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 CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

vu la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et en particulier son article 41[2],

A ADOPTÉ LE PRÉSENT AVIS:

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»)[3], 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.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM (2012) 529 final.

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»)[4] 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» [5] , 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[6];

- le 1er juillet 2012, le groupe de travail «Article 29»[7] a adopté un avis sur l'informatique en nuage (ci-après l'«avis du groupe de travail "Article 29"»)[8], 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[9];

- 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[10].

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:

---

[4] COM (2012) 11 final.
[5] COM (2010) 245 final.
[6] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf.
[7] 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.
[8] 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.
[9] 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.
[10] 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).

- 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 [11] que le règlement proposé répond à de nombreuses questions soulevées par les fournisseurs de services en nuage et par leurs clients[12].

1.4. 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, dans sa formulation actuelle[13], 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») [14] et le complète en examinant en

[11] Voir page 9 de la communication, «Actions relevant de la stratégie numérique et visant à susciter la confiance dans le numérique».
[12] 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.
[13] 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.
[14] Cet avis est disponible à l'adresse suivante: www.edps.europa.eu.

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[15]) 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).

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 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.

II. L'ENVIRONNEMENT DE L'INFORMATIQUE EN NUAGE

II.1. Définitions

15. L'informatique en nuage évolue et comprend une large gamme de solutions technologiques et de pratiques commerciales. Le terme revêt différentes significations dans des contextes variés. La définition la plus couramment utilisée est celle du *US National Institute of Standards and Technology* (NIST)[16], qui indique que l'informatique en nuage est un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques

[15] Voir l'avis du CEPD, en particulier les paragraphes 140 à 158.
[16] US NIST SP 800-145, The NIST Definition of Cloud Computing (Définition de l'informatique en nuage du NIST), septembre 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

configurables mutualisées (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort de gestion ou d'intervention d'un prestataire de services. Le document du NIST définit trois modèles de services [*SaaS: Software as a Service* (logiciel en tant que service), *PaaS: Platform as a Service* (plateforme en tant que service), et *IaaS: Infrastructure as a Service* (infrastructure en tant que service)] et quatre modèles de déploiement: les environnements en nuage publics, privés, communautaires et hybrides. Dans le présent avis, les termes et acronymes utilisés ont le sens qui leur est donné par le NIST.

II.2. Impact de l'informatique en nuage sur les entreprises et les consommateurs

16. L'un des principaux impacts anticipés de l'informatique en nuage est la réduction des coûts des services informatiques, obtenue grâce à des économies d'échelle et à une utilisation plus efficace des infrastructures d'information et de communication. Une répartition dynamique et une réutilisation des ressources dans des pools plus importants permettront de réduire les dépenses d'infrastructure informatique et de rationaliser les opérations.

17. Si des économies sont attendues de tous les modèles de déploiement d'informatique en nuage, les services publics (et, dans une moindre mesure, communautaires) d'informatique en nuage pourraient également réduire les coûts supportés par les clients car ceux-ci ne paieraient que les services effectivement utilisés, en fonction du temps d'utilisation, de l'espace de stockage et des autres ressources nécessaires, ce qui supprimerait la quasi-totalité des coûts fixes liés aux services informatiques. Ce modèle de paiement à l'utilisation permettrait un achat de services plus dynamique répondant aux besoins réels des entreprises. De plus, il permettrait aux petites organisations, telles que les PME, d'accéder à des services de meilleure qualité, que celles-ci n'auraient pas les moyens de se procurer dans le cadre des modèles traditionnels en raison des coûts d'entrée élevés des infrastructures, des licences et de l'installation, et en raison de l'absence d'évolutivité[17]. Ces nouvelles possibilités devraient ouvrir la voie à des start-up innovantes offrant un vaste éventail de nouveaux services.

18. Les applications de tiers sur les services de médias sociaux peuvent être considérées comme un exemple de ces nouveaux outils dans un environnement SaaS (*Software as a Service*). Toute personne disposant de connaissances techniques suffisantes, d'un équipement informatique de base et d'un accès à l'internet peut développer et proposer des applications opérant dans l'environnement fourni par le service de médias sociaux. La capacité multi-utilisateurs intrinsèque de l'informatique en nuage en fait un modèle idéal pour de nouvelles applications de réseaux sociaux.

[17] Les magasins en ligne hébergés constituent un exemple du potentiel existant de modèles plus dynamiques et évolutifs.

19. L'informatique mobile et l'informatique en nuage se complètent et se renforcent mutuellement et constituent la base de l'intelligence ambiante[18] et de l'internet des objets. Les dispositifs mobiles offrent un accès universel aux services d'informatique en nuage et les services d'informatique en nuage offrent un accès mobile à des services très spécialisés et à des bases de données de très grande envergure, au-delà des limites physiques des dispositifs mobiles. L'accès à l'informatique en nuage offre de nouvelles opportunités dans le domaine de l'utilisation des smart phones et des tablettes informatiques, dans la mesure où les navigateurs et les applications peuvent être utilisés comme interfaces des services d'informatique en nuage.

II.3. Future consolidation du marché de l'informatique en nuage

20. Alors que le marché des services d'informatique en nuage est encore dans une phase de forte croissance, à long terme, il devrait se consolider de la même manière que les autres secteurs et pourrait évoluer vers l'établissement d'un nombre de fournisseurs limité offrant leurs services à un grand nombre de consommateurs.

21. Cette concentration pourrait renforcer le déséquilibre qui existe déjà sur le marché des services d'informatique en nuage entre les prestataires de services et la majorité des utilisateurs de ces services. En effet, si les gouvernements et les grandes entreprises peuvent disposer de nuages privés établis selon leurs propres exigences ou négocier des accords de services avec les prestataires de services en nuage sur un pied d'égalité, les petites et moyennes organisations des secteurs public et privé et les consommateurs individuels devront accepter les clauses et conditions imposées par les prestataires de services pour les services en nuage publics. Les prestataires de services pourraient exploiter cette asymétrie pour fixer des conditions de services défavorables aux clients, qui limiteraient les obligations et responsabilités des prestataires, restreindraient les droits des clients et conféreraient aux prestataires des privilèges et des pouvoirs importants, voire la possibilité de modifier de manière unilatérale les clauses et conditions de service, au détriment des clients des services en nuage.

II.4. Importance de la protection des données dans un environnement d'informatique en nuage

22. L'informatique en nuage permet de traiter un grand volume de données[19] et de créer de nouveaux services et de nouvelles applications pour monétiser ces données; il peut s'agir d'applications de médias sociaux ou de services d'informatique en nuage

---

[18] L'intelligence ambiante et l'informatique omniprésente sont des expressions qui renvoient à une vision selon laquelle les êtres humains seront entourés d'interfaces intelligentes présentes partout, parfois intégrées à des objets de la vie quotidienne, connectées partout et à tout moment, permettant aux personnes et aux dispositifs d'interagir les uns avec les autres ainsi qu'avec l'environnement [A social and technological view of Ambient Intelligence in Everyday Life (Une approche sociale et technologique de l'intelligence ambiante dans la vie quotidienne), EC IPTS, 2003].

[19] «Grand volume de données» est l'expression utilisée pour décrire un volume massif de données structurées et non structurées qui est si important qu'il peut difficilement être traité par des bases de données et des techniques logicielles traditionnelles. Voir «Big data: The next frontier for innovation, competition, and productivity», mai 2011, McKinsey Global Institute, http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation.

fournis via des dispositifs mobiles. Dans la mesure où ces volumes de données importants contiennent des données à caractère personnel, ils engendrent des risques spécifiques pour la protection de la vie privée et des données. Dès lors, une surveillance et des garanties appropriées doivent être mises en œuvre.

23. L'informatique en nuage soulève un certain nombre de problèmes liés à la protection de la vie privée et des données à caractère personnel, qui doivent être résolus de manière adéquate dès la conception et le lancement des services. La majorité de ces problèmes sont pertinents, quel que soit le modèle de service ou de déploiement concerné. De plus, certains modèles d'informatique en nuage font appel à des sous-traitants, des accès à distance et des infrastructures informatiques multi-utilisateurs. Ainsi, les risques pour la protection des données liés à ces caractéristiques doivent également être pris en compte.

24. Premièrement, dans les environnements d'informatique en nuage, l'emplacement physique des données n'est généralement pas connu du client et n'est, en principe, pas pertinent pour le service lui-même. Sur le plan des services, il est plus important de se pencher sur la question de l'endroit d'où il est possible d'accéder aux données. Cependant, le lieu d'hébergement des données demeure un point pertinent en ce qui concerne l'application de la législation nationale. Cela sera d'autant plus évident si les autorités (nationales) doivent accéder de manière physique aux données.

