaluation de ce point nécessite également un contrôle permanent.

Les parties prenantes de l'industrie soulignent que l'innovation exige que le RGPD soit appliqué sur la base des principes, conformément à sa conception, et non pas de manière rigide et formelle. Elles sont d'avis que les lignes directrices du comité sur la manière d'appliquer les principes, les concepts et les règles du RGPD aux nouvelles technologies, telles que l'intelligence artificielle, la chaîne de blocs ou l'internet des objets, en tenant compte de l'approche fondée sur les risques, contribueraient à apporter davantage de clarté et une plus grande sécurité juridique. L'emploi de tels outils juridiques non contraignants est idéal pour accompagner l'application du RGPD aux nouvelles technologies, étant donné qu'il en résulte une plus grande sécurité

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

juridique et qu'ils peuvent être revus en fonction des évolutions technologiques. Par ailleurs, certaines parties prenantes sont d'avis que des orientations sectorielles sur la manière d'appliquer le RGPD aux nouvelles technologies pourraient être utiles.

Le comité a indiqué qu'il continuera à examiner l'incidence des technologies émergentes sur la protection des données à caractère personnel.

Les parties prenantes soulignent également l'importance pour les autorités de réglementation d'acquérir une compréhension approfondie de la manière dont la technologie est utilisée et d'engager un dialogue avec l'industrie sur le développement des technologies émergentes. Elles estiment qu'une approche de «sas réglementaire» - en tant que moyen d'obtenir des orientations sur l'application des règles - pourrait constituer une option intéressante pour tester de nouvelles technologies et aider les entreprises à appliquer la protection des données dès la conception et par défaut aux nouvelles technologies.

En ce qui concerne les mesures supplémentaires à prendre, les parties prenantes recommandent que toute future proposition stratégique sur l'intelligence artificielle s'appuie sur les cadres juridiques existants et soit alignée sur le RGPD. Il conviendra d'évaluer soigneusement toute question spécifique éventuelle, sur la base des éléments de preuve pertinents, avant de proposer de nouvelles dispositions prescriptives.

Le livre blanc de la Commission sur l'intelligence artificielle propose un certain nombre d'options stratégiques sur lesquelles parties prenantes ont été invités à donner leur avis jusqu'au 14 juin 2020. En ce qui concerne la reconnaissance faciale, une technologie susceptible d'avoir une incidence significative sur les droits individuels, le livre blanc rappelle le cadre législatif en vigueur et ouvre un débat public sur les circonstances particulières, le cas échéant, qui pourraient justifier le recours à l'intelligence artificielle pour la reconnaissance faciale et à d'autres fins d'identification biométrique à distance dans les lieux publics, ainsi que sur les garanties communes à mettre en place.

7 TRANSFERTS INTERNATIONAUX ET COOPÉRATION MONDIALE

7.1 la protection de la vie privée: un problème mondial

La demande de protection des données à caractère personnel ne connaît pas de frontières, dans la mesure où les individus du monde entier chérissent et apprécient de plus en plus la confidentialité et la sécurité de leurs données.

Dans le même temps, l'importance des flux de données pour les particuliers, les gouvernements, les entreprises et, plus généralement, la société dans son ensemble, est une donnée incontournable dans notre monde interconnecté. Ces flux font partie intégrante du commerce, de la coopération entre les différents pouvoirs publics, et des interactions sociales. À cet égard, l'actuelle pandémie de COVID-19 souligne également l'importance cruciale du transfert et de l'échange de données à caractère personnel pour de nombreuses activités essentielles, y compris la garantie de la continuité des interventions gouvernementales et des opérations commerciales; en effet, ces transferts et échanges permettent le télétravail et la mise en oeuvre d'autres solutions qui dépendent fortement des technologies de l'information et de la communication, développent la coopération dans le domaine de la recherche scientifique sur les diagnostics, les traitements et les vaccins, et permettent de lutter

contre de nouvelles formes de cybercriminalité comme par exemple les systèmes de fraude en ligne proposant des médicaments contrefaits pour prévenir ou guérir la COVID-19.

Dans ce contexte, et plus que jamais, la protection de la vie privée et la facilitation des flux de données doivent aller de pair. Avec son régime de protection des données, qui combine l'ouverture aux transferts internationaux et un niveau élevé de protection individuelle, l'UE est très bien placée pour promouvoir des flux de données sûrs et dignes de confiance. Le RGPD est déjà devenu un point de référence au niveau international et il a agi comme un catalyseur dans de nombreux pays du monde, qu'il a incités à envisager l'introduction de règles modernes en matière de protection de la vie privée.

Il s'agit d'une tendance véritablement mondiale, présente du Chili à la Corée du Sud, du Brésil au Japon, du Kenya à l'Inde, de la Tunisie à l'Indonésie ou de la Californie à Taïwan, pour ne citer que quelques exemples. Ces évolutions sont remarquables, d'un point de vue non seulement quantitatif, mais aussi qualitatif: de nombreuses lois sur la protection de la vie privée récemment adoptées ou en voie d'adoption reposent sur un socle de garanties, de droits et de mécanismes d'exécution communs, partagés par l'UE. Dans un monde trop souvent caractérisé par des approches réglementaires différentes, voire divergentes, cette tendance à une convergence au niveau mondial est une évolution très positive qui offre de nouvelles possibilités de renforcer la protection des personnes en Europe, tout en facilitant dans le même temps les flux de données et en réduisant les coûts de transaction pour les opérateurs économiques.

Pour saisir ces opportunités et mettre en œuvre la stratégie exposée dans sa communication de 2017 intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation»[108], la Commission a considérablement intensifié ses travaux sur la dimension internationale de la protection de la vie privée en exploitant pleinement la «boîte à outils» de transfert disponible, comme expliqué ci-après. Elle a notamment collaboré activement avec les principaux partenaires concernés en vue de parvenir à un «constat d'adéquation», ce qui a permis d'obtenir des résultats importants, tels que la création du plus grand espace au monde de flux de données libres et sûrs entre l'UE et le Japon.

Outre son travail d'adéquation, la Commission a collaboré étroitement avec les autorités chargées de la protection des données au sein du comité, ainsi qu'avec d'autres parties prenantes, afin d'exploiter pleinement le potentiel des règles flexibles du RGPD pour les transferts internationaux. Ce point concerne la modernisation d'instruments tels que les clauses contractuelles types, l'élaboration de systèmes de certification, de codes de conduite ou de dispositions administratives pour les échanges de données entre les pouvoirs publics, ainsi que la clarification de concepts clés concernant, par exemple, le champ d'application territorial des règles de l'UE en matière de protection des données ou le recours à des «dérogations» pour le transfert de données à caractère personnel.

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

Enfin, la Commission a intensifié son dialogue dans un certain nombre de forums bilatéraux, régionaux et multilatéraux afin de promouvoir une culture mondiale du respect de la vie privée et de développer des éléments de convergence entre les différents systèmes de protection de la vie privée. Dans le cadre de ses efforts, la Commission pourrait compter sur le soutien actif du Service européen pour l'action extérieure et du réseau des délégations de l'UE dans les pays tiers et des missions auprès d'organisations internationales. Cela a également permis de garantir une complémentarité accrue entre les différents aspects de la dimension extérieure des politiques de l'UE et de veiller à leur cohérence, dans des domaines comme le commerce ou le nouveau partenariat Afrique-UE.

7.2 La boîte à outils du RGPD en ce qui concerne les transferts

Étant donné que de plus en plus d'opérateurs privés et publics s'appuient sur des flux internationaux de données dans le cadre de leurs opérations de routine, il est de plus en plus nécessaire de disposer d'instruments flexibles pouvant être adaptés à différents secteurs, modèles économiques et situations en matière de transferts. Reflétant ces besoins, le RGPD propose une boîte à outils modernisée qui facilite le transfert de données à caractère personnel de l'UE vers un pays tiers ou une organisation internationale, tout en veillant à ce que les données continuent à bénéficier d'un niveau élevé de protection. Cette continuité de la protection est importante, étant donné que, dans le monde actuel, les données franchissent facilement les frontières et les protections garanties par le RGPD seraient incomplètes si elles se limitaient au traitement à l'intérieur de l'UE.

Avec le chapitre V du RGPD, le législateur a confirmé l'architecture des règles de transfert qui existaient déjà dans le cadre de la directive 95/46: des transferts de données peuvent avoir lieu lorsque la Commission a effectué un constat d'adéquation à l'égard d'un pays tiers ou d'une organisation internationale ou, à défaut, lorsque le responsable du traitement ou le sous-traitant dans l'UE («exportateur de données») a fourni des garanties appropriées, par exemple au moyen d'un contrat avec le destinataire («importateur de données»). En outre, des motifs légaux de transfert («dérogations») restent disponibles pour des situations spécifiques pour lesquelles le législateur a décidé que la mise en balance des intérêts permet un transfert de données sous certaines conditions. Dans le même temps, la réforme a clarifié et simplifié les règles existantes, notamment en fixant en détail les conditions d'un constat d'adéquation ou de règles d'entreprise contraignantes, en limitant les exigences d'autorisation à un nombre très limité de cas particuliers et en supprimant complètement les exigences en matière de notification. En outre, de nouveaux outils de transfert, tels que des codes de conduite ou des systèmes de certification, ont été introduits et les possibilités d'utiliser les instruments existants (par exemple les clauses contractuelles types) ont été étendues.

L'économie numérique d'aujourd'hui permet aux opérateurs étrangers de participer (à distance mais) directement au marché intérieur de l'UE et d'entrer en concurrence pour décrocher des clients européens et accéder à leurs données à caractère personnel. Lorsqu'ils ciblent spécifiquement des clients européens par l'offre de biens ou de services ou le suivi de leur comportement, ils devraient se conformer au droit de l'Union de la même manière que les opérateurs de l'UE. C'est ce qui ressort de l'article 3 du RGPD, qui étend l'applicabilité directe des règles de l'UE en matière de

protection des données à certaines opérations de traitement des responsables du traitement et des sous-traitants en dehors de l'UE. Les garanties nécessaires sont ainsi assurées, de même qu'une égalité des conditions de concurrence pour toutes les entreprises opérant sur le marché de l'UE.

Sa grande portée est l'une des raisons pour lesquelles le RGPD a également produit des effets dans d'autres régions du monde. Les lignes directrices détaillées publiées par le comité sur la portée territoriale du RGPD, à la suite d'une consultation publique approfondie, sont donc importantes pour aider les opérateurs étrangers à déterminer quelles activités de traitement sont directement soumises aux garanties fournies par le RGPD, le cas échéant, notamment grâce à l'apport d'exemples concrets[109].

