CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Résumé de l'avis du Contrôleur européen de la protection des données relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe»

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

(2013/C 253/03)

I. **Introduction**

I.1. *Objectif de l'avis*

1. Compte tenu de l'importance de l'informatique en nuage dans notre société de l'information en pleine évolution, et du débat politique actuel à ce sujet au sein de l'Union européenne, le CEPD a décidé de publier le présent avis de sa propre initiative.

2. Cet avis est une réponse à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», du 27 septembre 2012 (ci-après la «communication») ([1]), qui établit les actions et mesures politiques clés qui doivent être prises pour accélérer l'utilisation des services d'informatique en nuage en Europe. Le CEPD a été consulté de manière informelle avant l'adoption de la communication et a formulé des commentaires informels. Il se félicite que certains de ses commentaires aient été pris en considération dans la communication.

3. Cependant, compte tenu de l'étendue et de l'importance du débat en cours sur la relation entre l'informatique en nuage et le cadre juridique de la protection des données, le présent avis ne se limite pas aux sujets traités dans la communication.

4. L'avis concerne particulièrement les difficultés suscitées par l'informatique en nuage pour la protection des données, et la manière dont la proposition de règlement sur la protection des données (ci-après le «règlement proposé») ([2]) pourrait résoudre ces difficultés. Il aborde également certains domaines d'action complémentaires identifiés dans la communication.

I.2. *Contexte*

5. Dans le contexte du débat de politique générale en cours dans l'Union européenne au sujet de l'informatique en nuage, les activités et documents suivants revêtent une importance particulière:

— suite à sa communication de 2010 intitulée «Une stratégie numérique pour l'Europe» ([3]), la Commission a lancé une consultation publique sur l'informatique en nuage en Europe, qui s'est déroulée du 16 mai au 31 août 2011, et dont les résultats ont été publiés le 5 décembre 2011 ([4]);

— le 1er juillet 2012, le groupe de travail «Article 29» ([5]) a adopté un avis sur l'informatique en nuage (ci-après l'«avis du groupe de travail "Article 29"») ([6]), dans lequel il analyse l'application des règles de protection des données actuellement prévues par la directive 95/46/CE aux fournisseurs de services d'informatique en nuage opérant dans l'Espace économique européen (EEE) et à leurs clients ([7]);

— le 26 octobre 2012, les commissaires à la protection des données et à la vie privée ont adopté une résolution sur l'informatique en nuage lors de leur 34e conférence internationale ([8]).

([1]) COM(2012) 529 final.
([2]) COM(2012) 11 final.
([3]) COM(2010) 245 final.
([4]) http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
([5]) Le groupe de travail «Article 29» est un organe consultatif établi par l'article 29 de la directive 95/46/CE. Il est composé de représentants des autorités nationales de contrôle et du CEPD, et d'un représentant de la Commission.
([6]) Avis 05/2012 du groupe de travail «Article 29» sur l'informatique en nuage, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf
([7]) De plus, au niveau national, les autorités de protection des données de plusieurs États membres ont publié leurs propres recommandations sur l'informatique en nuage; c'est le cas notamment de l'Italie, de la Suède, du Danemark, de l'Allemagne, de la France et du Royaume-Uni.
([8]) Résolution relative à l'informatique en nuage adoptée lors de la 34e conférence internationale des commissaires à la protection des données et à la vie privée, le 26 octobre 2012 (Uruguay).

I.3. *Communication sur l'informatique en nuage*

6. Le CEPD se félicite de la communication. Celle-ci identifie trois mesures spécifiques essentielles devant être prises au niveau de l'Union européenne pour accompagner et promouvoir l'utilisation de l'informatique en nuage en Europe:

— action essentielle 1: mettre de l'ordre dans le chaos des normes;

— action essentielle 2: des clauses et des conditions contractuelles sûres et équitables;

— action essentielle 3: mettre en place un partenariat européen en faveur de l'informatique en nuage pour faire du secteur public un moteur d'innovation et de croissance.

7. Des mesures politiques supplémentaires sont également prévues pour accroître l'utilisation de l'informatique en nuage en soutenant la recherche et le développement ou en sensibilisant l'opinion publique, et pour répondre à certaines questions clés liées aux services en nuage (notamment la protection des données, l'accès aux données par les autorités répressives, la sécurité, la responsabilité des prestataires de services intermédiaires) par un dialogue international plus intense.