25. Deuxièmement, du fait de l'asymétrie contractuelle décrite plus haut entre les prestataires de services et leurs clients, il pourra s'avérer très difficile, voire impossible, pour les clients des services en nuage agissant en tant que responsables du traitement des données de se conformer aux exigences applicables en matière de traitement des données à caractère personnel dans le cadre d'un environnement d'informatique en nuage. Cette asymétrie pourrait également conduire à une répartition inadéquate des responsabilités liées au respect de la législation sur la protection des données. Si la qualification du responsable du traitement et du sous-traitant ne reflète pas correctement le niveau de contrôle sur les moyens de traitement, la responsabilité de la protection des données à caractère personnel risque d'être dispersée avec l'utilisation de l'informatique en nuage.

26. Troisièmement, dans le cadre de l'informatique en nuage, les différents intervenants coopèrent généralement le long d'une chaîne de valeurs pour fournir le service au client. Cela soulève également des questions complexes quant à la répartition des responsabilités, notamment en ce qui concerne les exigences liées au traitement des données à caractère personnel, telles que la sécurité des données, l'accès aux données et l'audit. Ces problèmes peuvent être considérablement aggravés lorsque de nouveaux prestataires peuvent être ajoutés de manière dynamique au service en cours de fonctionnement[20].

27. Quatrièmement, avec l'informatique en nuage, les transferts de données à caractère personnel augmentent considérablement sur les réseaux; ces transferts impliquent de nombreuses parties différentes et traversent les frontières, tant à l'intérieur qu'à l'extérieur de l'Union européenne. En fonction du type de service proposé, les

[20] Les difficultés de répartition des responsabilités entre les différents acteurs, tels que les responsables du traitement et les sous-traitants (mentionnées aux points 25 et 26), seront abordées plus en détail dans la section IV.2.

données peuvent être reproduites dans de nombreux endroits pour être plus accessibles en tous lieux dans le monde. Lorsque des données à caractère personnel sont traitées dans le cadre de ces services, les responsables du traitement et les sous-traitants doivent assurer la conformité de ces transferts avec les règles relatives à la protection des données.

28. Enfin, il ne faut pas négliger le fait que l'informatique en nuage évolue encore. Les caractéristiques technologiques et le développement de nouvelles tendances dans le domaine de l'informatique en nuage poseront de nouveaux problèmes en matière de protection des données. Il est impossible de prédire exactement la manière dont l'informatique en nuage évoluera. Le présent avis repose donc sur les tendances qui peuvent être observées actuellement dans ce domaine[21].

III. APERÇU DU CADRE JURIDIQUE DE L'UNION EUROPÉENNE EN MATIÈRE DE PROTECTION DES DONNÉES APPLICABLE À L'INFORMATIQUE EN NUAGE

III.1. Le cadre juridique actuel de l'UE

29. Les traitements de données réalisés dans un environnement d'informatique en nuage qui relève des critères du champ d'application territorial de la législation de l'Union européenne sur la protection des données[22] doivent respecter le cadre de protection des données de l'UE actuellement fixé par la directive 95/46/CE. L'avis du groupe de travail «Article 29» fournit des indications sur l'application à l'informatique en nuage des principes et des règles établis par la directive générale sur la protection des données[23].

30. Dans la mesure où tout traitement réalisé dans un environnement d'informatique en nuage implique le traitement de données à caractère personnel en rapport avec la prestation de services de communications électroniques accessibles au public au sein de réseaux publics de communications (opérateurs télécoms), ce traitement doit également être conforme à la directive 2002/58/CE «Vie privée et communications électroniques»[24].

---

[21] Certaines de ces questions sont soulignées dans le protocole d'accord Sopot adopté le 2 avril 2012 par le Groupe de travail international de Berlin sur la protection des données dans les télécommunications, http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083.

[22] Les traitements relèvent du champ d'application de la protection des données de l'Union européenne lorsqu'ils impliquent le traitement automatisé de données à caractère personnel et lorsque ce traitement est réalisé dans le cadre des activités d'un établissement du responsable du traitement situé dans l'Union européenne ou lorsque ce traitement est réalisé hors de l'Union européenne avec des équipements situés dans l'Union européenne, conformément aux articles 3 et 4 de la directive 95/46/CE.

[23] Voir la note de bas de page n° 8.

[24] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, JO L 337 du 18.12.2009, p. 11.

31. La directive 2000/31/CE sur le commerce électronique [25] définit les règles applicables à certains aspects des services de la société de l'information. Les services d'informatique en nuage entrent généralement dans la définition des services de la société de l'information. La directive sur le commerce électronique établit un régime de responsabilité limité pour les prestataires de services intermédiaires en ce qui concerne la légalité des contenus transmis ou hébergés à la demande des destinataires du service. L'article 1, paragraphe 5, point b), de la directive sur le commerce électronique précise que ses dispositions sont sans préjudice des règles établies par la directive 95/46/CE en matière de protection des données. Conformément à la directive 95/46/CE, le traitement des données à caractère personnel par des prestataires de services par l'internet relève du champ d'application de la législation sur la protection des données. Le niveau de responsabilité de ces prestataires peut varier selon qu'ils agissent en tant que sous-traitants ou en tant que responsables du traitement. Dans le premier cas, leur responsabilité vise à garantir la confidentialité et la sécurité des données, tandis que dans le deuxième cas, les prestataires ont l'entière responsabilité de garantir la conformité aux exigences en matière de protection des données. Dans de nombreux cas, les intermédiaires en ligne qui fournissent des services à valeur ajoutée (par exemple, les réseaux sociaux et les services fondés sur le nuage) peuvent être considérés comme responsables du traitement des données[26] (voir analyse détaillée, section IV.2 ci-après).

III.2. La proposition de règlement relatif à la protection des données

32. La proposition de règlement relatif à la protection des données adoptée par la Commission le 25 janvier 2012 vise à fournir un ensemble unique de règles applicables au sein de l'Union européenne pour le traitement des données à caractère personnel par les sociétés privées et par le secteur public[27]. Dans le cadre de la réforme, l'étendue territoriale de la législation de l'Union européenne sur la protection des données est redéfinie. Le règlement proposé repose sur les principes généraux établis par la directive 95/46/CE, qu'il vise à mettre à jour et adapter à l'environnement numérique. Il vise également à simplifier certaines procédures administratives (telles que les notifications préalables) et à renforcer les droits des individus, la responsabilité des responsables du traitement et des sous-traitants de

---

[25] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1.

[26] Voir en particulier le considérant 47 de la directive 95/46/CE: «considérant que, lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service» (italique ajouté). Voir également, par exemple, l'avis 5/2009 du groupe de travail «Article 29» sur les réseaux sociaux en ligne, 12 juin 2009, page 5: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_fr.pdf.

[27] Selon l'article 2, paragraphe 2, point e), de la proposition de règlement, le règlement proposé ne sera pas applicable aux traitements de données à caractère personnel effectués 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.

données à caractère personnel, ainsi que les prérogatives des autorités nationales de contrôle.

33. Le règlement proposé introduit un certain nombre de nouvelles obligations pour les responsables du traitement, telles que la «protection des données dès la conception» et la «protection des données par défaut», la responsabilité, l'analyse d'impact relative à la protection des données, les notifications de violation des données à caractère personnel, ainsi que le droit à l'oubli et le droit à la portabilité des données. Puisque ces nouvelles propositions conservent l'approche neutre d'un point de vue technologique de la protection des données dans l'Union européenne et ne sont axées sur aucune technologie en particulier, elles englobent également l'environnement de l'informatique en nuage et s'y appliquent.

III.3. Importance de garantir un niveau élevé de protection des données dans les services d'informatique en nuage

34. À l'échelle internationale, les autorités chargées de la protection des données ont récemment souligné[28] qu'il était essentiel que les problèmes posés par l'utilisation des services d'informatique en nuage ne donnent pas lieu à un affaiblissement des normes relatives à la protection des données par rapport à celles qui sont applicables aux traitements de données conventionnels.

35. Le CEPD souhaite souligner que tous les principes de protection des données énoncés à l'article 6 de la directive 95/46/CE et à l'article 5 du règlement proposé (tels que la loyauté et la licéité, la limitation des finalités, la proportionnalité, l'exactitude, la limitation de la durée de conservation des données) doivent être pleinement pris en compte pour le traitement de données à caractère personnel par des prestataires de services d'informatique en nuage.

36. Dans l'ensemble, compte tenu de la diversité de l'offre disponible en matière de services d'informatique en nuage, et de l'absence de normes légales et contractuelles bien établies et couvrant toutes les couches de l'architecture de l'informatique en nuage, l'impact de chaque type de service d'informatique en nuage en matière de protection des données doit actuellement être évalué sur une base *ad hoc*, afin de définir les garanties les plus appropriées devant être mises en œuvre.

IV. ANALYSE DE L'IMPACT DU RÈGLEMENT PROPOSÉ SUR LES SERVICES D'INFORMATIQUE EN NUAGE

37. Le règlement proposé prévoit un cadre modernisé pour la protection des données, qui tient compte des évolutions technologiques tout en restant neutre sur ce plan. Il contient des dispositions particulièrement pertinentes pour l'environnement de l'informatique en nuage.