Toutefois, l'extension du champ d'application du droit de l'Union en matière de protection des données ne suffit pas, en soi, à garantir son respect dans la pratique. Comme l'a également souligné le Conseil[110], il est essentiel de veiller à ce que les opérateurs étrangers respectent leurs obligations et à ce qu'ils appliquent effectivement le règlement. La désignation d'un représentant dans l'Union (article 27, paragraphes 1 et 2, du RGPD), auquel peuvent s'adresser les particuliers et les autorités de contrôle en plus ou à la place de la société responsable agissant depuis l'étranger[111], devrait jouer un rôle essentiel à cet égard. Cette approche, qui est également de plus en plus souvent adoptée dans d'autres contextes[112], devrait être suivie plus rigoureusement afin d'envoyer un message clair selon lequel le fait qu'ils ne soient pas établis dans l'UE ne dispense pas les opérateurs étrangers des responsabilités qui leur incombent en vertu du RGPD. Lorsque ces opérateurs ne satisfont pas à l'obligation qui leur incombe de désigner un représentant[113], les autorités de contrôle devraient faire usage de toute la panoplie d'outils de mise en œuvre visée à l'article 58 du RGPD (par exemple, avertissement public, interdiction temporaire ou définitive de traitement dans l'UE, mesure d'exécution contre des responsables conjoints du traitement établis dans l'UE).

---

[109] Comité européen de la protection des données, lignes directrices 2/2018 relatives au champ d'application territorial du RGPD, 12.11.2019. Les lignes directrices abordent plusieurs points soulevés lors de la consultation publique, par exemple l'interprétation des critères de ciblage et de suivi.

[110] Voir position et conclusions du Conseil, points 34, 35 et 38.

[111] Voir l'article 27, paragraphe 4, et le considérant 80 du RGPD («Le représentant désigné devrait faire l'objet de procédures coercitives en cas de non-respect du présent règlement par le responsable du traitement ou le sous-traitant»).

[112] Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale (COM/2018/226 final), article 3; Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne [COM(2018) 640 final], article 16, paragraphes 2 et 3.

[113] D'après une des contributions à la consultation publique, l'une des principales questions qu'il convient d'aborder «est le respect effectif de cette exigence et les conséquences réelles de sa non-observation pour ceux qui ont choisi de ne pas en tenir compte [...] Il convient de garder à l'esprit, en particulier, que cela place par ailleurs les entreprises établies dans l'Union dans une position concurrentielle désavantageuse par rapport aux entreprises en infraction établies en dehors de l'Union et faisant du commerce dans l'Union». Voir *EU Business Partners*, contribution du 29 avril 2020.

Enfin, il est très important que le comité achève ses travaux visant à apporter un éclairage supplémentaire sur le lien entre l'article 3 relatif à l'application directe du RGPD et les règles relatives aux transferts internationaux figurant au chapitre V[114].

Décisions d'adéquation

Les contributions reçues des parties prenantes confirment que les décisions d'adéquation demeurent un outil essentiel pour permettre aux opérateurs de l'UE de transférer en toute sécurité des données à caractère personnel vers des pays tiers[115]. Ces décisions constituent la solution la plus complète, la plus simple et la plus efficace au regard des coûts pour les transferts de données, étant donné que ces transferts sont dès lors assimilés à des transmissions à l'intérieur de l'UE, ce qui garantit la circulation libre et sécurisée des données à caractère personnel sans autres conditions ni nécessité d'autorisation. Les décisions d'adéquation ouvrent donc des canaux commerciaux aux opérateurs de l'UE et facilitent la coopération entre les autorités publiques, tout en offrant un accès privilégié au marché unique de l'UE. Le RGPD, qui s'appuie sur les pratiques visées à la directive de 1995, prévoit explicitement une évaluation du caractère adéquat de la protection offerte sur un territoire particulier d'un pays tiers ou dans un secteur particulier d'un pays tiers (l'«adéquation partielle»).

Le RGPD s'appuie sur l'expérience des dernières années et sur les clarifications apportées par la Cour de justice en établissant un catalogue détaillé des éléments que la Commission doit prendre en compte dans son évaluation. La norme d'adéquation exige un niveau de protection comparable (ou «substantiellement équivalent») à celui qui est garanti au sein de l'UE[116]. Elle prévoit une évaluation complète du système du pays tiers dans son ensemble, y compris du contenu des mesures de protection de la vie privée, de leur transposition et respect effectifs, ainsi que des règles relatives à l'accès aux données à caractère personnel par les pouvoirs publics, en particulier à des fins répressives et de sécurité nationale[117].

Cela ressort également des orientations adoptées par l'ancien groupe de travail «article 29» (et approuvées par le comité), en particulier les «critères de référence pour l'adéquation», qui clarifient plus avant les éléments que la Commission doit prendre en considération lorsqu'elle procède à une évaluation de l'adéquation, y compris en fournissant une vue d'ensemble des «garanties essentielles» en ce qui

---

[114] Plusieurs contributions à la consultation publique ont soulevé ce point, par exemple en ce qui concerne la transmission de données à caractère personnel à des destinataires situés en dehors de l'UE mais couverts par le RGPD.

[115] Position et conclusions du Conseil, point 17; contribution du comité, p. 5 et 6. Plusieurs contributions à la consultation publique, y compris de plusieurs associations d'entreprises [telles que l'Association française des entreprises privées, l'Europe numérique (Digital Europe), la Global Data Alliance/BSA, la Computer & Communication Industry Association (CCIA) ou la Chambre de commerce des États-Unis] ont appelé à intensifier les travaux sur les constats d'adéquation, en particulier avec les grands partenaires commerciaux.

[116] Arrêt de la Cour de justice du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner (ci-après l'arrêt «Schrems»), points 73, 74 et 96. Voir également le considérant 104 du RGPD, qui fait référence à la norme de l'équivalence essentielle.

[117] Article 45, paragraphe 2, et considérant 104 du RGPD. Voir également arrêt Schrems, points 75, 91-91.

concerne l'accès des autorités publiques aux données à caractère personnel[118]. Ce dernier se fonde notamment sur la jurisprudence de la Cour européenne des droits de l'homme. Si la norme de l'«équivalence essentielle» n'exige pas une reproduction à l'identique («photocopie») des règles de l'UE, étant donné que les moyens de garantir un niveau de protection comparable peuvent varier selon les différents systèmes de protection de la vie privée, qui reflètent souvent différentes traditions juridiques, elle exige néanmoins un niveau élevé de protection.

Cette norme se justifie par le fait qu'essentiellement, une décision d'adéquation étend à un pays tiers les avantages du marché unique en ce qui concerne la libre circulation des données. Toutefois, cela signifie également qu'il y aura parfois un écart important entre le niveau de protection garanti dans le pays tiers en question et le RGPD, qu'il est nécessaire de combler, par exemple par la négociation de garanties supplémentaires. Ces garanties devraient être perçues de manière positive dans la mesure où elles renforcent encore les protections offertes aux particuliers dans l'UE. Dans le même temps, la Commission partage l'avis du comité sur l'importance d'une surveillance permanente de leur application dans la pratique, y compris en ce qui concerne l'application effective par l'autorité de protection des données du pays tiers[119].

Il est précisé dans le RGPD que les décisions d'adéquation sont des «instruments vivants» qui devraient faire l'objet d'un suivi continu et d'un réexamen périodique[120]. Conformément à ces exigences, la Commission communique régulièrement avec les autorités compétentes afin d'assurer un suivi proactif des dernières évolutions en la matière. Ainsi, depuis l'adoption de la décision sur le bouclier de protection des données UE-États-Unis en 2016[121], la Commission, conjointement avec des représentants du comité, a procédé à trois examens annuels afin d'évaluer tous les aspects du fonctionnement du cadre[122]. Ces examens reposaient sur des informations

---

[118] Critères de référence pour l'adéquation, WP 254 rév. 01, 6 février 2018 (disponible à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Contribution du comité, p. 5 et 6.

[120] L'article 45, paragraphes 4 et 5, du RGPD impose à la Commission de suivre, de manière permanente, les évolutions dans les pays tiers et de réexaminer régulièrement, au moins tous les quatre ans, un constat d'adéquation. Il donne également à la Commission le pouvoir d'abroger, de modifier ou de suspendre une décision d'adéquation si elle constate que le pays ou l'organisation internationale concerné n'offre plus un niveau de protection adéquat. L'article 97, paragraphe 2, point a), du RGPD dispose en outre que la Commission doit présenter un rapport d'évaluation au Parlement européen et au Conseil d'ici 2020. Voir également l'arrêt de la Cour du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner, point 76.

[121] Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, Cette décision d'adéquation est un cas particulier qui, en l'absence de législation générale en matière de protection des données aux États-Unis, se fonde sur les engagements pris par les entreprises participantes (qui sont exécutoires en vertu du droit américain) d'appliquer les normes de protection des données énoncées dans ce dispositif. En outre, le bouclier de protection s'appuie sur les déclarations et les garanties spécifiques formulées par le gouvernement américain en ce qui concerne l'accès aux données à des fins de sécurité nationale, qui étayent le constat d'adéquation

[122] Les examens ont eu lieu en 2017 [rapport de la Commission au Parlement européen et au Conseil sur le premier examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis, COM (2018) 611 final], 2018 [rapport de la Commission au Parlement européen et au Conseil sur le deuxième examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis, COM (2018) 860 final] et 2019 [rapport de la Commission au Parlement européen et au

obtenues au moyen d'échanges avec les autorités américaines, ainsi que sur des contributions d'autres parties prenantes, telles que les autorités de l'UE chargées de la protection des données, la société civile et les associations professionnelles. Ils ont permis d'améliorer le fonctionnement pratique de différents éléments du cadre. Dans une perspective plus large, les examens annuels ont contribué à la mise en place d'un dialogue plus large avec l'administration américaine sur la protection de la vie privée en général, ainsi que sur les limitations et garanties relatives à la sécurité nationale en particulier.

Dans le cadre de sa première évaluation du RGPD, la Commission est également tenue de réexaminer les décisions d'adéquation adoptées en vertu de la directive de 1995[123] Les services de la Commission ont engagé un dialogue approfondi avec chacun des 11 pays et territoires concernés afin d'évaluer la manière dont leurs systèmes de protection des données à caractère personnel ont évolué depuis l'adoption de la décision d'adéquation et de déterminer s'ils satisfont à la norme fixée par le RGPD. La nécessité de veiller à la continuité de ces décisions, étant donné qu'elles constituent un outil essentiel pour le commerce et la coopération internationale, est l'un des facteurs qui ont amené plusieurs de ces pays et territoires à moderniser et à renforcer leur législation en matière de protection de la vie privée. Ces évolutions sont évidemment bienvenues. Des garanties supplémentaires sont en cours de discussion avec certains de ces pays et territoires en vue de faire face aux différences en matière de protection qu'il convient de prendre en considération.

