COMMISSION
EUROPÉENNE

Bruxelles, le 24.7.2019
COM(2019) 374 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan

Communication de la Commission au Parlement européen et au Conseil

Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan

I. Introduction

Le règlement général sur la protection des données[1] (ci-après le «règlement») s'applique dans toute l'Union européenne depuis plus d'un an. Il est au cœur d'un cadre de l'Union pour la protection des données cohérent et modernisé qui inclut également la directive en matière de protection des données dans le domaine répressif[2] et le règlement relatif à la protection des données par les institutions et organes de l'Union[3]. Ce cadre doit être complété par le règlement «vie privée et communications électroniques», qui en est actuellement au stade de la procédure législative.

Il est essentiel de disposer de règles solides en matière de protection des données pour garantir le droit fondamental à la protection des données à caractère personnel. Ces règles sont indispensables à une société démocratique[4] et constituent un élément important d'une économie de plus en plus fondée sur les données. L'UE aspire à saisir les nombreuses occasions que la transformation numérique offre sur le plan des services, des emplois et de l'innovation, tout en relevant les défis que cela comporte. Le vol d'identité, la fuite de données sensibles, la discrimination à l'égard de certaines personnes, les préjugés innés, le partage de contenus illégaux et le développement d'outils de surveillance intrusifs ne sont que quelques exemples de questions qui sont de plus en plus souvent soulevées dans le débat public et à l'égard desquelles il est évident que les citoyens souhaitent que leurs données soient protégées.

---

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 (règlement général sur la protection des données (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1): https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

2 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016: https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32016L0680. Les États membres devaient transposer la directive au plus tard le 6 mai 2018. Les rapports sur l'union de la sécurité indiquent l'état d'avancement de sa transposition.

3 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R1725. Il est applicable depuis le 11 décembre 2018.

4 La Cour suprême indienne a, dans un arrêt historique du 24 août 2017, reconnu que le respect de la vie privée constituait un droit fondamental, une «facette essentielle de la dignité de l'être humain».

La protection des données est devenue un phénomène véritablement mondial, les personnes du monde entier s'attachant et tenant de plus en plus à la protection et à la sécurité de leurs données. De nombreux pays ont adopté ou sont en train d'adopter des règles exhaustives en matière de protection des données fondées sur des principes similaires à ceux ancrés dans le règlement, ce qui entraîne une convergence mondiale des règles en la matière et offre de nouvelles possibilités de faciliter les flux de données entre opérateurs commerciaux ou pouvoirs publics, tout en rehaussant le niveau de protection des données à caractère personnel au sein de l'UE et dans le monde entier.

La protection des données est prise plus au sérieux que jamais et a des incidences multiples sur différentes parties prenantes et différents secteurs. La Commission est déterminée à faire en sorte que l'UE mette bien en œuvre le nouveau régime de protection des données et à soutenir tous les aspects nécessaires pour qu'il devienne pleinement opérationnel. Par la présente communication, la Commission dresse le bilan des résultats obtenus jusqu'à présent concernant la mise en œuvre cohérente des règles de protection des données dans l'ensemble de l'Union, le fonctionnement du nouveau système de gouvernance, les incidences sur les citoyens et les entreprises et les efforts déployés par l'UE pour promouvoir une convergence mondiale des régimes de protection des données. La présente communication fait suite à la communication de la Commission relative à l'application du règlement de janvier 2018[5] et repose sur les travaux du groupe multipartite[6], en particulier sa contribution à l'exercice consistant à dresser un bilan après un an et les discussions tenues lors de l'événement relatif au bilan organisé par la Commission le 13 juin 2019[7]. Elle constitue également une contribution à l'examen que la Commission prévoit de réaliser d'ici mai 2020 [8].

Le cadre législatif de l'UE en matière de protection des données est une pierre angulaire de l'approche européenne de l'innovation axée sur le facteur humain. Il commence à faire partie du fondement réglementaire d'un nombre croissant de politiques dans des domaines tels que la santé et la recherche, l'intelligence artificielle, les transports, l'énergie, la concurrence et l'application des lois. La Commission n'a eu de cesse d'insister sur l'importance d'une mise en œuvre et d'une application correctes des nouvelles règles en matière de protection des données, comme elle le souligne dans sa communication relative à l'application du règlement publiée en janvier 2018 et dans ses orientations relatives à l'utilisation de données à caractère personnel dans le contexte électoral publiées en septembre 2018[9]. Au moment de la publication de la présente communication, de nombreux progrès avaient été accomplis sur la

---

5 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) 43 final: https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

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

7 https://europa.eu/rapid/press-release_IP-19-2956_fr.htm.

8 Article 97 du règlement.

9 «Orientations de la Commission relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral», COM(2018) 638 final: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0638&from=FR.

voie de la réalisation de cet objectif, bien que des efforts supplémentaires soient certainement nécessaires pour que le règlement devienne pleinement opérationnel.

II. Un continent, une législation: le cadre de protection des données est en place dans les États membres

Un objectif clé du règlement consistait à mettre un terme à la fragmentation due aux 28 législations nationales différentes qui existaient en vertu de la directive antérieure relative à la protection des données[10] et à garantir la sécurité juridique aux personnes et aux entreprises dans toute l'UE. Cet objectif a été largement atteint.

L'harmonisation du cadre juridique

Bien que le règlement soit directement applicable dans les États membres, il les a obligés à prendre plusieurs mesures juridiques au niveau national, en particulier à créer des autorités nationales de protection des données et à leur conférer des pouvoirs[11], à élaborer des règles sur des questions spécifiques, telles que la conciliation de la protection des données à caractère personnel avec la liberté d'expression et d'information, et à modifier ou abroger certains actes législatifs sectoriels renfermant des aspects liés à la protection des données. Au moment de la publication de la présente communication, tous les États membres sauf trois[12] avaient actualisé leur législation nationale en matière de protection des données. Les travaux relatifs à l'adaptation des actes législatifs sectoriels sont toujours en cours au niveau national. À la suite de son intégration dans l'accord sur l'Espace économique européen, l'application du règlement a été étendue à la Norvège, à l'Islande et au Liechtenstein, lesquels ont également adopté leur législation nationale en matière de protection des données.

Cependant, les parties prenantes réclament un degré d'harmonisation plus élevé encore dans certains domaines[13]. En effet, le règlement laisse aux États membres une certaine marge pour préciser son application dans certains domaines, comme l'âge de consentement des enfants pour les services en ligne[14] ou le traitement des données à caractère personnel dans des domaines tels que la médecine ou la santé publique. Dans ce cas, l'action des États membres est encadrée par deux éléments:

---

[10] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31995L0046.

[11] Comme le pouvoir d'infliger des amendes administratives.

[12] Au 23 juillet 2019, le processus d'adoption de la législation nationale était toujours en cours en Grèce, au Portugal et en Slovénie.