38. Ce chapitre de l'avis analyse la manière dont le règlement proposé permettra de répondre aux questions posées par l'utilisation de services d'informatique en nuage et met en évidence d'autres questions que le législateur devra prendre en considération au cours du processus législatif. Il met également en exergue de

[28] Voir la note de bas de page n° 10.

bonnes pratiques en matière de traitement des données réalisé dans le cadre de services d'informatique en nuage.

IV.1. Clarification concernant l'applicabilité de la législation communautaire relative à la protection des données aux traitements de données réalisés dans le cadre de services d'informatique en nuage

39. L'article 2 du règlement proposé concerne le champ d'application matériel dudit règlement. Il précise notamment que le règlement proposé ne s'appliquera pas aux traitements réalisés par «une personne physique sans but lucratif dans le cadre de ses activités exclusivement personnelles ou domestiques» (ce qu'il est convenu d'appeler l'«exception domestique»). Néanmoins, le considérant 15[29] indique que les règles énoncées par le règlement proposé s'appliqueront aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des informations à caractère personnel pour ces activités personnelles ou domestiques. Cette précision au sujet des fournisseurs de services d'informatique en nuage est importante pour les consommateurs: même si les consommateurs utilisent les services en question à des fins personnelles, le fournisseur est néanmoins une entité qui, d'une part, fournit les moyens de traitement et, d'autre part, exerce cette activité à des fins commerciales. L'«exception domestique» ne s'appliquera donc pas à ces fournisseurs.

40. Pour ce qui est des utilisateurs, le CEPD constate que le règlement proposé ne définit pas, au sein de l'«exception domestique», l'activité personnelle des «autres» utilisateurs (par exemple, les contacts ou les amis sur les réseaux sociaux ou les tiers en général), ce qui laisse ouverte la question de l'application de l'exception lorsqu'un utilisateur peut être amené (via des services d'informatique en nuage) à traiter des données à caractère personnel qui peuvent être consultées par un nombre indéfini de personnes. Le CEPD a déjà indiqué[30] que l'application de l'exception à ce type de cas ne serait pas conforme aux décisions rendues par la Cour de justice dans les affaires *Lindqvist* et *Satamedia*[31].

41. Par exemple, une personnalité publique pourrait afficher sur sa page de réseau social le nom complet de ses «amis» ou fans afin de promouvoir une initiative culturelle. Dans un tel scénario, la personnalité en question semble n'avoir aucun but lucratif dans l'activité de traitement. Cependant, les données à caractère personnel pourraient bien être divulguées à un nombre indéfini de personnes, non seulement sur la page du réseau social[32], mais aussi, éventuellement, à travers des moteurs de recherche. Dans ce cas, l'exception domestique ne serait pas applicable au souscripteur, lequel serait donc également soumis à la législation relative à la protection des données[33].

---

[29] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 93, en ce qui concerne la formulation du considérant 15.

[30] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 91.

[31] Voir les arrêts de la Cour de justice du 6 novembre 2003, Lindqvist, C-101/01, [2003], Rec. I-12971, et du 16 décembre 2008, Satamedia, C-73/07, [2008], Rec. I-983.

[32] Dès lors que les paramètres concernant le respect de la vie privée de la personne le permettent.

[33] L'utilisateur doit être considéré comme un responsable du traitement des données car il choisit les moyens du traitement (le fournisseur de service en nuage) et détermine, dans une certaine mesure, les finalités du traitement.

42. En ce qui concerne le champ d'application territorial, l'article 3 du règlement proposé va au-delà des règles existantes sur deux plans: en indiquant explicitement que la présence de l'établissement[34] d'un sous-traitant dans l'Union européenne déclenchera l'application du règlement, et en introduisant de nouveaux critères concernant l'«offre de biens ou de services» aux personnes concernées dans l'Union européenne, ou l'«observation de leur comportement». Cette nouvelle disposition, accueillie de manière favorable par le CEPD dans son avis sur le paquet de mesures pour une réforme de la protection des données[35], est également particulièrement pertinente dans le cadre de l'informatique en nuage.

43. Lorsque l'on recherche de possibles exemples concrets de relations client/fournisseur de services en nuage, différents scénarios peuvent être envisagés. Les nouvelles règles donnent au règlement proposé un champ d'application territorial large dans le domaine des services d'informatique en nuage, ce qui pourrait conduire à des situations complexes; cependant, comme expliqué ci-après, une légère clarification du libellé de l'article 3 pourrait contribuer à lever quelques doutes d'interprétation.

Le fournisseur de services en nuage est un sous-traitant

44. Comme nous le verrons ci-après, dans certains cas, le fournisseur de services en nuage est considéré comme un sous-traitant plutôt que comme le responsable du traitement. Dans ce cas, si l'établissement du client (le responsable du traitement) se trouve sur le territoire de l'Union européenne, l'applicabilité du règlement proposé au responsable du traitement, et, par contrat, au sous-traitant, sera incontestable.

45. Par ailleurs, si le sous-traitant/fournisseur est établi dans l'UE et le client/responsable du traitement ne réside pas dans l'Union européenne, le règlement sera applicable à toutes les activités de traitement du sous-traitant. Cela implique que les fournisseurs de services en nuage établis en Europe devront respecter les obligations qui leurs sont imposées par le règlement proposé et, le cas échéant, assumer les conséquences d'une violation de ces obligations. Conformément à l'article 27 du règlement proposé, le sous-traitant ne peut traiter des données à caractère personnel que sur instruction du responsable du traitement, «à moins d'y être obligé par la législation de l'Union ou d'un État membre». Dès lors, un fournisseur de services en nuage/sous-traitant établi en Europe doit toujours agir conformément à la législation de l'Union européenne relative à la protection des données, même si cette législation diffère des instructions reçues d'un

[34] Voir également les paragraphes 106 et 107 de l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, où une observation critique est formulée au sujet de la définition de l'«établissement principal».

[35] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 99.

client/responsable du traitement (non européen)[36]. Comme indiqué précédemment, il est essentiel que les défis posés par l'utilisation des services d'informatique en nuage ne conduisent pas à un affaiblissement des normes de l'Union européenne en matière de protection des données. L'article 27 du règlement proposé doit donc être accueilli favorablement puisqu'il offre des garanties pour l'environnement en nuage.

Le fournisseur de services en nuage est le responsable du traitement

46. Si le fournisseur de services est considéré comme le responsable du traitement et est établi dans l'Union européenne, l'applicabilité du règlement à ses activités de traitement ne suscitera aucun doute.

47. Si le fournisseur de services en nuage est considéré comme étant un responsable du traitement, voire l'unique responsable, plutôt que comme un sous-traitant[37], mais qu'il n'est pas établi dans l'Union européenne, le scénario est différent. Les fournisseurs de services en nuage sont souvent établis en dehors de l'Union européenne et proposent leurs services dans l'Union européenne via l'internet. Conformément aux règles actuelles, en l'absence d'un équipement situé sur le territoire de l'UE, les activités de traitement ne seront pas soumises à la réglementation européenne[38]. Conformément au règlement proposé, le traitement de données à caractère personnel de personnes résidant dans l'Union européenne par un fournisseur de services en nuage situé en dehors de l'Union européenne (qui peut être considéré comme un responsable du traitement) peut relever du champ d'application du règlement proposé s'il vise des personnes concernées situées dans l'UE. Le critère d'application du règlement proposé sera le nouveau critère d'«offre de biens ou de services [aux] personnes concernées dans l'Union» visé à l'article 3, paragraphe 2, point a), dudit règlement. Puisque, selon l'article 4, une personne concernée ne peut être qu'une personne physique, le libellé dudit article peut être interprété comme signifiant que seul un traitement lié à des produits ou à des services proposés à des *personnes* résidant dans l'Union européenne relève du champ d'application du règlement.

48. Cependant, dans le domaine de l'informatique en nuage, la cible du service est souvent constituée d'entreprises de toutes tailles, c'est-à-dire d'entités juridiques qui ne peuvent être considérées comme des personnes concernées au regard de la législation européenne[39]. Même si d'un point de vue commercial, le service est

---

[36] L'application des règles de l'Union européenne ne doit cependant pas donner lieu à des contraintes excessives pour les entreprises européennes par rapport aux responsabilités du responsable du traitement non européen. À cet égard, le texte du règlement proposé comprend la possibilité d'exonérer (le responsable du traitement ou) le sous-traitant de la responsabilité d'un dommage subi par une personne du fait d'un traitement illicite, si le sous-traitant prouve que le fait qui a provoqué le dommage ne lui est pas imputable (article 77, paragraphe 3). De plus, l'article 75 énonce explicitement que les sanctions que les autorités de contrôle pourront infliger en cas de violation ou d'infraction doivent également tenir dûment compte du «degré de responsabilité de la personne physique ou morale en cause» (article 79, paragraphe 2).