Toutefois, étant donné que, dans un arrêt qui sera rendu le 16 juillet, la Cour de justice pourrait apporter des éclaircissements présentant un intérêt pour certains éléments du principe d'adéquation, la Commission rendra compte séparément de l'évaluation des 11 décisions d'adéquation mentionnées après que la Cour aura rendu son arrêt dans cette affaire[124].

En mettant en œuvre la stratégie définie dans sa communication de 2017 intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», la Commission s'est également engagée dans de nouveaux dialogues en matière d'adéquation[125]. Ces travaux ont déjà permis d'obtenir des résultats significatifs avec

---

Conseil sur le troisième examen annuel du fonctionnement du bouclier de protection des données UE-États-Unis, COM (2019) 495 final].

[123] Ces décisions d'adéquation existantes concernent des pays qui sont étroitement associés à l'Union européenne et à ses États membres (Suisse, Andorre, Îles Féroé, Guernesey, Jersey, Île de Man), des partenaires commerciaux importants (par exemple, l'Argentine, le Canada, Israël) et des pays qui ont joué un rôle de pionnier dans l'élaboration d'une législation en matière de protection des données dans leur région (Nouvelle-Zélande, Uruguay).

[124] L'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems («Schrems II»), porte sur une demande de décision préjudicielle concernant les clauses contractuelles types. Toutefois, certains éléments de la norme d'adéquation peuvent également être clarifiés plus avant par la Cour. L'audience dans cette affaire a eu lieu le 9 juillet 2019 et l'arrêt a été annoncé pour le 16 juillet 2020.

[125] Voir note de bas de page 109 supra. La Commission a expliqué que les critères suivants seront pris en compte pour évaluer avec quels pays tiers un dialogue sur l'adéquation devrait être poursuivi: i) l'étendue des relations commerciales (existantes ou potentielles) de l'UE avec un pays tiers donné, y compris l'existence d'un accord de libre-échange ou des négociations en cours; ii) l'étendue des flux de données à caractère personnel provenant de l'UE, preuve de liens géographiques et/ou culturels; iii) le rôle précurseur du pays tiers dans le domaine de la protection de la vie privée et des données, qui peut servir de modèle pour d'autres pays de sa région, et iv) la

la participation de partenaires clés de l'UE. En janvier 2019, la Commission a adopté sa décision d'adéquation concernant le Japon, qui repose sur un degré élevé de convergence, notamment grâce à des garanties spécifiques (dans le domaine de transferts ultérieurs, par exemple) et à la création d'un mécanisme permettant d'enquêter sur les plaintes de particuliers concernant l'accès des pouvoirs publics aux données à caractère personnel à des fins répressives et de sécurité nationale et d'y répondre.

En tant que premier constat d'adéquation adopté au titre du RGPD, le cadre convenu avec le Japon constitue un précédent utile pour de futures décisions[126]. Cela inclut une réciprocité du côté japonais avec un constat d'«adéquation» pour l'UE. Ensemble, ces constats d'adéquation mutuelle créent le plus grand espace au monde de flux de données à caractère personnel libres et sécurisés et complètent ainsi l'accord de partenariat économique UE-Japon. Dans les faits, l'accord soutient chaque année quelque 124 milliards d'euros d'échanges de biens et 42,5 milliards d'euros d'échanges de services.

Le processus d'adéquation est également à un stade avancé avec la Corée du Sud. Un résultat significatif de ce processus est la récente réforme législative de la Corée du Sud, qui a conduit à la mise en place d'une autorité indépendante chargée de la protection des données dotée d'importants pouvoirs d'exécution. Cela illustre la manière dont un dialogue sur l'adéquation peut contribuer à accroître la convergence entre les règles de l'UE en matière de protection des données et celles d'un pays étranger.

La Commission souscrit pleinement à l'appel lancé par les parties prenantes en vue d'intensifier le dialogue avec certains pays tiers en vue d'éventuels nouveaux constats d'adéquation[127]. Elle explore activement cette possibilité avec d'autres partenaires importants en Asie, en Amérique latine et dans les pays du voisinage, en s'appuyant sur la tendance actuelle à une convergence mondiale accrue en matière de normes de protection des données. Ainsi, une législation détaillée en matière de protection de la vie privée a été adoptée ou est à un stade avancé du processus législatif en Amérique latine (Brésil, Chili), et des avancées prometteuses ont lieu en Asie (par exemple, en Inde, en Indonésie, en Malaisie, au Sri Lanka, à Taïwan et en Thaïlande), en Afrique (par exemple, en Éthiopie, au Kenya) ainsi que dans le voisinage oriental et méridional de l'Europe (par exemple en Géorgie et en Tunisie). Dans la mesure du possible, la Commission s'efforcera de parvenir à des décisions globales d'adéquation couvrant à la fois le secteur privé et le secteur public[128].

---

relation politique globale avec le pays, notamment en ce qui concerne la promotion de valeurs communes et d'objectifs partagés au niveau international.

[126] Résolution du Parlement européen du 13 décembre 2018 sur l'adéquation de la protection des données à caractère personnel assurée par le Japon [2018/2979(RSP)], point 27; contribution du comité, p. 5 et 6.

[127] Voir, par exemple, résolution du Parlement européen du 12 décembre 2017, intitulée «Vers une stratégie pour le commerce numérique» [2017/2065 (INI)], points 8 et 9; position et conclusions du Conseil relatives à l'application du règlement général sur la protection des données (RGPD), 19.12.2019 (14994/1/19), point 17; contribution du comité, p. 5 et 6.

[128] Comme demandé également par le Conseil, voir position et conclusions du Conseil relatives à l'application du règlement général sur la protection des données (RGPD), 19.12.2019 (14994/1/19),

En outre, le RGPD a également introduit la possibilité pour la Commission de faire des constats d'adéquation pour les organisations internationales. À l'heure où certaines organisations internationales modernisent leurs régimes de protection des données en mettant en place des règles détaillées, ainsi que des mécanismes garantissant une surveillance et des recours indépendants, cette piste pourrait être explorée pour la première fois.

L'adéquation joue également un rôle important dans le contexte des relations avec le Royaume-Uni à la suite du Brexit, sous réserve du respect des conditions applicables. Elle constitue un facteur favorisant les échanges, y compris dans le contexte du commerce numérique, et constitue une condition préalable essentielle à une coopération étroite et ambitieuse dans le domaine répressif et dans celui de la sécurité[129]. En outre, étant donné l'importance des flux de données avec le Royaume-Uni et la proximité du pays avec le marché de l'Union, un degré élevé de convergence entre les règles en matière de protection des données de part et d'autre de la Manche constitue un élément important pour garantir une égalité des conditions de concurrence. Conformément à la déclaration politique sur les relations futures entre l'UE et le Royaume-Uni, la Commission procède actuellement à une évaluation de l'adéquation au regard du RGPD et de la directive en matière de protection des données dans le domaine répressif[130]. Compte tenu de la nature autonome et unilatérale d'une évaluation de l'adéquation, ces discussions suivent une voie distincte de celle des négociations portant sur un accord sur les relations futures entre l'UE et le Royaume-Uni.

Enfin, la Commission se félicite que d'autres pays mettent en place des mécanismes de transfert de données similaires à un constat d'adéquation. Ce faisant, ils considèrent souvent l'UE et les pays pour lesquels la Commission a adopté une décision d'adéquation comme des destinations sûres pour les transferts[131]. Le nombre croissant de pays bénéficiant de décisions d'adéquation de l'Union, d'une part, et cette forme de reconnaissance par d'autres pays, d'autre part, ont le potentiel de créer un réseau de pays au sein duquel les données peuvent circuler librement et en toute sécurité. La Commission considère qu'il s'agit là d'une évolution positive qui augmentera encore les avantages d'une décision d'adéquation pour les pays tiers et contribuera à la convergence au niveau mondial. Ce type de synergies peut également contribuer utilement à la mise en place de cadres pour la circulation libre et sécurisée des données, notamment dans le cadre de l'initiative du «libre flux de données en toute confiance» (voir ci-dessous).

---

points 17 et 40. Cela suppose toutefois que les conditions nécessaires à un constat d'adéquation concernant les transferts de données aux autorités publiques soient remplies, y compris en ce qui concerne une supervision indépendante.

[129] Voir les directives de négociation annexées à la décision du Conseil autorisant l'ouverture de négociations en vue d'un nouveau partenariat avec le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (ST 5870/20 ADD 1 REV 3), points 13 et 118.

[130] Voir la version révisée du texte de la déclaration politique fixant le cadre des relations futures entre l'Union européenne et le Royaume-Uni, tel qu'il a été convenu au niveau des négociateurs le 17 octobre 2019, points 8 à 10 (disponible à l'adresse suivante: https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] Par exemple, par l'Argentine, la Colombie, Israël, la Suisse ou l'Uruguay.

Garanties appropriées

Le RGPD prévoit un certain nombre d'autres instruments de transfert au-delà de la solution globale d'un constat d'adéquation. La flexibilité de cette «boîte à outils» est démontrée à l'article 46 du RGPD, qui subordonne les transferts de données à l'existence de «garanties appropriées», notamment à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. Pour assurer des garanties appropriées, différents instruments sont disponibles afin de répondre aux besoins de transfert tant des opérateurs commerciaux que des organismes publics.

- Clauses contractuelles types (CCT)

Le premier groupe de ces instruments concerne les instruments contractuels, qui peuvent être soit des clauses de protection des données sur mesure, ad hoc, convenues entre un exportateur de données de l'UE et un importateur de données se trouvant à l'extérieur de l'UE autorisé par l'autorité compétente en matière de protection des données [article 46, paragraphe 3, point a), du RGPD], soit des clauses types préalablement approuvées par la Commission [article 46, paragraphe 2, points c) et d), du RGPD[132]]. Les plus importants de ces instruments sont les «clauses contractuelles types (CCT)», c'est-à-dire des clauses de protection des données types que l'exportateur de données et l'importateur de données peuvent intégrer dans leurs dispositions contractuelles (par exemple, un contrat de services requérant le transfert de données à caractère personnel) sur une base volontaire et qui fixent les exigences relatives aux garanties appropriées.

Les CCT représentent de loin le mécanisme de transfert de données le plus largement utilisé[133]. Des milliers de sociétés de l'UE s'appuient sur les CCT pour fournir un large éventail de services à leurs clients, fournisseurs, partenaires et employés, y compris les services essentiels au fonctionnement de l'économie. Leur large utilisation indique que les CCT sont très utiles aux entreprises dans leurs efforts de mise en conformité et qu'elles bénéficient tout particulièrement aux entreprises qui ne disposent pas des ressources nécessaires pour négocier des contrats individuels avec chacun de leurs partenaires commerciaux. Grâce à leur caractère standard et à l'autorisation préalable qui y est liée, les CCT fournissent aux entreprises un outil facile à mettre en œuvre pour satisfaire aux exigences en matière de protection des données dans un contexte de transferts.