[13] Voir le rapport du groupe multipartite sur le règlement publié le 13 juin 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

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

i) toute loi nationale visant à préciser le règlement doit satisfaire aux exigences de la charte des droits fondamentaux[15] (et ne pas dépasser les limites fixées par le règlement, qui s'appuie sur la charte);
ii) elle ne peut empiéter sur la libre circulation des données à caractère personnel au sein de l'UE[16].

Dans certains cas, les États membres ont introduit des exigences nationales en plus du règlement, notamment au moyen de nombreux actes législatifs sectoriels, ce qui entraîne une fragmentation et crée des charges inutiles. Un exemple d'exigence supplémentaire introduite par les États membres en plus du règlement est l'obligation prévue par la législation allemande de désigner un délégué à la protection des données dans les entreprises comptant 20 employés ou plus participant en permanence au traitement automatisé de données à caractère personnel.

Poursuite des efforts vers une harmonisation accrue

La Commission mène des dialogues bilatéraux avec les autorités nationales, dans le cadre desquels elle accorde une attention particulière aux mesures nationales concernant:

- l'indépendance effective des autorités de protection des données, y compris au moyen de ressources financières, humaines et techniques suffisantes;
- la manière dont la législation nationale limite les droits des personnes concernées;
- le fait que la législation nationale ne devrait pas introduire d'exigences allant plus loin que le règlement lorsqu'il n'existe pas de marge pour préciser le règlement, comme des conditions supplémentaires pour le traitement;
- le respect de l'obligation de concilier le droit à la protection des données à caractère personnel avec la liberté d'expression et d'information, compte tenu du fait qu'il ne faut pas abuser de cette obligation pour créer un effet dissuasif sur le travail journalistique.

Le travail des autorités de protection des données, qui coopèrent dans le contexte du comité européen de la protection des données (ci-après le «comité»), est essentiel pour assurer une application cohérente des nouvelles règles: les actions coercitives concernant plusieurs États membres passent par le mécanisme de coopération et de cohérence[17] au sein dudit comité et les lignes directrices adoptées par ce dernier contribuent à harmoniser l'interprétation du règlement. Néanmoins, les parties prenantes attendent des autorités de protection des données qu'elles aillent plus loin dans cette direction.

Le travail des juridictions nationales et de la Cour de justice de l'Union européenne contribue également à créer une interprétation cohérente des règles en matière de protection des

---

15 Article 8.
16 Conformément à l'article 16, paragraphe 2, du traité sur le fonctionnement de l'Union européenne.
17 L'article 60 du règlement prévoit une coopération entre les autorités de protection des données en vue d'appliquer une seule et même interprétation du règlement dans des cas concrets. L'article 64 du règlement dispose que le comité européen de la protection des données émet des avis dans certains cas afin de garantir une application cohérente du règlement. Enfin, le comité a le pouvoir d'adresser des décisions contraignantes aux autorités de protection des données en cas de désaccord entre elles.

données. Des juridictions nationales ont récemment rendu des jugements invalidant des dispositions nationales s'écartant du règlement[18].

III. Tous les éléments du nouveau système de gouvernance se mettent en place

Le règlement a créé une nouvelle structure de gouvernance, plaçant en son centre les autorités nationales indépendantes de protection des données, chargées de faire appliquer le règlement et de faire office de premiers points de contact pour les parties prenantes. Bien que la plupart des autorités de protection des données aient bénéficié l'année dernière de ressources accrues, de grandes différences demeurent entre les États membres[19].

Les autorités de protection des données utilisent leurs nouveaux pouvoirs

Le règlement dote les autorités de protection des données de pouvoirs d'exécution renforcés. Contrairement aux craintes exprimées par certaines parties prenantes avant mai 2018, les autorités nationales de protection des données ont adopté une approche équilibrée à l'égard des pouvoirs d'exécution. Elles se sont concentrées sur le dialogue plutôt que sur les sanctions, surtout pour les plus petits opérateurs dont le traitement de données à caractère personnel n'est pas l'activité principale. Dans le même temps, elles n'ont pas hésité à utiliser leurs nouveaux pouvoirs de manière effective chaque fois que nécessaire, y compris en ouvrant des enquêtes dans le domaine des médias sociaux[20] et en infligeant des amendes administratives allant de quelques milliers à plusieurs millions d'euros, en fonction de la gravité des infractions aux règles de protection des données.

Exemples d'amendes infligées par des autorités de protection des données[21]:

- 5 000 EUR pour un café de paris sportifs en Autriche, pour surveillance vidéo illégale;
- 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;
- 50 000 000 EUR pour Google en France, en raison des conditions d'obtention du consentement des utilisateurs.

Lorsqu'elles mènent des enquêtes, il est essentiel que les autorités de protection des données collectent des éléments de preuve pertinents, respectent toutes les étapes procédurales prévues par la législation nationale et garantissent un traitement équitable dans des dossiers souvent complexes. Cela nécessite du temps et beaucoup de travail, ce qui explique la raison pour

---

18 Tel a été le cas en Allemagne et en Espagne.

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 Par exemple, la commission irlandaise de protection des données a ouvert 15 enquêtes officielles concernant le respect du règlement par des entreprises multinationales du secteur de la technologie. Voir p. 49 du rapport annuel 2018 de ladite commission: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Plusieurs décisions infligeant des amendes font toujours l'objet d'un contrôle juridictionnel.

laquelle la plupart des enquêtes ouvertes après l'entrée en vigueur du règlement sont toujours en cours.

Cela dit, le succès du règlement ne devrait pas être mesuré à l'aune du nombre d'amendes infligées, mais bien à l'aune des changements dans la culture et le comportement de tous les acteurs concernés. Dans ce contexte, les autorités de protection des données disposent d'autres outils, tels que l'imposition d'une limitation temporaire ou définitive du traitement, y compris une interdiction, ou la suspension des flux de données vers un destinataire dans un pays tiers[22].

Certaines autorités de protection des données ont créé de nouveaux outils, comme des lignes d'assistance et des boîtes à outils pour les entreprises, tandis que d'autres ont élaboré des approches innovantes, comme des bacs à sable réglementaires[23] pour aider les entreprises dans leurs efforts de mise en conformité. Toutefois, certaines parties prenantes considèrent toujours qu'elles n'ont pas reçu suffisamment de soutien et d'informations, surtout des petites et moyennes entreprises de certains États membres[24]. Pour contribuer à remédier à cette situation, la Commission octroie des subventions aux autorités de protection des données pour qu'elles prennent contact avec les parties prenantes, en particulier les personnes et les petites et moyennes entreprises[25].

Le comité européen de la protection des données est opérationnel

Les autorités de protection des données ont intensifié leurs travaux au sein du comité européen de la protection des données[26], ce qui a permis à ce dernier d'adopter quelque 20 lignes directrices sur des aspects clés du règlement[27]. Les futurs domaines de travail du comité sont présentés dans un programme de deux ans[28], ainsi que l'exige le règlement.