[37] Par exemple dans le cas où le fournisseur des services traite des informations à caractère personnel pour ses propres fins.

[38] Il convient de noter cependant que si le fournisseur place des cookies sur le dispositif de l'utilisateur/client, ces cookies sont considérés comme un «équipement» situé sur le territoire de l'Union européenne au titre de la législation de l'Union européenne.

[39] Voir la définition de la personne concernée énoncée à l'article 4, paragraphe 1, du règlement proposé.

proposé à des entreprises de l'Union européenne (qui ne sont donc pas des «personnes concernées»), le CEPD considère que les dispositions du règlement proposé devraient également s'appliquer lorsque le service implique le traitement de données à caractère personnel de personnes résidant dans l'Union. Pour éviter tout doute interprétatif, l'article 3, paragraphe 2, point a), du règlement proposé pourrait être modifié comme suit: «l'offre de biens ou de services *impliquant le traitement de données à caractère personnel de* ces personnes concernées dans l'Union». Une autre solution consisterait à ajouter un nouveau considérant indiquant que le traitement de données à caractère personnel de personnes concernées situées dans l'Union par des responsables du traitement situés hors de l'UE offrant des services à des personnes morales situées dans l'Union européenne relève également du champ d'application territorial du règlement proposé.

IV.2. Améliorer la répartition des rôles et des responsabilités (notions de responsable du traitement et de sous-traitant)

49. L'applicabilité des notions de responsable du traitement et de sous-traitant à l'environnement de l'informatique en nuage est l'un des aspects les plus importants du régime de protection des données applicable à ce modèle commercial. Le point crucial concerne la répartition des responsabilités aux fins de la mise en œuvre des règles relatives à la protection des données[40].

50. L'avis du groupe de travail «Article 29» concerne la qualification de la relation fournisseur de services en nuage/client des services en nuage sur la base des dispositions de la directive 95/46/CE actuellement applicables. En résumé, le client des services en nuage détermine l'objectif ultime du traitement et décide s'il convient d'externaliser ce traitement et/ou de déléguer une partie ou la totalité des activités de traitement à une entreprise externe. Il devrait donc être considéré comme un responsable du traitement. Par conséquent, le client des services en nuage, en tant que responsable du traitement, est garant (en principe par la mise en œuvre de garanties contractuelles appropriées) de la conformité des traitements réalisés par le fournisseur de services avec la législation applicable en matière de protection des données. Lorsque le fournisseur de services en nuage fournit les moyens et la plateforme en agissant au nom du client, il est généralement considéré comme un sous-traitant au titre de la directive 95/46/CE[41]. Pour assurer la conformité des traitements, le sous-traitant devra respecter de manière stricte les exigences énoncées à l'article 17 de la directive.

51. Dans son avis, le groupe de travail «Article 29» reconnaît que, selon les circonstances, le fournisseur de services en nuage pourra être considéré, soit comme un coresponsable, soit comme un responsable de plein droit. Cela pourrait être le cas, par exemple, lorsque le fournisseur de services traite des données pour ses propres fins.

52. Le CEPD soutient la position du groupe de travail «Article 29» sur la qualification de la relation entre fournisseurs de services en nuage et clients sur la base des

---

[40] Voir l'avis 1/2010 du groupe de travail «Article 29» sur les notions de «responsable du traitement» et de «sous-traitant»: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf.

[41] La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite, seul ou conjointement avec d'autres, des données à caractère personnel pour le compte du responsable du traitement (article 2, point e), de la directive 95/46/CE).

dispositions en vigueur. Il constate cependant que la complexité des moyens techniques déployés dans l'environnement en nuage a maintenant atteint un tel niveau qu'il est nécessaire de préciser que le client des services en nuage/responsable du traitement peut ne pas être le seul à pouvoir déterminer les «finalités et les moyens» du traitement. Il est de plus en plus fréquent que le choix des éléments essentiels des moyens (qui constitue une prérogative du responsable du traitement) ne soit pas entre les mains du client des services en nuage. En général, le fournisseur des services en nuage conçoit, exploite et entretient l'infrastructure informatique des services en nuage (qu'il s'agisse simplement du matériel informatique de base et des services logiciels dans une structure IaaS ou de la plateforme dans une structure PaaS, ou de l'ensemble du service, y compris les applications logicielles, dans une structure SaaS).

53. Ainsi que le reconnaît le groupe de travail «Article 29» dans son avis, le fournisseur de services en nuage est souvent la partie qui, en fonction de son infrastructure technique et de son type d'entreprise, élabore les contrats types ou SLA qui sont proposés aux clients des services en nuage. Lesdits clients n'ont donc qu'une marge de manœuvre très limitée – ou n'en ont aucune – pour modifier les dispositions techniques ou contractuelles relatives au service. Cela est d'autant plus vrai avec la consolidation du marché des services d'informatique en nuage (voir point II.3. supra). Dès lors, il peut être particulièrement difficile de garantir le respect des règles de protection des données.

54. En outre, selon les définitions formulées dans le règlement proposé, le responsable du traitement est la personne physique ou morale qui, «seul[e] ou conjointement avec d'autres, détermine les finalités, les *conditions* et les moyens»[42] (italique ajouté) du traitement de données à caractère personnel». Les dispositions actuelles (article 2, point d), de la directive 95/46/CE) ne comprennent pas le terme «conditions». Cet ajout permettrait d'insister davantage sur la responsabilité des personnes qui déterminent la manière dont les traitements seront concrètement organisés.

55. Dans ce scénario, la qualification de la relation entre fournisseur et client sous l'appellation de responsabilité conjointe reflèterait mieux le niveau sous-jacent d'influence sur les traitements. Cette modification conduirait à une répartition plus réaliste des responsabilités entre les parties, ce qui devrait être pris en compte lors de la négociation sur les clauses générales du service. Cela signifie, par exemple, que les clauses générales du service devraient identifier clairement le responsable du traitement en charge, les domaines de traitement dont il a la charge et/ou les obligations imposées par la législation pertinente sur la protection des données. Par conséquent, le client des services en nuage devrait être responsable des parties du traitement sur lesquelles il a un contrôle effectif. Cependant, la différence de niveau d'influence des parties concernées pourrait toujours faire obstacle à des négociations équilibrées. Ce problème pourrait être surmonté par l'élaboration et l'utilisation de clauses et conditions contractuelles types[43].

56. Le CEPD soutient la disposition du règlement proposé qui envisage de rendre obligatoire un accord entre responsables conjoints (article 24). Un tel accord devrait

---

[42] Article 4, paragraphe 5.
[43] Voir le chapitre V.3 ci-après.

dans tous les cas préciser la répartition des responsabilités entre les différents acteurs, conformément à l'influence réelle que ceux-ci ont sur les différents types d'activités.

57. Dans le cadre des solutions IaaS, le client des services en nuage (qui est généralement une entreprise) pourrait exercer une certaine influence sur les clauses et conditions du service, même s'il est possible qu'il ne soit pas en mesure de négocier les mesures de sécurité que le fournisseur doit mettre en œuvre. Le client des services en nuage demeurerait néanmoins le responsable du traitement des données à caractère personnel de ses employés, parce qu'il choisirait les moyens et les conditions du traitement réalisé par le fournisseur, et en déterminerait la finalité. La répartition des responsabilités entre les deux parties devrait dès lors être explicitement clarifiée en ce qui concerne les clauses générales de service. S'agissant des solutions Saas, telles que les outils de productivité basés sur le nuage ou les outils de renseignement professionnel, le client des services en nuage n'a généralement pas la possibilité d'influer sur le type de service proposé par le fournisseur. En outre, la relation entre fournisseur et client peut ne pas impliquer de négociation directe et se résumer à un simple processus d'enregistrement. Par conséquent, le niveau de contrôle du client des services en nuage sur les moyens de traitement à disposition peut être extrêmement limité. Dans ce cas, le CEPD considère qu'il pourrait être plus approprié de nommer «coresponsable» le fournisseur du service en nuage.

58. En outre, le règlement proposé introduit, à l'article 26, paragraphe 4, une nouvelle disposition selon laquelle, si un sous-traitant «traite des données à caractère personnel d'une manière autre que celle définie dans les instructions du responsable du traitement, il est considéré comme responsable du traitement à l'égard de ce traitement et il est soumis aux dispositions applicables aux responsables conjoints du traitement prévues à l'article 24». Cette disposition peut être primordiale dans le cadre des services d'informatique en nuage: elle pourrait s'appliquer lorsqu'un fournisseur de solutions SaaS à des entreprises clientes traite, par exemple, des adresses et des listes de contacts d'employés ou de clients de l'utilisateur de services en nuage, voire lorsqu'il scanne le contenu de courriels auxquels il a accès, afin de promouvoir ses services à valeur ajoutée.