---

[132] Les clauses contractuelles types (CCT) pour les transferts internationaux requièrent toujours l'approbation de la Commission, mais peuvent être élaborées soit par la Commission elle-même, soit par une autorité nationale de protection des données. Toutes les CCT existantes relèvent de la première catégorie.

[133] D'après le rapport annuel 2019 de l'IAPP et d'EY sur la gouvernance de la protection de la vie privée, les plus populaires de ces outils [de transfert] — année après année — sont, de loin, les contrats contractuels classiques: 88 % des personnes interrogées dans le cadre de l'enquête de cette année ont déclaré que les CCT étaient leur méthode de prédilection pour les transferts extraterritoriaux de données, suivies du dispositif du bouclier de protection des données UE-États-Unis (60 %). S'agisssant des répondants qui transfèrent des données de l'UE vers le Royaume-Uni (52 %), 91 % d'entre eux déclarent qu'ils ont l'intention d'utiliser les CCT pour garantir le respect de leurs obligations en matière de transfert de données après le Brexit.

Les séries de CCT existantes[134] ont été adoptées et approuvées sur la base de la directive de 1995. Ces CCT restent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées, si nécessaire, par une décision de la Commission (article 46, paragraphe 5, du RGPD). Le RGPD élargit les possibilités d'utilisation des CCT tant au sein de l'UE que pour les transferts internationaux. La Commission collabore avec les parties prenantes pour faire usage de ces possibilités et pour mettre à jour les clauses existantes[135]. Afin de veiller à ce que la conception future des CCT soit adaptée à leur finalité, la Commission a recueilli les avis des parties prenantes sur leur expérience avec les CCT, par l'intermédiaire du «groupe multipartite sur le RGPD» et d'un atelier consacré à cette question organisé en septembre 2019, mais aussi par l'intermédiaire de multiples contacts avec des sociétés utilisant des CCT, ainsi que des organisations de la société civile. Par ailleurs, le comité met à jour un certain nombre de lignes directrices qui pourraient être pertinentes pour le réexamen des CCT, par exemple sur les notions de responsable du traitement et de sous-traitant.

En s'appuyant sur les retours d'information reçus, les services de la Commission travaillent actuellement à la révision des CCT. Dans ce contexte, un certain nombre de domaines à améliorer ont été recensés, notamment en ce qui concerne les aspects suivants:

1. Mettre à jour les CCT à la lumière des nouvelles exigences introduites par le RGPD, telles que celles concernant la relation entre le responsable du traitement et le sous-traitant au titre de l'article 28 du RGPD (en particulier les obligations du sous-traitant), les obligations en matière de transparence de l'importateur des données (en ce qui concerne les informations nécessaires à fournir à la personne concernée), etc.
2. Se pencher sur un certain nombre de scénarios de transfert qui ne sont pas couverts par les CCT actuelles, tels que le transfert de données d'un sous-traitant de l'UE vers un (sous-)sous-traitant non européen, mais aussi, par exemple, les situations dans lesquelles le responsable du traitement est situé en dehors de l'UE[136].
3. Mieux refléter les réalités des opérations de traitement des données dans l'économie numérique moderne, où ces opérations impliquent souvent de multiples importateurs et exportateurs de données, des chaînes de traitement

[134] Il existe actuellement trois séries de clauses contractuelles types adoptées par la Commission pour le transfert de données à caractère personnel vers des pays tiers: deux pour les transferts d'un contrôleur de l'EEE vers un contrôleur établi en dehors de l'EEE et une autre pour les transferts effectués par un contrôleur de l'EEE vers un sous-traitant non établi dans l'EEE. Elles ont été modifiées en 2016, à la suite de l'arrêt de la Cour de justice dans l'affaire Schrems I (C-362/14), afin de supprimer toute restriction imposée aux autorités de contrôle compétentes dans l'exercice de leur pouvoir de surveillance des transferts de données. Voir https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[135] Voir aussi contribution du comité, p. 6 et 7. De même, le Conseil a invité la Commission à «réexaminer et à réviser [les CCT] dans un avenir proche afin de tenir compte des besoins des responsables du traitement et des sous-traitants». Voir position et conclusions du Conseil.

[136] Plusieurs contributions à la consultation publique ont fait état de ce dernier scénario, qui soulève souvent des inquiétudes quant au fait qu'exiger des sous-traitants de l'UE qu'ils assurent des garanties appropriées dans le cadre de leurs relations avec les contrôleurs de pays tiers pourrait les placer dans une situation de désavantage concurrentiel vis-à-vis des sous-traitants étrangers offrant des services similaires.

longues et souvent complexes, l'évolution des relations d'affaires, etc. Afin de faire face à de telles situations, les solutions envisagées sont, par exemple, la possibilité de permettre la signature de CCT par de multiples parties ou l'adhésion de nouvelles parties tout au long de la durée du contrat.

En abordant ces points, la Commission étudie également les moyens de rendre l'«architecture» actuelle des CCT plus conviviale, par exemple en remplaçant les multiples séries de CCT par un unique document exhaustif. Le défi consiste à trouver un juste équilibre entre, d'une part, le besoin de clarté et d'un certain degré de normalisation et, d'autre part, la souplesse nécessaire qui permettra l'utilisation des clauses par un certain nombre d'opérateurs ayant des exigences différentes, dans des contextes différents et pour différents types de transferts.

Un autre aspect important à prendre en considération est la possible nécessité, à la lumière des litiges en cours devant la Cour de justice[137], de clarifier davantage les garanties relatives à l'accès des autorités publiques étrangères aux données transférées sur la base des CCT, en particulier à des fins de sécurité nationale. Il peut s'agir d'exiger de l'importateur de données ou de l'exportateur de données, ou des deux, qu'ils prennent des mesures, et clarifient le rôle des autorités chargées de la protection des données dans ce contexte. Bien que la révision des CCT soit en bonne voie, il sera nécessaire d'attendre l'arrêt de la Cour pour intégrer toute exigence supplémentaire éventuelle dans les clauses révisées, avant qu'un projet de décision concernant un nouvel ensemble de CCT puisse être soumis au comité pour avis, puis proposé pour adoption selon la «procédure de comitologie»[138].

Parallèlement, la Commission est en contact avec des partenaires internationaux qui développent des outils similaires[139]. Ce dialogue, qui permet un échange d'expériences et de bonnes pratiques, pourrait contribuer de manière significative à développer davantage la convergence «sur le terrain» et faciliter ainsi le respect des règles en matière de transferts transfrontières pour les entreprises opérant dans différentes régions du monde.

- Règles d'entreprise contraignantes (REC)

Les règles d'entreprise contraignantes constituent un autre instrument important. Il s'agit de politiques et de dispositifs juridiquement contraignants qui s'appliquent aux membres d'un groupe d'entreprises, y compris à leurs salariés [article 46, paragraphe 2, point b), et article 47 du RGPD]. L'utilisation de REC permet donc de

[137] Voir arrêt Schrems II.

[138] Conformément à l'article 46, paragraphe 2, point c), du RGPD, les clauses contractuelles types doivent être adoptées en conformité avec la procédure d'examen visée à l'article 5 du règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13-18). Il peut notamment s'agir d'une décision favorable d'un comité composé de représentants des États membres.

[139] Cela inclut, par exemple, les travaux actuellement menés par les États membres de l'ASEAN pour développer des «clauses contractuelles types ASEAN». Voir ASEAN, Approches clés pour le mécanisme des flux de données transfrontières de l'ASEAN (disponible à l'adresse suivante: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

faire circuler les données à caractère personnel librement entre les diverses entités d'un groupe partout dans le monde en les dispensant de l'obligation de passer des accords contractuels entre elles, tout en garantissant que le même niveau élevé de protection de données à caractère personnel est respecté dans l'ensemble du groupe. Elles offrent une solution particulièrement satisfaisante pour les groupes d'entreprises complexes et de grande taille et pour une coopération étroite entre les entreprises échangeant des données dans plusieurs juridictions. Contrairement à ce qui est le cas pour la directive de 1995, en vertu du RGPD, les REC peuvent être utilisées par un groupe d'entreprises exerçant une activité économique conjointe, mais qui ne font pas partie du même groupe d'entreprises.

Sur le plan procédural, les REC doivent être approuvées par les autorités compétentes en matière de protection des données, sur la base d'un avis non contraignant émis par le comité[140]. Pour orienter ce processus, le comité a examiné les «référentiels» des REC (énonçant des normes de fond) pour les responsables du traitement[141] et les sous-traitants[142] à la lumière du RGPD et il continue de mettre ces documents à jour sur la base de l'expérience pratique acquise par les autorités de contrôle. Il a également adopté plusieurs documents d'orientation pour aider les demandeurs et rationaliser le processus de demande et d'approbation des REC[143]. Selon le comité, plus de 40 REC sont actuellement en attente d'approbation et la moitié d'entre elles devraient être approuvées d'ici la fin de 2020[144]. Il est important que les autorités chargées de la protection des données continuent d'œuvrer à la rationalisation du processus d'approbation, étant donné que la longueur de ces procédures est souvent mentionnée par les parties prenantes comme constituant un obstacle pratique à une utilisation plus large des REC.

Enfin, en ce qui concerne plus spécifiquement les REC approuvées par l'autorité britannique chargée de la protection des données (le *Information Commissioner Office*), les entreprises pourront continuer à les utiliser en tant que mécanisme de transfert valide au titre du RGPD après la fin de la période de transition dans le cadre de l'accord de retrait conclu entre l'UE et le Royaume-Uni, mais uniquement si elles sont modifiées de manière à ce que tout lien avec l'ordre juridique britannique soit remplacé par des références appropriées aux sociétés et aux autorités compétentes au sein de l'UE. L'approbation de toute nouvelle REC devrait être sollicitée auprès de l'une des autorités de contrôle de l'UE.