8. Dans la communication, la protection des données est qualifiée d'élément essentiel pour assurer le succès du déploiement de l'informatique en nuage en Europe. La communication souligne ([1]) que le règlement proposé répond à de nombreuses questions soulevées par les fournisseurs de services en nuage et par leurs clients ([2]).

I.4. *Messages principaux et structure de l'avis*

9. Le présent avis poursuit trois objectifs.

10. Le premier objectif est d'insister sur la pertinence de la protection de la vie privée et des données dans les discussions actuellement menées sur l'informatique en nuage. Plus précisément, l'avis souligne que le niveau de protection des données dans un environnement d'informatique en nuage ne doit pas être inférieur à celui qui est requis dans tout autre contexte de traitement de données. Les pratiques d'informatique en nuage ne peuvent être développées et légalement appliquées que si elles garantissent ce niveau de protection des données (voir le chapitre III.3). L'avis tient compte des recommandations formulées dans l'avis du groupe de travail «Article 29».

11. Le deuxième objectif vise à approfondir l'analyse des principaux défis posés par l'informatique en nuage en matière de protection des données dans le cadre du règlement proposé, et concerne notamment la difficulté d'établir sans ambigüité les responsabilités des différents acteurs et les notions de responsable du traitement et de sous-traitant. L'avis (principalement son chapitre IV) analyse la manière dont le règlement proposé pourrait, ainsi que cela est actuellement suggéré ([3]), contribuer à garantir un niveau élevé de protection des données dans les services d'informatique en nuage. Il s'inspire de l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données (ci-après «l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données») ([4]) et le complète en examinant en particulier l'environnement de l'informatique en nuage. Le CEPD souligne que son avis sur le paquet de mesures pour une réforme de la protection des données est tout à fait pertinent en matière de services d'informatique en nuage et doit être considéré comme une base pour le présent avis. De plus, certaines des questions soulevées dans ledit avis [comme l'analyse des nouvelles dispositions relatives aux droits des personnes concernées ([5])] sont suffisamment claires pour ne pas être développées plus avant dans le présent avis.

12. Le troisième objectif est d'identifier des domaines dans lesquels de nouvelles mesures sont nécessaires au niveau de l'Union européenne sur le plan de la protection des données et de la vie privée, compte tenu de la stratégie en matière d'informatique en nuage proposée par la Commission dans sa communication. Ces nouvelles mesures pourraient comprendre, notamment, de nouvelles recommandations, des efforts d'uniformisation, la réalisation de nouvelles évaluations des risques pour des secteurs spécifiques (tels que le secteur public), le développement de clauses et conditions contractuelles standard, l'ouverture d'un dialogue international sur les questions liées à l'informatique en nuage et sur la mise en œuvre de moyens permettant d'assurer une véritable coopération internationale (aspect développé dans le chapitre V).

([1]) Voir page 9 de la communication, «Actions relevant de la stratégie numérique et visant à susciter la confiance dans le numérique».

([2]) Le terme «clients de services en nuage» est généralement utilisé dans cet avis pour désigner deux types de clients: les clients agissant en qualité d'entreprises et les clients agissant en qualité d'usagers particuliers finaux.

([3]) Il convient de tenir compte du fait que le règlement proposé est actuellement discuté par le Conseil et le Parlement européen dans le cadre de la procédure législative ordinaire.

([4]) Cet avis est disponible à l'adresse suivante: http://www.edps.europa.eu

([5]) Voir l'avis du CEPD, en particulier les paragraphes 140 à 158.

13. L'avis est structuré comme suit: la section II fournit un aperçu des principales caractéristiques de l'informatique en nuage et les difficultés qui en découlent pour la protection des données. La section III passe en revue les éléments les plus pertinents du cadre juridique de l'Union européenne en vigueur et du règlement proposé. La section IV analyse la manière dont le règlement proposé contribuerait à résoudre les problèmes de protection des données liés à l'utilisation de services d'informatique en nuage. La section V analyse les suggestions de la Commission pour de nouvelles mesures politiques et identifie les domaines dans lesquels des travaux restent à accomplir. La section VI présente les conclusions.