59. Pour conclure, la complexité de l'infrastructure technique de l'environnement de l'informatique en nuage requiert un élargissement des circonstances dans lesquelles un fournisseur de services en nuage peut être qualifié de responsable. Le règlement proposé pourrait introduire un nouvel élément de responsabilité («conditions») conforme à cette tendance. Dès lors, le fait de considérer les fournisseurs de services en nuage comme des coresponsables reflètera souvent mieux le niveau réel d'influence sur la finalité, les conditions et les moyens des traitements.

IV.3. Responsabilité dans le nuage: assurer une protection des données plus efficace

60. Le règlement proposé accroît la responsabilité des responsables du traitement et des sous-traitants d'une manière générale (voir principalement l'article 22) et plus particulièrement en introduisant des obligations spécifiques telles que la protection des données dès la conception ou par défaut, la notification des violations de la sécurité des données à caractère personnel et une analyse d'impact relative à la protection des données. Sur un plan général, les responsabilités accrues du responsable du traitement garantissent une amélioration qui arrive véritablement à

point nommé pour la protection des personnes concernées[44]. La majorité des innovations peuvent également être considérées comme des améliorations majeures de l'environnement de l'informatique en nuage.

61. D'autre part, certains types d'obligations nouvelles[45] peuvent être difficiles à respecter si le responsable du traitement est considéré comme étant le client des services en nuage. Même si, conformément à l'article 26, le sous-traitant est tenu de coopérer avec le responsable pour l'aider à satisfaire à son obligation de garantir le respect des droits des personnes concernées et de se conformer aux exigences en matière de sécurité, de notification des violations de données, d'analyse d'impact relative à la protection des données et de consultation préalable, la responsabilité ultime repose principalement sur le responsable du traitement.

62. Dans un environnement d'informatique en nuage, cela signifie que le client/responsable devra être capable, par exemple, de mettre en œuvre des mesures et des procédures techniques et organisationnelles appropriées visant à garantir que le traitement effectué par le fournisseur de services en nuage est conforme au règlement (article 23, protection des données dès la conception). Cela pourrait s'avérer difficile. Dans le cadre d'un service IaaS de base, il semble particulièrement difficile pour un client professionnel (notamment une PME) d'influencer la structure technique et organisationnelle du service. Il n'est pas réaliste d'attendre d'un fournisseur de grande taille ayant de nombreux clients qu'il adapte son infrastructure ou son organisation technique pour répondre aux exigences spécifiques de chaque client en fonction de contrats négociés de manière individuelle.

63. Par conséquent, une définition appropriée du responsable du traitement et du sous-traitant expliquée dans les chapitres précédents est essentielle pour garantir que les obligations accrues en matière de responsabilité sont véritablement respectées.

Analyse d'impact relative à la protection des données dans le cadre des services d'informatique en nuage

64. L'article 33 du règlement proposé dispose que le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement doit réaliser une analyse d'impact relative à la protection des données. L'article comprend une liste non exhaustive des traitements pour lesquels une telle analyse devrait être obligatoire. Le CEPD a déjà indiqué qu'il n'était pas entièrement satisfait du fait que la liste omette certains types de risques importants[46]. En l'absence de dispositions claires dans le règlement proposé ou dans les lignes directrices concernant les modalités de réalisation des analyses d'impact relatives à la protection des données, la mise en œuvre de cette exigence repose entièrement sur

[44] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 166 et suivants.

[45] En particulier, la mise en œuvre de politiques visant à garantir que le traitement de données à caractère personnel est conforme au règlement, aux exigences relatives à la sécurité des données, à l'analyse d'impact relative à la protection des données, à la protection des données dès la conception, aux notifications de violation des données à caractère personnel, en particulier en rapport avec l'article 31, paragraphe 3, points c) et e).

[46] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 201.

l'appréciation subjective de chaque responsable du traitement, ce qui peut donner des résultats très différents.

65. Le recours aux services d'informatique en nuage pour le traitement de données à caractère personnel pourrait, dans certains cas, engendrer des risques spécifiques (ainsi que le montre le présent avis) pour la protection des données, qui requièrent une analyse d'impact préalable relative à la protection des données, sur la base de laquelle il serait possible de définir des mesures d'atténuation.

66. Le CEPD souhaite notamment souligner l'importance d'effectuer des analyses d'impact relatives à la protection des données en ce qui concerne l'utilisation de services d'informatique en nuage par le secteur public, en particulier lorsque le traitement peut impliquer des données sensibles (telles que des données concernant la santé, les opinions politiques, etc.).

67. Le CEPD recommande que soient précisés par un acte délégué les critères et conditions déterminant la nécessité de réaliser une analyse d'impact relative à la protection des données, ainsi que les éléments à analyser[47]. Le CEPD souligne que, dans le contexte des services d'informatique en nuage, il serait utile que la Commission élabore des modèles que les services publics (ainsi que les particuliers et les entreprises) pourraient utiliser afin d'évaluer et de gérer les risques.

Audits et certifications

68. Plus généralement, l'application des exigences de responsabilité dans un environnement en nuage peut s'avérer complexe car différents intervenants peuvent interagir tout au long de la chaîne de valeurs afin de fournir des services aux clients finaux. Dès lors, l'interaction de parties multiples implique que celles-ci se fassent mutuellement confiance pour agir de manière responsable et prendre les mesures nécessaires pour garantir que les traitements de données sont effectués dans le respect des règles de protection des données.

69. À cet égard, les audits internes et ceux de tiers accrédités, ainsi que les certificats délivrés à leur issue, sont utiles pour vérifier la responsabilité des différentes parties impliquées. Ces audits devraient être fondés sur des certificats et des modèles de normalisation appropriés (qui seront examinés ci-après au point V.2).

70. En termes de contenu, l'article 22 du règlement proposé précise les mesures de protection des données que les responsables du traitement sont tenus de prendre[48]. En particulier, l'article 22, paragraphe 3, requiert du responsable du traitement qu'il mette en œuvre des mécanismes permettant de garantir que l'efficacité de ces mesures de protection des données peut être vérifiée. Sous réserve de la proportionnalité d'une telle mesure, des auditeurs internes ou externes indépendants peuvent procéder à cette vérification.

---

[47] Cet avis confirme l'avis 08/2012 du groupe de travail «Article 29», adopté le 5 octobre 2012, apportant des contributions supplémentaires au débat sur la réforme de la protection des données, pages 31-32, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

[48] Ainsi que, indirectement, les sous-traitants, en vertu de l'article 26.

71. Le CEPD salue cette disposition mais souligne également que des directives plus spécifiques sont nécessaires pour clarifier les mécanismes à mettre en œuvre afin de vérifier l'efficacité des mesures de protection des données prises, en particulier dans le contexte de l'informatique en nuage. Sans cela, ces exercices de vérification risquent d'évaluer la conformité uniquement «sur le papier» et non dans la «réalité». Le CEPD prend note de ce que le texte actuel du règlement proposé (article 22, paragraphe 4) prévoit que la Commission adopte des actes délégués pour préciser, notamment, les conditions de vérification et les mécanismes d'audit visés à l'article 22, paragraphe 3. Que cette disposition relative aux actes délégués soit ou non conservée dans le texte définitif [49], les codes de conduite spécifiques à l'informatique en nuage établis par le secteur et approuvés par les autorités chargées de la protection des données concernées pourraient constituer un outil qui permettrait d'améliorer la conformité et la confiance mutuelle entre les différents acteurs[50].

IV.4. Adapter les mécanismes de transfert international de données à l'environnement de l'informatique en nuage

Difficultés liées à l'application des règles de transfert de données de l'Union européenne à l'environnement de l'informatique en nuage

72. Les services d'informatique en nuage reposent sur les flux continus d'informations provenant des clients à travers l'infrastructure des fournisseurs de services en nuage. Les données circulent des clients vers les serveurs et les centres de données de fournisseurs situés dans diverses parties du monde. L'informatique en nuage implique donc souvent des transferts de données mondiaux, massifs et continus.

73. Les règles édictées par l'Union européenne en matière de transferts de données internationaux que comporte la législation actuelle et celles qui figurent dans le règlement proposé imposent des conditions pour le transfert de données à caractère personnel: le pays du destinataire doit assurer un niveau de protection adéquat et, en l'absence d'une telle protection[51], des garanties suffisantes doivent être apportées. Cependant, l'application des règles de l'Union européenne en matière de transferts aux traitements effectués via des services d'informatique en nuage est souvent perçue comme particulièrement difficile.

74. En premier lieu, il n'existe aucune définition claire, dans le règlement proposé, de la notion de «transfert» de données à caractère personnel. Cette absence est problématique dans un environnement de réseau tel que celui de l'informatique en

---

[49] Dans son avis 8/2012 du 5 octobre 2012 apportant des contributions supplémentaires au débat sur la réforme de la protection des données, le groupe de travail «Article 29» suggère de supprimer le paragraphe 4 de l'article 22, car «il semble inutile de proposer des critères ou exigences supplémentaires concernant les mesures appropriées autres que ceux déjà prévus au paragraphe 2, ou concernant les conditions pour le mécanisme de vérification et d'audit».