- Mécanismes de certification et codes de conduite

Outre la modernisation et l'élargissement de l'application des outils de transfert existants, le RGPD a également introduit de nouveaux instruments, élargissant ainsi les possibilités pour les transferts internationaux. Cela inclut l'utilisation, sous

---

[140] Pour un aperçu des avis rendus jusqu'à présent par le comité, voir https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

[143] Ces documents ont été adoptés (par l'ancien groupe de travail «article 29») à la suite de l'entrée en vigueur du RGPD, mais avant la fin de la période de transition. Voir WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056); WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf); WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Contribution du comité, p. 7.

certaines conditions, de codes de conduite et de mécanismes de certification approuvés (tels que les labels ou les marquages de protection des données personnelles) en vue d'offrir des garanties appropriées. Il s'agit d'outils ascendants qui permettent d'apporter des solutions sur mesure – en tant que mécanisme général de responsabilité (voir les articles 40 à 42 du RGPD) et, plus particulièrement, pour les transferts internationaux de données – reflétant, par exemple, les caractéristiques et les besoins particuliers d'un secteur ou d'une industrie donnés, ou de flux de données spécifiques. Les obligations étant adaptées aux risques, ces codes de conduite peuvent aussi être un moyen très utile et d'un rapport coût-efficacité satisfaisant pour les petites et moyennes entreprises de remplir leurs obligations au regard du RGPD.

En ce qui concerne les mécanismes de certification, bien que le comité ait adopté des lignes directrices pour favoriser leur utilisation au sein de l'UE, les travaux de ce dernier sur l'élaboration de critères pour l'approbation des mécanismes de certification en tant qu'outils de transferts internationaux sont toujours en cours. Il en va de même pour les codes de conduite, le comité travaillant actuellement à l'élaboration de lignes directrices permettant de les utiliser comme outils de transfert.

Étant donné qu'il est important que les opérateurs disposent d'un large éventail d'instruments de transfert adaptés à leurs besoins et, en particulier, que les mécanismes de certification soient à même de faciliter les transferts de données tout en garantissant un niveau élevé de protection des données, la Commission invite instamment le comité à parachever dès que possible ses orientations à cet égard. Cela porte à la fois sur les questions de fond (critères) et les aspects relatifs aux procédures (approbation, contrôle, etc.). Les parties prenantes ont exprimé un grand intérêt pour ces mécanismes de transfert, qui devraient leur permettre de tirer pleinement parti de la boîte à outils du RGPD. Les lignes directrices du comité contribueront également à promouvoir le modèle de l'UE en matière de protection des données à l'échelle mondiale et à favoriser la convergence, dans la mesure où d'autres systèmes de protection de la vie privée utilisent des instruments similaires.

Des enseignements précieux peuvent être tirés des efforts de normalisation existants dans le domaine de la protection de la vie privée, tant au niveau européen qu'au niveau international. Un exemple intéressant est celui de la norme internationale ISO 27701[145] publiée récemment, qui vise à aider les entreprises à respecter les exigences en matière de protection de la vie privée et à gérer les risques liés au traitement des données à caractère personnel par l'intermédiaire de «systèmes de gestion des informations à caractère privé». Bien que la certification au titre de la norme ne réponde pas en soi aux exigences des articles 42 et 43 du RGPD, l'application de systèmes de gestion des informations à caractère privé peut contribuer au respect de l'obligation de rendre des comptes, y compris dans le contexte des transferts internationaux de données.

- Accords internationaux et arrangements administratifs

Le RGPD permet également d'assurer des garanties appropriées pour les transferts de données entre les autorités ou organismes publics sur la base d'accords internationaux [article 46, paragraphe 2, point a)] ou des arrangements administratifs appropriés

[145]La liste des exigences spécifiques qui constituent cette norme ISO est disponible à l'adresse suivante: https://www.iso.org/standard/71670.html.

[article 46, paragraphe 3, point b)]. Si les deux instruments doivent garantir le même résultat en ce qui concerne les garanties, y compris les droits opposables des personnes concernées et des voies de recours effectives, ils diffèrent quant à leur nature juridique et à leur procédure d'adoption.

Contrairement aux accords internationaux, qui créent des obligations contraignantes au regard du droit international, les arrangements administratifs (par exemple sous la forme d'un protocole d'accord) sont généralement non contraignants et nécessitent donc l'autorisation préalable de l'autorité compétente en matière de protection des données (voir également le considérant 108 du RGPD). Un premier exemple concerne l'arrangement administratif pour le transfert de données à caractère personnel entre les autorités de surveillance financière de l'EEE et hors EEE qui coopèrent sous l'égide de l'Organisation internationale des commissions de valeurs (OICV), sur lesquelles le comité a rendu son avis[146] au début de l'année 2019. Depuis lors, le comité a développé son interprétation des «garanties minimales» que les accords (de coopération) internationaux et les arrangements administratifs conclus entre les autorités ou organismes publics (y compris les organisations internationales) doivent garantir pour respecter les exigences de l'article 46 du RGPD. Le 18 janvier 2020, il a adopté un projet de lignes directrices[147], répondant ainsi à la demande de clarifications et d'orientations supplémentaires des États membres concernant ce qui peut être considéré comme des garanties appropriées pour les transferts entre les autorités publiques[148]. Le comité recommande vivement que les autorités publiques utilisent ces lignes directrices comme point de référence pour leurs négociations avec des tiers[149].

Les lignes directrices démontrent la souplesse dans la conception de ces instruments, y compris en ce qui concerne des aspects importants tels que la surveillance[150] et les

---

[146] Comité européen de la protection des données, avis 4/2019 sur le projet d'arrangement administratif relatif au transfert de données à caractère personnel entre les autorités de surveillance financière de l'Espace économique européen (EEE) et les autorités de surveillance financière hors EEE, 12.2.2019.

[147] Comité européen de la protection des données, Lignes directrices 2/2020 relatives à l'article 46, paragraphe 2, point a), et paragraphe 3, point b), du règlement (UE) 2016/679 pour les transferts de données à caractère personnel entre les autorités et organismes publics de l'EEE et hors EEE (projet disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). Selon le comité, «[l]'autorité [de contrôle] compétente fondera son examen sur les recommandations générales énoncées dans les [présentes] lignes directrices, mais pourrait également demander davantage de garanties, selon le cas.»

[148] Position et conclusions du Conseil, point 20.

[149] Dans le même temps, le comité précise que les autorités publiques restent «libres de s'appuyer sur d'autres instruments pertinents prévoyant des garanties appropriées conformément à l'article 46 du RGPD». En ce qui concerne le choix de l'instrument, le comité souligne qu'«[i]l convient d'évaluer avec soin si, compte tenu de la finalité du traitement et de la nature des données en question, il y a lieu ou non de recourir à des dispositifs administratifs juridiquement non contraignants pour fournir des garanties dans le secteur public. Si la législation nationale du pays tiers ne prévoit pas de droits et de recours en matière de protection des données pour les particuliers ressortissants de pays de l'EEE, il convient de donner la préférence à la conclusion d'un accord juridiquement contraignant. Indépendamment du type d'instrument adopté, les mesures en place doivent être efficaces pour assurer la mise en œuvre, l'application et la surveillance appropriées» (point 67).

[150] Il peut s'agir, par exemple, de combiner les contrôles internes (avec un engagement à informer l'autre partie de tout cas de non-respect) avec un contrôle indépendant au moyen de mécanismes

voies de recours[151]. Cela devrait permettre aux pouvoirs publics de surmonter les difficultés qu'ils rencontrent pour, par exemple, garantir les droits opposables aux personnes concernées au moyen de dispositions non contraignantes. Un élément important de ces dispositions réside dans leur suivi permanent par l'autorité compétente en matière de protection des données, qui repose sur les exigences en matière d'informations et de tenue de registres, et la suspension des flux de données si des garanties appropriées ne peuvent plus être garanties dans la pratique.

Dérogations

Enfin, le RGPD apporte des éclaircissements en ce qui concerne le recours aux «dérogations». Il s'agit de motifs spécifiques pour les transferts de données (par exemple le consentement explicite[152], l'exécution d'un contrat ou des motifs importants d'intérêt public) reconnus en droit et sur lesquels les entités peuvent se fonder en l'absence d'autres outils de transfert et sous certaines conditions.

Afin de clarifier l'utilisation de ces motifs légaux, le comité a publié des orientations spécifiques[153] et a interprété l'article 49 dans un certain nombre de cas au regard de scénarios de transfert spécifiques[154]. Compte tenu de leur caractère exceptionnel, le comité considère que les dérogations doivent être interprétées de manière restrictive, au cas par cas. En dépit de cette interprétation stricte, ces motifs couvrent un large éventail de scénarios de transfert. Il s'agit notamment des transferts de données effectués tant par des pouvoirs publics que par des entités privées pour des «motifs importants d'intérêt public», par exemple entre les autorités compétentes en matière de concurrence, les autorités financières, fiscales ou douanières, les services compétents en matière de sécurité sociale ou de santé publique (par exemple, aux fins de la recherche des contacts de personnes atteintes de maladies contagieuses ou en

---

externes ou, du moins, autonomes d'un point de vue fonctionnel, ainsi que de la possibilité pour l'organisme public de transfert de suspendre ou de résilier le transfert.

151 Il peut s'agir, par exemple, de mécanismes quasi-judiciaires contraignants (tels que l'arbitrage) ou de règlement extrajudiciaire des litiges, associés à la possibilité, pour l'autorité publique qui transfère, de suspendre ou de résilier le transfert de données à caractère personnel si les parties ne parviennent pas à résoudre un litige à l'amiable, ainsi qu'à l'engagement de l'organisme public qui reçoit les données de renvoyer ou de supprimer les données à caractère personnel concernées. Lorsque des mécanismes de recours alternatifs relevant d'instruments contraignants et exécutoires sont choisis parce qu'il n'existe pas de possibilité de garantir un recours juridictionnel effectif, le comité recommande que l'avis de l'autorité de contrôle compétente soit sollicité avant l'utilisation de ces instruments.

152 Il s'agit là d'un changement par rapport à la directive 95/46, qui requiert uniquement un consentement «donné indubitablement». En outre, les exigences générales applicables au consentement en vertu de l'article 4, paragraphe 11, du RGPD s'appliquent.

153 Comité européen de la protection des données, lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 25.5.2018 (disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf).

154 Cela inclut, par exemple, les transferts internationaux de données relatives à la santé à des fins de recherche dans le contexte de la pandémie de COVID-19. Voir Comité européen de la protection des données, lignes directrices 03/2020 sur le traitement des données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19, 21.4.2020 (disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_fr.pdf).

vue d'éliminer le dopage dans le sport)[155]. Un autre domaine est celui de la coopération transfrontière à des fins répressives en matière pénale, notamment en ce qui concerne les formes graves de criminalité[156].

Le comité a précisé que, si l'intérêt public visé doit être reconnu dans le droit de l'Union ou des États membres, il peut également être établi comme suit: «l'existence d'un accord international ou d'une convention internationale qui reconnaît un certain objectif et qui prévoit une coopération internationale afin de favoriser cet objectif peut être un indicateur au moment d'évaluer l'existence d'un intérêt public en vertu de l'article 49, paragraphe 1, point d), tant que l'Union ou les État membres sont parties à cet accord ou à cette convention»[157].

