EUROPEAN DATA PROTECTION SUPERVISOR

Avis n° 3/2015

Une grande opportunité pour l'Europe

Recommandations du CEPD relatives aux options de l'UE en matière de réforme de la protection des données

28 juillet 2015

Le 24 juin 2015, les trois principales institutions de l'UE, le Parlement européen, le Conseil et la Commission européenne, ont engagé des négociations de codécision relatives à la proposition de règlement général sur la protection des données, une procédure connue sous le nom de «trilogue» informel.[1] Le trilogue est fondé sur la proposition de la Commission de janvier 2012, la résolution législative du Parlement du 12 mars 2014 et l'orientation générale du Conseil adoptée le 15 juin 2015.[2] Les trois institutions se sont engagées à traiter le règlement général sur la protection des données dans le cadre du train de réformes élargi de la protection des données qui inclut la proposition de directive relative aux activités policières et judiciaires. Ce processus devrait s'achever à la fin de l'année 2015 et probablement permettre l'adoption formelle des deux instruments au début de l'année 2016, qui sera suivie d'une période transitoire de deux ans. [3]

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE. Le contrôleur ne fait pas partie du trilogue, mais il est chargé en vertu de l'article 41, paragraphe 2, du règlement 45/2001 «[e]n ce qui concerne le traitement de données à caractère personnel… de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», *et* «… de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel»*. Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être plus constructifs et proactifs, et ils ont publié en mars 2015 une stratégie quinquennale exposant la manière dont ils entendaient mettre en œuvre ce mandat et en rendre compte.[4]*

Cet avis est la première étape de la stratégie du CEPD. En s'inspirant des discussions avec les institutions, les États membres, la société civile, l'industrie et d'autres parties prenantes de l'UE, nos conseils visent à aider les participants au trilogue à trouver un consensus à temps. Il aborde le règlement général sur la protection des données dans deux parties:

- *la conception du CEPD concernant des règles relatives à la protection des données orientées vers l'avenir, avec des exemples illustrant nos recommandations; et*
- *une annexe («Annexe à l'avis 3/2015: tableau comparatif de textes du règlement général sur la protection des données avec une recommandation du CEPD») avec un tableau à quatre colonnes comparant, article par article, le texte du règlement général sur la protection des données tel qu'adopté respectivement par la Commission, le Parlement et le Conseil, et la recommandation du CEPD.*

L'avis est publié sur notre site web et consultable via une application mobile. Il sera complété en automne 2015 par des recommandations pour les considérants du règlement général sur la protection des données et, après que le Conseil aura adopté sa position générale, sur la protection des données applicable aux activités judiciaires et policières.

L'avis exhaustif du CEPD concernant la proposition de train de mesures de la Commission en mars 2012 reste valide. Trois ans après, il fallait toutefois mettre à jour notre avis pour soutenir plus directement les positions des colégislateurs et proposer des recommandations spécifiques. [5] Comme pour l'avis de 2012, le présent avis s'aligne sur les avis et déclarations du groupe de travail «Article 29», y compris l'«Annexe» intitulée «Core

topics in the view of trilogue» adoptée le 18 juin, à laquelle le CEPD a contribué en tant que membre à part entière du groupe de travail.[6]

Une rare opportunité: Pourquoi cette réforme est-elle si importante?

L'UE est dans le dernier kilomètre d'un marathon visant à réformer ses règles sur les données à caractère personnel. Le règlement général sur la protection des données affectera potentiellement, pour les décennies à venir, toute la population de l'UE, toutes les organisations de l'UE qui traitent des données à caractère personnel et les organisations extérieures à l'UE qui traitent les données à caractère personnel de personnes physiques vivant dans l'UE.[7] Il est grand temps de sauvegarder les libertés et les droits fondamentaux des personnes physiques dans la société de l'avenir basée sur les données.

Une protection efficace des données responsabilise les personnes physiques et galvanise les entreprises responsables et les pouvoirs publics. Les législations en vigueur dans ce domaine sont complexes et techniques; elles nécessitent des conseils d'experts, en particulier ceux d'autorités indépendantes compétentes en matière de protection des données qui sont à même de comprendre les enjeux de la conformité. Le règlement général sur la protection des données est probablement l'un des plus longs textes de loi de l'Union; l'UE doit donc désormais tâcher d'être sélective, se concentrer sur les dispositions qui sont réellement nécessaires et éviter des détails qui pourraient avoir comme conséquence involontaire d'interférer indûment avec les technologies futures. Les textes de chacune des institutions prêchent clarté et intelligibilité dans le traitement des données à caractère personnel: le règlement général sur la protection des données doit donc mettre en pratique ce qu'il préconise, en étant aussi clair et compréhensible que possible.

