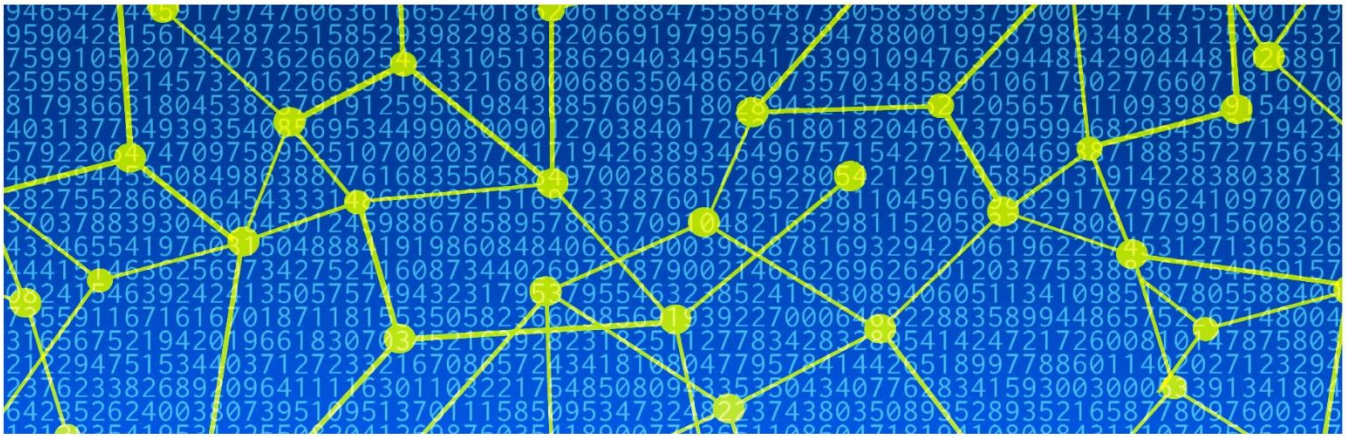

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 3/2020

Avis du CEPD sur la stratégie européenne pour les données

EDPS

16 juin 2020

Synthèse

La Commission européenne a publié le 19 février 2020 une communication intitulée «Une stratégie européenne pour les données», qui fait partie d'un paquet plus vaste de documents stratégiques, comprenant également une communication intitulée «Façonner l'avenir numérique de l'Europe» et un livre blanc intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance».

L'objectif de la stratégie pour les données est de créer un espace européen unique des données, et donc de faciliter l'accès des entreprises et des pouvoirs publics à des données de haute qualité afin de stimuler la croissance et de créer de la valeur. De plus, elle devrait «permettre à l'UE de devenir l'économie habile à tirer parti des données la plus attrayante, la plus sûre et la plus dynamique du monde». Un élément clé de la stratégie pour les données est le développement d'espaces européens communs des données dans des secteurs économiques stratégiques et des domaines d'intérêt public, comme l'espace européen commun des données relatives à la santé.

Cet avis présente le point de vue du CEPD sur la stratégie pour les données dans son ensemble, ainsi que sur certains aspects spécifiques, tels que la notion de «bien public», les données ouvertes, l'utilisation de données à des fins de recherche scientifique, les intermédiaires en matière de données, l'altruisme en matière de données, le partage de données au plan international, etc.

Le CEPD comprend l'importance croissante des données pour l'économie et la société, et soutient les objectifs stratégiques plus vastes de l'Union, tels que la création du marché unique numérique et la souveraineté numérique de l'Union. Parallèlement, il rappelle que «les mégadonnées vont de pair avec de grandes responsabilités», et que des garanties appropriées en matière de protection des données doivent donc être en place.

À cet égard, le CEPD salue l'engagement pris par la Commission de veiller à ce que les valeurs et droits fondamentaux européens, y compris le droit à la protection des données à caractère personnel, sous-tendent tous les aspects de la stratégie pour les données et de sa mise en œuvre. Il apprécie en particulier l'assurance que la stratégie sera élaborée dans le plein respect du règlement général sur la protection des données, qui prévoit une base solide, notamment du fait de son approche neutre sur le plan technologique.

Le CEPD souligne qu'un des objectifs de la stratégie pour les données devrait être de prouver la viabilité et la durabilité d'un autre modèle d'économie fondée sur les données – ouvert, équitable et démocratique. Contrairement au modèle économique qui prévaut actuellement, qui se caractérise par une concentration inédite de données aux mains d'une poignée de puissants acteurs, ainsi que par un traçage systématique, l'espace européen des données devrait servir d'exemple de transparence, de responsabilité effective et d'équilibre adéquat entre les intérêts des différentes personnes concernées et l'intérêt commun de la société dans son ensemble.

Par ailleurs, le présent avis tient compte de la crise mondiale sans précédent causée par la pandémie de COVID-19, qui a des incidences sur tous les aspects de notre vie. Dans ce contexte, le CEPD rappelle que, selon lui, la protection des données n'est pas le problème, mais est une partie de la solution. Les données et la technologie peuvent jouer un rôle important pour surmonter la crise, en combinaison avec d'autres facteurs, car il n'y a pas de panacée pour venir à bout d'une situation aussi complexe.

Le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour leur prodiguer des conseils supplémentaires lors des prochaines étapes de la mise en œuvre de la stratégie européenne pour les données, que ce soit du point de vue du cadre juridique ou des aspects pratiques. Les observations contenues dans le présent avis s'entendent sans préjudice d'éventuelles observations supplémentaires qui pourraient être présentées à l'avenir sur des questions particulières et/ou si de nouvelles informations devenaient disponibles.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le 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)[1],

vu le 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[2], et notamment son article 58, paragraphe 3, point c),

vu la 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[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. La Commission européenne a présenté le 19 février 2020 une communication intitulée «Une stratégie européenne pour les données»[4], qui fait partie d'un paquet plus vaste de documents stratégiques, comprenant également une communication intitulée «Façonner l'avenir numérique de l'Europe»[5] et un livre blanc intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance»[6].

2. L'objectif de la stratégie européenne pour les données (ci-après la «stratégie pour les données» ou la «stratégie») est de créer un espace européen unique des données, et donc de faciliter l'accès des entreprises et des pouvoirs publics à des données de haute qualité afin de stimuler la croissance et de créer de la valeur, tout en réduisant l'empreinte carbone de l'économie de l'Union européenne. De plus, elle jouerait un rôle clé dans la réalisation de l'ambition de la Commission de «permettre à l'UE de devenir l'économie habile à tirer parti des données la plus attrayante, la plus sûre et la plus dynamique du monde».