Dans les affaires transfrontières, chaque autorité de protection des données n'est plus simplement une autorité nationale, mais fait partie d'un processus couvrant véritablement l'ensemble de l'Union à tous les stades, de l'enquête à la décision. Cette étroite coopération est devenue une pratique quotidienne: fin juin 2019, 516 affaires transfrontières avaient été gérées par l'intermédiaire du mécanisme de coopération.

---

22 Article 58, paragraphe 2, points f) et j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 Voir le rapport du groupe multipartite sur le RGPD: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670

25 2 000 000 EUR ont été alloués à neuf autorités de protection des données en 2018 pour des activités en 2018-2019: Belgique, Bulgarie, Danemark, Hongrie, Lettonie, Lituanie, Pays-Bas, Slovénie et Islande: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
1 000 000 EUR doit être alloué en 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Le comité est doté de la personnalité juridique et est composé des chefs des autorités nationales de contrôle de la protection des données et du Contrôleur européen de la protection des données.

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

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_fr

La Commission contribue activement aux travaux du comité[29] visant à promouvoir la lettre et l'esprit du règlement et rappelle les principes généraux du droit de l'Union[30].

Vers la création d'une culture de la protection des données au sein de l'UE

Le nouveau système de gouvernance doit encore réaliser son plein potentiel. Il importe que le comité européen de la protection des données continue de rationaliser son processus décisionnel et développe une culture commune de la protection des données au sein de l'UE parmi ses membres. Les possibilités, pour les autorités de protection des données, de mettre en commun leurs efforts[31] concernant des questions touchant plus d'un État membre, par exemple d'effectuer des enquêtes conjointes et de prendre des mesures répressives conjointes, peuvent contribuer à cet objectif, tout en diminuant les contraintes du point de vue des ressources.

De nombreuses parties prenantes souhaitent voir encore plus de coopération et une approche uniforme de la part des autorités nationales de protection des données[32]. Elles réclament aussi plus de cohérence dans les conseils prodigués par les autorités de protection des données[33] et l'alignement de l'ensemble des lignes directrices nationales sur celles du comité européen de la protection des données. Certaines espèrent aussi des clarifications de notions clés du règlement, comme l'approche fondée sur les risques, tenant particulièrement compte des inquiétudes notamment des petites et moyennes entreprises.

Dans ce contexte, autoriser les parties prenantes à participer davantage aux travaux du comité est essentiel. C'est pourquoi la Commission se félicite de la consultation publique systématique organisée par le comité au sujet des lignes directrices. Cette pratique, à l'instar de l'organisation d'ateliers pour les parties prenantes sur des sujets ciblés à un stade précoce de la réflexion, devrait être perpétuée et amplifiée afin de garantir la transparence, l'inclusivité et la pertinence des travaux du comité.

IV. Les personnes se prévalent de leurs droits, mais la sensibilisation devrait se poursuivre

Un autre objectif clé du règlement consistait à renforcer les droits des personnes. Le règlement est largement considéré par les associations de défense des droits civils et les organisations de consommateurs comme apportant une importante contribution à une société numérique juste fondée sur la confiance mutuelle.

---

29 En tant que participant sans droit de vote.

30 La Commission a aussi contribué à faciliter la mise en place du comité et soutient son fonctionnement en fournissant son système de communication.

31 Article 62 du règlement.

32 Voir le rapport du groupe multipartite sur le règlement: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Par exemple, les entreprises pensent que les listes nationales des types d'opérations de traitement qui nécessitent une analyse d'impact relative à la protection des données au titre de l'article 35 du règlement auraient pu être mieux harmonisées.

33 Y compris entre les diverses autorités des États fédéraux.

Une meilleure sensibilisation aux droits en matière de protection des données

Les personnes au sein de l'UE connaissent de mieux en mieux les règles en matière de protection des données et leurs droits: 67 % des personnes interrogées dans le cadre d'un Eurobaromètre de mai 2019[34] ont connaissance du règlement et 57 % savent qu'il existe une autorité nationale de protection des données vers laquelle elles peuvent se tourner pour demander des informations ou introduire une réclamation. 73 % ont entendu parler d'au moins un des droits conférés par le règlement. Toutefois, un nombre non négligeable de personnes au sein de l'UE ne prennent toujours pas activement des mesures pour protéger leurs données à caractère personnel lorsqu'elles se rendent sur l'internet. Par exemple, 44 % des personnes n'ont pas modifié leurs paramètres de confidentialité par défaut sur les réseaux sociaux.

Les personnes se prévalent de plus en plus de leurs droits

Grâce à cette prise de conscience accrue des droits, les personnes se prévalent davantage de ceux-ci en posant des questions en tant que clients et en se tournant plus fréquemment vers les autorités de protection des données pour demander des informations ou introduire des réclamations[35]. Les entreprises font également état d'une hausse des demandes d'accès aux données à caractère personnel dans plusieurs secteurs, comme le secteur bancaire et celui des télécommunications. Les personnes ont aussi plus souvent retiré leur consentement et exercé leur droit de s'opposer aux communications commerciales[36].

Cependant, certains opérateurs ont signalé des malentendus au sujet des règles de protection des données, comme le fait que certaines personnes pensent qu'elles doivent consentir à tout traitement ou que le droit à l'effacement est absolu (alors que, par exemple, des données à caractère personnel doivent parfois être conservées par les opérateurs en raison d'obligations légales)[37]. Les organisations de la société civile, quant à elles, se plaignent des longs délais de réponse de certaines entreprises et autorités de protection des données.

Il importe de relever que plusieurs actions collectives ont été engagées par des organisations non gouvernementales mandatées par des personnes, faisant usage de la nouvelle possibilité offerte par le règlement[38]. Le recours aux actions collectives aurait été facilité si davantage d'États membres avaient fait usage de la possibilité prévue par le règlement d'autoriser des organisations non gouvernementales à engager des actions sans mandat[39].

---

34 https://europa.eu/rapid/press-release_IP-19-2956_fr.htm
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
36 Voir le rapport du groupe multipartite sur le règlement général sur la protection des données.
37 Voir le rapport du groupe multipartite sur le règlement général sur la protection des données.
38 Article 80, paragraphe 1, du règlement.
39 Article 80, paragraphe 2, du règlement.

La nécessité de poursuivre les efforts de sensibilisation

Le dialogue et les efforts de sensibilisation axés sur le grand public doivent donc se poursuivre aux niveaux national et de l'UE. À cette fin, la Commission a lancé en juillet 2019 une nouvelle campagne en ligne[40] en vue d'encourager les personnes à lire les déclarations de confidentialité et à optimiser leurs paramètres de confidentialité.

