Résumé de l'avis du contrôleur européen de la protection des données sur les systèmes de gestion des informations personnelles

(Le texte complet de l'avis en anglais, français et allemand est disponible sur le site internet du CEPD www.edps.europa.eu)

(2016/C 463/10)

Le présent avis étudie le concept de technologies et d'écosystèmes visant à habiliter les personnes à contrôler le partage de leurs données à caractère personnel («systèmes de gestion des informations personnelles», ou «PIMS» en abrégé).

Notre vision est de créer une réalité nouvelle où les personnes gèrent et contrôlent leur identité en ligne. Notre but est de transformer le système actuel, centré sur les fournisseurs, en un système centré sur l'humain, qui protège les personnes du traitement illicite de leurs données et des techniques intrusives de traçage et de profilage tendant à contourner les principes fondamentaux de la protection des données.

Cette réalité nouvelle sera facilitée par le cadre réglementaire actualisé de l'Union européenne et par les possibilités découlant d'une application rigoureuse et conjointe de la législation par l'ensemble des autorités compétentes en matière de contrôle et de réglementation.

Le règlement général sur la protection des données récemment adopté renforce et modernise le cadre réglementaire de manière à ce qu'il reste efficace à l'ère des données massives en raffermissant la confiance des personnes dans la sécurité en ligne et le marché unique numérique. Les nouvelles règles, notamment celles concernant la transparence accrue et les puissants droits d'accès et de portabilité des données, visent à permettre aux utilisateurs de mieux contrôler leurs données. Elles peuvent également contribuer à l'efficacité des marchés de données à caractère personnel, dans l'intérêt des consommateurs et des entreprises.

Récemment encore, nous avons rendu un avis sur l'application effective des droits fondamentaux à l'ère des données massives. Celui-ci met en évidence les conditions du marché et les pratiques des entreprises qui font obstacle à l'exercice effectif des droits des personnes à la protection de leurs données à caractère personnel ainsi que d'autres droits fondamentaux. Il demande de redoubler d'efforts pour faire appliquer de manière concertée et cohérente la législation en matière de concurrence et de protection des consommateurs et des données. Nous espérons que cette meilleure application de la législation contribuera à créer des conditions du marché dans lesquelles les services qui respectent la vie privée pourront prospérer. L'approche développée dans le présent avis vise à renforcer les droits fondamentaux dans cet univers numérique qui est le nôtre, tout en envisageant des possibilités nouvelles qui permettront aux entreprises de développer des services innovants basés sur les données à caractère personnel et reposant sur une confiance mutuelle. Les PIMS promettent non seulement une nouvelle architecture technique et une nouvelle organisation de la gestion des données, mais aussi des cadres basés sur la confiance et, de ce fait, des modèles commerciaux différents pour collecter et traiter les données à caractère personnel à l'ère des données massives d'une manière plus respectueuse de la législation européenne en matière de protection des données.

Dans le présent avis, nous expliquerons brièvement en quoi les PIMS consistent, les problèmes qu'ils sont censés résoudre et les solutions qu'ils mettent en œuvre à cet effet. Nous analyserons ensuite la contribution qu'ils peuvent apporter à l'amélioration de la protection des données à caractère personnel, ainsi que les défis qui les attendent. Enfin, nous dégagerons des pistes permettant d'exploiter les possibilités qu'ils offrent. Pour que les nouveaux modèles commerciaux dans le domaine de la protection des données prospèrent, il sera peut-être nécessaire d'adopter des mesures d'incitation supplémentaires à l'intention des fournisseurs de services qui les offrent. Il convient d'examiner en particulier les initiatives politiques susceptibles d'encourager les responsables du traitement des données à accepter cette nouvelle manière de fournir des données. En outre, une initiative des services publics visant à accepter les PIMS comme source de données en remplacement de la collecte directe de données pourrait favoriser l'acceptation des PIMS.