3. La stratégie européenne pour les données a fait l'objet d'une consultation publique. L'objectif de la consultation est de recueillir des avis sur la stratégie pour les données dans son ensemble, ainsi que sur certains de ses aspects particuliers. Une consultation publique similaire a été lancée sur le livre blanc sur l'intelligence artificielle.

4. Le CEPD a été consulté de manière informelle par la Commission le 29 janvier 2020 sur le projet initial de stratégie pour les données et a présenté des observations préliminaires. Le CEPD salue le fait qu'on lui ait demandé son avis à un stade précoce de la procédure, et encourage la Commission à poursuivre cette bonne pratique.

5. Le présent avis développe certaines des observations informelles et apporte une contribution plus ciblée à la lumière de la consultation publique. Il devrait, en principe, être lu en combinaison avec les autres avis pertinents du CEPD, mentionnés tout au long du présent document, tels que, notamment, l'avis préliminaire sur la recherche scientifique[7], l'avis sur les données ouvertes[8] et l'avis sur les systèmes de gestion des informations personnelles[9]. Par ailleurs, le présent avis s'entend sans préjudice de toutes éventuelles observations supplémentaires que le CEPD pourrait formuler sur la base de nouvelles données qui deviendraient disponibles à un stade ultérieur, y compris dans le contexte des futures consultations législatives sur les actes juridiques prévus dans la stratégie pour les données et le programme de travail de la Commission.

6. Enfin, le CEPD prend acte des discussions en cours concernant la mesure dans laquelle les données et la technologie peuvent contribuer à lutter contre la COVID-19. Dans ce contexte, le CEPD tient à rappeler sa position, partagée par les autres autorités de contrôle au sein du comité européen de la protection des données (EDPB)[10], selon laquelle les règles en matière de protection des données n'entravent pas les mesures prises en réponse à la pandémie de coronavirus. La protection des données n'est pas le problème, mais est une partie de la solution. Le CEPD considère que les données et la technologie jouent un rôle important pour surmonter cette crise sans précédent, qui a des incidences sur tous les aspects de notre vie, mais elles ne sont en aucun cas une panacée. Les données et la technologie peuvent contribuer à lutter contre la pandémie et contre d'autres menaces similaires si elles responsabilisent efficacement les personnes physiques et si elles s'accompagnent de garanties appropriées et d'autres mesures globales.

2. OBSERVATIONS GÉNÉRALES

2.1. Application des principes clés en matière de protection des données

7. Le CEPD salue l'engagement pris dans la stratégie pour les données visant à garantir que les **valeurs et droits fondamentaux européens**, y compris le droit à la protection des données à caractère personnel prévu à l'article 8 de la charte des droits fondamentaux de l'Union et à l'article 16 du TFUE, soient pleinement respectés dans toutes les actions qui feront suite à la stratégie.

8. En particulier, le CEPD soutient l'engagement pris par la Commission d'élaborer la stratégie dans le plein respect du règlement général sur la protection des données (ci-après le «RGPD»). Il est convaincu que le **RGPD constitue une base solide**, notamment de par son approche neutre sur le plan technologique, pour l'élaboration et la mise en œuvre de la stratégie.

9. Le CEPD rappelle que, conformément à l'article 5 du RGPD, le traitement de données à caractère personnel doit toujours respecter les **principes** de licéité, de loyauté et de transparence; de limitation des finalités; de minimisation des données; d'exactitude; de limitation de la conservation; d'intégrité et de confidentialité.

10. Ces principes restent pleinement applicables lors du traitement de données à caractère personnel aux fins du «bien public». La **limitation des finalités** est une garantie essentielle pour assurer aux personnes physiques que les données qu'elles fournissent ne seront pas utilisées à leur encontre de manière inattendue. L'importance du principe de limitation des finalités est clairement démontrée dans le contexte des mesures qui sont envisagées pour lutter contre la COVID-19; par exemple, les données de santé doivent être traitées sous le contrôle d'autorités de santé en leur qualité de responsables du traitement et ne doivent pas être utilisées à des fins commerciales ou à d'autres fins incompatibles.

11. Les principes **de transparence et de responsabilité** sont tout aussi importants. La transparence devrait être entendue comme étant l'obligation de fournir des informations claires, compréhensibles et aisément accessibles tant aux citoyens et au public qu'aux autorités de protection des données. Par ailleurs, la possibilité de réaliser des audits indépendants des opérations de traitement de données et d'adopter des mesures répressives, chaque fois que nécessaire, constitue un aspect important de la responsabilité et ne saurait être remplacée par la seule autorégulation.

12. Dans le contexte de la future **loi sur les données** proposée, le CEPD recommande de fixer des exigences imposant aux producteurs de biens, de services et d'applications reposant sur le traitement de données à caractère personnel ou traitant des données à caractère personnel de se conformer également à la législation relative à la protection des données, en particulier aux exigences relatives à la **protection des données dès la conception et par défaut**. Cette obligation devrait compléter les obligations en vigueur qui incombent aux responsables du traitement et aux sous-traitants au titre du RGPD, et pourrait les aider considérablement à s'acquitter de leurs obligations en matière de protection de données, par exemple lors de la sélection des solutions matérielles et logicielles appropriées.

13. Le CEPD rappelle que l'adoption de la proposition de **règlement «vie privée et communications électroniques»**[11] est cruciale pour protéger les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel à l'ère numérique. Dès lors, l'achèvement du cadre juridique de l'Union pour la protection des données et la confidentialité des communications constitue une condition importante pour la réussite de la stratégie pour les données.

14. Le CEPD fait observer que la mise en œuvre de la stratégie supposera inévitablement une augmentation de l'ampleur et de la gravité des risques pour la protection des données, y compris des **risques pour la sécurité**. Par exemple, les dispositifs connectés de l'internet des objets augmentent la «surface d'attaque» pour les cyberattaques et amplifient les éventuelles incidences négatives pour les personnes physiques ou en produisent de nouvelles. Ce problème devrait être abordé dans le contexte de la révision de la directive relative à la sécurité des réseaux et des systèmes d'information (directive SRI) ou dans le cadre de nouvelles initiatives législatives, et pourrait également être lié à la législation et la politique de l'Union ayant trait aux consommateurs, par exemple à la sécurité des produits.

2.2. Droits des personnes concernées et rôle des intermédiaires en matière de données

15. Le CEPD se félicite de l'objectif de la stratégie de permettre aux personnes physiques de contrôler leurs données, notamment en fournissant des outils et moyens leur permettant de décider, à un niveau détaillé, de l'utilisation faite de leurs données (les «espaces de données à caractère personnel»). Dans le même ordre d'idées, la stratégie vise à renforcer le droit à la portabilité pour les personnes physiques au titre de l'article 20 du RGPD.

