LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Réponse du CEPD à la consultation publique de la Commission sur l'environnement règlementaire concernant les plateformes, les intermédiaires en ligne, les données et l'informatique en nuage ainsi que l'économie collaborative

Le 24 septembre 2015, la Commission européenne a lancé une consultation publique sur les plateformes en ligne (et, séparément, sur le blocage géographique), dans le cadre de sa stratégie pour un marché unique numérique.

L'éventail des questions dans la consultation est très large et suggère une approche plutôt complète de la Commission sur les questions soulevées par les plateformes en ligne. En particulier, la consultation couvre le rôle social et économique des plateformes en ligne; la transparence (par exemple, les résultats de la recherche); les conditions d'utilisation; les notations et les appréciations; l'utilisation des informations par les plateformes; la relation entre les plateformes et leurs fournisseurs; les conditions pour passer d'un service à un autre entre les services comparables proposés par les plateformes; le rôle des intermédiaires en ligne et notamment les manières de lutter contre le contenu illégal sur internet.

Le CEPD, en qualité de conseiller des institutions de l'Union européenne dans le domaine de la protection de la vie privée et des données, exprime depuis longtemps ses préoccupations au sujet de l'utilisation non contrôlée des données à caractère personnel afin de soutenir le fonctionnement des modèles d'entreprise mis en œuvre par les plateformes en ligne (ou liés à celles-ci) (par exemple, avis du CEPD «Meeting the Challenges of Big Data» (Relever les défis de la collecte des données massives), visé dans la note de bas de page 5).

Nous aspirons ainsi à contribuer à cette consultation publique en limitant les commentaires aux parties de la consultation qui se rapportent aux droits à la vie privée et à la protection des données ou qui ont une incidence sur ceux-ci. Pour ce faire, nous avons examiné les questions et choisi celles que nous considérons se rapporter le plus aux droits des personnes à la vie privée et à la protection des données, qui sont protégés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, par l'article 16 du Traité sur le fonctionnement de l'Union européenne et dans la directive 95/46/CE (la «directive sur la protection des données»).

Remarques préliminaires

De manière générale, nous sommes préoccupés par la formulation de nombreuses questions dans la consultation publique qui ne tient pas suffisamment compte du fait que la plupart (voire toutes) les plateformes en ligne prospèrent grâce au traitement des données à caractère personnel. Au contraire, nous constatons, dans tout le texte, des référence à des données à caractère «non personnel», visant à prévenir les points de vue des répondants sur la façon dont les données à caractère personnel devraient être traitées par les plateformes. Nous voyons cela, par exemple, dans la première question en page 16,[1] qui ne mentionne que les données à caractère non personnel alors que la question cruciale concerne le transfert des données à caractère personnel entre les services en ligne. Il y a malheureusement d'autres exemples dans le texte. À nouveau, en page 24, la question indique «*Selon vous, pour*

garantir la libre circulation des données dans l'UE, réglementer l'accès aux données à caractère non personnel, leur transfert et leur utilisation au niveau européen est…». La question passe complètement sous silence le fait que lorsque nous pensons aux plateformes en ligne, les données à caractère personnel sont les informations les plus précieuses qui sont partagées.

En page 26, les questions concernent «*L'accès aux données scientifiques (À CARACTÈRE NON PERSONNEL) et la réutilisation de ces données*» et, à nouveau, les répondants n'ont pas l'opportunité de commenter sur la valeur des données à caractère personnel dans le cadre de la recherche scientifique, ni non plus sur leur valeur commerciale pour les sociétés pharmaceutiques.

Bien que nous reconnaissions que toutes les données stockées et en transit sur les plateformes en ligne ne sont pas des données à caractère personnel, nous ne pouvons pas nous empêcher de noter qu'une grande partie sont à caractère personnel et sont également fort précieuses. Les questions indiquées dans les exemples ont pour conséquence que d'importantes questions sur la protection des données sont complètement laissées de côté. Par ailleurs, les réponses des répondants pourraient être faussées par le fait qu'elles souhaiteraient également mentionner, sans le pouvoir, le traitement des données à caractère personnel, ce qui a pour conséquence que la conclusion que la Commission tirera de cet exercice pourrait être entachée d'erreurs substantielles.