V. Les entreprises adaptent leurs pratiques

Le règlement vise à aider les entreprises dans l'économie numérique en offrant des solutions d'avenir. Les entreprises se félicitent en général du principe de responsabilité prévu par le règlement, qui représente une évolution par rapport à l'ancienne approche ex ante, qui était fastidieuse (suppression des exigences de notification, modularité des obligations et souplesse du principe de la protection des données dès la conception et par défaut permettant une concurrence sur la base de solutions respectueuses de la vie privée). Dans le même temps, certaines entreprises réclament une sécurité juridique accrue et des lignes directrices supplémentaires ou plus claires de la part des autorités de protection des données[41].

Bonne gestion des données

Alors que des entreprises affirment avoir rencontré un certain nombre de difficultés à l'heure de s'adapter aux nouvelles règles[42], nombre d'entre elles soulignent que c'était également l'occasion de porter la question de la protection des données à l'attention des conseils d'administration, de mettre de l'ordre concernant les données qu'elles détiennent, d'améliorer la sécurité, d'être mieux préparées aux incidents, de réduire l'exposition à des risques superflus et de consolider les relations de confiance avec leurs clients et partenaires commerciaux. Pour ce qui est de la transparence, les entreprises et les organisations de la société civile mentionnent le délicat équilibre à ménager entre, d'une part, la fourniture aux personnes de toutes les informations requises au titre du règlement et, d'autre part, l'utilisation d'un langage clair et simple et d'un formulaire que les personnes sont en mesure de comprendre. Les opérateurs développent des solutions innovantes en ce sens.

En général, les entreprises ont indiqué qu'elles étaient en mesure de mettre en œuvre les nouveaux droits des personnes concernées, même s'il était parfois difficile de respecter les délais en raison d'un nombre accru de demandes et de leur caractère plus varié[43] ou de vérifier l'identité de la personne à l'origine de la demande.

---

[40] Celle-ci fait suite à une campagne précédente qui visait à diffuser du matériel d'information pour les personnes et les entreprises, disponible à l'adresse suivante: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr.

[41] Voir le rapport du groupe multipartite sur le règlement.

[42] La mise à jour du système informatique est souvent citée comme étant l'une des principales difficultés, surtout en ce qui concerne la mise en œuvre des principes de protection des données dès la conception et par défaut, le droit à l'effacement dans les sauvegardes, etc.

[43] Les entreprises plaident également en faveur de lignes directrices du comité européen de la protection des données sur les demandes non fondées et excessives.

Incidences sur l'innovation

Le règlement non seulement permet, mais encourage aussi le développement de nouvelles technologies dans le respect du droit fondamental à la protection des données à caractère personnel. C'est le cas dans des domaines tels que l'intelligence artificielle.

Les entreprises ont commencé à développer leur offre de nouveaux services, plus respectueux de la vie privée. Ainsi, des moteurs de recherche qui ne suivent pas la trace des utilisateurs ou n'utilisent pas de publicité comportementale gagnent progressivement des parts de marché dans certains États membres. D'autres entreprises développent des services qui reposent sur de nouveaux droits accordés aux personnes, comme la portabilité de leurs données à caractère personnel. Un nombre croissant d'entreprises ont encouragé le respect des données à caractère personnel en tant qu'atout concurrentiel et argument de vente. Ces évolutions ne se limitent pas à l'UE, mais concernent aussi des économies étrangères très innovantes[44].

La situation particulière des micro et petites entreprises «à faible risque»

Bien que la situation varie d'un État membre à l'autre, les micro et petites entreprises[45] dont le traitement de données à caractère personnel ne constitue pas l'activité principale comptent parmi les parties prenantes qui se posent le plus de questions au sujet de l'application du règlement. Si ces questions semblent être dues en partie à un manque de connaissance des règles en matière de protection des données, les inquiétudes de ces entreprises sont aussi parfois exacerbées par des campagnes de cabinets de consultance cherchant à prodiguer des conseils payants, par la diffusion d'informations incorrectes, par exemple sur la nécessité d'obtenir systématiquement le consentement des personnes[46], ainsi que par les exigences supplémentaires imposées au niveau national.

Dans ce contexte, les micro et petites entreprises réclament des lignes directrices adaptées à leur situation spécifique et fournissant des informations très concrètes. Certaines autorités de protection des données en ont déjà adopté au niveau national[47]. Pour compléter les initiatives nationales, la Commission a publié du matériel d'information pour aider ces entreprises à se conformer aux nouvelles règles en suivant une série d'étapes pratiques[48].

Utilisation de la boîte à outils prévue par le règlement

Le règlement prévoit des outils permettant de démontrer la conformité, comme des clauses contractuelles types, des codes de conduite et les nouveaux mécanismes de certification.

---

44 Par exemple, d'après un rapport publié par l'association israélienne de l'industrie de la cybersécurité, en 2018, le sous-secteur «protection des données et respect de la vie privée» de la cybersécurité était celui qui connaissait la croissance la plus rapide, notamment grâce à l'entrée en vigueur du RGPD.

45 Telles que définies dans la définition des PME, disponible à l'adresse suivante: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_fr.

46 En fait, le règlement ne repose pas seulement sur le consentement, mais prévoit plusieurs motifs juridiques pour le traitement de données à caractère personnel.

47 Par exemple, le guide élaboré par l'autorité française de protection des données: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-fr-n.pdf.

Les clauses contractuelles types sont des clauses modèles qui peuvent être incluses sur une base volontaire dans un contrat, par exemple entre un responsable du traitement et un sous-traitant, et qui définissent les obligations des parties contractantes au titre du règlement. Le règlement étend les possibilités de recours à des clauses contractuelles types pour les transferts tant internationaux qu'au sein de l'UE[49]. Dans le domaine des transferts internationaux, l'important recours à ces clauses indique[50] qu'elles sont très utiles pour les entreprises dans leurs efforts de mise en conformité et qu'elles bénéficient particulièrement aux sociétés qui ne disposent pas des ressources nécessaires pour négocier des contrats individuels avec chacun de leurs sous-traitants.

Plusieurs secteurs considèrent aussi que l'adoption de clauses contractuelles types constitue une manière utile de favoriser l'harmonisation, en particulier lorsque c'est la Commission qui les adopte. La Commission collaborera avec les parties prenantes pour faire usage des possibilités prévues par le règlement et actualiser les clauses existantes.

L'adhésion à des codes de conduite est un autre outil opérationnel et pratique dont dispose l'industrie pour faciliter la démonstration du respect du règlement[51]. Ces codes devraient être élaborés par des associations commerciales ou des organismes représentant certaines catégories de responsables du traitement et de sous-traitants et devraient décrire la façon dont les règles en matière de protection des données peuvent être mises en œuvre dans un secteur donné. En définissant les obligations compte tenu des risques[52], ces codes peuvent aussi se révéler être un moyen très utile et rentable pour les petites et moyennes entreprises de remplir leurs obligations.