16. Une condition préalable importante pour que les personnes physiques puissent exercer effectivement leurs droits en tant que personnes concernées est la capacité de déterminer ce qui a été fait avec leurs données, et par qui, dans la mesure où la mise en commun de données facilitera l'accès par de nombreux acteurs différents. Par conséquent, l'approche habituelle de la transparence sous la forme de longues déclarations de confidentialité rédigées en des termes abstraits ou ambivalents, toujours appliquée par certains responsables du traitement, est contraire à l'exigence du RGPD selon laquelle il faut fournir les informations «d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples»[12]. Dans ce contexte, et particulièrement à la lumière des évolutions technologiques, le CEPD rappelle que, conformément à l'article 12, paragraphes 7 et 8, du RGPD, les informations pouvaient être

communiquées aux personnes concernées accompagnées d'**icônes normalisées et lisibles par machine** afin d'offrir une bonne vue d'ensemble, facilement visible et compréhensible du traitement prévu. D'ici 2022, la Commission devrait déterminer, à l'aide d'actes délégués, la manière dont les informations requises seront présentées accompagnées d'icônes normalisées.

17. Les **systèmes de gestion des informations personnelles (PIMS)** se révèlent être des plateformes prometteuses pour permettre aux personnes concernées de mieux contrôle leurs données à caractère personnel. De plus, certains modèles de PIMS pourraient être considérés comme étant des moteurs de la portabilité des données, puisqu'ils peuvent fonctionner en tant qu'infrastructures de données centralisées permettant aux personnes physiques de gérer leurs données à caractère personnel. Le CEPD a déjà publié un avis sur les systèmes de gestion des informations personnelles[13], dans lequel il insiste sur la nécessité d'élaborer des outils et normes techniques pour simplifier l'exercice des droits des personnes concernées (par exemple au moyen de tableaux de bord de la confidentialité des données), en tant que moyen important pour leur permettre de gérer leurs données. Dans son avis sur les PIMS, le CEPD a aussi signalé en particulier que ces systèmes doivent être pleinement transparents à l'égard des utilisateurs et garantir un véritable contrôle par les utilisateurs.

18. Le CEPD fait remarquer qu'il existe d'autres types d'**intermédiaires en matière de données**, tels que les fiducies et coopératives de données, les marchés des données, les courtiers en données, etc. À cet égard, le CEPD insiste sur la nécessité d'opérer une claire distinction entre les intermédiaires en matière de données qui se concentrent exclusivement sur les données à caractère personnel et qui cherchent une amélioration individuelle, d'une part, et ceux qui sont mus par des incitations économiques et qui visent à soutenir principalement un échange de données entre entreprises, d'autre part.

19. Le CEPD considère que les intermédiaires qui cherchent à doter les personnes concernées d'outils techniques et autres pour gérer l'utilisation de leurs données méritent considération, et **doivent faire l'objet d'une recherche plus approfondie et bénéficier d'un soutien efficace**, car ils contribuent à une utilisation durable et éthique des données, conformément aux principes du RGPD.

20. Parallèlement, le CEPD souligne qu'il faut faire preuve de prudence à l'égard du rôle des **courtiers en données** qui procèdent activement à la collecte d'immenses ensembles de données, dont des données à caractère personnel émanant de différentes sources. Ils exploitent toute une série de sources de données utilisées pour des services liés aux données, comme des données qui sont divulguées à d'autres fins non liées, des données issues de registres publics (données ouvertes), ainsi que des données «recueillies» sur l'internet et les médias sociaux, souvent en violation de la législation relative à la protection des données. Dans ce contexte, le CEPD constate que les activités des courtiers en mégadonnées sont de plus en plus contrôlées et font l'objet d'enquêtes par un certain nombre d'autorités nationales de protection des données[14].

2.3. Notion de «bien public»

21. La stratégie pour les données accorde une attention particulière à la «**disponibilité des données pour le bien public**» au sens large – des soins de santé à la protection de l'environnement, en passant par la lutte contre la criminalité. Le CEPD salue le point de vue de la Commission concernant l'encouragement de l'utilisation des données pour le «bien public». Il rappelle l'un des grands principes du RGPD, à savoir que le traitement des données à caractère personnel devrait être conçu pour servir l'humanité[15].

22. Le CEPD constate aussi que la stratégie fait également référence à la notion d'«**intérêt public**» et l'emploie de manière interchangeable avec la notion de «bien public». L'«intérêt public» peut constituer la base d'un traitement licite au sens de l'article 6, paragraphe 1, point e), du RGPD et peut servir de base au traitement de catégories particulières de données (par exemple, les données relatives à la santé) au titre de l'article 9, paragraphe 2, points g) et i), du RGPD. Conformément à l'article 6, paragraphe 3, du RGPD, le fondement du traitement de données à caractère personnel, nécessaire à l'exécution d'une mission d'intérêt public, doit être prévu par la législation de l'Union ou des États membres. Par conséquent, le traitement de données à caractère personnel pour le «bien public» répond aux mêmes objectifs importants, exprimés dans le RGPD, que ceux de l'«intérêt public», et devrait être soumis aux mêmes exigences.

23. Dans ce contexte, le CEPD fait remarquer que les données, en particulier les informations du secteur public, pourraient jouer un rôle clé dans le marché unique numérique. Par ailleurs, l'utilisation intelligente des données, y compris leur traitement au moyen de l'intelligence artificielle, peut avoir un effet de transformation sur divers secteurs de l'économie. Parallèlement, le CEPD signale que le partage de données pour répondre à des besoins sociaux et d'autres besoins communs devrait être soumis aux **garanties appropriées en matière de protection des données**, conformément aux principes **de nécessité et de proportionnalité**.

24. L'utilisation de données pour le bien public/l'intérêt public peut supposer un traitement à grande échelle, combinant des données qui proviennent de diverses sources, concernant potentiellement des catégories particulières de données et/ou des données à caractère personnel de groupes vulnérables de personnes concernées. Lorsque tel est le cas, il est probable que ce traitement entraîne un risque élevé et que les responsables du traitement doivent mener des **analyses d'impact relatives à la protection des données** conformément à l'article 35 du RGPD16. En outre, le CEPD recommande de publier les résultats de ces analyses chaque fois que cela sera possible, afin d'améliorer la confiance et la transparence.

25. Toute utilisation ultérieure de données collectées et/ou partagées à des fins de bien public/d'intérêt public (par exemple, pour améliorer les transports/la mobilité ou pour s'attaquer aux menaces transfrontières graves sur la santé), à des fins commerciales lucratives (par exemple, assurance, marketing, etc.), devrait être évitée. Un tel «**détournement d'usage**» non seulement pourrait constituer une violation des principes en matière de protection des données ancrés à l'article 5 du RGPD, mais pourrait aussi miner la confiance des citoyens, qui est un élément fondamental de la stratégie.