L'environnement émergent des PIMS, qui visent à permettre aux personnes et aux consommateurs de reprendre le contrôle de leurs données à caractère personnel, mérite d'être pris en considération, soutenu et mieux étudié afin de contribuer à une utilisation durable et éthique des données massives et à la mise en œuvre effective des principes du RGPD

I. PIMS: UN PARTAGE DE DONNÉES MUTUELLEMENT PROFITABLE?

1. Les conditions actuelles du traitement de données à caractère personnel sont souvent inéquitables pour les personnes dont les données sont traitées. Les conditions juridiques et les outils techniques empêchent les personnes d'exercer aisément leurs droits et permettent aux responsables du traitement de limiter leur responsabilité. Les courtiers en données, les réseaux publicitaires, les fournisseurs de réseaux sociaux et d'autres acteurs économiques détiennent des fichiers de plus en plus complets sur les personnes participant à la société numérique actuelle, qui perdent le contrôle des empreintes numériques qu'elles laissent derrière elles. Ciblées, profilées et évaluées par des acteurs hors de leur portée ou dont elles ne soupçonnent même pas l'existence, les personnes peuvent se sentir démunies. Elles doivent être habilitées à prendre le contrôle de leur identité. Même lorsqu'elles ont officiellement

reçu une forme ou l'autre de «notification» et qu'elles ont eu l'occasion de «consentir» aux conditions générales, les personnes se retrouvent souvent dans un système conçu pour maximiser la monétisation des données à caractère personnel, sans leur laisser vraiment ni le choix ni une possibilité de contrôle.

2. La communication de la Commission européenne relative aux données massives ([1]) expose un plan d'actions axées à la fois sur les données à caractère personnel et sur la protection des consommateurs. Elle encourage en particulier l'utilisation d'«espaces de données personnelles» en tant qu'espaces sûrs et sécurisés, centrés sur l'utilisateur, pour stocker des données à caractère personnel et éventuellement permettre à des tiers d'y accéder. Nous sommes d'avis qu'il convient d'encourager les outils numériques et les modèles commerciaux innovants basés sur l'autonomisation des personnes. Les personnes pourraient ainsi bénéficier d'un tel partage de données, c'est-à-dire participer à l'utilisation et à la diffusion de leurs informations personnelles.

3. Dans notre avis intitulé «Relever les défis des données massives» ([2]), nous avons fait valoir que l'obligation légale concernant le consentement effectif devrait être complétée par un contrôle réel et pratique sur les informations personnelles. Nous avons expliqué que «*plutôt qu'une charge administrative, la fourniture de droits d'accès pourrait devenir une caractéristique du service offert aux clients*» et que les organisations qui exploitent les «données massives» «*devraient être prêtes à partager les profits générés par le traitement des données à caractère personnel avec les personnes concernées dont les données sont traitées*». Dans ce contexte, nous avons noté que les «*entrepôts de données personnelles pourraient aider à dissiper certaines des inquiétudes concernant la perte du contrôle individuel sur les données à caractère personnel*». Le règlement général sur la protection des données (RGPD) récemment adopté ([3]) a renforcé les exigences légales de consentement ([4]) et introduit les principes modernes et efficaces de protection dès la conception et par défaut ([5]), ainsi qu'un droit nouveau à la portabilité des données ([6]). Pour que le nouveau cadre relatif à la protection des données remplisse ses promesses, nous avons besoin d'outils pratiques qui permettront aux personnes d'exercer leurs droits d'une manière pratique et conviviale.

4. Le présent avis étudie les nouvelles technologies et les écosystèmes visant à habiliter les personnes à contrôler la collecte et le partage de leurs données à caractère personnel. Nous désignerons ce concept sous le vocable de «système de gestion des informations personnelles» («PIMS») ([7]). Le concept de PIMS offre une nouvelle approche qui consiste à faire des personnes les détenteurs de leurs propres informations personnelles. Il pourrait entraîner un changement de paradigme dans la gestion et le traitement des données à caractère personnel et avoir des conséquences sur le plan social et économique. Par comparaison, l'environnement actuel des services en ligne se caractérise par un nombre restreint de fournisseurs de services qui dominent le marché en monétisant les données à caractère personnel des utilisateurs en échange de services «gratuits». Cela va souvent de pair avec une relation déséquilibrée, dans laquelle le client se voit proposer une offre «à prendre ou à laisser», et avec une information asymétrique entre les fournisseurs de services et les utilisateurs caractérisée par une transparence limitée, voire inexistante, sur le sort réservé aux données à caractère personnel des personnes.