1. ***Définition des plateformes en ligne***

Tout en admettant qu'il est difficile d'adopter une définition globale de plateforme en ligne, eu égard à la diversité des modèles d'entreprise, la consultation publique suggère et cherche à évaluer une définition provisoire.

Nous recommandons d'intégrer dans la définition que les plateformes en ligne impliquent le traitement de données à caractère personnel, une approche finaliste qui souligne le rôle central des données à caractère personnel pour les plateformes.

Si la Commission choisissait de réglementer les plateformes, une telle définition attirerait l'attention du législateur sur les questions de la protection des données, telles que le respect de la vie privée dès la conception («*privacy-by-design*»), la responsabilité, la transparence, le contrôle de l'utilisateur sur ses données (notamment la portabilité des données («*data portability*»), les mesures de sécurité et autres techniques d'atténuation des risques telles que la minimisation des données.

Enfin, nous constatons que la définition exclut les fournisseurs d'accès internet (FAI), en tant que catégorie, de son champ d'application. Nous considérons à cet égard qu'une dérogation générale ne fonctionnerait pas dans la mesure où il se peut qu'un FAI héberge des publicités en ligne sur son site web, opérant ainsi comme une plateforme connectant ses clients à des annonceurs tiers. Cette modalité commerciale était plus évidente dans le passé lorsque de nombreux FAI opéraient également des portails web avec des services gratuits (courriels, prévisions météo, cours des actions) et des publicités en ligne, mais pourrait encore être utilisée de nos jours.[2]

2. ***Transparence pour les utilisateurs des plateformes en ligne : protection du consommateur et du citoyen***

Les plateformes en ligne ont créé des modèles d'entreprise qui (dans la majorité des cas) monétisent le volume croissant de données à caractère personnel qu'elles collectent par le biais de la fourniture de services gratuits. La complexité de ces modèles d'entreprise accroît l'asymétrie de l'information entre les prestataires de services et les clients. Ces derniers considèrent ainsi qu'il est souvent difficile de comprendre complètement et clairement la manière dont les plateformes ont une incidence sur leur vie et leur situation économique.

La transparence constitue un principe fondamental de la loi sur la protection du consommateur et de la loi sur la protection des données (voir, en particulier, l'article 8 de la Charte des droits fondamentaux de l'Union européenne). Dans le cadre de la loi sur la protection du consommateur, la transparence contribuera à assurer l'équilibre et l'équité entre les parties contractantes (le prestataire et les clients). Concernant la loi sur la protection des données, la transparence veille à ce que les personnes concernées maintiennent un contrôle sur leurs données à caractère personnel et la manière dont elles sont utilisées. Conformément à la législation européenne sur la protection des données, les plateformes doivent fournir des informations claires sur l'ensemble des conditions des accords contractuels qu'elles concluent avec les clients. Elles doivent également fournir des informations claires et transparentes sur la collecte des données à caractère personnel et leur traitement. En particulier, cette obligation découle de l'exigence fondamentale de traitement loyal et affecte l'exercice par les personnes physiques de leurs droits d'accès, de rectification et d'opposition.[3]

Nous craignons que le niveau de transparence actuel du traitement de données à caractère personnel soit souvent insuffisant pour assurer un niveau de compréhension adéquat concernant le traitement de leurs données et leur permettre de faire un choix éclairé. La transparence peut contribuer à permettre aux consommateurs, une fois parfaitement informés des mécanismes du traitement des données et de leur monétisation, d'exiger un traitement plus loyal de leurs données ou de passer à des plateformes utilisant leurs données de manière plus loyale et plus efficace.

Du point de vue des politiques, la transparence et la possibilité pour les consommateurs de passer d'une plateforme à une autre sont des caractéristiques fortement souhaitables, susceptibles de conduire à une «course à la première place», encourageant les entreprises à se livrer concurrence en matière de normes de protection des données proposées à leurs clients.