Il appartient au Parlement et au Conseil en tant que colégislateurs d'arrêter le texte législatif définitif préparé par la Commission en tant qu'institution gardienne des traités ayant l'initiative législative. Le CEPD ne participe pas aux négociations du «trilogue», mais nous sommes légalement habilités à fournir des conseils, et à le faire de manière proactive, conformément aux mandats du contrôleur européen et du contrôleur adjoint, et à la nouvelle stratégie du CEPD. Le présent avis tire parti d'une décennie d'expérience en matière de contrôle du respect de la protection des données et de conseil stratégique afin de pouvoir guider les institutions en vue de l'obtention d'un résultat qui servira les intérêts de la personne physique.

La législation est l'art du possible. Parmi les options qui se présentent à nos yeux sous la forme des textes spécifiques préconisés par la Commission, le Parlement et le Conseil, toutes contiennent des dispositions valables, mais chacune peut être améliorée. De notre point de vue, le résultat ne sera pas parfait, mais nous voulons aider les institutions à parvenir aux meilleurs résultats possibles. Voilà pourquoi nos recommandations s'inscrivent dans les limites des trois textes. Nous sommes animés par trois préoccupations constantes:

- un meilleur compromis pour les citoyens,
- des règles applicables en pratique,
- des règles qui dureront le temps d'une génération.

Le présent avis est un exercice de transparence et de responsabilité, deux principes qui sont peut-être l'innovation la plus remarquable du règlement général sur

la protection des données. La procédure de trilogue fait plus que jamais l'objet d'une attention accrue. Nos recommandations sont publiques, et nous exhortons toutes les institutions de l'UE à prendre l'initiative et à montrer l'exemple, de manière à ce que cette réforme législative soit le résultat d'un processus transparent et non d'un compromis secret.

L'UE a besoin d'un nouvel accord sur la protection des données, un nouveau chapitre. Le reste du monde suit de près ce qui se passe actuellement. La qualité de la nouvelle législation et la manière dont elle interagit avec les systèmes juridiques et les tendances du monde entier revêtent une importance capitale. Par le présent avis, le CEPD souligne sa volonté et sa disponibilité à veiller à ce que l'UE tire le meilleur parti de cette occasion historique.

I. TABLE DES MATIÈRES

1 De meilleurs conditions pour les citoyens

Les règles de l'UE ont toujours visé à faciliter les flux de données, tant au sein de l'Union qu'avec ses partenaires commerciaux, en faisant montre cependant d'une préoccupation majeure pour les droits et les libertés de la personne. L'internet garantit un niveau sans précédent de connectivité, de capacité d'expression personnelle et de potentialité en matière de valeur ajoutée aux entreprises et aux consommateurs. Toutefois, le respect de la vie privée importe plus que jamais aux Européens. Selon l'enquête Eurobaromètre sur la protection des données de juin 2015,[8] plus de six citoyens sur dix ne font pas confiance aux activités de commerce en ligne et deux tiers d'entre eux sont préoccupés par le fait de ne pas avoir un contrôle total des informations qu'ils mettent en ligne.

Le cadre remanié doit maintenir et, le cas échéant, relever les normes relatives aux personnes. Le train de mesures pour une réforme de la protection des données a d'abord été proposé comme un instrument de «renforcement des droits à la vie privée en ligne» en garantissant aux personnes d'«être mieux informées sur leurs droits et d'avoir davantage de contrôle de leurs données.»[9] Des représentants d'organisations de la société civile ont écrit à la Commission européenne en avril 2015 pour exhorter les institutions à rester fidèles à ces intentions.[10]

Les principes existants établis dans la Charte, le droit primaire de l'UE, doivent s'appliquer de manière cohérente, dynamique et innovante de façon à être efficaces pour le citoyen dans la pratique. La réforme doit être globale, d'où le recours à un ensemble de mesures, mais comme le traitement des données est susceptible de relever d'instruments juridiques distincts, il convient d'être clair quant à leur champ d'application précis et à la manière dont ils interagissent, et de veiller à éviter qu'ils contiennent des lacunes compromettant les garanties.[11]