26. Autre point tout aussi important, le traitement de données pour le bien public ne devrait **pas créer ou renforcer des situations d'oligopole de données** (dans lesquelles le secteur public, les PME, etc. dépendent de quelques puissantes sociétés informatiques, dites «grandes entreprises technologiques»)[17]. Cela est également pertinent du point de vue de la protection des données, étant donné que les monopoles et les oligopoles créent des situations de verrouillage des utilisateurs et, en fin de compte, limitent la possibilité pour les personnes physiques d'exercer effectivement leurs droits.

2.4. Données ouvertes

27. En ce qui concerne la réutilisation des informations du secteur public par les entreprises envisagée dans la stratégie, à savoir l'accès aux données détenues par les pouvoirs publics et le traitement de ces données, telle que définie dans la «directive ISP»[18], révisée par la directive 2019/1054/UE (la **directive concernant les données ouvertes**)[19], le CEPD a publié un avis[20], dans lequel il faisait référence aux principes clés suivants:

(i) la **transparence** et la **participation de la société** sur la finalité de la réutilisation vis-à-vis des citoyens/personnes concernées ainsi que la transparence et la **définition d'une finalité** claire entre le donneur de licence (le pouvoir public) et les bénéficiaires de la licence;

(ii) une **analyse d'impact relative à la protection des données** pour les traitements de données relevant de l'article 35, paragraphe 3, du RGPD afin de recenser les risques et les garanties appropriées en matière de protection des données visant à y remédier, avant la réutilisation des données.

28. Le CEPD fait remarquer qu'en raison des spécificités technologiques, économiques et juridiques de chaque «secteur» (par exemple, le traitement de données de santé à des fins de recherche est différent du traitement de données sur l'énergie intelligente pour mettre en œuvre un «modèle économique vert»)[21], une **approche sectorielle**, exigeant notamment une évaluation «sectorielle» de la protection des données, pourrait se révéler nécessaire.

29. Du point de vue de la technologie de l'information, le CEPD se félicite que la stratégie vise à encourager la réutilisation des informations du secteur public en poursuivant les objectifs suivants: réduire les obstacles à l'accès au marché, en particulier pour les petites et moyennes entreprises; réduire autant que possible le risque d'un avantage de «premier arrivant» excessif, qui bénéficie aux grandes entreprises et limite par conséquent le nombre d'utilisateurs potentiels des données en question; ainsi qu'accroître les perspectives commerciales en encourageant la publication de données dynamiques et le recours à des interfaces de programmation (API).

2.5. Données à caractère personnel et à caractère non personnel

30. Le CEPD relève que la stratégie opère une distinction entre **trois catégories de données**, à savoir les ensembles de données à caractère non personnel, à caractère personnel et mixtes. Dans ce contexte, le CEPD tient à rappeler que, dans la pratique, une combinaison de données à caractère non personnel peut supposer ou générer des données à caractère personnel, par exemple des données relatives à une personne identifiée ou identifiable.

31. La stratégie mentionne également les données «**anonymisées**» et «**agrégées**», laissant entendre que les données agrégées pourraient être les mêmes que les données anonymisées[22]. À cet égard, le CEPD tient à signaler que les données agrégées ne sont pas nécessairement des données à caractère non personnel, car elles peuvent toujours être liées à une personne identifiée ou identifiable. À ce propos, le CEPD rappelle que, conformément au considérant 26 du RGPD et à la jurisprudence de la Cour de justice[23], il convient de prendre dûment en considération l'ensemble des facteurs objectifs, dont le coût de l'identification et le temps nécessaire à celle-ci, les technologies disponibles, ainsi que les moyens juridiques et autres disponibles pour accéder à des données supplémentaires au sujet de la personne.

32. Par ailleurs, les processus d'anonymisation ne sont pas simples[24]. Plus les données sont variées, plus il est difficile de les anonymiser en réduisant le risque de réidentification à un seuil acceptable. Les difficultés pratiques associées à un processus d'anonymisation solide peuvent empêcher les responsables du traitement, et en particulier les PME, de partager des données précieuses. Afin de réduire l'effort requis, tout en veillant à ce que les données soient anonymisées correctement, le CEPD encourage la Commission à investir dans de bonnes pratiques et normes d'anonymisation et à continuer de soutenir et de favoriser ces dernières.

33. À cet égard, le CEPD voudrait également mentionner quelques bonnes pratiques relatives à la réutilisation de données anonymisées dans le secteur public, telles que les orientations détaillées élaborées par l'Agence européenne des médicaments (EMA) à l'intention du secteur afin de

faciliter le respect de cette politique[25] ou encore la mise à disposition de statistiques en tant que «bien public» de grande qualité par le système statistique européen (SSE)[26].

2.6. Institutions, organes et organismes de l'Union européenne

34. Le CEPD constate que la stratégie n'aborde pas spécifiquement le rôle des institutions, organes et organismes de l'Union européenne et les règles qui leur sont applicables. Il est vrai que les règles en matière de protection des données qui leur sont applicables, à savoir le règlement (UE) 2018/1725, sont très largement alignées sur le RGPD et la directive (UE) 2016/680; par conséquent, tous ces actes doivent être interprétés de manière homogène[27]. Dans le même temps, les institutions et autres organes de l'Union sont des acteurs importants dans l'économie fondée sur les données à titre individuel – en tant que fournisseurs de données (par exemple, par l'intermédiaire du portail des données ouvertes de l'Union européenne), qu'utilisateurs de données (par exemple, pour améliorer l'élaboration des politiques), ou que prestataires de services (par exemple, l'infrastructure de services numériques dans le domaine de la santé en ligne)[28].

35. Dès lors, le CEPD, en sa qualité d'autorité de contrôle surveillant le traitement des données à caractère personnel par les institutions et organes de l'Union, est convaincu que la stratégie pour les données et les actes juridiques et non juridiques y afférents relatifs à sa mise en œuvre devraient tenir dûment compte du rôle spécifique des institutions, organes et organismes de l'Union européenne. Ainsi, l'Union non seulement garantira la transparence et la sécurité juridique nécessaires, mais tiendra aussi la promesse de «montrer l'exemple», comme l'a annoncé la Commission dans la stratégie[29].

3. DONNÉES À DES FINS DE RECHERCHE SCIENTIFIQUE

36. Le CEPD prend note de l'intention de la Commission d'augmenter la quantité et de multiplier les types de données disponibles à des fins de recherche scientifique conformément au principe «aussi ouvert que possible, aussi fermé que nécessaire». L'une des initiatives clés visant à permettre aux chercheurs d'avoir accès aux données et services et de les découvrir, de les partager et de les réutiliser plus facilement est le **nuage européen pour la science ouverte**. Ce dernier sera aussi utilisé comme modèle pour la création des futurs espaces européens communs des données.