Les plateformes en ligne doivent clairement afficher des politiques en matière de respect de la vie privée qui expliquent les modes de traitement et de protection des données à caractère personnel, les personnes assurant le traitement, les finalités et les périodes de conservation. Ces politiques doivent être rédigées de manière claire et accessible, les clients pouvant être peu disposés à lire de longues politiques de confidentialité.

3. ***Utilisation des données à caractère personnel pour des finalités légitimes et non légitimes.***

Aux termes de l'article 6, point b), de la directive 95/46/CE, les données à caractère personnel doivent être collectées et utilisées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. À cet égard, la préoccupation majeure de la politique est que les plateformes en ligne soient

économiquement motivées à utiliser les données pour des finalités différentes et potentiellement incompatibles avec la finalité originale pour laquelle elles ont été initialement collectées.

Les plateformes en ligne facilitent également un partenariat entre les entreprises qui n'auraient autrement aucun lien. Bien que ceci soit une fonction économique importante, ceci rend difficile d'informer les personnes sur la manière dont leurs données vont être utilisées.

À cet égard, il est important que les plateformes communiquent des informations claires, ex ante, aux clients/utilisateurs sur leur modèle d'entreprise et le rôle joué par les données à caractère personnel dans ce contexte. En cas d'élément inconnu dans le cadre du traitement des données (par exemple, parce que des partenariats commerciaux nouveaux et imprévisibles se forment sur la plateforme), la plateforme doit avoir mis en place une technologie qui informera les utilisateurs en temps utile de tout éventuel nouveau traitement de leurs données *avant* son commencement (par exemple, des mécanismes de notification sur des dispositifs intelligents) pour leur permettre de réagir, s'ils le souhaitent. À cet égard également, le respect de la vie privée dès la conception («*privacy-by-design*») et par défaut («*by-default*») peut aider les entreprises à répondre aux exigences règlementaires à l'avance.

4. Lutter contre le contenu illicite en ligne

À titre de remarque préliminaire, nous notons que les prestataires de services (par exemple, les plateformes en ligne) qui «hébergent» (ou stockent) du contenu fourni par l'un de leurs utilisateurs bénéficient de la dérogation de «simple transport» en vertu de la directive sur le commerce électronique. Cette dérogation, toutefois, est soumise à la condition que le prestataire n'ait pas connaissance de la nature illicite du contenu ou, lorsqu'il en prend connaissance, prenne des mesures pour supprimer ou désactiver l'accès au contenu. Par conséquent, la dérogation ne s'applique pas lorsqu'une violation des règles de protection des données est ou devient apparente pour l'opérateur de la plateforme (par exemple, les informations à caractère personnel sont utilisées à des fins de harcèlement).

La consultation de la Commission insiste à juste titre sur le contenu, comme clé du succès d'une plateforme. Bien que les infrastructures technologiques nécessaires pour opérer une plateforme soient réglementées et, par ailleurs, soumises aux règles générales de concurrence, l'utilisation du contenu est largement soumise aux dynamiques contractuelles entre des parties privées. Il est donc nécessaire de déterminer quand le contenu est légal et, par conséquent, entièrement négociable, et quand il ne l'est pas.

Bien qu'il n'y ait aucun (ou peu) de doute qu'un contenu utilisé en violation d'un droit d'auteur est illégal et que des mécanismes soient mis en place pour surveiller les violations de droit d'auteur sur les plateformes, nous souhaitons encourager les plateformes à mettre en place de manière proactive des mesures de protection tout aussi efficaces (par exemple, des mécanismes de demande de suppression efficaces[4]) lorsque le traitement des données à caractère personnel est contraire aux règles de protection des données. La question de savoir si les opérateurs d'une plateforme doivent activement surveiller le contenu stocké sur leur environnement en ligne est également liée.

5. ***Concurrence entre les plateformes et contraintes pesant sur les utilisateurs souhaitant changer de plateforme***

La capacité des consommateurs à changer de plateforme joue un rôle crucial pour stimuler la concurrence et l'innovation, notamment dans le domaine des garanties relatives à la protection des données, dans l'intérêt des utilisateurs.