Pour le CEPD, le point de départ est la dignité de la personne qui transcende les questions de simple conformité juridique.[12] Nos recommandations s'appuient sur une analyse de chaque article du règlement général sur la protection des données, individuellement et cumulativement, selon qu'il renforcera ou non la position de la personne par rapport au cadre existant. Les principes qui se trouvent au cœur de la protection des données, à savoir, l'article 8 de la Charte des droits fondamentaux, constituent le point de référence.[13]

1. Définitions: de la nécessité de clarifier la notion d'informations à caractère personnel

- Les personnes devraient pouvoir exercer plus efficacement leurs droits concernant toute information susceptible de les identifier ou de les distinguer, même si l'information est considérée comme «pseudonymisée».[14]

2. Tout traitement de données doit être licite *et* justifié

- Les exigences qui impliquent que tout traitement de données soit limité à des fins spécifiques et fondé sur une base juridique sont cumulatives et non alternatives. Nous recommandons d'éviter tout amalgame et d'affaiblir ainsi ces principes. En revanche, l'UE doit préserver, simplifier et rendre opératoire la

notion établie selon laquelle les données à caractère personnel ne devraient être utilisées que de manière compatible avec les fins initiales de collecte.[15]

- Le consentement constitue un fondement juridique éventuel du traitement, mais nous devons empêcher toute contrainte visant à faire en sorte qu'une personne coche des cases lorsqu'elle n'a pas de choix véritable et que le traitement des données n'est pas nécessaire du tout. Nous recommandons d'autoriser les personnes à donner un consentement large ou limité, par exemple à des études cliniques, lequel doit être respecté et peut être retiré.[16]

- Le CEPD soutient des solutions saines et innovantes pour les transferts internationaux d'informations à caractère personnel, qui facilitent les échanges de données et respectent les principes de la protection et du contrôle des données. Nous déconseillons vivement d'autoriser des transferts sur la base d'intérêts légitimes du responsable du traitement en raison de la protection insuffisante accordée aux personnes; de même, l'UE ne doit pas laisser la porte ouverte à un accès direct par des autorités de pays tiers à des données situées dans l'UE. Toute demande de transfert émise par des autorités d'un pays tiers ne devrait être reconnue que si elle respecte les normes fixées dans les traités d'entraide judiciaire, les accords internationaux ou dans d'autres canaux légaux de coopération internationale.[17]

3. Une surveillance plus indépendante, plus sûre

- Les autorités de protection des données de l'UE doivent être en mesure d'exercer leurs rôles au moment où le règlement général sur la protection des données entrera en vigueur, le Comité européen de la protection des données devenant pleinement opérationnel dès que le règlement sera applicable.[18]

- Les autorités doivent être en mesure d'entendre et d'examiner les plaintes et les réclamations introduites par des personnes concernées ou par des organes, organisations et associations.

- L'application des droits individuels nécessite un système efficace de responsabilité et d'indemnisation en cas de dommages causés par le traitement illicite des données. Étant donné les obstacles évidents pour obtenir réparation dans la pratique, les personnes devraient avoir la possibilité d'être représentées en justice par des organes, des organisations et des associations.[19]

2 Des règles applicables en pratique

Il convient de ne pas confondre garanties et formalités. L'excès de détails ou les tentatives de microgestion des processus d'entreprise risquent de devenir obsolètes à l'avenir. Nous pouvons nous inspirer ici du manuel de la concurrence de l'UE, dans lequel un corpus relativement limité de législation dérivée est rigoureusement appliqué, encourageant une culture de la responsabilité et de la prise de conscience parmi les entreprises.[20]

Chacun des trois textes exige une clarté et une simplicité accrues de la part des responsables du traitement des informations à caractère personnel.[21] De même, les

contraintes techniques doivent également être concises et faciles à comprendre pour être correctement mises en œuvre par les responsables du traitement.[22]

Les procédures existantes ne sont pas sacrées: nos recommandations visent à trouver des voies de simplification administrative, en réduisant les prescriptions pour la documentation et les formalités superflues. Il est recommandé de ne légiférer qu'en cas de véritable nécessité. Cela offre une marge de manœuvre aux entreprises, aux pouvoirs publics ou aux autorités de protection des données: un espace qui doit être occupé par la responsabilité et les orientations des autorités de protection des données. De manière générale, nos recommandations permettraient d'élaborer un texte du règlement général sur la protection des données plus court de presque 30 % par rapport à la longueur moyenne de ceux des trois institutions.[23]