Décisions de juridictions ou d'autorités étrangères: pas un motif de transfert

Outre qu'il énonce sans ambiguïté les motifs des transferts de données, le chapitre V du RGPD précise également, à son article 48, que les décisions des juridictions ou des autorités administratives de pays tiers ne fournissent pas *en soi* de tels motifs, à moins qu'elles ne soient reconnues ou rendues exécutoires sur la base d'un accord international (par exemple, un traité d'entraide judiciaire). Toute divulgation par l'entité requise dans l'UE à la juridiction ou à l'autorité étrangère en réponse à de telles décisions constitue un transfert international de données qui doit être fondé sur l'un des instruments de transfert mentionnés[158].

Le RGPD ne constitue pas une «loi de blocage» et, sous certaines conditions, permettra un transfert en réponse à une demande d'application de la loi appropriée émanant d'un pays tiers. Le point important est que c'est le droit de l'Union qui

---

[155] Voir considérant 112.

[156] Voir intervention de la Commission européenne, au nom de l'Union européenne, en qualité d'amicus curiae à l'appui d'aucune des parties dans l'affaire États-Unis/Microsoft, p. 15: «D'une manière générale, le droit de l'Union ainsi que celui des États membres reconnaissent l'importance de la lutte contre les formes graves de criminalité et, partant, l'application de la législation pénale et la coopération internationale à cet égard, comme un objectif d'intérêt général. [...] L'article 83 du TFUE recense plusieurs domaines de criminalité particulièrement grave revêtant une dimension transfrontière, comme le trafic de drogue.» (Disponible à l'adresse: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

[157] Comité européen de la protection des données, lignes directrices relatives aux dérogations (note de bas de page 153 supra), p. 10. Le comité a également précisé que, si les transferts de données fondés sur une dérogation d'intérêt public ne doivent pas se faire «à grande échelle» ou «de façon systématique», mais doivent «être limit[és] à des situations particulières et [...] respecter le strict critère de nécessité», il n'est pas exigé qu'ils soient «occasionnels».

[158] Cela ressort clairement du libellé de l'article 48 du RGPD («sans préjudice d'autres motifs de transfert en vertu du présent chapitre») et du considérant 115 qui l'accompagne («[l]es transferts ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies. Ce peut être le cas, entre autres, lorsque la divulgation est nécessaire pour un motif important d'intérêt public reconnu par le droit de l'Union ou d'un État membre auquel le responsable du traitement est soumis». Cela est également reconnu par le comité européen de la protection des données, voir lignes directrices relatives aux dérogations (voir note de bas de page 153 supra), p. 5. Comme pour toutes les opérations de traitement, les autres garanties prévues par le règlement doivent également être respectées (par exemple, les données sont transférées pour une finalité spécifique, sont pertinentes, limitées à ce qui est nécessaire aux fins de la demande, etc.).

devrait déterminer si tel est le cas, et sur la base de quelles garanties ces transferts peuvent avoir lieu.

La Commission a expliqué le fonctionnement de l'article 48 du RGPD, y compris l'invocation éventuelle de la dérogation en raison d'un intérêt public, dans le cadre d'une injonction de production (*warrant*) d'une autorité répressive étrangère en matière pénale dans l'affaire Microsoft devant la Cour suprême des États-Unis[159]. Dans sa déclaration, la Commission a souligné l'intérêt, pour l'UE, de faire en sorte que la coopération entre les services répressifs intervienne «dans un cadre juridique permettant d'éviter les conflits de lois et soit fondée sur [...] le respect des intérêts fondamentaux de chacun, tant dans le domaine de la protection de la vie privée que de l'application de la loi»[160]. En particulier, «du point de vue du droit international public, lorsqu'une autorité publique exige d'une société établie sur son territoire qu'elle produise des données électroniques stockées sur un serveur situé dans une juridiction étrangère, les principes de territorialité et de courtoisie en vertu du droit public international sont en jeu»[161].

C'est ce qui ressort également de la proposition de la Commission relative à un règlement sur les injonctions européennes de production et de conservation de preuves électroniques en matière pénale[162], qui contient une «clause de courtoisie» spécifique qui permet d'émettre une objection contre une injonction de production si le respect de l'injonction fait naître un conflit avec les dispositions législatives d'un pays tiers, interdisant la divulgation, en particulier au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées[163].

---

[159] Déclarations de Microsoft (note de bas de page 156 supra). Ainsi que la Commission l'a expliqué, le règlement général sur la protection des données fait de ces traités l'«option privilégiée» pour les transferts, étant donné que ces traités «prévoient la collecte de preuves par consentement, et incarnent un équilibre soigneusement négocié entre les intérêts des différents États qui est conçu pour atténuer les conflits de compétences qui, sans quoi, peuvent se produire». Voir également comité européen de la protection des données, lignes directrices relatives aux dérogations (voir note de bas de page 153 supra), p. 5 («Dans les situations où il existe un accord international, tel qu'un traité d'entraide judiciaire, les entreprises de l'Union devraient généralement refuser les demandes directes et renvoyer l'autorité du pays tiers requérante aux traités d'entraide judiciaire ou à un accord existant»).

[160] Déclarations de Microsoft (note de bas de page 156 supra), p. 4

[161] Déclarations de Microsoft (note de bas de page 156 supra), p. 6

[162] Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, 17.4.2018, COM(2018) 225 final. Le Conseil a adopté son orientation générale sur le règlement proposé le 7.12.2018 (disponible à l'adresse: https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Voir également comité européen de la protection des données, avis 7/19 sur les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (disponible à l'adresse suivante: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] L'exposé des motifs, p. 21, précise qu'outre le fait que la clause garantit la courtoisie envers les intérêts souverains des pays tiers, protège la personne concernée et évite des conflits de lois pour les prestataires de services, une motivation importante de la clause de courtoisie est la réciprocité, c'est-à-dire qu'elle vise à garantir le respect des règles de l'UE, y compris en ce qui concerne la protection des données à caractère personnel (article 48 du RGPD). Voir également la déclaration du groupe de travail «article 29» du 29 novembre 2017 sur les aspects relatifs à la protection des données et de la vie privée liés à l'accès transfrontière aux preuves électroniques (déclaration du

Il est important de garantir la courtoisie, étant donné que l'application de la loi, notamment en matière de criminalité et en particulier de cybercriminalité, est de plus en plus transfrontière, soulève donc souvent des questions juridictionnelles et crée des conflits de lois potentiels[164]. Sans surprise, le meilleur moyen d'aborder ces questions passe par des accords internationaux qui prévoient les limitations et garanties nécessaires en ce qui concerne l'accès transfrontière aux données à caractère personnel, y compris la garantie d'un niveau élevé de protection des données de la part de l'autorité requérante.

La Commission, agissant au nom de l'UE, mène actuellement des négociations multilatérales en vue de la conclusion d'un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe («convention de Budapest»), qui vise à renforcer les règles existantes concernant l'obtention d'un accès transfrontière aux preuves électroniques dans le cadre des enquêtes pénales, tout en assurant des garanties appropriées en matière de protection des données dans le cadre du protocole[165]. De même, des négociations bilatérales ont commencé sur un accord entre l'UE et les États-Unis concernant l'accès transfrontière aux preuves électroniques pour la coopération judiciaire en matière pénale[166]. La Commission compte sur le soutien du Parlement européen et du Conseil, et sur les orientations du comité européen de la protection des données, pendant toute la durée de ces négociations.

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

---

groupe de travail «article 29») (disponible à l'adresse suivante: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), p. 9.

164 Voir déclaration du groupe de travail «article 29» (note de bas de page 163 supra), p. 6.

165 Voir recommandation de décision du Conseil autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STE nº 185), 5.2.2019 [COM(2019) 71 final] Voir également comité européen de la protection des données, avis 3/2019 relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité, 2.4.2019 (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_fr.pdf); Comité européen de la protection des données, contribution à la consultation sur un projet de deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest), 13.11.2019 (disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

166 Voir recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, 5.2.2019 [COM(2019) 70 final]. Voir également comité européen de la protection des données, avis 2/2019 sur le mandat de négociation d'un accord UE-États-Unis sur l'accès transfrontière aux preuves électroniques (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

efficaces, notamment en prévoyant les garanties nécessaires en matière de protection des données, et de contribuer ainsi à une lutte plus efficace contre la criminalité.

7.3 Coopération internationale dans le domaine de la protection des données

Favoriser la convergence entre les différents systèmes de protection de la vie privée implique également un apprentissage mutuel, par l'échange de connaissances, d'expériences et de bonnes pratiques. Ces échanges sont essentiels pour s'attaquer aux nouveaux défis dont la nature et la portée revêtent une dimension de plus en plus mondiale. C'est la raison pour laquelle la Commission a intensifié son dialogue sur la protection des données et les flux de données avec un large éventail d'acteurs et dans différentes enceintes, au niveau bilatéral, régional et multilatéral.

La dimension bilatérale

Depuis l'adoption du RGPD, l'expérience de l'UE dans la conception, la négociation et la mise en œuvre de règles modernes en matière de protection de la vie privée suscite un intérêt croissant. Le dialogue avec les pays qui suivent des processus similaires a pris plusieurs formes.

Les services de la Commission ont contribué à un certain nombre de consultations publiques organisées par des gouvernements étrangers sur la législation dans le domaine de la protection de la vie privée, par exemple par les États-Unis[167], l'Inde[168], la Malaisie et l'Éthiopie. Dans certains pays tiers, les services de la Commission ont eu le privilège de témoigner devant les instances parlementaires compétentes, par exemple au Brésil[169], au Chili[170], en Équateur et en Tunisie[171].

---

[167] Voir les observations de la DG Justice et consommateurs du 9 novembre 2018 en réponse à une demande de commentaires du public concernant une proposition d'approche de la protection de la vie privée des consommateurs [dossier nº 180821780-8780-01] par l'administration nationale des télécommunications et de l'information des États-Unis (disponible à l'adresse suivante: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf)

[168] Voir la communication de la DG Justice et consommateurs du 19 novembre 2018 sur le projet de loi sur la protection des données à caractère personnel de l'Inde de 2018 au ministère de l'électronique et des technologies de l'information (disponible à l'adresse https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Voir la réunion plénière du Sénat brésilien du 17 avril 2018 (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), la réunion du 10 avril 2019 du comité mixte concernant la MP 869/2018 du Congrès brésilien (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392), et la réunion du 26 novembre 2019 de la commission spéciale de la Chambre des députés du Brésil (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Voir les réunions du 29 mai 2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1), du 24 avril 2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) et de la commission des affaires constitutionnelles, législatives et de la justice du Sénat chilien.