[50] Voir l'article 38 du règlement proposé.

[51] En vertu du cadre juridique actuel, la Commission a adopté plusieurs décisions constatant un niveau de protection adéquat concernant Andorre, l'Argentine, l'Australie, le Canada, la Suisse, les Îles Féroé, Guernesey, l'État d'Israël, l'Île de Man, Jersey, US PNR, et l'«US Safe Harbor». Conformément à l'article 41 du règlement proposé, la Commission pourra adopter des décisions relatives au caractère adéquat du niveau de protection ainsi que des décision négatives, non seulement à l'égard d'un pays tiers, mais également à l'égard d'un territoire ou d'un secteur de traitement de données dans ce pays tiers, ou à l'égard d'une organisation internationale.

nuage, dans lequel les données sont non seulement activement transférées, mais également mises à la disposition d'un certain nombre de destinataires situés dans différents pays (souvent inconnus du client/utilisateur final du service en nuage). Dans son avis sur le paquet de mesures pour une réforme de la protection des données, le CEPD demande que soit établie une définition claire de la notion de «transfert»[52].

75. En deuxième lieu, l'application des règles de transfert international des données repose généralement sur une évaluation visant à déterminer s'il existe un niveau de protection adéquat dans le ou les pays vers lequel ou lesquels les données doivent être transférées. Cependant, les services d'informatique en nuage ne sont en général pas attachés à un lieu fixe et les données à caractère personnel sont susceptibles de ne pas demeurer en permanence à un endroit donné. En outre, certains fournisseurs de services peuvent refuser d'indiquer la localisation des serveurs en nuage[53].

76. En troisième lieu, dans les cas où le client des services en nuage est réputé être le responsable du traitement des données (et en particulier le responsable unique), il lui est très difficile d'apporter des garanties adéquates pour le transfert international de ses données car il n'a qu'une connaissance limitée et/ou un contrôle restreint sur la conception de l'architecture du nuage de son fournisseur de services en nuage et des lieux où celui-ci, et tout autre sous-traitant ou sous-traitant du sous-traitant, traitent les données. Cela découle de l'asymétrie du contrôle des traitements entre le client des services en nuage et le fournisseur desdits services (mentionnée supra au point II.3).

Le règlement proposé apporte des améliorations significatives aux transferts internationaux de données

77. Le règlement proposé introduit davantage de flexibilité dans l'application des règles de transfert afin de faciliter les transferts internationaux tout en maintenant un niveau élevé de protection pour ces données. Il établit en particulier de nouveaux mécanismes de transfert international de données. En outre, l'article 42, paragraphe 1, du règlement proposé exige des responsables, mais également des sous-traitants, qu'ils apportent des garanties appropriées pour les transferts de données internationaux. Cela constitue un pas en avant significatif particulièrement pertinent pour l'environnement en nuage.

78. Par exemple, l'article 42 prévoit le recours à plusieurs types de clauses contractuelles (standard ou *ad hoc)* en précisant que seules les clauses *ad hoc* doivent faire l'objet d'une demande d'autorisation auprès d'une autorité de contrôle. Les fournisseurs de services d'informatique en nuage peuvent, s'ils le souhaitent, utiliser cette flexibilité en souscrivant aux clauses contractuelles types adoptées par la Commission ou par une autorité de contrôle, conformément à l'article 42, paragraphe 2, point c). Ils peuvent également souscrire à des clauses *ad hoc* adaptées à leur environnement spécifique, sous réserve d'obtenir l'autorisation nécessaire auprès de l'autorité de contrôle compétente. Quelles que soient les clauses retenues par les fournisseurs de services en nuage, elles doivent toutes

[52] Voir l'avis du CEPD, pages 18 et 19.
[53] Voir, par exemple, la demande de décision préjudicielle pendante devant la Cour de justice de l'Union européenne dans l'affaire C-131/12, Google/Espagne.

contenir des garanties minimales sur des aspects essentiels, tels que les exigences concourant à la signature d'un accord écrit avec les sous-traitants de sous-traitants, les engageant à respecter les mêmes obligations de protection des données (y compris les mesures de sécurité), les notifications/informations préalables du client sur le recours à des sous-traitants de sous-traitants, les clauses d'audit, les droits des tiers, les règles en matière de responsabilité et de réparation, le contrôle, etc. Lorsqu'elles élaboreront des clauses types ou réviseront des clauses *ad hoc* soumises à leur approbation, les autorités de contrôle porteront une attention particulière à ces aspects essentiels.

79. En outre, l'article 43 du règlement proposé établit un mécanisme détaillé concernant l'utilisation de règles d'entreprise contraignantes (ci-après «REC»)[54], qui peuvent être davantage adaptées à des schémas multilatéraux. Les REC sont un mécanisme particulièrement adapté à l'environnement de l'informatique en nuage car elles permettent de transférer des données entre toutes les entités d'une organisation tout en imposant des obligations légales à cette organisation en matière de protection des données à caractère personnel, dans tout endroit où ces données sont traitées au sein de l'organisation. L'extension de l'usage des REC aux sous-traitants est la bienvenue, notamment parce que les sous-traitants qui ont un établissement dans l'Union européenne pourront utiliser ce mécanisme pour faciliter leurs transferts de données intra-groupes vers des entités situées en dehors de l'Union européenne.

Opportunités fournies par le règlement proposé pour adapter davantage les mécanismes de transfert de données à l'environnement de l'informatique en nuage

80. L'environnement de l'informatique en nuage repose sur certaines spécificités qui, ainsi qu'expliqué supra, ne sont pas toutes entièrement prises en compte dans les mécanismes de transfert développés à ce jour. Le règlement proposé offre la possibilité d'adapter davantage ces mécanismes à un secteur spécifique, tel que l'environnement de l'informatique en nuage. Le comité européen de la protection des données pourrait fournir des orientations supplémentaires dans ce domaine[55].

(i) Clauses contractuelles types

81. Les clauses contractuelles types[56] sont particulièrement bien adaptées pour les transferts de données «point à point» d'un responsable du traitement vers des destinataires identifiés (que ce soit un ou des responsable(s) du traitement, un ou des sous-traitants et/ou un ou des sous-traitant(s) d'un sous-traitant) dont la localisation est connue. Ces clauses peuvent cependant être difficiles à appliquer dans la majorité des environnements en nuage, où les données peuvent être transférées en continu tout au long d'une chaîne de destinataires.

---

[54] Les règles d'entreprise contraignantes ont été conçues par les autorités de protection des données dans le cadre du groupe de travail «Article 29» afin de disposer d'un autre mécanisme approprié utilisable dans le cadre de transferts internationaux de données (voir les documents du groupe de travail «Article 29»: http://ec.europa.eu/justice/data-protection/article-29/index_fr.htm). Le règlement proposé s'inspire des travaux du groupe dans ce domaine.

[55] Voir l'avis 08/2012 du groupe de travail «Article 29».

[56] Pour plus d'informations sur les clauses contractuelles types actuelles, voir: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

82. Si le fournisseur de services en nuage est considéré comme étant le sous-traitant défini par les clauses contractuelles types adoptées par la Commission pour le transfert d'un responsable du traitement vers un sous-traitant, il revient à celui-ci d'informer et d'obtenir le consentement du client des services en nuage avant tout traitement en sous-traitance et tout transfert à un tiers externe. Néanmoins, dans de nombreux cas, le client des services en nuage n'aura qu'un pouvoir réel restreint – ou n'en aura aucun – pour autoriser ou interdire ce type de transfert. Par contraste, si le fournisseur des services en nuage est effectivement considéré comme étant le responsable du traitement des données, il lui incombe entièrement d'assurer la conformité de ses transferts de données à des entités internes ou externes au sein de son organisation; il contrôle pleinement et est entièrement responsable des décisions qu'il prend concernant l'architecture de ses services d'informatique en nuage. À cet égard, le CEPD a démontré au point IV.2 supra que le fournisseur de services en nuage serait souvent considéré comme le coresponsable.

83. En outre, il n'existe actuellement pas de clause contractuelle régissant les transferts de données réalisés par des sous-traitants situés dans l'Union européenne vers des sous-traitants situés en dehors de l'Union européenne. Cela constitue un manque important, notamment dans le contexte des services d'informatique en nuage, à propos duquel il serait nécessaire d'entreprendre des travaux supplémentaires en vue de proposer un nouvel ensemble de clauses appropriées.

84. Il conviendrait donc que la Commission et/ou les autorités de contrôle utilisent les possibilités prévues à l'article 42, paragraphe 2, points b) et c), du règlement proposé et adoptent des clauses contractuelles types actualisées et adaptées à l'environnement de l'informatique en nuage. Ces clauses devraient notamment régler les questions des transferts entre sous-traitants de l'Union européenne, des transferts continus entre juridictions multiples, de l'absence d'identification précise de l'endroit où les données peuvent se trouver à un moment donné, ainsi que des informations/notifications et des mécanismes de responsabilité. Elles devraient également préciser les conditions d'accès par les autorités répressives, ainsi que cela sera décrit ci-après au point IV.7.