Enfin, la certification peut également constituer un instrument utile pour démontrer le respect d'exigences spécifiques du règlement. Elle peut renforcer la sécurité juridique pour les entreprises et promouvoir le règlement au niveau mondial. Les lignes directrices relatives à la certification et à l'agrément[53] adoptées récemment par le comité européen de la protection des données permettront la mise en place de régimes de certification au sein de l'UE. La Commission suivra ces évolutions et, le cas échéant, fera usage des pouvoirs qui lui sont conférés par le règlement pour encadrer les exigences en matière de certification. Elle peut également adresser une demande de normalisation à des organismes de normalisation de l'UE concernant des éléments pertinents pour le règlement.

---

49 Voir article 28 du règlement. Les clauses contractuelles types adoptées par la Commission sont valables dans l'ensemble de l'UE. En revanche, celles adoptées en vertu de l'article 28, paragraphe 8, par une autorité de protection des données ne lient que l'autorité qui les a adoptées et peuvent donc être utilisées en tant que clauses contractuelles types pour les opérations de traitement qui relèvent de la compétence de ladite autorité, conformément aux articles 55 et 56.

50 Elles constituent en fait le principal outil sur lequel les entreprises se fondent pour leurs exportations de données.

51 Le comité européen de la protection des données a adopté des lignes directrices sur les codes de conduite le 4 juin 2019. Celles-ci précisent les procédures et les règles encadrant la présentation, l'approbation et la publication des codes tant au niveau national qu'au niveau de l'UE.

52 Considérant 98 du règlement.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_fr

VI. La convergence vers le haut progresse au niveau international

L'exigence de protection des données à caractère personnel ne se limite pas à l'UE. Comme démontré par une récente enquête mondiale sur la sécurité de l'internet, le déficit de confiance s'aggrave dans le monde, de sorte que les personnes modifient la manière dont elles se comportent en ligne[54]. Un nombre croissant d'entreprises répondent à ces inquiétudes en étendant de leur propre gré les droits créés par le règlement à leurs clients non établis dans l'UE.

De plus, alors que les pays de par le monde sont de plus en plus confrontés à des défis similaires, ils se dotent de nouvelles règles de protection des données ou modernisent les règles existantes. Ces règles présentent souvent plusieurs points communs qui sont partagés par le régime de protection des données de l'UE, comme une législation globale plutôt que des règles sectorielles, des droits individuels opposables et une autorité de contrôle indépendante. Cette tendance est véritablement mondiale et s'observe de la Corée du Sud au Brésil, en passant par le Chili, la Thaïlande, l'Inde et l'Indonésie. L'universalité croissante des parties à la «convention 108» du Conseil de l'Europe[55] – récemment modernisée[56] avec une contribution significative de la Commission – est un autre signe clair de cette tendance à la convergence vers le haut.

Promotion de la libre circulation de flux de données sécurisés au moyen de décisions d'adéquation, etc.

Cette convergence qui se développe offre de nouvelles possibilités de faciliter les flux de données, et donc le commerce et la coopération entre les pouvoirs publics, tout en améliorant le niveau de protection des données des personnes au sein de l'UE lorsqu'elles sont transférées à l'étranger.

---

54 Voir enquête mondiale 2019 de CIGI-Ipsos sur la sécurité de l'internet et la confiance. Selon cette enquête, 78 % des personnes interrogées nourrissaient des inquiétudes quant au respect de la confidentialité en ligne, 49 % affirmant que leur méfiance les avait poussées à divulguer moins d'informations à caractère personnel en ligne, tandis que 43 % indiquaient se soucier davantage de la sécurisation de leur appareil et 39 % ont répondu qu'elles utilisaient l'internet de manière plus sélective, entre autres précautions. L'enquête a été réalisée dans 25 économies: l'Afrique du Sud, l'Allemagne, l'Australie, le Brésil, le Canada, la Chine, l'Égypte, les États-Unis, la France, la Grande-Bretagne, Hong Kong, l'Inde, l'Indonésie, l'Italie, le Japon, le Kenya, le Mexique, le Nigeria, le Pakistan, la Pologne, la République de Corée, la Russie, la Suède, la Tunisie et la Turquie.

55 Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) et protocole additionnel de 2001 à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE nº 181). C'est le seul instrument multilatéral contraignant dans le domaine de la protection des données. Les derniers pays à avoir ratifié la convention sont l'Argentine, le Mexique, le Cap-Vert et le Maroc.

56 Protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) adopté lors de la 128e session du Comité des ministres tenue à Elseneur, au Danemark, les 17 et 18 mai 2018. Le texte consolidé de la convention 108 modernisée est disponible à l'adresse: https://rm.coe.int/16808ade9d.

Dans le cadre de la mise en œuvre de la stratégie définie dans sa communication de 2017 sur l'échange et la protection de données à caractère personnel à l'ère de la mondialisation[57], la Commission a renforcé ses contacts avec les pays tiers et d'autres partenaires internationaux en se fondant sur des éléments de convergence entre les systèmes de protection de la vie privée et en les développant plus avant. Elle a notamment étudié la possibilité d'adopter des constats d'adéquation avec certains pays tiers[58]. Ces travaux ont généré d'importants résultats, en particulier l'entrée en vigueur, en février 2019, de la décision d'adéquation mutuelle UE-Japon qui a donné lieu à la création de la zone de libre circulation de flux de données sécurisés la plus grande au monde. Les négociations relatives à l'adéquation avec la Corée du Sud en sont à un stade avancé et les travaux exploratoires ont débuté en vue de lancer des pourparlers sur l'adéquation avec plusieurs pays d'Amérique latine (comme le Chili ou le Brésil), en fonction de l'achèvement de processus législatifs en cours. L'évolution de la situation est également prometteuse dans certaines parties d'Asie, notamment en Inde, en Indonésie et à Taïwan, ainsi que dans le voisinage oriental et méridional de l'Europe, ce qui pourrait ouvrir la voie à de futures décisions d'adéquation.

Parallèlement, la Commission salue le fait que d'autres pays ayant mis en place des instruments de transfert similaires à l'adéquation prévue par le règlement ont reconnu que l'UE et les pays reconnus par cette dernière comme étant «adéquats» garantissent le niveau requis de protection[59], ce qui pourrait permettre la mise en place d'un réseau de pays au sein duquel les données peuvent circuler librement.

Par ailleurs, d'intenses travaux sont en cours avec d'autres pays tiers, tels que le Canada, la Nouvelle-Zélande, l'Argentine et Israël, afin d'assurer la continuité, au titre du règlement, des décisions d'adéquation adoptées sur la base de la directive sur la protection des données de 1995. Par ailleurs, le bouclier de protection des données UE-États-Unis s'est révélé être un outil utile pour garantir des flux de données transatlantiques fondés sur un niveau élevé de protection, plus de 4 700 entreprises y participant[60]. Son examen annuel garantit que le bon fonctionnement du cadre est vérifié régulièrement et que les nouveaux problèmes peuvent être traités à temps.