14. Si de nombreuses réflexions formulées dans le présent avis s'appliquent à tous les environnements dans lesquels l'informatique en nuage est utilisée, le présent avis n'aborde pas le thème de l'utilisation des services d'informatique en nuage par les institutions et organes de l'Union européenne qui font l'objet du contrôle du CEPD en vertu du règlement (CE) n° 45/2001. Le CEPD publiera des lignes directrices distinctes à l'intention de ces institutions et organes sur ce sujet.

VI. **Conclusions**

121. Ainsi qu'indiqué dans la communication, l'informatique en nuage ouvre bon nombre de nouvelles perspectives aux entreprises, aux clients et au secteur public en matière de gestion des données via des ressources informatiques externes et distantes. Parallèlement, elle présente de nombreuses difficultés, notamment en ce qui concerne le niveau adéquat de protection des données proposé pour les données traitées dans ce contexte.

122. L'utilisation de services d'informatique en nuage comporte un risque majeur: celui de voir la responsabilité des fournisseurs de services en nuage s'évaporer lorsqu'ils procèdent à des traitements de données, si les critères d'applicabilité de la législation de l'Union européenne relative à la protection des données ne sont pas suffisamment clairs et si le rôle et la responsabilité des fournisseurs de ces services sont définis ou compris de manière trop restrictive, ou si ces critères ne sont pas mis en œuvre de manière efficace. Le CEPD souligne que l'utilisation de ces services ne saurait justifier un abaissement des normes de protection des données par comparaison avec celles qui sont applicables aux traitements de données conventionnels.

123. À cet égard, le règlement sur la protection des données proposé, tel qu'il a été présenté, apporterait de nombreuses précisions et des outils qui contribueraient à garantir un niveau satisfaisant de protection de la part des fournisseurs de services en nuage proposant leurs services à des clients situés en Europe. En particulier:

— l'article 3 préciserait le champ d'application territorial des règles de protection des données de l'Union européenne et élargit sa portée afin que les services d'informatique en nuage soient couverts;

— l'article 4, paragraphe 5, introduirait un nouvel élément de contrôle, à savoir des «conditions». Cela serait conforme à la tendance actuelle voulant que, compte tenu de la complexité informatique et technique sous-jacente à la fourniture de services d'informatique en nuage, il est nécessaire d'élargir les conditions dans lesquelles un fournisseur de services en nuage peut être considéré comme responsable du traitement. Cela reflèterait mieux le niveau réel d'influence sur les traitements;

— le règlement proposé accroîtrait la responsabilité des responsables du traitement et des sous-traitants en introduisant des obligations spécifiques telles que la protection des données dès la conception et par défaut (article 23), la notification de violation des données à caractère personnel (articles 31 et 32) et l'analyse d'impact relative à la protection des données (article 33). En outre, il imposerait aux responsables du traitement et aux sous-traitants de mettre en œuvre des mécanismes visant à démontrer l'efficacité des mesures prises en faveur de la protection des données (article 22);

— les articles 42 et 43 du règlement proposé permettraient une utilisation plus souple des mécanismes internationaux de transfert de données, afin d'aider les clients et les fournisseurs de services en nuage à mettre en œuvre des garanties de protection des données appropriées pour les transferts de données à caractère personnel vers des centres de traitement ou des serveurs situés dans des pays tiers;

— les articles 30, 31 et 32 du règlement proposé clarifieraient les obligations des responsables du traitement et des sous-traitants concernant la sécurité des traitements et les exigences d'information en cas de violation des données, ce qui créerait la base d'une approche globale et coopérative de la gestion de la sécurité par les différents acteurs de l'environnement en nuage;

— les articles 55 à 63 du règlement proposé renforceraient la coopération entre les autorités de contrôle et leur contrôle coordonné sur les traitements transfrontaliers, ce qui est essentiel dans un environnement tel que celui de l'informatique en nuage.