À cet égard, nous considérons qu'un obstacle peut être lié au défaut de portabilité des données, qui implique la nécessité de fournir ex novo l'ensemble des données à caractère personnel de la personne concernée, à une nouvelle plateforme. La portabilité des données est un concept que nous avons maintes fois préconisé.[5] Comme indiqué dans le texte de la consultation publique, la portabilité des données est limitée lorsque des données à caractère personnel ne sont pas entièrement accessibles ou lorsqu'elles sont fournies dans un format non exploitable. Si le transfert des données à caractère personnel en ligne n'est pas disponible, est techniquement difficile ou coûteux, les utilisateurs risquent de confirmer les choix initiaux qu'ils ont faits. Le fait d'assurer la portabilité des données constitue, par conséquent, un point clé pour assurer une concurrence loyale entre les plateformes et permet par ailleurs d'assurer un contrôle par l'utilisateur. Les activités de standardisation soutenues par la législation ou l'auto-régulation effective sont essentielles pour soutenir la portabilité des données et doivent être encouragées. Parallèlement, il est essentiel que la mise en œuvre de la portabilité des données ne soit pas entravée ou retardée dans l'attente des résultats d'éventuelles standardisation et auto-régulation futures, lesquelles pourraient prendre un certain temps.

6. ***Internet des choses: fonctionnement, garanties et répartition des responsabilités.***

Presque toutes les plateformes opérant en ligne (par exemple, Amazon, Google, Facebook, Ebay) développent des applications logicielles qui fonctionnent sur les dispositifs intelligents des utilisateurs (par exemple, téléphones, tablettes, télévisions connectées, montres) avec un taux important de pénétration du marché. Par ailleurs, les produits et les objets proposant les services offerts via ces plateformes sont de plus en plus connectés et peuvent assurer une communication directe entre eux et un retour à la plateforme elle-même. Tout ceci contribue à l'internet des objets («IdO»)[6], qui entraîne une capacité importante à «recueillir» des données à caractère personnel à grande échelle, associée à l'augmentation de la puissance informatique («mégadonnées»).[7]

L'interaction entre l'IdO et les mégadonnées peut présenter des risques pour la protection des données entre autres parce qu'elle autorise l'établissement de connections entre des informations qui semblent isolées et sans lien. Par ailleurs, le fait de générer des connaissances à partir de données banales, voire de données considérées comme «anonymes» sera facilité par la prolifération des capteurs, révélant des aspects spécifiques des habitudes, des comportements et des préférences de la personne.[8]

Ce scénario semble même plus complexe, compte tenu du fait que les objets connectés sont généralement fabriqués par divers fabricants qui, à leur tour, peuvent traiter les données de manière autonome ou confier le traitement à des tiers. Par conséquent, le marché peut être (et est effectivement) composé d'une multitude de co-responsables de traitements et de sous-traitants, rendant ainsi la répartition de la responsabilité plus difficile et pouvant poser des obstacles aux personnes concernées à leur capacité d'exercer leurs droits, de contrôler leurs données et d'obtenir des mesures de redressement.

À l'égard de ce qui précède, la réponse réglementaire la plus efficace consiste à appliquer de manière cohérente la directive sur la protection des données, qui identifie le responsable du traitement comme «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel» et lui confère la responsabilité de plusieurs obligations destinées à protéger les droits à la vie privée et à la protection des données des personnes. Par conséquent, avant de procéder à un quelconque traitement de données, les opérateurs de plateformes et autres prestataires de services doivent s'identifier en tant que responsables (ou co-responsables) du traitement de données dans les informations qu'ils fournissent aux utilisateurs dont ils traitent les données. Ils peuvent identifier leur statut de responsables du traitement simplement parce qu'ils traitent des données à caractère personnel à leurs propres fins. Cette approche garantit que les entreprises agissent de manière responsable et conformément à la directive ainsi qu'une répartition efficace de cette responsabilité.

Pour conclure, nous souhaitons rappeler que dans l'arrêt *Google Spain*, la Cour a rejeté la tentative du moteur de recherche de se dégager de sa responsabilité pour violation des obligations de protection des données, en arguant que les données étaient traitées dans les pages web de tiers (à leurs fins).[9]

7. ***Données à caractère personnel et informatique en nuage***

Dans la mesure où la plupart des plateformes en ligne sont basées sur l'informatique en nuage, elles partagent les défis posés par l'informatique en nuage concernant les données à caractère personnel.