1. Des garanties efficaces, pas des procédures

- La documentation devrait être un moyen de se conformer au règlement, non une fin en soi; la réforme doit être axée sur les résultats. Nous recommandons une approche évolutive qui permette de réduire les obligations de documentation imposées aux responsables du traitement à une politique unique sur la manière de se conformer à la réglementation en tenant compte des risques, avec une exposition transparente de la conformité, qu'il s'agisse de transferts, de contrats avec des sous-traitants ou de notifications des violations de données.[24]

- À partir de critères explicites d'évaluation des risques, et d'après notre expérience de contrôle des institutions de l'UE, nous suggérons d'exiger une notification des violations de données auprès de l'autorité de contrôle et une analyse d'impact relative à la protection des données uniquement dans les cas où les droits et libertés des personnes concernées sont en danger.[25]

- Les initiatives sectorielles, que ce soit par l'intermédiaire de règles d'entreprise contraignantes ou par l'utilisation de labels de protection de la vie privée, devraient être activement encouragées.[26]

2. Un meilleur équilibre entre l'intérêt public et la protection des données à caractère personnel

- Les règles de protection des données ne devraient pas entraver la recherche historique, statistique et scientifique qui sert réellement l'intérêt général. Les responsables doivent prendre les dispositions nécessaires pour empêcher que les informations à caractère personnel soient utilisées contre l'intérêt de la personne, en accordant une attention particulière aux règles régissant les informations sensibles concernant, par exemple, la santé.[27]

- Sous réserve de ces garanties, les chercheurs et les archivistes devraient pouvoir stocker des données aussi longtemps que nécessaire.[28]

3. Faire confiance aux autorités de contrôle et leur donner les moyens d'agir

- Nous recommandons de laisser les autorités de contrôle fournir des orientations aux responsables du traitement de données et élaborer leurs propres règles de procédure internes dans le sens d'une application simplifiée, facilitée du

règlement général sur la protection des données par une autorité de contrôle unique (le «guichet unique») proche des citoyens («proximité»). [29]

- Ces autorités devraient pouvoir déterminer des sanctions correctives et administratives efficaces, proportionnées et dissuasives en fonction de toutes les circonstances pertinentes.[30]

3 Des règles qui dureront le temps d'une génération

Le pilier principal du cadre actuel, la directive 95/46/CE, a servi de modèle à la nouvelle législation sur le traitement des données dans l'UE et dans le monde, et a même servi de base pour le libellé du droit à la protection des données à caractère personnel prévu à l'article 8 de la Charte des droits fondamentaux. Cette réforme définira le traitement des données pour une génération qui n'a jamais connu la vie sans l'internet. L'UE doit donc comprendre toutes les implications de ce texte de loi pour les individus et sa durabilité face à l'évolution des technologies.

Ces dernières années, on a observé une augmentation exponentielle en matière de génération, de collecte, d'analyse et d'échange d'informations à caractère personnel, le résultat d'innovations technologiques telles que l'internet des objets, l'informatique en nuage, les mégadonnées et données ouvertes dont l'exploitation est considérée par l'UE comme indispensable à sa compétitivité.[31] À en juger par la longévité de la directive 95/46/CE, il est raisonnable de supposer un délai comparable avant la prochaine grande révision des règles en matière de protection des données, peut-être pas avant la fin des années 2030. Longtemps avant cela, on pourra s'attendre à ce que les technologies axées sur les données aient convergé avec les systèmes biométriques, d'intelligence artificielle et de traitement du langage naturel, dotant les applications d'une capacité d'apprentissage automatique et permettant ainsi d'obtenir des renseignements d'un niveau avancé.

Ces technologies posent un défi aux principes de la protection des données. Une réforme orientée vers l'avenir doit donc reposer sur la dignité de la personne et être guidée par l'éthique. Elle doit réduire le déséquilibre entre l'innovation dans la protection des données à caractère personnel et son exploitation, en renforçant l'efficacité des garanties au sein de notre société numérisée.

1. Pratiques commerciales responsables et ingénierie innovante

- La réforme devrait inverser la tendance récente à la surveillance secrète et à la prise de décision sur la base de profils cachés de la personne. Le problème ne concerne pas la publicité ciblée ou la pratique du profilage, mais plutôt l'absence d'informations significatives concernant la logique algorithmique qui élabore ces profils et a un effet sur la personne concernée.[32] Nous proposons une plus grande transparence des responsables du traitement.