37. Tant l'avis préliminaire du CEPD sur la protection des données et la recherche scientifique[30] que les lignes directrices du comité européen de la protection des données sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19[31] soulignent que **les règles en matière de protection des données, telles que le RGPD, sont pleinement compatibles avec la véritable recherche scientifique et ne l'entravent pas**. Parallèlement, le partage de données à caractère personnel suppose toujours un risque pour les personnes concernées, même lorsque la finalité est la recherche scientifique, surtout lorsqu'il s'agit de données sensibles. Les règles en matière de protection des données sont destinées à servir de filet de sécurité robuste pour les personnes physiques dont les données sont nécessaires pour soutenir la science, ainsi que de cadre guidant les chercheurs vers l'innovation qui reflète les valeurs européennes.

38. On croit souvent que la recherche scientifique est bénéfique pour l'ensemble de la société et que les connaissances scientifiques sont un bien public qu'il faut encourager et soutenir. Bien que le CEPD partage de manière générale ce point de vue, accomplir une activité réputée être de la recherche ne saurait être une carte blanche pour prendre des risques irresponsables à l'égard des droits fondamentaux. Du point de vue de la protection des données, les principes de nécessité, de proportionnalité et de limitation des finalités sont essentiels. Comme indiqué dans l'avis

préliminaire sur la protection des données et la recherche scientifique, les autorités de protection des données, les comités d'éthique et la communauté des chercheurs ont un intérêt commun à collaborer pour contribuer à faire avancer les connaissances, tout en veillant à ce que les personnes ne soient pas traitées comme de simples ensembles de données.

39. Alors que la recherche scientifique bénéficie d'un régime spécial de protection des données, le CEPD tient à rappeler à la Commission et aux chercheurs qui s'appuient sur les espaces communs des données que chacun des principes ancrés à l'article 5 du RGPD (licéité, loyauté et transparence; limitation des finalités; minimisation des données; exactitude; limitation de la conservation; intégrité et confidentialité; et responsabilité) s'applique pleinement à tout traitement de données à caractère personnel à des fins de recherche.

40. La recherche scientifique suppose souvent le traitement et le partage de catégories particulières de données à caractère personnel des personnes concernées et pourrait donc, dans certains cas, être considérée comme constituant un traitement de données à risque élevé au sens du RGPD. C'est pourquoi le CEPD recommande que les **garanties appropriées** soient en place et que l'accès aux données stockées dans les espaces de données se fasse sur la base de divers facteurs, dont, entre autres, une demande d'accès de l'acteur; la finalité du traitement et son niveau de risque; l'existence de cadres et de garanties au regard de la responsabilité; etc. Par ailleurs, des analyses d'impact relatives à la protection des données devraient être menées lorsque la recherche porte sur des données sensibles, avec la participation des délégués à la protection des données (DPD) et des comités d'éthique respectifs.

41. Le RGPD prévoit des dérogations à certaines obligations [par exemple, octroi du droit d'accès (article 15), du droit de rectification (article 16), du droit à la limitation (article 18) et du droit d'opposition (article 21) de la personne concernée] à des fins de recherche scientifique, lorsque le traitement est proportionné à l'objectif poursuivi, respecte l'essence du droit à la protection des données et prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. Néanmoins, ce régime spécial ne peut être appliqué d'une manière compromettant l'essence du droit à la protection des données. Les dérogations à ces droits de la personne concernée doivent faire l'objet d'un contrôle particulièrement strict. Elles exigent une analyse au cas par cas, une mise en balance des intérêts et des droits en jeu, ainsi qu'une évaluation flexible tenant compte de multiples facteurs. Toute limitation des droits fondamentaux prévue par la législation doit être interprétée de manière restrictive, et il ne faut pas en abuser. Par ailleurs, en vertu de l'article 89, paragraphe 2, du RGPD, les dérogations ne peuvent être appliquées que «dans la mesure où» les droits devant faire l'objet d'une dérogation «risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités».

42. Il n'existe pas de définition universellement admise de la recherche ou de la recherche scientifique. De plus, les limites entre l'intérêt public, la liberté académique et le gain privé sont plus floues que jamais. Cette incertitude peut créer des lacunes dans la protection des droits fondamentaux, y compris du droit au respect de la vie privée et à la protection des données à caractère personnel. Par conséquent, le CEPD recommande fortement que la stratégie et la législation envisagée mentionnent spécifiquement la définition et la portée des notions clés telles que la recherche scientifique, l'innovation et l'intérêt public, afin d'éviter les incohérences avec les notions existant dans le RGPD[32].

4. ESPACES EUROPÉENS COMMUNS DES DONNÉES

4.1. Observations générales sur la notion

43. Un élément clé de la stratégie pour les données est le développement d'espaces européens communs des données dans des secteurs économiques stratégiques et des domaines d'intérêt public. Les espaces de données combineraient de vastes réserves communes de données, les outils et infrastructures techniques nécessaires pour utiliser et échanger des données, ainsi que des mécanismes de gouvernance. Ils seraient régis par un cadre horizontal complété, le cas échéant, par une législation sectorielle relative à l'accessibilité et à l'utilisation des données.

44. Les espaces européens communs des données s'inscrivent dans le cadre d'objectifs stratégiques plus vastes de l'Union, tels que la mise en place d'un **marché unique numérique** équitable et concurrentiel, l'adoption de nouvelles technologies telles que l'intelligence artificielle et, en particulier, l'apprentissage automatique, ainsi que l'affirmation de la **souveraineté numérique de l'Union européenne**, et soutiennent ces objectifs.

45. Le CEPD se félicite de l'engagement pris dans la stratégie de développer les espaces européens communs des données «**dans le strict respect des règles en matière de protection des données et conformément aux normes les plus élevées disponibles en matière de cybersécurité**» et se réjouit d'examiner les propositions et initiatives spécifiques visant à mettre cet engagement en œuvre.

46. Le CEPD accueille favorablement l'intention de la Commission d'envisager l'adoption d'une législation sectorielle pour accompagner la création de certains espaces européens communs des données. Le législateur européen a la responsabilité de mettre en place des garanties juridiques supplémentaires dans les situations dans lesquelles la stratégie entraînerait une disponibilité et une réutilisation accrues de données à caractère personnel. La nécessité d'une spécification et d'une particularisation supplémentaires des règles générales contenues dans le RGPD au niveau de l'Union semble la plus pressante au regard du partage de données de santé et à des fins de recherche scientifique en général. Dans le même temps, cette spécification, qui vise à harmoniser le plus possible les règles relatives au traitement de données à caractère personnel à des fins de recherche scientifique en particulier, pourrait favoriser le partage de données.