Malgré le rôle essentiel joué par les services en nuage pour le déploiement des services en ligne, les consommateurs de l'UE ne semblent toujours pas entièrement avoir confiance dans les services informatiques en nuage, et ce pour plusieurs raisons: des incertitudes sur le lieu d'hébergement effectif des données et le droit applicable, le manque de transparence du niveau de sécurité garanti par le fournisseur de services en nuage et, dernier point et non des moindres, la répartition imprévisible des risques entre le fournisseur de services en nuage et l'utilisateur au titre des violations de données et des responsabilités en découlant.[10]

Par conséquent, l'un des défis majeurs des plateformes en ligne consiste à trouver des solutions respectueuses de la vie privée pour les services informatiques en nuage. En son nom propre et en tant que membre du groupe de travail «Article 29», le CEPD a déjà exprimé son point de vue par le passé[11] et continue de proposer son soutien et ses conseils.

Le fait de promouvoir la recherche et la commercialisation de solutions améliorant la transparence et le contrôle de ses données par l'utilisateur (telles que des «systèmes de gestion des données à caractère personnel») est essentiel pour offrir un niveau de protection plus élevé et renforcer la confiance des utilisateurs.

Les plateformes en nuage peuvent également procéder à des transferts de donnés vers des pays tiers, de sorte qu'il convient d'assurer un niveau de protection des données adéquat comme l'impose la directive. Plus particulièrement, le pays destinataire doit fournir des garanties pour la protection des donnés substantiellement équivalentes à celles garanties au sein de l'Union européenne, comme confirmé par la jurisprudence récente de la Cour de justice.[12]

Conclusion

Notre commentaire le plus important, en réponse à la consultation publique de la Commission, est la nécessité (voire l'urgence, compte tenu de la vitesse de développement des plateformes) de bien définir les questions pertinentes concernant l'utilisation des données à caractère personnel sur les plateformes en ligne. À cet égard, limiter les questions aux donnés à caractère «non personnel» n'aboutit qu'à contourner ou reporter les problèmes, avec pour conséquence de poser les politiques sur des considérations erronées (au mieux incomplètes). Tout instrument futur doit avoir pour postulat le traitement très probable de données à caractère personnel. Une simple référence au GDPR peut être insuffisante pour garantir la sécurité juridique, il convient donc de réfléchir de manière approfondie sur la manière précise d'intégrer les prescriptions en matière de protection des données à la politique européenne relative aux plateformes en ligne.

En termes d'approche réglementaire sur les questions de protection des données, nous considérons que les principes et règles existants en matière de protection des données (sur le caractère nécessaire, la proportionnalité, la minimisation des données, la limitation de finalité et la transparence) complétés par des nouveaux principes (tels que la responsabilité et la protection des données, le respect de la vie privée dès la conception et par défaut), suite à la réforme en matière de protection des données, fourniront une assise solide pour garantir le droit à la vie privée et à la protection des données des personnes. Une transparence accrue, des droits d'accès appropriés, la portabilité des données et des mécanismes de renonciation efficaces peuvent assurer aux utilisateurs plus de contrôle sur leurs données, ainsi que contribuer à des marchés plus efficaces pour les données à caractère personnel, dans l'intérêt des consommateurs et des entreprises. Une pénétration plus importante des principes de protection des donnés dans la législation spécifique du secteur sera également nécessaire.

Une bonne réglementation bien qu'essentielle reste cependant insuffisante. Les sociétés et autres organisations qui consacrent beaucoup d'énergie à trouver des méthodes innovantes pour utiliser les données à caractère personnel doivent avoir le même esprit novateur en vue de la mise en œuvre des principes de protection des données. Il reste nécessaire d'adopter régulièrement des solutions visant à renforcer la protection de la vie privée qui peuvent être concurrentielles sur le marché, une auto-réglementation transparente et efficace du secteur, qui s'appuie sur des principes juridiques et des normes techniques et un plus haut niveau d'éducation et de sensibilisation des utilisateurs et des prestataires.