Étant donné qu'il n'existe pas de solution universelle pour les flux de données, la Commission collabore également avec les parties prenantes et le comité pour exploiter pleinement le potentiel de la boîte à outils du règlement pour les transferts internationaux. Cela concerne des instruments tels que les clauses contractuelles types, la mise en place de régimes de certification, de codes de conduite ou d'arrangements administratifs pour les organismes publics. À cet égard, la Commission souhaite échanger les expériences et les bonnes pratiques

---

57 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», COM(2017) 7 final.

58 Le règlement a aussi créé la possibilité d'établir des constats d'adéquation également à l'égard d'organisations internationales, dans le cadre des efforts de l'UE visant à faciliter les échanges de données avec ces entités.

59 C'est l'approche adoptée, par exemple, par l'Argentine, la Colombie, Israël et la Suisse.

60 Cela signifie qu'au cours de ses trois premières années d'existence, le bouclier de protection comptait plus d'entreprises participantes que son prédécesseur, la sphère de sécurité, n'en avait après 13 ans de fonctionnement.

avec d'autres systèmes pouvant avoir développé une expertise spécifique concernant certains de ces outils. Elle envisagera le recours aux pouvoirs conférés par le règlement en ce qui concerne ces instruments de transfert, en particulier les clauses contractuelles types.

Outre les outils purement bilatéraux, il pourrait aussi s'avérer utile d'étudier si des pays partageant la même vision pourraient établir un cadre multinational en la matière à une époque où les flux de données constituent une composante de plus en plus cruciale du commerce, des communications et des interactions sociales. Un tel instrument permettrait aux données de circuler librement entre les parties contractantes, tout en assurant le niveau de protection requis sur la base de valeurs partagées et de systèmes convergents. Il pourrait être élaboré, par exemple, en se basant sur la convention 108 modernisée ou en s'inspirant de l'initiative «libre flux de données en toute confiance» lancée par le Japon au début de cette année.

Création de nouvelles synergies entre les instruments commerciaux et de protection des données

Tout en promouvant la convergence des normes de protection des données au niveau international, la Commission est aussi déterminée à s'attaquer au protectionnisme numérique. 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 lors de ses négociations bilatérales et multilatérales, comme les actuels pourparlers sur le commerce électronique avec l'OMC. Ces dispositions horizontales excluent les mesures purement protectionnistes, telles que les exigences relatives à la localisation forcée des données, tout en préservant l'autonomie réglementaire des parties pour protéger le droit fondamental à la protection des données.

Bien que les dialogues sur la protection des données et les négociations commerciales doivent suivre des voies différentes, ils peuvent se compléter: la décision d'adéquation mutuelle UE-Japon est le meilleur exemple de ces synergies, puisqu'elle a encore facilité les échanges commerciaux, amplifiant ainsi les avantages de l'accord de partenariat économique. En fait, ce type de convergence, reposant sur des valeurs partagées et des normes élevées et soutenue par une mise en œuvre effective, constitue le fondement le plus solide pour l'échange de données à caractère personnel, ainsi que nos partenaires internationaux le reconnaissent de plus en plus[61]. 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 le commerce et améliorant la confiance entre les partenaires commerciaux.

---

[61] Comme en témoigne, par exemple, la référence à la notion de «libre flux de données en toute confiance» employée dans la déclaration d'Osaka des dirigeants du G20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

Facilitation de l'échange d'informations pour lutter contre la criminalité et le terrorisme sur la base de garanties appropriées

Une meilleure compatibilité entre les régimes de protection des données peut aussi faciliter considérablement les échanges d'informations nécessaires entre les autorités réglementaires, policières et judiciaires étrangères et de l'UE et, ainsi, contribuer à rendre la coopération en matière répressive plus efficace et plus rapide[62]. À cette fin, la Commission envisage de recourir à la possibilité d'adopter des décisions d'adéquation au titre de la directive en matière de protection des données dans le domaine répressif afin d'approfondir sa coopération avec des partenaires clés dans la lutte contre la criminalité et le terrorisme. De plus, l'«accord-cadre» UE-États-Unis[63], qui est entré en vigueur en février 2017, peut servir de modèle pour des accords similaires avec d'autres partenaires importants en matière de sécurité.

D'autres exemples montrant l'importance de normes élevées de protection des données comme base pour une coopération stable en matière répressive avec les pays tiers sont le transfert de données des dossiers passagers (données PNR)[64] et l'échange d'informations opérationnelles entre Europol et d'importants partenaires internationaux. À cet égard, des négociations sur des accords internationaux sont en cours ou sur le point de débuter avec plusieurs pays du voisinage méridional[65].

De solides garanties en matière de protection des données seront également un élément essentiel de tout futur accord sur l'accès transfrontière aux preuves électroniques dans les enquêtes pénales, au niveau bilatéral (accord UE-États-Unis) ou multilatéral (deuxième protocole additionnel à la «convention de Budapest» sur la cybercriminalité du Conseil de l'Europe[66]).

---

62 Voir la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Le programme européen en matière de sécurité», COM(2015) 185 final.

63 Accord entre l'Union européenne et les États-Unis sur la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et judiciaire en matière pénale: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:22016A1210(01) (l'«accord-cadre»). L'accord-cadre est le premier accord international bilatéral dans le domaine répressif prévoyant un catalogue complet de droits et obligations en matière de protection des données conformément à l'acquis de l'UE. C'est un exemple probant de la manière dont la coopération en matière répressive avec un partenaire international majeur peut être améliorée en négociant un ensemble solide de garanties au regard de la protection des données.

64 Dans sa résolution 2396 du 21 décembre 2017, le Conseil de sécurité des Nations unies invite tous les États membres des Nations unies à renforcer leur capacité de collecter, de traiter et d'analyser les données PNR, dans le plein respect des droits de l'homme et des libertés fondamentales. Voir aussi la communication de la Commission intitulée «Le programme européen en matière de sécurité», COM(2015) 185 final: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_fr.pdf.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

66 http://europa.eu/rapid/press-release_IP-19-2891_fr.htm

Promotion de la coopération entre instances chargées de veiller à la protection des données

À une époque où des problèmes de respect de la confidentialité ou des incidents de sécurité peuvent toucher un grand nombre de personnes simultanément dans plusieurs juridictions, des formes de coopération plus étroites entre les autorités de contrôle au niveau international peuvent contribuer à garantir une protection plus efficace des droits individuels et un environnement plus stable pour les opérateurs commerciaux. Dans ce contexte, et en étroite collaboration avec le comité européen de la protection des données, la Commission cherchera des moyens de faciliter la coopération en matière répressive et l'assistance mutuelle entre les autorités de contrôle de l'UE et étrangères, y compris en faisant usage des nouveaux pouvoirs prévus dans ce domaine par le règlement[67]. Cela pourrait couvrir différentes formes de coopération, allant de l'élaboration d'outils pratiques ou d'interprétation communs[68] à l'échange d'informations sur des enquêtes en cours.