47. Outre les normes horizontales relatives à la protection des données et à la cybersécurité, la Commission devrait investir dans la poursuite de l'encouragement de l'**interopérabilité**, y compris dans le contexte de la portabilité des données. Ainsi, les espaces communs des données permettraient l'émergence et l'essor de davantage de modèles économiques conformes à la protection des données.

48. Bien que le CEPD convienne qu'une approche unique pourrait ne pas être appropriée, il encourage néanmoins la Commission à mieux préciser que les espaces européens communs des données ne devraient contenir que des données à caractère personnel dont il a été démontré qu'elles ont été obtenues dans le respect de la législation relative à la protection des données, y compris, en particulier, des principes de licéité, de limitation des finalités et de minimisation des données.

49. D'après la stratégie, les espaces de données seront utilisés à diverses fins. Dès lors, il faudrait définir clairement dès le départ, pour chaque espace de données, les finalités qui sont autorisées (par exemple, les finalités de recherche et autres que de recherche, etc.). De plus, la protection des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, ainsi que de la valeur de la dignité humaine qui sous-tend ces droits, garantit, dans certains scénarios, une limitation claire de l'utilisation des données dans différents contextes, y

compris l'**interdiction de l'utilisation de données à caractère personnel sensibles à d'autres fins** (par exemple, l'utilisation de données génétiques à des fins d'assurance). C'est particulièrement pertinent pour l'utilisation transsectorielle de données à caractère personnel dans le contexte de l'internet des objets.

50. Les espaces européens communs des données, qui sont fondés sur les valeurs et les droits fondamentaux européens au centre desquels se trouve l'être humain, pourraient également servir de preuve de la **viabilité d'autres modèles** que le modèle actuel de concentration des données aux mains de quelques sociétés privées situées en dehors de l'Union européenne, qui jouent le rôle de gardiens autoproclamés de l'internet ou de grands fournisseurs de solutions informatiques. Par conséquent, les espaces européens des données envisagés devraient servir d'exemple **de transparence, de responsabilité effective et d'équilibre adéquat** entre les intérêts des personnes concernées et l'intérêt commun de la société dans son ensemble.

51. Le succès des espaces européens communs des données et de la stratégie dans son ensemble dépendra fortement de la capacité de créer un niveau solide de **confiance** entre les différentes parties prenantes (personnes concernées, gouvernements, sociétés privées, communauté de la recherche scientifique et organisations de la société civile, ainsi qu'autorités de protection des données et autres régulateurs compétents). À cette fin, le modèle de gouvernance devrait spécifiquement aborder la participation des citoyens et de la société civile.

4.2. Partage de données obligatoire

52. Le CEPD prend acte de l'intention de la Commission de rendre **le partage de données obligatoire dans certaines circonstances**. Des appels ont récemment été lancés en faveur d'un accès réglementé dans l'ensemble de l'Union aux données à caractère personnel détenues par le secteur privé à des fins de recherche qui servent un intérêt public, tel que l'amélioration de la fourniture des soins de santé et la lutte contre la crise climatique[33]. De telles initiatives devraient devenir encore plus importantes dans le contexte de la pandémie de COVID-19. De plus, dans son avis préliminaire sur la recherche scientifique, le CEPD a souligné la question du secret d'entreprise, en particulier dans le secteur des technologies, qui contrôle certaines des données les plus précieuses, en tant qu'obstacle majeur à la recherche en matière de sciences sociales.

53. Une éventuelle base fondée sur l'intérêt public qui serait prévue dans le droit relatif à la protection des données pour la divulgation de données doit être clairement formulée et prévue dans le droit de l'Union ou des États membres, et s'accompagner d'un critère de proportionnalité rigoureux et de garanties appropriées contre l'abus et l'accès illicite. C'est pourquoi le CEPD recommande de tenir un **débat ouvert et inclusif** sur cette question, auquel toutes les parties prenantes, telles que la communauté des chercheurs, les sociétés de technologie, les groupes de défense des libertés civiles, les autorités de contrôle, etc., devraient être associées.

54. Enfin, le CEPD appelle à adopter une approche prudente à l'égard des initiatives visant à rendre obligatoire **l'accès aux données à caractère personnel dans le contexte de la concurrence**, c'est-à-dire l'accès des concurrents aux données à caractère personnel détenues par l'entreprise titulaire. Pareils partage et accès aux données entre concurrents doivent être mis en balance avec d'autres considérations stratégiques, en particulier la protection des données. Tout partage de données à caractère personnel ou accès à celles-ci doit être strictement défini sur le plan de la portée et de la finalité, et doit avoir lieu dans le plein respect du RGPD, en tenant compte des exigences de licéité, de limitation des finalités et de confiance légitime des utilisateurs.

4.3. Espace européen commun des données relatives à la santé

55. L'un des neuf secteurs stratégiques dans lesquels la Commission voit une valeur ajoutée évidente pour l'Union résultant de la mise en commun de données et de ressources techniques est celui des **soins de santé**. L'objectif de l'espace européen commun des données relatives à la santé proposé est d'améliorer l'accès aux soins de santé et la qualité de ces derniers, de soutenir la recherche scientifique et d'aider les autorités compétentes à prendre des décisions stratégiques fondées sur des données probantes.

56. Compte tenu des incidences significatives et de la sensibilité des échanges transfrontières de données de santé, le CEPD tient à souligner que toutes les opérations de traitement susceptibles de résulter de la mise en place d'un espace européen commun des données relatives à la santé nécessiteront une **base juridique solide** conforme aux règles de l'Union européenne en matière de protection des données. À cet égard, il indique aussi la nécessité de **poursuivre l'harmonisation des règles en matière de protection des données applicables aux données de santé** entre les États membres. En outre, un code de conduite européen sur le traitement des données de santé à des fins de recherche scientifique pourrait effectivement permettre d'intensifier les échanges transfrontières de données de santé au sein de l'Union.

57. Le partage de données de santé pourrait jouer un rôle important pour remédier à d'importants problèmes individuels et sociétaux, lorsqu'il s'accompagne de garanties appropriées en matière de protection des données. La pandémie de COVID-19, qui a affecté nos vies de manière inédite, l'a souligné de manière très convaincante. À cet égard, le CEPD reconnaît que le partage de données pourrait contribuer substantiellement à la gestion de la crise actuelle et de ses conséquences à long terme, ainsi qu'aider l'Union européenne à se préparer à d'éventuelles futures crises de nature similaire.