5. L'idée maîtresse qui sous-tend le concept de PIMS est de transformer le système actuel, centré sur les fournisseurs, en un système centré sur des personnes capables de gérer et de contrôler leur identité en ligne ([8]). En principe, les personnes devraient être en mesure de décider si elles partagent leurs informations personnelles et avec qui, pour quelles finalités et pour quelle durée, ainsi que de conserver la trace de ces données et de décider de les retirer si elles le souhaitent. Il serait utile d'étudier de quelle manière les PIMS pourraient aider à dissiper certaines des inquiétudes concernant la perte du contrôle individuel sur les données à caractère personnel, qui ressort comme étant l'une des principales préoccupations soulevées par les données massives ([9]).

([1]) Communication COM(2014)442 relative à une économie de la donnée prospère: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy

([2]) Avis n° 7/2015 du CEPD: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_FR.pdf. Voir en particulier la section 3.

([3]) 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) (JO L 119 du 4.5.2016, p. 1).

([4]) Voir entre autres l'article 6, paragraphe 1, point a), les articles 7 et 8 et les considérants 42 et 43 du RGPD.

([5]) Article 25 du RGPD.

([6]) Article 20 du RGPD.

([7]) Parmi les concepts connexes figurent les «entrepôts de données personnelles», les «espaces de données personnelles» et les «coffres de données personnelles». Le terme «PIMS» sera utilisé dans le présent avis étant donné qu'il décrit le mieux le concept d'une manière générale et aisément compréhensible. Tel qu'il est utilisé dans le présent avis, l'acronyme «PIMS» est soit au singulier, soit au pluriel – système ou systèmes de gestion des informations personnelles.

([8]) Voir le considérant 7 du RGPD: «Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant». Voir aussi, par exemple, Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).

([9]) Voir, par exemple, Ira S. Rubinstein, *Big Data*: *The End of Privacy or a New Beginning?* International Data Privacy Law, 2013, vol. 3, n° 2.

6. Cette approche vise à renforcer les droits fondamentaux dans cet univers numérique qui est le nôtre, tout en envisageant des possibilités nouvelles qui permettront aux entreprises de développer des services innovants basés sur les données à caractère personnel et reposant sur une confiance mutuelle. Les PIMS promettent une nouvelle architecture technique et une nouvelle organisation de la gestion des données qui mettent en place des cadres basés sur la confiance. Ils cherchent à rendre possibles des modèles commerciaux différents de collecte et de traitement des données à caractère personnel à l'ère des données massives d'une manière plus respectueuse de la législation européenne en matière de protection des données.

7. Dans le présent avis, nous expliquerons brièvement en quoi les PIMS consistent, les problèmes qu'ils sont censés résoudre et les solutions qu'ils mettent en œuvre à cet effet ([1]). Nous analyserons la contribution qu'ils peuvent apporter à l'amélioration de la protection des données à caractère personnel, ainsi que les défis qui les attendent. Enfin, nous dégagerons des pistes permettant d'exploiter les possibilités qu'ils offrent.

IV. CONCLUSIONS ET PROCHAINES ÉTAPES

4.1. Vers une application intégrale du RGPD — Perspectives

54. Comme indiqué ci-dessus, le législateur de l'Union européenne a adopté récemment un train de réformes sur la protection des données qui renforce et modernise le cadre réglementaire de manière à ce qu'il reste efficace à l'ère des données massives.

55. Le nouveau RGPD, qui comprend des règles relatives à une transparence accrue, à des droits d'accès puissants et à la portabilité des données, devrait contribuer à donner aux personnes un plus grand contrôle sur leurs données. Il pourrait aussi contribuer à des marchés plus efficaces pour les données à caractère personnel, dans l'intérêt des consommateurs comme dans celui des entreprises.

56. Les codes de conduite et les systèmes de certification prévus par le RGPD constituent des instruments privilégiés pour donner une visibilité et un rôle spécifiques aux technologies et aux produits qui – comme les PIMS – peuvent contribuer à une application plus efficace de la législation relative à la protection des données sur le plan pratique.