De plus, dans le cadre des réformes en cours de la législation sur la protection des données, des réunions spécifiques ont eu lieu avec des représentants des gouvernements ou des délégations parlementaires de nombreuses régions du monde (par exemple la Géorgie, le Kenya, Taïwan, la Thaïlande et le Maroc). Il s'agissait notamment d'organiser des séminaires et des visites d'étude, par exemple avec des représentants du gouvernement indonésien et une délégation de membres du personnel du Congrès américain. Cela a permis de clarifier des notions importantes du RGPD, d'améliorer la compréhension mutuelle des questions relatives à la protection de la vie privée et d'illustrer les avantages de la convergence pour garantir un niveau élevé de protection des droits individuels ainsi qu'en matière de commerce et de coopération. Dans certains cas, cela a également permis de mettre en garde contre certaines idées fausses en matière de protection des données, qui peuvent conduire à l'introduction de mesures protectionnistes telles que des exigences de localisation forcée.

Depuis l'adoption du RGPD, la Commission a également noué un dialogue avec plusieurs organisations internationales, notamment à la lumière de l'importance des échanges de données avec ces organisations dans un certain nombre de domaines d'action. Un dialogue spécifique a notamment été engagé avec les Nations unies, en vue de faciliter les discussions avec toutes les parties prenantes concernées afin de garantir la fluidité des transferts de données et de renforcer la convergence entre les différents régimes de protection des données. Dans le cadre de ce dialogue, la Commission travaillera en étroite collaboration avec le comité afin de préciser comment les opérateurs publics et privés de l'UE peuvent satisfaire aux obligations qui leur incombent en vertu du RGPD lorsqu'ils échangent des données avec des organisations internationales telles que les Nations unies.

La Commission est disposée à continuer à partager les enseignements tirés de son processus de réforme avec les pays intéressés et les organisations internationales, de la même manière qu'elle a tiré des enseignements d'autres systèmes lors de l'élaboration de sa proposition de nouvelles règles de l'UE en matière de protection des données. Ce type de dialogue est mutuellement bénéfique pour l'UE et ses partenaires, car il permet de mieux comprendre l'évolution rapide du paysage de la protection de la vie privée et de procéder à des échanges de vues sur des solutions juridiques et technologiques émergentes.

C'est dans cet esprit que la Commission met en place une «Académie pour la protection des données» pour favoriser les échanges entre les régulateurs des pays européens et des pays tiers et, de cette manière, améliorer la coopération «sur le terrain».

En outre, il est nécessaire de mettre au point des instruments juridiques appropriés pour renforcer les formes de coopération et d'assistance mutuelle, notamment en permettant l'échange d'informations nécessaire dans le cadre d'enquêtes. La Commission fera donc usage des pouvoirs qui lui sont conférés dans ce domaine par l'article 50 du RGPD et, en particulier, demandera l'autorisation d'ouvrir des

[171] Voir la réunion du 2 novembre 2018 du Comité des droits, des libertés et des relations extérieures de l'Assemblée des représentants du peuple de Tunisie (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

négociations en vue de la conclusion d'accords de coopération en matière d'exécution avec les pays tiers concernés. Dans ce contexte, elle tiendra également compte du point de vue du comité en ce qui concerne les pays auxquels il convient d'accorder la priorité à la lumière du volume des transferts de données, du rôle et des pouvoirs de l'autorité chargée de la protection de la vie privée dans le pays tiers et de la nécessité d'une coopération des services répressifs pour traiter les cas d'intérêt commun.

La dimension multilatérale

Outre les échanges bilatéraux, la Commission participe activement à un certain nombre de forums multilatéraux afin de promouvoir des valeurs communes et de renforcer la convergence au niveau régional et mondial.

L'adhésion de plus en plus universelle à la «convention 108» du Conseil de l'Europe, qui est le seul instrument multilatéral juridiquement contraignant dans le domaine de la protection des données à caractère personnel, témoigne clairement de cette tendance à une convergence accrue[172]. La convention, qui est également ouverte aux pays qui ne sont pas membres du Conseil de l'Europe, a déjà été ratifiée par 55 pays, dont un certain nombre d'États africains et d'Amérique latine[173]. La Commission a largement contribué au succès des négociations sur la modernisation de la convention[174] et a veillé à ce qu'elle reflète les mêmes principes que ceux qui sont consacrés par les règles de l'UE en matière de protection des données. La plupart des États membres de l'UE ont maintenant signé le protocole de modification, bien que les signatures du Danemark, de Malte et de la Roumanie soient toujours en attente. À ce jour, seuls quatre États membres (la Bulgarie, la Croatie, la Lituanie et la Pologne) ont ratifié le protocole de modification. La Commission demande instamment aux trois États membres restants de signer la convention modernisée, et à tous les États membres de procéder rapidement à la ratification, afin de permettre son entrée en vigueur dans un avenir proche[175]. Par ailleurs, elle continuera à encourager de manière proactive l'adhésion de pays tiers.

---

[172] Il est important de noter que la convention modernisée n'est pas seulement un traité établissant des garanties solides en matière de protection des données, mais qu'elle crée également un réseau d'autorités de surveillance dotées d'outils de coopération en matière d'exécution et, avec le comité de la convention, un forum de discussion, d'échange de bonnes pratiques et de développement de normes internationales.

[173] Voir la liste complète des membres: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures. Les pays d'Afrique comprennent le Cabo-Verde, Maurice, le Maroc, le Sénégal et la Tunisie; ceux d'Amérique latine comprennent l'Argentine, le Mexique et l'Uruguay. Le Burkina Faso a été invité à rejoindre la Convention.

[174] Voir le texte de la convention modernisée: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

[175] Conformément à sa décision relative au protocole d'amendement du 18 mai 2018, le Comité des ministres «appelle instamment les États membres et les autres Parties à la Convention à prendre sans délai les mesures nécessaires pour permettre l'entrée en vigueur du Protocole dans un délai de trois ans à compter de son ouverture à la signature et à engager immédiatement, et dans tous les cas au plus tard un an après la date à laquelle le Protocole aura été ouvert à la signature, le processus prévu par leur législation nationale menant à la ratification...». Il «charge ses Délégués de procéder à un examen semestriel, et pour la première fois, une année après la date d'ouverture à la signature du Protocole, des progrès réalisés en vue de la ratification sur la base des informations à fournir par chacun des États membres et autres Parties à la Convention au Secrétaire Général au plus tard un

Les flux de données et la protection des données ont également été abordés récemment dans le cadre du G20 et du G7. En 2019, les dirigeants mondiaux ont approuvé pour la première fois l'idée que la protection des données contribue à la confiance dans l'économie numérique et facilite les flux de données. Avec le soutien actif de la Commission[176], les dirigeants ont approuvé le concept de «libre flux de données en toute confiance» initialement proposé par le Japon dans la déclaration d'Osaka du G20[177], ainsi que lors du sommet du G7 à Biarritz[178]. Cette approche se retrouve également dans la communication de la Commission de 2020 intitulée «Une stratégie européenne pour les données»[179], qui souligne son intention de continuer à promouvoir l'échange de données avec des partenaires de confiance tout en luttant contre les abus tels qu'un accès disproportionné des pouvoirs publics (étrangers) aux données.

Ce faisant, l'UE pourra également s'appuyer sur un certain nombre d'outils dans différents domaines d'action qui prennent de plus en plus en considération les répercussions sur la vie privée: par exemple, le tout premier cadre de l'UE pour l'examen des investissements étrangers, qui deviendra pleinement applicable en octobre 2020, donne à l'UE et à ses États membres la possibilité de filtrer les opérations d'investissement qui ont des effets sur l'«accès à des informations sensibles, y compris des données à caractère personnel, ou la capacité de contrôler de telles informations» si elles portent atteinte à la sécurité ou à l'ordre public[180].

La Commission collabore avec des pays partageant les mêmes valeurs dans plusieurs autres enceintes multilatérales pour promouvoir activement ses valeurs et ses normes. Un forum important est le groupe de travail sur la gouvernance et la protection des données (DPG) créé récemment par l'OCDE, qui mène un certain nombre d'initiatives importantes liées à la protection des données, au partage des données et aux transferts de données. Cela inclut l'évaluation des lignes directrices de l'OCDE sur la protection de la vie privée mises à jour en 2013. En outre, la Commission a contribué activement à la recommandation du Conseil de l'OCDE sur l'intelligence artificielle[181] et a veillé à ce que l'approche de l'UE axée sur l'humain, selon laquelle les applications de l'IA doivent respecter les droits fondamentaux et en particulier la

---

mois avant un tel examen.» Voir https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016808a3959.

[176] En marge du sommet UE-Japon d'avril 2019, le président Juncker a exprimé son soutien à l'initiative du Japon intitulée «Libre flux de données en toute confiance» et au lancement de l'«approche d'Osaka» et a engagé la Commission à «jouer un rôle actif dans les deux initiatives».

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

[178] Voir le texte de la stratégie de Biarritz du G7 pour une transformation numérique ouverte, libre et sûre https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

[179] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Une stratégie européenne pour les données, 19.2.2020 [COM(2020) 66 final] (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_fr.pdf), p. 23 et 24.

[180] Article 4, paragraphe 1, point d), du règlement (UE) 2019/452 du Parlement européen et du Conseil du 19.3.2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79I du 21.3.2019).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

protection des données, figure dans le texte final. Il est important de noter que la recommandation sur l'IA, qui a ensuite été intégrée dans les principes relatifs à l'IA du G20 annexés à la déclaration d'Osaka des dirigeants du G20[182], énonce les principes de transparence et d'explicabilité visant à «permettre à ceux qui subissent les effets nuisibles d'un système d'IA d'en contester les résultats sur la base d'informations claires et faciles à comprendre sur les facteurs et la logique qui ont servi de base à la prédiction, à la recommandation ou à la décision concernée», reflétant ainsi fidèlement les principes du RGPD en matière de prise de décision automatisée[183].

Par ailleurs, la Commission intensifie son dialogue avec les organisations et réseaux régionaux, qui jouent de plus en plus un rôle central dans l'élaboration de normes communes en matière de protection des données[184], en favorisant l'échange de bonnes pratiques ainsi que la coopération entre les autorités de contrôle. Cela concerne, en particulier, l'Association des nations de l'Asie du Sud-Est (ASEAN), notamment dans le cadre de ses travaux en cours sur les outils de transfert de données, l'Union africaine, le forum des autorités de protection de la vie privée pour l'Asie-Pacifique (APPA) et le réseau ibéro-américain de protection des données, qui ont tous lancé d'importantes initiatives dans ce domaine et offrent des forums permettant un dialogue fructueux entre les autorités de réglementation en matière de protection de la vie privée et les autres parties prenantes.