58. Le CEPD tient à attirer l'attention sur les lignes directrices du comité européen de la protection des données sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19 récemment adoptées, qui mettent en lumière et expliquent plus avant les exigences essentielles en matière de protection des données, en particulier la légalité, la transparence, la nécessité et la proportionnalité, ainsi que l'intégrité et la confidentialité. Les données à caractère personnel ne peuvent être traitées à des fins légitimes spécifiées que lorsque cela est nécessaire à ces fins, et ne peuvent être utilisées d'une manière incompatible avec ces finalités.

59. Enfin, tout en reconnaissant les limites des compétences de l'Union dans le domaine des soins de santé, conformément aux traités, le CEPD invite la Commission à considérer le possible rôle de l'espace européen des données relatives à la santé envisagé comme un instrument pour améliorer **la préparation et la réaction aux futures crises sanitaires, ainsi que leur gestion**, en combinaison avec l'infrastructure de services numériques dans le domaine de la santé en ligne (eHDSI) et d'autres structures et initiatives pertinentes de l'Union européenne.

5. QUESTIONS SPÉCIFIQUES

5.1. Cadres de gouvernance pour l'accès aux données et leur utilisation

60. Le CEPD partage l'avis de la Commission selon lequel mettre en place un **cadre législatif générique pour la gouvernance** est une priorité pour concrétiser la stratégie pour les données et son élément central - les espaces européens communs des données. Il devrait garantir la sécurité juridique et la cohérence avec les autres cadres juridiques existants, en particulier concernant la protection des données, en s'inspirant de ceux-ci et en les renforçant.

61. Le CEPD s'attend à être consulté sur les futures propositions législatives, telles que la loi sur les données envisagée, conformément à l'article 42 du règlement (UE) 2018/1725. Sans préjudice de ses éventuels futurs avis, le présent avis sur la stratégie pour les données vise à formuler des observations et recommandations préliminaires liées au cadre de gouvernance.

62. En fonction des risques, de la nature, de la portée, du contexte et des finalités du traitement, un certain type de «**contrôle**» formel des organisations demandant à avoir accès aux espaces européens communs des données pourrait être garanti, par exemple sous la forme d'une centralisation. Par ailleurs, les organisations participant à la mise en commun de données ou à des accords de partage devraient adhérer à certaines normes communes, pas seulement au regard de l'interopérabilité, mais aussi en vue de garantir la licéité du traitement et de faciliter les droits des personnes concernées (par exemple, au moyen d'accords sur les responsables conjoints du traitement conformément à l'article 26 du RGPD).

63. Ensuite, pour garantir la responsabilité du responsable du traitement, le cadre de gouvernance devrait inclure des exigences en matière de **traçabilité des données**. Ce point est particulièrement pertinent pour les espaces européens communs des données qui combineraient des données de différents États membres et de diverses sources, tant publiques que privées.

64. Enfin, le CEPD souligne que, dans le contexte de futurs mécanismes de gouvernance, les compétences des **autorités indépendantes de contrôle de la protection des données** doivent être bien respectées. De plus, la mise en œuvre de la stratégie entraînera une utilisation accrue de données, de sorte qu'il faudra augmenter significativement les ressources des autorités chargées de la protection des données et des autres organes de contrôle public, en particulier sur le plan de l'expertise et des capacités techniques. La coopération et les enquêtes conjointes entre tous les organes de contrôle public compétents, y compris les autorités de contrôle de la protection des données, devraient être encouragées.

5.2. Technologies de préservation de la vie privée

65. Le CEPD apprécie le fait que la stratégie mentionne que les technologies de préservation de la vie privée sont «essentielles pour les prochaines étapes de l'économie fondée sur les données». Dans le même esprit, le CEPD rappelle le potentiel des **technologies renforçant la protection de la vie privée** pour permettre un partage de données à la fois respectueux de la vie privée et socialement bénéfique.

66. Il existe un certain nombre de solutions technologiques prometteuses, comme l'utilisation de **données synthétiques**, qui pourraient, notamment, faciliter l'accès aux données d'apprentissage pour l'apprentissage automatique. Bien qu'il règne toujours une incertitude et que des questions restent ouvertes concernant la faisabilité et l'efficacité de ces solutions pour atténuer les risques en matière de protection des données, le CEPD incite la Commission à investir dans la poursuite de la recherche et des tests.

67. En outre, afin d'optimiser les avantages des différentes technologies de protection de la vie privée, le CEPD insiste sur l'importance **de leur normalisation et de leur interopérabilité**. À cette fin, il salue l'engagement pris dans le cadre de la stratégie, qui consiste à faciliter l'élaboration de normes et exigences européennes communes pour les marchés publics de services de traitement de données, et encourage la Commission à continuer de poursuivre cet objectif.

5.3. «Altruisme en matière de données»

68. Dans la stratégie, la Commission s'engage à «permettre aux particuliers d'autoriser plus facilement l'utilisation des données qu'ils produisent pour le bien public, s'ils le souhaitent ("altruisme en matière de données"), dans le respect du RGPD». Le CEPD considère que la valeur ajoutée de la notion d'«altruisme en matière de données», qui porte également le nom de «don de données», n'est pas tout à fait claire, compte tenu du fait que cet «altruisme en matière de données» reposerait sur le consentement de la personne concernée et que le RGPD prévoit déjà des principes et des règles ayant trait au consentement. Dès lors, le CEPD invite la Commission à mieux définir cet «altruisme en matière de données» et à en délimiter la portée, y compris ses possibles finalités (par exemple, l'altruisme en matière de données à des fins de recherche scientifique dans le secteur de la santé).

69. Le CEPD souhaite également rappeler que le droit fondamental à la protection des données à caractère personnel ne peut en aucun cas être «abandonné» par la personne concernée, que ce soit par un «don» ou par une «vente» de données à caractère personnel. Le responsable du traitement reste pleinement tenu par les règles et principes en matière de protection des données, même lorsqu'il traite des données qui ont été «données», c'est-à-dire lorsque la personne concernée a donné son consentement au traitement.

5.4. Compétences et culture numérique

70. Le CEPD se réjouit de l'engagement pris par la Commission d'**investir dans les compétences et l'éducation générale aux données**. À cet égard, il souhaite souligner que l'éducation à la protection des données est importante pour que les personnes physiques connaissent leurs droits en général et puissent décider de manière éclairée d'autoriser ou non certaines utilisations de leurs données. C'est particulièrement important pour les jeunes, qui font partie des utilisateurs les actifs des services numériques.

71. La sensibilisation à la protection des données est indispensable pour garantir que le consentement des personnes est valable. Par ailleurs, les personnes qui ont conscience de la protection des données utiliseront mieux les droits dont elles jouissent en tant que personnes concernées et pousseront donc tous les acteurs de l'écosystème de données à se conformer à l'esprit et à la lettre du RGPD.