- Nous soutenons fermement l'introduction des principes de protection des données dès la conception et de protection des données par défaut comme un moyen de lancer des solutions axées sur le marché dans l'économie numérique. Nous recommandons une formulation plus simple pour demander que les droits et intérêts des individus soient intégrés dans le développement du produit et les paramètres par défaut.[33]

2. Individus disposant de moyens d'agir

- La portabilité des données est, dans l'environnement numérique, la voie d'accès au contrôle des utilisateurs dont les individus réalisent à présent qu'il leur échappe. Nous recommandons de permettre un transfert direct des données d'un responsable du traitement à un autre, à la demande de la personne concernée, et d'autoriser les personnes concernées à recevoir une copie des données qu'ils pourront eux-mêmes transférer à un autre responsable du traitement.[34]

3. Des règles évolutives

- Nous suggérons d'éviter un langage et des pratiques susceptibles de se révéler obsolètes ou discutables.[35]

4 Questions en suspens

L'adoption d'un train de réformes européen des données tourné vers l'avenir sera une réalisation impressionnante mais néanmoins incomplète.

Toutes les institutions conviennent que les principes du règlement général sur la protection des données doivent s'appliquer uniformément aux institutions de l'UE. Nous avons préconisé une sécurité juridique et une uniformité du cadre juridique, tout en acceptant le caractère unique du secteur public de l'UE et la nécessité d'éviter tout affaiblissement du niveau actuel des obligations (ainsi que la nécessité de prévoir la base juridique et organisationnelle du CEPD). Une proposition cohérente avec le règlement général sur la protection des données en vue de la révision du règlement 45/2001 devrait donc être faite par la Commission dès que possible après la fin des négociations sur le règlement général, de façon à ce que les deux textes puissent être applicables en même temps.[36]

Dans un second temps, il est évident que la directive 2002/58/CE (la «directive vie privée et communications électroniques») devra être modifiée. Aspect plus important encore, l'UE exige un cadre précis pour la confidentialité des communications, un élément à part entière du droit à la vie privée, qui régisse l'ensemble des services permettant les communications, pas seulement les fournisseurs de services de communications électroniques accessibles au public. Cela doit se faire au moyen d'un règlement juridiquement sûr et harmonisé, prévoyant au moins les mêmes normes de protection que celles visées par la directive vie privée et communications électroniques dans des conditions de concurrence équitables.

Par conséquent, le présent avis conseille de s'engager à adopter les propositions formulées dans ces deux domaines le plus rapidement possible.

5 Un tournant important pour les droits numériques en Europe et au-delà

Pour la première fois en une génération, l'UE a l'occasion de moderniser et d'harmoniser les règles relatives au traitement des données à caractère personnel. Le respect de la vie privée et la protection des données ne concurrencent ni la croissance économique et le commerce international, ni les grands services et produits; ils font partie de la proposition de qualité et de valeur. Comme le reconnaît le Conseil européen,

la confiance est une condition préalable indispensable pour des produits et des services innovants reposant sur le traitement de données à caractère personnel.

En 1995, l'UE était un précurseur en matière de protection des données. Aujourd'hui, plus de cent pays à travers le monde disposent de lois relatives à la protection des données et moins de la moitié d'entre eux sont des pays européens.[37] L'UE continue néanmoins d'enjoindre à suivre de près les pays qui songent à mettre en place ou réviser leurs cadres juridiques. À un moment où la confiance des personnes dans les entreprises et les gouvernements a été ébranlée par des révélations sur la surveillance de masse et les violations de données, cela confère une responsabilité considérable aux législateurs de l'UE dont les décisions devraient cette année avoir des répercussions au-delà de l'Europe.

Selon le CEPD, les textes du règlement général sur la protection des données sont sur la bonne voie, mais des inquiétudes demeurent, certaines très sérieuses. La procédure de codécision comporte toujours le risque que certaines dispositions soient fragilisées par les bonnes intentions de négociateurs en quête de compromis politique. En ce qui concerne la réforme sur la protection des données, c'est toutefois différent parce que nous traitons de droits fondamentaux et de la façon dont ils seront garantis pendant une génération.

Par conséquent, le présent avis cherche à aider les principales institutions de l'UE à résoudre les problèmes. Nous ne voulons pas seulement des droits renforcés pour la personne concernée et une responsabilité accrue pour le responsable du traitement; nous voulons faciliter l'innovation au moyen d'un cadre juridique qui soit neutre à l'égard de la technologie, mais positif par rapport aux avantages que celle-ci peut procurer à la société.

Les négociations arrivant à leur terme, nous espérons que nos recommandations aideront l'UE à franchir la ligne avec une réforme qui demeurera adaptée au cours des prochaines années et des prochaines décennies: un nouveau chapitre pour la protection des données qui s'inscrit dans une perspective mondiale, l'UE montrant l'exemple.