(ii) Règles d'entreprise contraignantes

85. Les règles d'entreprise contraignantes (REC), qui reprennent entièrement le principe de la responsabilité, semblent particulièrement bien adaptées aux services d'informatique en nuage. Les fournisseurs de services en nuage doivent donc être encouragés à utiliser ce mécanisme dans le cadre de leurs transferts internationaux.

86. Pour ce qui est de l'applicabilité des REC aux sous-traitants externes et/ou à leurs propres sous-traitants, le CEPD souligne que, bien que les REC aient été élaborées pour fournir un mécanisme juridiquement contraignant dans des situations intragroupes, l'article 43, paragraphe 2, point c), du règlement proposé prévoit qu'elles indiquent également leur nature juridiquement contraignante pour les organisations externes. Les travaux actuellement entrepris par le groupe de travail «Article 29» en vue d'élaborer des REC pour les sous-traitants seront particulièrement utiles pour déterminer, entre autres, la nature contraignante de ces REC pour les sous-traitants externes des sous-traitants.

87. En outre, l'article 43, paragraphe 3, du règlement proposé prévoit l'adoption d'actes délégués par la Commission aux fins de préciser le champ d'application de

l'article 43, paragraphe 2, points b), d), e) et f) aux REC auxquelles adhèrent les sous-traitants. Le groupe de travail «Article 29»[57] a approuvé la formulation de précisions dans un acte délégué et a également recommandé que le comité européen de la protection des données fournisse des orientations à cet égard.

88. Enfin, il convient de souligner que l'adaptation plus poussée des mécanismes internationaux de transfert tirerait également d'importants avantages de travaux complémentaires effectués sur les programmes de normalisation et de certification en vue d'atteindre le niveau de protection requis à tous les niveaux du traitement, ce qui permettrait aux clients des services en nuage de faire preuve de la confiance nécessaire dans ces mécanismes (voir point V.2).

IV.5. Sécurité du traitement

89. Des mesures techniques et organisationnelles doivent être prises pour protéger la confidentialité, l'intégrité et la disponibilité des données en empêchant notamment tout accès, modification, suppression ou retrait non autorisé. En vertu du règlement proposé, le responsable du traitement et le sous-traitant seront tenus de réaliser une évaluation des risques présentés par le traitement et la nature des données traitées, et de sélectionner les mesures à mettre en œuvre en conséquence.

90. Dans les environnements d'informatique en nuage, il est particulièrement important que toutes les parties concernées, que ce soit le responsable du traitement ou le sous-traitant, évaluent les risques liés à leurs traitements, car (ainsi qu'indiqué supra) ces environnements sont facteurs de complexification. Une évaluation globale des risques et une bonne gestion de la sécurité dans un environnement en nuage demandent une coopération et une coordination entre les différentes parties concernées, le niveau de sécurité global étant déterminé par l'élément le plus faible. Par exemple, un ordinateur personnel ou un PC client qui a été mis en échec et qui autorise l'accès à des personnes non autorisées peut anéantir les mesures de sécurité prises dans les sites centraux. Dans un environnement en nuage utilisé par différents clients, les failles dans la sécurité de l'un d'entre eux peuvent affecter la sécurité des autres, sauf si le fournisseur a prévu des mesures très énergiques et très fiables en vue de séparer les services et les données entre ses clients, rendant ainsi toute interférence mutuelle impossible.[58]

91. Pour que les utilisateurs de services en nuage puissent prendre les mesures nécessaires de leur côté, ils doivent être informés de l'évaluation des risques et des mesures de sécurité prises par le fournisseur, et comprendre l'efficacité et les limites de ces mesures. Cependant, en matière de sécurité, les mesures informatiques mises en place ne sont généralement pas transparentes. Les informations relatives aux incidents de sécurité sont souvent tues aux clients. Il est donc difficile pour les clients des services en nuage d'évaluer la sécurité des traitements.

---

[57] Voir l'avis 08/2012 du groupe de travail «Article 29», pages 37 et 38.

[58] D'aucuns affirment parfois que les environnements d'informatique en nuage pourraient être plus sûrs que certains dispositifs de traitement traditionnels. Cependant, cette affirmation n'est valable que dans un nombre de cas très limité, par ex. lorsqu'une petite entreprise ou un particulier qui n'a prévu aucune mesure de sécurité systématique confie les traitements à des centres de traitement des données dans le nuage dont la sécurité est gérée de manière professionnelle.

92. Les responsables du traitement des données ne peuvent respecter leurs obligations en matière de sécurité que s'ils disposent d'informations complètes et fiables leur permettant d'évaluer si le fournisseur des services en nuage respecte les obligations qui lui incombent en la matière en tant que responsable du traitement ou sous-traitant. Ils ne doivent pas confier le traitement de données à caractère personnel à des fournisseurs de services en nuage qui n'apportent pas suffisamment d'informations sur leurs mesures de sécurité et ne confèrent pas suffisamment de transparence à ces dernières.

93. Le règlement proposé vise à imposer une obligation globale aux responsables du traitement, conformément à laquelle ils seraient tenus d'informer les autorités de contrôle et les personnes concernées de toute violation des données à caractère personnel. Les fournisseurs de services en nuage devront signaler toute violation des données à caractère personnel intervenue dans leurs services, soit directement aux autorités de contrôle et aux personnes concernées, le cas échéant, s'ils agissent en tant que responsables du traitement, soit au client des services en nuage responsable du traitement s'ils sont seulement sous-traitants.

94. Le règlement proposé permettrait à la Commission de préciser, en adoptant lorsque nécessaire des actes d'exécution, les exigences applicables en matière de sécurité et les critères et circonstances permettant d'établir des violations de données, ainsi que le format et la procédure de notification. Dans un environnement en nuage complexe, notamment, ces actes d'exécution devraient viser à clarifier la responsabilité des différents acteurs. Ils pourraient tirer parti de l'élaboration de normes européennes en matière de protection des données et de sécurité informatique dans les environnements d'informatique en nuage, ainsi que de la conception et de la reconnaissance des méthodes de mesure annoncées dans la communication (comme cela sera davantage détaillé au chapitre V).

IV.6. Renforcer la coopération et la surveillance coordonnée des traitements transfrontaliers

95. L'un des défis posés par le traitement de données à caractère personnel via des services d'informatique en nuage est la difficulté, pour les autorités de contrôle situées dans l'Union européenne, de contrôler tous les aspects des traitements réalisés dans cet environnement. Il peut notamment être difficile pour ces autorités d'exercer un contrôle effectif sur des données situées dans des juridictions étrangères ou disponibles et accessibles à un sous-traitant ou à un responsable du traitement situé dans une juridiction étrangère.

96. Comme cela a été expliqué au point IV.1, les nouvelles dispositions du règlement proposé sur le droit applicable contribueraient à régler certains de ces problèmes en faisant en sorte que les traitements réalisés par des fournisseurs de services en nuage disposant d'un établissement dans l'Union européenne ou certains traitements réalisés à partir de pays extérieurs à l'UE relèvent du champ d'application de la législation sur la protection des données de l'Union européenne et soient soumis au contrôle des autorités compétentes chargées de la protection des données dans l'UE. En outre, les dispositions concernant le renforcement de la coopération (articles 55 et 56) et le mécanisme de cohérence (articles 57 à 63) devraient aider les autorités de contrôle en Europe à collaborer et à adopter une approche coordonnée sur des sujets qui sont, par nature, transnationaux, comme, par exemple, les services d'informatique en nuage. Enfin, les pouvoirs répressifs des

autorités de contrôle seraient renforcés. Les autorités compétentes auraient ainsi la possibilité d'infliger des sanctions financières aux responsables du traitement ou aux sous-traitants qui ne respecteraient pas la législation sur la protection des données de l'UE (comme prévu par l'article 79).

97. Ces mécanismes de coopération et de cohérence, tels que prévus au chapitre VII du règlement proposé, sont particulièrement opportuns. Néanmoins, il convient de tenir compte du contexte mondial dans lequel les traitements sont effectués dans le cadre des services d'informatique en nuage. Sur le plan international, plusieurs mesures ont été prises pour répondre à la nécessité d'une coopération transfrontalière dans le domaine de la protection de la vie privée et de la protection des données[59]. En 2011, la conférence internationale des commissaires à la protection des données et à la vie privée a également appelé à un renforcement de la coordination en matière de répression et une meilleure application des dispositions relatives à la vie privée et à la protection des données[60] à l'échelle internationale.

98. Le CEPD encourage donc la Commission et les autorités de contrôle à s'engager plus activement dans la coopération internationale (en élaborant, par exemple, des mécanismes efficaces de coopération internationale, en prévoyant une assistance mutuelle internationale pour l'application de la législation relative à la protection des données à caractère personnel, etc.), afin de mettre en œuvre une coopération étroite, en particulier sur les questions relatives à l'environnement de l'informatique en nuage. Le CEPD rappelle que le lancement de ces activités ne doit pas dépendre de l'entrée en vigueur du règlement proposé.