5.5. Partage de données au plan international

72. Le CEPD se félicite de l'engagement clair en ce sens que toutes les entreprises et autres organisations qui vendent des biens ou fournissent des services liés à l'économie fondée sur les données en Europe doivent respecter la législation européenne et cela ne doit pas être remis en cause par des recours juridictionnels provenant de l'extérieur de l'Europe.

73. Le CEPD tient à rappeler que tous les **transferts de données à caractère personnel vers des pays tiers ou des organisations internationales** doivent être conformes au chapitre V et aux autres dispositions pertinentes du RGPD ou, dans le cas des institutions et organes de l'Union, au règlement (UE) 2018/1725. Cette obligation s'applique pleinement à l'**informatique en nuage**, ainsi que l'illustrent les lignes directrices du CEPD sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'Union européenne[34] et la création du forum de La Haye – le premier conseil des clients des fournisseurs de logiciels et de services d'informatique en nuage de l'Union[35].

74. Le CEPD partage entièrement l'avis de la Commission selon lequel la coopération internationale doit se fonder sur une approche qui promeut les valeurs fondamentales de l'Union européenne, y compris la protection de la vie privée et des données à caractère personnel. Cette même approche guide le CEPD dans sa coopération avec les autres organisations partenaires et au sein des forums internationaux tels que la Global Privacy Assembly.

6. CONCLUSIONS

75. Le CEPD comprend l'importance croissante des données pour l'économie et la société et soutient l'ambition de faire de l'Union européenne «l'économie habile à tirer parti des données la plus attrayante, la plus sûre et la plus dynamique du monde». Parallèlement, il tient à rappeler que «les mégadonnées vont de pair avec de grandes responsabilités», et que des garanties appropriées en matière de protection des données doivent donc être en place et effectivement appliquées.

76. Le CEPD salue l'engagement pris par la Commission de veiller à ce que les valeurs et droits fondamentaux européens, y compris le droit à la protection des données à caractère personnel, sous-tendent tous les aspects de la stratégie pour les données et de sa mise en œuvre. Il apprécie en particulier l'assurance que la stratégie sera élaborée dans le plein respect du règlement général sur la protection des données, qui prévoit une base solide, notamment du fait de son approche neutre sur le plan technologique.

77. À l'heure actuelle, le modèle économique de l'économie numérique qui prévaut se caractérise par une concentration inédite de données aux mains d'une poignée de puissants acteurs, basés en dehors de l'Union européenne, ainsi que par un traçage systématique à grande échelle. Le CEPD croit fermement qu'un des objectifs les plus importants de la stratégie pour les données devrait être de prouver la viabilité et la durabilité d'**un autre modèle d'économie fondée sur les données** – ouvert, équitable et démocratique. Par conséquent, les espaces européens communs des données envisagés devraient servir d'exemple de transparence, de responsabilité effective et d'équilibre adéquat entre les intérêts des personnes concernées et l'intérêt commun de la société dans son ensemble.

78. Le CEPD s'attend à être consulté sur toute proposition législative faisant suite à la stratégie pour les données qui aura une incidence sur la protection des données, comme indiqué ci-dessus, conformément à l'article 42 du règlement (UE) 2018/1725, et reste à la disposition de la Commission, du Conseil et du Parlement européen pour leur prodiguer des conseils supplémentaires lors des prochaines étapes de la mise en œuvre de la stratégie européenne pour les données, sur le plan tant du cadre juridique que des aspects pratiques. Les observations contenues dans le présent avis s'entendent sans préjudice d'éventuelles observations supplémentaires qui pourraient être présentées à l'avenir sur des questions particulières et/ou si de nouvelles informations devenaient disponibles.

Bruxelles, le 16 juin 2020

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] COM(2020) 66 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_fr.
[5] COM(2020) 67 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_fr.
[6] COM(2020) 65 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_fr.
[7] https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[8] https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf.
[9] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf.
[10] Pour de plus amples informations, voir https://edps.europa.eu/data-protection/our-work/subjects/covid-19_fr.
[11] COM(2017) 10 final, proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»).
[12] Voir lignes directrices du groupe de travail «Article 29» sur la transparence au sens du règlement (UE) 2016/679 (wp260rev.01) https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025.
[13] https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf.
[14] https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem.
[15] Voir considérant 4 du RGPD.
[16] Voir lignes directrices du groupe de travail «Article 29» concernant l'analyse d'impact relative à la protection des données: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[17] À cet égard, d'après la règle générale définie à l'article 12, paragraphe 1, de la directive concernant les données ouvertes, sous réserve de l'exception limitée prévue à l'article 12, paragraphe 2: «La réutilisation des documents est ouverte à tous les acteurs potentiels du marché, même si un ou plusieurs d'entre eux exploitent déjà des produits à valeur ajoutée basés sur ces documents. Les contrats ou autres accords conclus entre les organismes du secteur public ou entreprises publiques détenteurs des documents et les tiers n'accordent pas de droits d'exclusivité.»
[18] Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (JO L 345 du 31.12.2003, p. 90).
[19] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (JO L 172 du 26.6.2019, p. 56).
20 Avis 5/2018 du CEPD sur la proposition de refonte de la directive concernant la réutilisation des informations du secteur public (ISP), disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf.
[21] Voir, par exemple, l'analyse d'impact relative à la protection des données pour l'environnement des réseaux et compteurs intelligents, disponible à l'adresse suivante: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment. Le modèle économique vert pourrait être appliqué pour tenir également compte de la réutilisation de données afin de recenser des solutions économes en énergie.
[22] Voir page 8 de la stratégie, qui mentionne l'«utilisation de données agrégées et anonymisées provenant des médias sociaux».
[23] Voir affaire C-582/14, Patrick Breyer/Bundesrepublik Deutschland, EU:C:2016:779.
[24] Voir avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.
[25] https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication/support-industry-clinical-data-publication.
[26] https://ec.europa.eu/eurostat/fr/web/european-statistical-system/reuse-ess-statistics.
[27] Voir considérant 5 du règlement (UE) 2018/1725.
[28] Avis conjoint 1/2019 de l'EDPB et du CEPD concernant le traitement des données des patients et le rôle de la Commission européenne dans l'infrastructure de services numériques dans le domaine de la santé en ligne (eHDSI), https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing_fr
[29] Voir page 15 de la stratégie pour les données.
[30] https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[31] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_fr.

[32] Pour plus d'informations à ce sujet, voir avis préliminaire du CEPD sur la protection des données et la recherche scientifique.
[33] Voir, par exemple, avis de la commission fédérale allemande pour l'éthique des données de 2019, recommandations 16 à 23.
[34] https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_fr.pdf.
[35] Pour de plus amples informations, voir: https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_fr.