Bruxelles, le 28 juillet 2015

(**signé**)

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

Addenda

Le 27 juillet 2015, nous avons publié (avis du CEPD 3/2015) nos recommandations relatives à la rédaction des clauses opérationnelles du règlement général sur la protection des données. Après mûre réflexion quant aux principes de base sur lesquels reposent les articles des trois versions préconisées respectivement par la Commission, le Parlement européen et le Conseil, nous souhaitons apporter, à titre de contribution supplémentaire aux négociations du «trilogue» en cours, nos recommandations concernant le contenu des considérants du règlement général sur la protection des données.

Les considérants du préambule d'un instrument juridique de l'UE sont importants dans la mesure où ils expliquent les raisons d'être de chaque disposition. Bien qu'ils soient dénués de toute valeur juridique indépendante, les considérants peuvent être utilisés dans le cadre de l'interprétation du champ d'application des dispositions de fond du texte. La CJUE a déclaré à plusieurs occasions que des considérants valables étaient nécessaires pour que la Cour puisse remplir sa fonction d'interprétation de la loi. Dans la mesure où ils présentent les principes de base sur lesquels repose l'acte juridique, ils méritent une attention particulière.

Ce faisant, nous réitérons dans ces recommandations qu'il convient de poser le respect de la dignité humaine comme base de tout traitement d'informations à caractère personnel. Le règlement général sur la protection des données doit servir de schéma directeur d'une démarche éthique tirant parti des avantages sociétaux de l'innovation et des changements technologiques tout en protégeant les personnes et en leur donnant les moyens de prendre le contrôle des informations les concernant qui se trouvent dans le cyberespace. Les considérants doivent inciter davantage à la responsabilisation des responsables du traitement et permettre aux autorités de contrôle au sein du comité européen de la protection des données d'émettre des orientations.

Nous continuons à préconiser une rédaction aussi claire, concise et intelligible que possible. Nous recommandons également de supprimer des considérants tous les détails superflus susceptibles de limiter la faculté d'adaptation aux défis futurs à une époque où la rapidité des changements est désormais la norme.

Bruxelles, le 9 octobre 2015

Giovanni Buttarelli

Notes

[1] Déclarations communes Parlement européen Conseil Commission Déclaration commune sur les modalités pratiques de la procédure de codécision (article 251 du traité CE) (2007/C 145/02), JO C 145, 30.6.2007.

[2] COM(2012)11 final; résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), P7_TA(2014)0212; proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) - Préparation d'une orientation générale, document du Conseil 9565/15, 11.06.2015.

[3] Le titre complet est Proposition de directive 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, COM(2012)10 final; résolution législative du Parlement européen du 12 mars 2014 sur la proposition de directive du Parlement européen et du Conseil 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, P7_TA(2014)0219. En ce qui concerne le calendrier et la portée du trilogue, voir les Conclusions du Conseil européen des 25 et 26 juin 2015, EUCO 22/15; une «feuille de route» pour le trilogue a été mentionnée à l'occasion d'une conférence de presse commune du Parlement et du Conseil http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed [dernière consultation le 20.7.2015] mais n'a pas été publiée officiellement. Le règlement général sur la protection des données entrera en vigueur le vingtième jour suivant celui de sa publication au Journal officiel et devrait être pleinement applicable deux ans après son entrée en vigueur (article 91).

[4] Avis de vacance pour le poste de contrôleur européen de la protection des données COM/2014/10354 (2014/C 163 A/02), JO C 163 A/6 28.5.2014. La stratégie du CEPD pour la période de 2015 à 2019 promettait de «rechercher des solutions réalisables qui requièrent moins d'administration, restent ouvertes aux innovations technologiques et aux flux de données transfrontaliers et garantissent que les personnes puissent faire valoir leurs droits plus efficacement tant en ligne qu'hors ligne»; en montrant l'exemple: La stratégie du CEPD pour la période allant de 2015 à 2019, mars 2015.

[5] Avis du CEPD sur le train de mesures pour une réforme de la protection des données, du 7.3.2015.

[6] Voir annexe à la lettre du groupe de travail «Article 29» à Věra Jourová, commissaire à la justice, aux consommateurs et à l'égalité des sexes, du 17.6.2015.