57. Les PIMS se heurtent toutefois à une difficulté générale: ils doivent pénétrer un marché dominé par des services en ligne qui reposent sur des modèles commerciaux et des architectures techniques où les personnes ne contrôlent pas leurs données, comme expliqué à la section 3.9. Le passage à une situation où les personnes ont la possibilité réelle d'accorder à un fournisseur de services l'accès à certaines données dans leur PIMS au lieu de les lui fournir directement nécessitera des mesures incitatives supplémentaires à l'intention des fournisseurs de services. La Commission peut mettre à profit les initiatives qu'elle a annoncées sur les flux et la propriété des données ([2]) pour envisager des initiatives politiques supplémentaires qui pourraient inciter les responsables du traitement à accepter cette manière de fournir des données. En outre, une initiative des services publics de gouvernement électronique visant à accepter les PIMS comme source de données en remplacement de la collecte directe de données pourrait favoriser l'acceptation des PIMS.

58. Cette analyse pourrait être complétée par des mesures visant à jeter les fondements techniques, sociétaux et économiques, notamment des efforts de normalisation et des incitations économiques et à encourager des projets pilotes et de recherche.

59. C'est en premier lieu dans le cadre des administrations publiques de l'Union européenne et des États membres et des projets cofinancés par eux que ce changement de perspective devrait être éprouvé, encouragé et, si tout va bien, réalisé.

4.2. Soutenir les PIMS et la technologie sous-jacente pour une protection efficace des données

60. Une bonne réglementation, même si elle est essentielle, n'est pas en soi suffisante. Comme nous l'avons affirmé dans notre avis intitulé «Relever les défis des données massives» ([3]), les entreprises et les autres organisations qui déploient d'importants efforts dans la recherche de solutions innovantes pour l'utilisation des données à caractère personnel devraient faire preuve du même esprit innovant dans la mise en œuvre des principes de protection des données.

([1]) Voir, par exemple, le rapport sur les entrepôts de données personnelles rédigé par l'université de Cambridge à la demande de la Commission européenne: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school

([2]) Communication: Passage au numérique des entreprises européennes — Tirer tous les avantages du marché unique numérique, http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm

([3]) Avis n° 7/2015 du CEPD, cité ci-dessus.

61. La contribution de la technologie au modèle des PIMS est fondamentale. Les PIMS peuvent servir à éprouver les approches basées sur la protection des données dès la conception et les technologies qui les sous-tendent. Les thèmes de recherche pertinents, qui nécessiteront un soutien et des investissements adéquats, sont notamment les suivants: la gestion des identités interopérable et respectueuse de la vie privée; les mécanismes d'autorisation; l'interopérabilité des données; la sécurité des données; ainsi que les mécanismes d'exécution automatique de «contrats» établis entre les personnes et d'autres parties. Ces thèmes seront favorisés par le chiffrement et la cryptographie et alimentés par la disponibilité d'une capacité informatique peu onéreuse. Il est nécessaire que les décideurs politiques, tels que la Commission, apportent un soutien décisif à la recherche fondamentale et à la recherche appliquée dans ces domaines technologiques à ce stade initial de manière à ne pas gaspiller les possibilités actuelles.

62. Afin d'encourager la recherche et le développement et le déploiement vers le marché dans le domaine des PIMS, nous recommandons à la Commission d'envisager des synergies éventuelles avec d'autres domaines de la stratégie pour un marché unique numérique, tels que l'informatique en nuage et l'internet des objets. Ainsi, des projets pilotes pourraient être mis en œuvre pour concevoir et expérimenter les interactions entre les services en nuage et l'internet des objets, d'une part, et les PIMS, d'autre part.

4.3. **Comment le CEPD fera-t-il avancer ce débat?**

63. Le CEPD entend contribuer à encourager les efforts des secteurs privé et public dans le sens décrit ci-dessus. Il continuera à faciliter les discussions, notamment par l'organisation d'événements et d'ateliers, par exemple, pour mettre en évidence, encourager et promouvoir les bonnes pratiques visant à accroître la transparence et le contrôle par les utilisateurs et à étudier les possibilités offertes par les PIMS. Il continuera également à faciliter les travaux du réseau d'ingénierie de la vie privée sur l'internet (IPEN) en tant que centre de connaissances interdisciplinaires pour les ingénieurs et les spécialistes de la vie privée. Dans ce contexte, il continuera à offrir une plateforme aux développeurs et aux promoteurs de PIMS pour leur permettre de communiquer avec des spécialistes d'autres technologies et de la protection des données.

Fait à Marrakech, le 20 octobre 2016.

Giovanni BUTTARELLI

Contrôleur européen de la protection des données