Fait à Bruxelles, le 15 décembre 2015

[1] La question indique «*Faut-il prévoir une disposition obligatoire en vertu de laquelle les données à caractère non personnel pourraient être aisément extraites et déplacées entre services en ligne comparables ?*»

[2] Voir, par exemple, le site web tiscali.it.

[3] Voir arrêt de la Cour de justice du 1er octobre 2015, dans l'affaire C-201/14, *Smaranda Bara e.a. contre Președintele Casei Naționale de Asigurări de Sănătate et autres*, points 33 et 34.

[4] Voir l'arrêt de la Cour de justice du 13 mai 2014, dans l'affaire C-131/12, *Google Spain contre AEPD*, où la Cour a considéré que le moteur de recherche doit effacer les informations qui ne sont plus pertinentes ou sont excessives au regard des finalités du traitement (point 94).

[5] Vois avis du CEPD 7/2015, «*Meeting the Challenges of Big Data*», disponible sur https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf; Avis 4/2015, «*Vers une nouvelle éthique numérique:* d*onnées, dignité et technologie*», disponible sur https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_FR.pdf et avis du 26 mars 2014, «*Vie privée et compétitivité à l'ère de la collecte de données massives*», disponible sur https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_FR.pdf.

[6] Voir avis du groupe de travail «Article 29» sur l'internet des objets («Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets»): «*La notion d'internet des objets (IdO) désigne une infrastructure dans laquelle des milliards de capteurs intégrés dans des dispositifs courants, quotidiens – des «objets» en tant que tels ou des choses liées à d'autres objets ou personnes – sont conçus pour enregistrer, traiter, conserver et transférer des données et, comme ils sont associés à des identifiants uniques, interagir avec d'autres dispositifs ou systèmes par un réseau.*»

[7] En particulier, à l'égard de ce qui précède, sont d'une particulière pertinence les appareils informatiques vestimentaires (par exemple, des montres, des lunettes, des bracelets, des lecteurs de musique, des t-shirts) qui intègrent de multiples capteurs interconnectés capables d'enregistrer des informations en matière de comportement, de fonctions corporelles et de style de vie.

[8] Voir avis du groupe de travail «Article 29» sur l'internet des objets, p. 8. Les plateformes, les fournisseurs d'applications et les dispositifs intelligents peuvent réunir des données suffisantes pour construire des statistiques de groupe (profils à l'échelle de la société ou régionale) sur tout paramètre des utilisateurs pour eux-mêmes ou pour leurs partenaires (par exemple des sociétés ou des gouvernements). Ceci peut inciter les plateformes, les prestataires de services et les autres acteurs du marché ayant accès aux données, à passer d'un soutien d'auto-évaluation des utilisateurs (par exemple la possibilité généralement gratuite, proposée aux utilisateurs, de mesurer leurs paramètres de santé) à un coaching intelligent volontaire (en permettant par exemple aux utilisateurs de suivre un style de vie sain avec des conseils de tiers) puis à une phase où ils peuvent se fier à des spécialistes du comportement pour «passer» le «bon» message aux utilisateurs au «bon» moment pour influencer le comportement de ces derniers.

[9] Voir arrêt de la Cour de justice du 13 mai 2014, dans l'affaire C-131/12, *Google Spain contre AEPD*, points 22 et 28 et suivants.

[10] Voir avis du CEPD du 26 novembre 2012 sur la communication de la Commission intitulée «*Exploiter le potentiel de l'informatique en nuage en Europe*», disponible à l'adresse https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_FR.pdf

[11] Voir avis du groupe de travail «Article 29» du 22 septembre 2015 sur le code de conduite relatif à l'informatique en nuage («Code of Conduct on Cloud Computing»), disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf et avis du 1er juillet 2012 sur l'informatique en nuage, disponible surhttp://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf

[12] Voir arrêt de la Cour de justice du 6 octobre 2015, dans l'affaire C-362/14, *Maximilian Schrems contre Data Protection Commissioner*, points 73 et 74.