L'Afrique est un exemple éloquent de la complémentarité entre les dimensions nationale, régionale et mondiale de la protection de la vie privée. Les technologies numériques transforment rapidement et profondément le continent africain. Cela peut accélérer la réalisation des objectifs de développement durable en stimulant la croissance économique, en réduisant la pauvreté et en améliorant la vie des citoyens. La mise en place d'un cadre moderne de protection des données permettant d'attirer les investissements et de favoriser le développement d'entreprises compétitives tout en contribuant au respect des droits de l'homme, de la démocratie et de l'état de droit est un élément essentiel de cette transformation. L'harmonisation des règles en matière de protection des données à travers l'Afrique permettrait l'intégration du marché numérique, tandis que la convergence avec les normes mondiales faciliterait les échanges de données avec l'UE. Ces différentes dimensions de la protection des données sont liées entre elles et se renforcent mutuellement.

Il existe actuellement un intérêt croissant pour la protection des données dans de nombreux pays africains, et le nombre de pays africains qui ont adopté ou sont en train d'adopter des règles modernes en matière de protection des données, ont ratifié la convention 108[185] ou la convention de Malabo[186] continue d'augmenter[187].

[182] Déclaration ministérielle du G20 sur le commerce et l'économie numérique: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf

[183] Voir l'article 13, paragraphe 2, point f), l'article 14, paragraphe 2, point g), et l'article 22 du RGPD.

[184] Voir, par exemple, la *convention sur la cybersécurité et la protection des données à caractère personnel* (la «convention de Malabo») de l'Union africaine et les *normes de protection des données des États ibéro-américains* élaborées par le réseau ibéro-américain de protection des données.

[185] Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD

Dans le même temps, le cadre réglementaire demeure très inégal et fragmenté sur le continent africain. De nombreux pays continuent à offrir peu de garanties en matière de protection des données, voire aucune Les mesures limitant les flux de données sont encore très répandues et entravent le développement d'une économie numérique régionale.

Afin de tirer parti des avantages mutuels de règles convergentes en matière de protection des données, la Commission coopérera avec ses partenaires africains, tant au niveau bilatéral que dans les enceintes régionales[188]. Cette coopération s'appuie sur les travaux du groupe de travail UE-UA sur l'économie numérique dans le cadre du nouveau partenariat Afrique-Europe pour une économie numérique[189]. C'est également pour faire progresser ces objectifs que le champ d'application de l'instrument de partenariat de la Commission «*Enhanced Data Protection and Data Flows*» (Renforcement de la protection des données et des flux de données) a été étendu à l'Afrique. Le projet sera mobilisé pour aider les pays africains qui ont l'intention de développer des cadres modernes de protection des données ou qui souhaitent renforcer la capacité de leurs autorités de réglementation, par la formation, le partage de connaissances et l'échange de bonnes pratiques.

[186] Convention sur la cybersécurité et la protection des données à caractère personnel de l'Union africaine https://au.int/fr/treaties/african-union-convention-cyber-security-and-personal-data-protection. En outre, plusieurs communautés économiques régionales (CER) ont mis au point des règles en matière de protection des données, par exemple la Communauté économique des États de l'Afrique de l'Ouest (Cedeao) et la Communauté de développement de l'Afrique australe (SADC). Voir, respectivement, http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf et http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Notamment grâce à l'initiative sur la politique et la réglementation en faveur de l'Afrique numérique (PRIDA), voir les informations sur: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189] Voir la communication conjointe de la Commission européenne et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité intitulée «Vers une stratégie globale avec l'Afrique» (disponible à l'adresse suivante: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Groupe de travail sur l'économie numérique, nouveau partenariat Afrique-Europe pour une économie numérique: Accélérer la réalisation des objectifs de développement durable (disponible à l'adresse suivante: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

Enfin, tout en promouvant la convergence des normes de protection des données au niveau international, en tant que moyen de faciliter les flux de données et, partant, le commerce, la Commission est également déterminée à lutter contre le protectionnisme numérique, comme elle l'a récemment souligné dans sa stratégie pour les données[190]. À cette fin, elle a élaboré des dispositions spécifiques sur les flux de données et la protection des données dans les accords commerciaux, qu'elle présente systématiquement dans ses négociations bilatérales (récemment, avec l'Australie, la Nouvelle-Zélande et le Royaume-Uni) et multilatérales, comme les pourparlers actuels sur le commerce électronique avec l'OMC. Ces dispositions horizontales excluent les restrictions injustifiées, telles que les exigences relatives à la localisation forcée des données, tout en préservant l'autonomie réglementaire des parties pour préserver le droit fondamental à la protection des données.

Bien que les dialogues sur la protection des données et les négociations commerciales doivent suivre des voies différentes, ils peuvent se compléter. En effet, la convergence, fondée sur des normes élevées et étayées par une application effective, constitue la base la plus solide pour l'échange de données à caractère personnel, ce qui est de plus en plus reconnu par nos partenaires internationaux. Étant donné que les entreprises mènent toujours plus d'activités transfrontières et préfèrent appliquer des ensembles de règles similaires dans toutes leurs opérations commerciales dans le monde, cette convergence contribue à créer un environnement propice aux investissements directs, facilitant les échanges et améliorant la confiance entre les partenaires commerciaux. Il convient donc d'étudier plus avant les synergies possibles entre les instruments commerciaux et les instruments de protection des données afin de garantir des flux de données internationaux libres et sûrs; ceux-ci sont essentiels pour les activités commerciales, la compétitivité et la croissance des entreprises européennes, y compris des PME, dans une économie de plus en plus numérisée.

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_fr.pdf, p. 23.

Annexe I – Clauses relatives aux spécifications facultatives par législation nationale

Objet	Champ d'application	Articles du RGPD
Spécifications relatives aux obligations légales et aux missions d'intérêt public	Adaptation de l'application des dispositions relatives au traitement aux fins du respect d'une obligation légale ou de l'exécution d'une mission d'intérêt public, y compris pour des situations particulières de traitement comme le prévoit le chapitre IX	article 6, paragraphes 2 et 3
Limite d'âge pour le consentement en ce qui concerne les services de la société de l'information	Fixation de l'âge minimal entre 13 et 16 ans	Article 8, paragraphe 1
Traitement de catégories particulières de données	Introduction ou maintien de conditions supplémentaires, y compris de limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données relatives à la santé.	Article 9, paragraphe 4
Dérogation aux exigences en matière d'information	Obtention ou communication expressément prévues par la loi ou en vertu d'une obligation de secret professionnel réglementée par la loi	Article 14, paragraphe 5, points c) et d)
Décision individuelle automatisée	Autorisation de prise de décision automatisée par dérogation à l'interdiction générale	Article 22, paragraphe 2, point b)
Limitations des droits des personnes concernées	Limitations visées aux articles 12 à 22, à l'article 34 et aux dispositions correspondantes de l'article 5, lorsque cela est nécessaire et proportionné pour garantir des objectifs importants énumérés de manière exhaustive	Article 23, paragraphe 1
Obligation de consultation et d'autorisation	Obligation pour les responsables du traitement de consulter ou d'obtenir l'autorisation de l'autorité chargée de la protection des données pour un traitement effectué dans le cadre d'une mission d'intérêt public	Article 36, paragraphe 5
Désignation d'un délégué à la protection des données dans des cas supplémentaires	Désignation d'un délégué à la protection des données dans les cas autres que ceux visés à l'article 37, paragraphe 1	Article 37, paragraphe 4

Limitations des transferts	Limitation des transferts de catégories spécifiques de données à caractère personnel	Article 49, paragraphe 5
Réclamations et actions en justice engagées par des organisations en leur nom propre	Droit pour les organisations actives dans le domaine de la protection de la vie privée d'introduire des réclamations et d'intenter des actions en justice indépendamment de tout mandat confié par une personne concernée	Article 80, paragraphe 2
Accès aux documents officiels	Conciliation du droit d'accès du public aux documents officiels et du droit à la protection des données à caractère personnel	Article 86
Traitement du numéro d'identification national	Conditions spécifiques applicables au traitement du numéro d'identification national	Article 87
Traitement des données dans le cadre des relations de travail	Règles plus spécifiques en ce qui concerne le traitement des données à caractère personnel des employés	Article 88
Dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche ou à des fins statistiques	Dérogations aux droits spécifiques des personnes concernées dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation de finalités spécifiques	Article 89, paragraphes 2 et 3
Conciliation de la protection des données et des obligations de secret	Règles spécifiques relatives aux pouvoirs d'enquête des autorités chargées de la protection des données à l'égard des responsables du traitement ou des sous-traitants soumis aux obligations de secret professionnel	Article 90

ANNEXE II – Aperçu des ressources des autorités chargées de la protection des données

Le tableau ci-dessous donne un aperçu des ressources (personnel et budget) des autorités chargées de la protection des données par État membre de l'UE/EEE[191].

Lorsque l'on compare les chiffres des différents États membres, il importe de garder à l'esprit que les autorités peuvent s'être vues attribuer des tâches qui vont au-delà de celles prévues par le RGPD et que celles-ci peuvent varier d'un État membre à l'autre. Le pourcentage de membres du personnel employés par les autorités par million d'habitants et la proportion du budget des autorités par million d'euros du PIB ne sont inclus que pour fournir des éléments de comparaison supplémentaires entre les États membres de taille similaire et ne devraient pas être considérés isolément. Les chiffres absolus, les ratios et l'évolution au cours des dernières années doivent être examinés conjointement lors de l'évaluation des ressources d'une autorité donnée.

	PERSONNEL (équivalents temps plein)					BUDGET (en euros)				
États membres UE/EEE	2019	Prévisions 2020	% de croissance 2016-2019	% de croissance 2016-2020 (prévisions)	Membres du personnel par million d'habitants	2019	Prévisions 2020	% de croissance 2016-2019	% de croissance 2016-2020 (prévisions)	Budget par million d'euros du PIB (2019)
Autriche	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgique	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgarie	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Croatie	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Chypre	24	22	S.O.	S.O.	27,4	503 855	S.O.	114 %	S.O.	23,0
République tchèque	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Danemark	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estonie	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finlande	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
France	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Allemagne	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Grèce	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Hongrie	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Islande	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irlande	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italie	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Lettonie	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Lituanie	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Luxembourg	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malte	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Pays-Bas	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norvège	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Pologne	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugal	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Roumanie	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovaquie	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovénie	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Espagne	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Suède	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5

[191] Sauf pour le Liechtenstein.

TOTAL	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Source des chiffres bruts: contribution du comité. Calculs de la Commission