[7] Il est difficile de résumer succinctement le champ d'application matériel et territorial du règlement général sur la protection des données. Tout au moins, les institutions semblent convenir que ce champ d'application couvre les organisations établies dans l'UE qui prennent en charge le traitement des données à caractère personnel soit dans l'Union ou à l'extérieure de celle-ci, les organisations établies à l'extérieure de l'UE qui traitent les données à caractère personnel des personnes physiques vivant dans l'UE lorsqu'elles offrent des biens ou des services ou surveillent des personnes physiques dans l'UE. (Voir l'article 2 sur le champ d'application matériel et l'article 3 sur le champ d'application territorial du règlement.)

[8] Selon d'autres résultats, sept citoyens sur dix se montrent préoccupés par le fait que leurs données soient utilisées à d'autres fins que celles pour lesquelles elles avaient été collectées, un sur sept déclarant que son accord explicite devrait être exigé dans tous les cas avant la collecte et le traitement de ses données, et deux tiers estimant qu'il est important de pouvoir transférer des données à caractère personnel d'un ancien prestataire de services vers un nouveau prestataire; Eurobaromètre spécial 431 sur la protection des données, juin 2015. Résultats comparables à ceux de Pew Research en 2014 qui relèvent que 91 % des Américains estiment avoir perdu le contrôle de la manière dont les entreprises collectent et exploitent les renseignements personnels; parmi les utilisateurs des réseaux sociaux, 80 % s'inquiètent du fait que des tiers tels que les annonceurs ou les entreprises obtiennent leurs données, et 64 % ajoutent que le gouvernement devrait faire davantage pour réguler les activités des annonceurs; Pew Research Privacy Panel Survey, janvier 2014.

[9] La Commission propose une réforme globale des règles de protection des données afin d'accroître le contrôle par les utilisateurs de leurs données et de réduire les coûts pour les entreprises.

[10] Lettre d'ONG au président Juncker, 21.4.2015 https://edri.org/files/DP_letter_Juncker_20150421.pdf et réponse du chef de cabinet du vice-président Timmermans, 17.7.2015 https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [consulté le 23.7.2015]. En mai 2015, le CEPD a rencontré des représentants de plusieurs de ces ONG afin de discuter de leurs préoccupations; COMMUNIQUÉ DE PRESSE CEPD/2015/04, 1.6.2015, Réforme de la protection des données dans l'UE: le CEPD rencontre des groupes internationaux de défense des libertés civiles; enregistrement longue durée de la discussion disponible sur le site web du CEPD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

[11] Article 2, paragraphe 2, point e).

[12] Article premier.

[13] L'article 8 de la Charte prévoit [gras ajouté]

> *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*
>
> *2. Ces données doivent être* ***traitées loyalement****, à des* ***fins déterminées*** *et sur la* ***base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi****. Toute personne a le* ***droit*** *d'accéder aux données collectées la concernant et* ***d'en obtenir la rectification****.*
>
> *3. Le respect de ces règles est soumis au* ***contrôle d'une autorité indépendante****.*

[14] Article 10. À moins qu'il n'existe de définition claire et juridiquement contraignante de l'expression «données pseudonymisées» par opposition à «données à caractère personnelle», ce type de données doit demeurer dans le champ d'application des règles de protection des données.

[15] Article 6, paragraphes 2 et 4. Étant donné qu'il y a eu quelque incertitude quant au sens de «compatibilité», nous recommandons, conformément à l'avis du groupe de travail «Article 29» sur la limitation des finalités, des critères généraux d'évaluation de la compatibilité du traitement (voir article 5, paragraphe 2).

[16] Une séparation fonctionnelle effective constitue un moyen de garantir un traitement licite en l'absence de consentement, mais l'intérêt légitime ne doit pas faire l'objet d'une interprétation excessive. Un droit de retrait inconditionnel peut également constituer une solution appropriée dans certains cas. Déterminer si un consentement est donné librement dépend en partie du fait a) qu'il existe un déséquilibre significatif entre la personne concernée et le responsable du traitement et b) en cas de traitement au titre de l'article 6, paragraphe 1, point b), du fait que l'exécution d'un contrat ou la prestation d'un service est subordonnée au consentement au

traitement de données qui n'est pas nécessaire à ces fins. (voir article 7, paragraphe 4.) Cela reflète les dispositions du droit européen de la consommation: en vertu de l'article 3, paragraphe 1, de la directive 93/13/CEE du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs, «Une clause d'un contrat n'ayant pas fait l'objet d'une négociation individuelle est considérée comme abusive lorsque, en dépit de l'exigence de bonne foi, elle crée au détriment du consommateur un déséquilibre significatif entre les droits et obligations des parties découlant du contrat.»