124. Le CEPD suggère néanmoins, après avoir pris en compte les spécificités des services d'informatique en nuage, que des précisions soient introduites dans le règlement proposé en ce qui concerne les aspects suivants:

— s'agissant du champ d'application territorial du règlement proposé, il convient de modifier l'article 3, paragraphe 2, point a), et de le libeller comme suit: «l'offre de biens ou de services *impliquant le traitement de données à caractère personnel de ces* personnes concernées dans l'Union», ou d'ajouter un nouveau considérant précisant que le traitement de données à caractère personnel de personnes concernées dans l'Union européenne par des responsables du traitement situés en dehors de l'Union européenne proposant des services à des personnes morales de l'Union européenne relève également du champ d'application territorial du règlement proposé;

— ajouter une définition claire de la notion de «transfert», ainsi que proposé dans l'avis sur le paquet de mesures pour une réforme de la protection des données;

— ajouter des dispositions spécifiques visant à clarifier les conditions dans lesquelles l'accès aux données stockées dans un espace de services en nuage par des autorités répressives situées dans des pays n'appartenant pas à l'EEE peut être autorisé. Cette disposition peut également prévoir, pour le destinataire de la demande, l'obligation d'informer et de consulter l'autorité de contrôle compétente dans l'Union européenne dans des cas spécifiques.

125. Le CEPD souligne par ailleurs que la Commission et/ou les autorités de contrôle devront proposer des orientations supplémentaires (en particulier via le futur comité européen de la protection des données) sur les aspects suivants:

— clarifier les mécanismes qui doivent être créés pour vérifier l'efficacité des mesures de protection des données dans la pratique;

— aider les sous-traitants à utiliser les RCE et à se conformer aux exigences en vigueur;

— préciser les meilleures pratiques sur des questions telles que la responsabilité du responsable du traitement/sous-traitant, la conservation appropriée des données dans l'environnement en nuage, la portabilité des données et l'exercice de leurs droits par les personnes concernées.

126. Le CEPD reconnaît que des codes de conduites rédigés par le secteur et approuvées par les autorités de contrôle compétentes pourraient être utiles pour améliorer la conformité et favoriser la confiance parmi les différents acteurs.

127. Le CEPD soutient l'élaboration par la Commission, en consultation avec les autorités de contrôle, de clauses contractuelles types relatives à la fourniture de services d'informatique en nuage conformes aux exigences de protection des données. Il s'agirait en particulier:

— d'élaborer des clauses et conditions contractuelles types qui figureront dans les clauses commerciales des offres de services d'informatique en nuage;

— d'élaborer des clauses et exigences communes pour la passation de marchés pour le secteur public, qui tiennent compte du degré de sensibilité des données traitées;

— de continuer d'adapter les mécanismes internationaux de transfert de données à l'environnement de l'informatique en nuage, notamment en mettant à jour les clauses contractuelles types existantes et en proposant des clauses contractuelles types spécifiques au transfert de données de sous-traitants situés dans l'Union européenne vers des sous-traitants situés en dehors de l'Union européenne.

128. Le CEPD souligne qu'il convient de tenir dûment compte des exigences de protection des données dans le cadre de l'élaboration de programmes de normes et de certification, notamment:

— de leur appliquer les principes de protection dès la conception et par défaut;

— d'y intégrer des exigences de protection des données telles que la limitation des finalités et du stockage;

— d'y intégrer l'obligation faite aux fournisseurs d'informer leurs clients de manière suffisante pour que ces derniers puissent correctement évaluer les risques et les mesures de sécurité mises en œuvre, et de les alerter de tout incident de sécurité.

129. Enfin, le CEPD souligne la nécessité de résoudre les difficultés posées par l'informatique en nuage à l'échelle internationale. Il encourage la Commission à entamer un dialogue international sur les problèmes soulevés par l'informatique en nuage, y compris sur les questions liées à la compétence juridictionnelle et à l'accès aux données par les autorités répressives, et indique qu'un grand nombre de ces questions pourraient être réglées par différents accords internationaux ou bilatéraux, tels que des accords d'assistance mutuelle et des accords commerciaux. Il conviendrait d'élaborer des normes mondiales à l'échelle internationale pour établir des conditions et principes de base relatifs à l'accès aux données par les autorités répressives. Le CEPD soutient enfin la création, par les autorités de contrôle, de mécanismes de coopération internationale efficaces, en particulier en ce qui concerne les questions propres à l'informatique en nuage.

Fait à Bruxelles, le 16 novembre 2012.

Peter HUSTINX

Contrôleur européen de la protection des données