Enfin, la Commission entend aussi renforcer son dialogue avec les organisations et réseaux régionaux, comme l'Association des nations de l'Asie du Sud-Est (ASEAN), l'Union africaine, le Forum des autorités chargées de la protection de la vie privée pour l'Asie-Pacifique (APPA) ou le réseau ibéro-américain de protection des données, qui jouent un rôle toujours plus important dans la définition de normes communes de protection des données, en promouvant l'échange de bonnes pratiques et en favorisant la coopération entre les instances chargées de veiller à la protection des données. Elle collaborera également avec l'Organisation de coopération et de développement économiques et l'Organisation de coopération économique Asie-Pacifique pour renforcer la convergence vers un niveau élevé de protection des données.

VII. La législation en matière de protection des données en tant que partie intégrante d'un large éventail de politiques

La protection des données à caractère personnel est garantie et intégrée dans plusieurs politiques de l'Union.

Services de télécommunications et de communication électronique

La Commission a adopté sa proposition de règlement «vie privée et communications électroniques» en janvier 2017[69]. Cette proposition vise à protéger la confidentialité des communications, telle que prévue dans la charte des droits fondamentaux, mais aussi à protéger les données à caractère personnel pouvant faire partie d'une communication ainsi que les équipements terminaux des utilisateurs finaux.

---

67 Voir article 50 du règlement sur la coopération internationale dans le domaine de la protection des données. Cette disposition couvre toute une série de formes de coopération, de l'échange d'informations sur la législation relative à la protection des données à la transmission des réclamations, en passant par l'entraide pour les enquêtes.

68 Comme des modèles communs pour la notification de violations.

69 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52017PC0010

La proposition de règlement «vie privée et communications électroniques» précise et complète le règlement en prévoyant des règles spécifiques aux fins susmentionnées. Elle modernise les règles actuelles de l'UE concernant la vie privée et les communications électroniques[70] afin de prendre en compte les évolutions technologiques et juridiques. Elle améliore le respect de la vie privée des personnes en étendant le champ d'application des nouvelles règles de sorte à couvrir également les prestataires de services de communication par contournement, créant ainsi des conditions de concurrence équitables pour tous les services de communications électroniques. Bien que le Parlement européen ait adopté un mandat pour lancer les trilogues en octobre 2017, le Conseil n'a pas encore approuvé une approche générale. La Commission reste pleinement attachée au règlement «vie privée et communications électroniques» et soutiendra les colégislateurs dans leurs efforts pour parvenir à une adoption rapide de la proposition de règlement.

Santé et recherche

Faciliter les échanges de données relatives à la santé, qui sont des données sensibles en vertu du règlement, entre États membres devient de plus en plus important dans le domaine de la santé publique pour des raisons d'intérêt général. Ces dernières incluent la fourniture de soins de santé ou d'un traitement, la protection contre les menaces transfrontières graves sur la santé, ainsi que la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux. Le règlement établit les règles qui garantissent le traitement et les échanges licites et sûrs des données de santé dans l'ensemble de l'UE. Ces règles s'appliquent également à l'accès de tiers aux données médicales des patients, y compris aux données contenues dans le dossier des patients, aux ordonnances électroniques et aux dossiers médicaux électroniques complets à long terme, ainsi qu'à leur utilisation à des fins scientifiques. Dans le domaine particulier des essais cliniques, la Commission a également élaboré des questions et réponses spécifiques sur l'interaction entre le règlement sur les essais cliniques[71] et le règlement général sur la protection des données[72].

Intelligence artificielle

Alors que l'intelligence artificielle gagne en importance stratégique, il est essentiel de définir des règles mondiales pour son développement et son utilisation. En promouvant le développement et l'adoption de l'intelligence artificielle, la Commission a opté pour une approche axée sur le facteur humain, ce qui signifie que les applications de l'intelligence artificielle doivent être conformes aux droits fondamentaux[73]. Dans ce contexte, les règles

---

70 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.

71 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

73 Communication de la Commission du 8 avril 2019 intitulée «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain»: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Lignes directrices en matière d'éthique pour une IA digne de confiance, présentées par le groupe d'experts de haut niveau sur l'intelligence artificielle le 8 avril 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Voir aussi la recommandation du Conseil de l'OCDE sur

énoncées dans le règlement fournissent un cadre général et contiennent des droits et obligations spécifiques qui sont particulièrement pertinents pour le traitement de données à caractère personnel dans le contexte de l'intelligence artificielle. Par exemple, le règlement inclut le droit de ne pas faire l'objet d'une prise de décision exclusivement automatisée, sauf dans certaines situations[74]. Il comprend aussi des obligations de transparence spécifiques concernant le recours à la prise de décision automatisée, à savoir l'obligation d'informer de l'existence de ces décisions, de fournir des informations utiles et d'expliquer l'importance et les conséquences prévues du traitement pour la personne[75]. Ces principes fondamentaux du règlement ont été reconnus par le groupe d'experts de haut niveau sur l'intelligence artificielle[76], l'Organisation de coopération et de développement économiques[77] et le G20[78] comme étant particulièrement pertinents pour relever les défis liés à l'intelligence artificielle et tirer parti des possibilités qu'elle offre. Le comité européen de la protection des données a défini l'intelligence artificielle comme l'un des thèmes possibles de son programme de travail 2019-2020[79].

Transports

Le développement des voitures connectées et des villes intelligentes repose de plus en plus sur le traitement et les échanges de grandes quantités de données à caractère personnel entre de nombreuses parties, y compris les véhicules, les constructeurs d'automobiles, les fournisseurs de services de télématique et les autorités publiques responsables des infrastructures routières. Cet environnement multipartite suppose une certaine complexité concernant l'attribution des rôles et responsabilités des différents acteurs participant au traitement de données à caractère personnel et la manière de garantir la licéité du traitement effectué par tous les acteurs. Le respect du règlement et de la législation relative à la vie privée et aux communications électroniques est essentiel pour déployer avec succès des systèmes de transport intelligents pour tous les modes de transport et pour déployer des outils et services numériques permettant une mobilité accrue des personnes et des marchandises[80].

Énergie

Le développement de solutions numériques dans le secteur de l'énergie passe de plus en plus par le traitement de données à caractère personnel. La législation adoptée dans le cadre du

---

l'intelligence artificielle: https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449, les principes relatifs à l'intelligence artificielle du G20 approuvés dans le cadre la déclaration d'Osaka des dirigeants du G20: https://www.g20.org/pdf/documents/en/annex_08.pdf et la 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.