[17] Ces règles comprennent des décisions d'adéquation pour des secteurs et des territoires spécifiques, des examens périodiques des décisions d'adéquation et des règles d'entreprise contraignantes. Voir les articles 40 à 45.

[18] Article 73.

[19] Article 76. En ce qui concerne la difficulté à obtenir réparation en cas de violations des règles portant sur la protection des données, voir le rapport de l'Agence des droits fondamentaux, Access to data protection remedies in EU Member States (Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE), 2013.

[20] Les règles de l'UE mettent l'accent sur l'autoévaluation par les entreprises de la conformité avec l'interdiction des accords anticoncurrentiels visée à l'article 101 TFUE, alors que les entreprises occupant une position dominante sur un marché ont une «responsabilité particulière» pour éviter toute action susceptible d'entraver une concurrence effective (paragraphe 9 des orientations de la Commission 2009/C 45/02); voir Avis préliminaire du CEPD sur la vie privée et la compétitivité à l'ère de la collecte de données massives, 14.3.2014.

[21] Les trois textes font diversement référence à «une manière et sous une forme intelligible, en des termes clairs et simples» (considérant 57, PE; article 19, COM et Conseil), à «des droits clairs et univoques» (considérant 99), PE; article 10 bis PE) et à la fourniture d'«informations claires et aisément compréhensibles» (article 10 PE, article 11 PE), ainsi qu'à des informations «concises, transparentes, claires et facilement accessibles» (considérant 25), PE, COM et Conseil; article 11 PE).

[22] Des dispositions en faveur d'actes délégués ont été en grande partie retirées des versions du Parlement et du Conseil. Nous estimons que l'UE pourrait aller plus loin et laisser ces questions techniques à l'expertise d'autorités indépendantes.

[23] Nos recommandations produiraient un texte d'environ 20 000 mots; la longueur moyenne des textes des trois institutions est d'à peu près 28 000 mots.

[24] Article 22.

[25] Articles 31 et 33.

[26] Article 39.

[27] Article 83. La recherche et l'archivage en soi ne constituent pas un fondement juridique au traitement, raison pour laquelle nous proposons de supprimer l'article 6, paragraphe 2.

[28] Article 83 bis.

[29] Le groupe de travail «Article 29» a défini un modèle de gouvernance: mécanisme de contrôle de la cohérence et guichet unique fondé sur la confiance dans des autorités de contrôle de la protection des données indépendantes et opérant à trois niveaux:

- les autorités de contrôle individuelles, fortes et dotées de suffisamment de ressources pour traiter de cas relevant de leur domaine de compétence;
- une coopération efficace entre les autorités de contrôle jouant un rôle clair dans les affaires transfrontalières;

- le Comité européen de la protection des données qui doit être autonome, avec sa propre personnalité juridique, disposant de moyens suffisants, constitué d'autorités de contrôle égales travaillant dans un esprit de solidarité, ayant le pouvoir de prendre des décisions contraignantes et appuyé par un secrétariat qui est au service du comité par le biais de la présidence.

[30] Nous préconisons également de clarifier la compétence des autorités de contrôle et la désignation d'une autorité chef de file dans les cas de traitement de données transnational, tout en préservant la capacité des autorités de contrôle à traiter des cas purement locaux. Nous recommandons une version simplifiée du mécanisme de contrôle de la cohérence avec plus de clarté sur la façon d'identifier les cas où les autorités de contrôle devraient consulter le Comité européen de la protection des données et où ledit Comité devrait rendre une décision contraignante afin de veiller à l'application cohérente du règlement.

[31] Communication de la Commission relative à une Stratégie pour un marché unique numérique en Europe, COM(2015) 192 final; conclusions du Conseil européen de juin 2015, EUCO 22/15; conclusions du Conseil sur la transformation numérique de l'industrie européenne, 8993/15.

[32] Article 14, point h).

[33] Article 23.

[34] Article 18. Pour qu'il soit effectif, nous recommandons également que le droit à la portabilité des données dispose d'un champ d'application élargi et ne s'applique pas uniquement aux opérations de traitement utilisant les données fournies par la personne concernée.

[35] Nous conseillons, par exemple, d'abandonner des termes comme «en ligne», «par écrit» et «la société de l'information».

[36] Une option, qui aurait notre préférence, serait que cela soit fait au moyen d'une disposition introduite dans le règlement général lui-même.

[37] Greenleaf, Graham, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (January 30, 2015); (2015) 133 Privacy Laws & Business International Report, February 2015; UNSW Law Research Paper No. 2015-21.