74 Article 22 du règlement.

75 Article 13, paragraphe 2, point f), du règlement.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

77 Recommandation du Conseil sur l'intelligence artificielle: https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449.

78 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.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

80 Par exemple, en facilitant leur planification et l'utilisation de différents moyens de transport tout au long de leur parcours.

paquet «Une énergie propre pour tous les Européens»[81] comprend de nouvelles dispositions permettant la transformation numérique du secteur de l'électricité et des règles sur l'accès aux données, la gestion des données et l'interopérabilité qui permettent le traitement des données en temps réel des consommateurs pour réaliser des économies et encourager l'autoproduction et la participation au marché de l'énergie. Par conséquent, le respect des règles en matière de protection des données est très important pour la bonne mise en œuvre de ces dispositions.

Concurrence

Le traitement de données à caractère personnel est un élément qu'il faut de plus en plus prendre en considération dans la politique de concurrence[82]. Les autorités de protection des données étant les seules autorités habilitées à examiner une violation des règles de protection des données, les autorités chargées de la concurrence, de la protection des consommateurs et de la protection des données coopèrent et continueront de coopérer lorsque nécessaire à l'intersection de leurs compétences respectives. La Commission encouragera cette coopération et suivra de près l'évolution de la situation.

Contexte électoral

Dans ses orientations relatives à l'utilisation de données à caractère personnel dans le contexte électoral[83], publiées en septembre 2018 dans le cadre du paquet électoral[84], la Commission a attiré l'attention sur des règles revêtant une importance particulière pour les acteurs associés aux élections, y compris les questions relatives au microciblage des électeurs. Ces orientations ont été reflétées dans une déclaration du comité européen de la protection des données[85] et plusieurs autorités de protection des données ont publié des orientations au niveau national. Le paquet électoral invitait également chaque État membre à mettre en place un réseau électoral national associant les autorités nationales compétentes pour les questions électorales et les autorités chargées de la surveillance et de l'application des règles, notamment en matière de protection des données, relatives aux activités en ligne pertinentes dans un contexte électoral. De nouvelles mesures ont aussi été adoptées afin de prévoir des sanctions en cas de violation des règles de protection des données par les fondations et les partis politiques européens. La Commission a recommandé que les États membres adoptent la même approche au niveau national. L'évaluation des élections au Parlement européen de 2019, qui devrait être publiée en octobre 2019, tiendra également compte des aspects liés à la protection des données.

Répression

Une union de la sécurité réelle et effective ne peut reposer que sur le plein respect des droits fondamentaux ancrés dans la charte de l'UE et dans le droit dérivé de l'Union, y compris en

---

81 En particulier, la directive sur l'électricité: https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32009L0072.

82 Par exemple, affaire M.8788 – Apple/Shazam et affaire M.8124 – Microsoft/LinkedIn.

83 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0638&from=FR

84 http://europa.eu/rapid/press-release_IP-18-5681_fr.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

ce qui concerne la mise en place de garanties appropriées en matière de protection des données pour permettre l'échange sûr de données à caractère personnel à des fins répressives. Toute restriction du droit fondamental au respect de la vie privée et à la protection des données doit répondre à des critères de nécessité et de proportionnalité stricts.

VIII. Conclusion

À la lumière des informations disponibles à l'heure actuelle et du dialogue avec les parties prenantes, la Commission estime, à titre préliminaire, que la première année d'application du règlement a été globalement positive. Néanmoins, ainsi qu'elle l'a montré dans la présente communication, des progrès doivent encore être accomplis dans un certain nombre de domaines.

Mettre en œuvre et compléter le cadre juridique:

- Les trois États membres qui n'ont pas encore actualisé leur législation nationale en matière de protection des données doivent le faire de toute urgence. Tous les États membres devraient achever l'alignement de leur législation sectorielle sur les exigences du règlement.

- La Commission utilisera tous les outils dont elle dispose, y compris les procédures d'infraction, pour veiller à ce que les États membres se conforment au règlement et limitent toute fragmentation du cadre de protection des données.

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

- Les États membres devraient allouer suffisamment de ressources humaines, financières et techniques aux autorités nationales de protection des données.

- Les autorités de protection des données devraient renforcer leur coopération, par exemple en effectuant des enquêtes conjointes. Les États membres devraient faciliter la conduite de ces enquêtes.

- Le comité européen de la protection des données devrait continuer de mettre en place une culture de la protection des données de l'UE et exploiter pleinement les outils prévus dans le règlement pour garantir une application harmonisée des règles. Il devrait poursuivre ses travaux sur les lignes directrices, en particulier pour les petites et moyennes entreprises.

- L'expertise du secrétariat du comité devrait être renforcée pour soutenir et diriger plus efficacement les travaux du comité.

- La Commission continuera de soutenir les autorités de protection des données et le comité, notamment en participant activement aux travaux du comité et en attirant son attention sur les exigences du droit de l'UE dans le cadre de la mise en œuvre du règlement.

- La Commission soutiendra l'interaction entre les autorités de protection des données et d'autres autorités, notamment dans le domaine de la concurrence, dans le plein respect de leurs compétences respectives.

Soutenir et associer les parties prenantes:

- Le comité européen de la protection des données devrait améliorer la manière dont il associe les parties prenantes à ses travaux. La Commission continuera de soutenir financièrement les autorités de protection des données pour les aider à prendre contact avec les parties prenantes.

- La Commission poursuivra ses activités de sensibilisation et ses travaux avec les parties prenantes.

Promouvoir la convergence internationale:

- La Commission intensifiera encore son dialogue sur l'adéquation avec les partenaires clés admissibles, y compris dans le domaine répressif. Elle aspire en particulier à conclure les négociations en cours avec la Corée du Sud dans les prochains mois. Elle élaborera, en 2020, un rapport sur l'examen des onze décisions d'adéquation adoptées au titre de la directive sur la protection des données.
- La Commission poursuivra ses travaux, notamment au moyen d'une assistance technique et de l'échange d'informations et de bonnes pratiques, avec les pays intéressés par l'adoption d'une législation moderne sur le respect de la vie privée et encouragera la coopération avec les autorités de contrôle et les organisations régionales de pays tiers.
- La Commission nouera le dialogue avec les organisations multilatérales et régionales pour promouvoir des normes élevées en matière de protection des données afin de favoriser le commerce et la coopération (par exemple, dans le cadre de l'initiative «libre flux de données en toute confiance» lancée par le Japon dans le contexte du G20).

Le règlement[86] exige que la Commission élabore un rapport sur sa mise en œuvre en 2020. Ce sera l'occasion d'évaluer les progrès accomplis et de déterminer si, après deux années d'application, les différents éléments du nouveau régime de protection des données sont pleinement opérationnels. À cette fin, la Commission coopérera avec le Parlement européen, le Conseil, les États membres, le comité européen de la protection des données, les parties prenantes et les citoyens.

[86] Article 97 du règlement.