IV.7. Accès des autorités répressives aux données à caractère personnel traitées via des services d'informatique en nuage

99. Les données stockées via des services d'informatique en nuage peuvent être saisies ou consultées par des autorités répressives locales de la juridiction où se trouvent les serveurs ou les centres de traitement des données, ou dans laquelle le fournisseur des services en nuage dispose d'un établissement. Les demandes peuvent émaner d'organes administratifs et/ou judiciaires situés non seulement dans l'Union européenne, mais également en dehors de cette dernière. En Europe, les demandes doivent être conforme à la loi[61] et respecter les exigences de protection des données[62]. Les membres du Conseil de l'Europe sont liés par la Convention n° 108 relative à la protection des données[63] et par d'autres actes. L'accès aux données par les autorités répressives est en outre sujet à un contrôle *ex post* des autorités de

---

[59] Par exemple, la recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée (2007) et la création récente du Global Privacy Enforcement Network (GPEN), https://www.privacyenforcement.net/about_the_network.

[60] Résolution intitulée «Privacy Enforcement Co-ordination at the International Level», adoptée lors de la 33e conférence internationale des commissaires à la protection des données et à la vie privée, 1er novembre 2011, Mexico.

[61] Souvent, les demandes d'accès reposent sur une demande légale autorisée par une autorité judiciaire.

[62] Le traitement de données par des autorités répressives doit respecter les exigences applicables en matière de protection des données. Le paquet de mesures pour une réforme de la protection des données contient une proposition de directive sur la protection des données qui contribuera à harmoniser les conditions du traitement des données à caractère personnel par ces autorités dans l'Union européenne.

[63] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ETS n° 108 du 28 janvier 1981).

contrôle de la protection des données. Cependant, les demandes d'accès émanant d'autorités répressives étrangères soulèvent des questions spécifiques en termes de protection des données, notamment pour assurer que la protection accordée aux individus en Europe pour les données les concernant ne soit pas affaiblie de manière significative ou ignorée dans un tel contexte.

100. Par exemple, des fournisseurs de services en nuage exerçant leurs activités dans certains pays ont été contraints de révéler des données à des autorités répressives nationales, ce qui a suscité des craintes concernant l'accès aux données stockées dans des services d'informatique en nuage à l'étranger[64]. De plus, il a été signalé que la probabilité que certains gouvernements demandent aux fournisseurs de services de communication proposant des services dans leur pays de disposer d'un équipement de communication dans le pays afin de faciliter l'accès à ces données[65] était accrue.

101. Les fournisseurs de services en nuage peuvent être pris entre des exigences juridiques contradictoires. Il s'agira, d'un côté, de répondre à une demande d'accès émanant d'une autorité répressive située dans un pays qui revendique compétence et, de l'autre, de garantir le respect de la législation sur la protection des données de l'Union européenne. Les conditions de service des fournisseurs indiquent souvent que ces derniers préserveront les informations et ne les divulgueront aux autorités répressives que lorsqu'une demande légale leur sera présentée. Cependant, le traitement réservé à ces demandes d'accès devrait être harmonisé avec les exigences en matière de protection des données de l'UE.

102. Premièrement, l'accès à des données à caractère personnel de personnes situées dans l'Union européenne ne doit être accordé qu'en accord avec la loi et sur la foi d'une base juridique adéquate autorisant le transfert des données[66]. À cet égard, le CEPD s'est prononcé, dans son avis sur le paquet de mesures pour une réforme de la protection des données[67], en faveur de l'inclusion d'une disposition importante visant à clarifier, dans le règlement proposé, les conditions requises pour ce type de demande d'accès. En outre, des garanties appropriées devraient être en place en pareils cas, impliquant des garanties judiciaires ainsi que des garanties relatives à la protection des données, y compris l'existence d'accords de coopération internationaux ou bilatéraux sur des questions spécifiques (par exemple, des accords d'entraide judiciaire). Cette question mériterait également d'être analysée pour d'autres types d'instruments internationaux, tels que les accords commerciaux avec des pays tiers. Il conviendrait en outre d'analyser, ainsi que souligné précédemment par le CEPD[68], de quelle façon les autorités de contrôle pourraient intervenir dans pareils cas, que ce soit en rendant un avis ou une autorisation sur le transfert. Pour

---

[64] «Lost in the Cloud», Jonathan Zittrain, New York Times, 19 juillet 2009, http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1.

[65] «Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future», Christopher Kuner, Tilburg University, Pays-Bas, document de travail n° 016/2010, octobre 2010, page 40.

[66] Voir le considérant 90 de la proposition de règlement sur la protection des données.

[67] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphes 229-232.

[68] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphe 231.

cela, il sera peut-être nécessaire d'insérer une disposition à cet effet dans le règlement proposé.

103. En deuxième lieu, des travaux complémentaires devront être réalisés pour améliorer et standardiser les clauses contractuelles des fournisseurs des services en nuage relatives aux modalités de traitement des demandes d'accès émanant d'autorités répressives (question abordée au point V.3 ci-après).

104. Enfin, il semble clairement nécessaire d'aborder, à l'échelle internationale, la question de l'accès aux données par les autorités répressives. À cet égard, les conditions dans lesquelles ces autorités répressives pourront demander d'accéder à des données stockées dans un espace de services d'informatique en nuage mériteraient encore d'être clarifiées, notamment en élaborant des concepts et des principes communs au niveau international en rapport avec les questions suivantes:

- ces normes globales devraient préciser les conditions d'accès, les mesures de sécurité applicables lors de la transmission des données aux autorités répressives[69], les droits des particuliers, les mécanismes de contrôle et de sanction;

- il convient de préciser la signification du mot «accès» dans ce contexte et d'indiquer s'il s'agit de retrouver ou de copier des données stockées dans un équipement spécifique. Dans cette perspective, il convient de tenir compte de ce que l'accès à des données traitées dans un espace de services d'informatique en nuage implique souvent de devoir localiser les données pertinentes et de les rassembler, voire de les convertir, dans un format exploitable;

- il convient également de déterminer si l'accès à des données stockées dans une infrastructure en nuage privée devrait être traité de la même manière que l'accès à des données stockées dans une infrastructure en nuage publique;

- la création de programmes de certification pour les services d'informatique en nuage pourrait également permettre de déterminer si, et comment, les données à caractère personnel sont protégées d'un tel accès.

105. En conclusion, le CEPD appelle à inclure une disposition spécifique dans le règlement proposé afin de clarifier les conditions dans lesquelles des pays n'appartenant pas à l'EEE pourraient être autorisés à accéder à ces données. 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. La question de l'accès aux données par des autorités répressives devrait être abordée à l'échelle internationale. La Commission et les États membres devraient unir leurs efforts pour élaborer des règles et des principes communs à ce niveau. En outre, ils devraient systématiquement intégrer des dispositions et des garanties spécifiques à ce sujet dans les différents accords internationaux (y compris les accords commerciaux) qu'ils concluent avec des pays n'appartenant pas à l'EEE.

---

[69] Par exemple, le recours à des mesures de codage en vue de protéger les données et la fourniture d'un accès à la clé de décodage en toute sécurité.

V. COMMENTAIRES SPÉCIFIQUES CONCERNANT LA COMMUNICATION DE LA COMMISSION

106. La communication de la Commission décrit un certain nombre de mesures à prendre ou à encourager pour faciliter le déploiement des services d'informatique en nuage en Europe. Les mesures suivantes sont, entre autres, envisagées: fournir des orientations, favoriser l'émergence de programmes appropriés de normalisation et de certification, élaborer des clauses contractuelles types et un code de conduite, mettre en place un partenariat européen en faveur de l'informatique en nuage et poursuivre le dialogue international avec des pays tiers et des forums multilatéraux.

107. Le CEPD se félicite du fait que la protection des données soit un élément central de la communication et que les initiatives politiques envisagées en relation avec les services d'informatique en nuage aient pour but de maintenir un niveau élevé de protection des données.

V.1. Fournir de nouvelles orientations

108. Le CEPD se félicite également de ce que la Commission envisage de fournir de nouvelles orientations sur l'application de la législation relative à la protection des données dans le cadre des services d'informatique en nuage, et ce en étroite collaboration avec les autorités de protection des données. Il salue le fait que l'avis du groupe de travail «Article 29» a été pris en compte et souligne que le présent avis présente également des orientations additionnelles eu égard au nouveau cadre législatif proposé pour la protection des données.

109. Des travaux complémentaires restent à accomplir en vue de préciser les meilleures pratiques relatives à certaines questions spécifiques, telles que la responsabilité du responsable du traitement/sous-traitant, la conservation appropriée de données dans l'environnement en nuage, la portabilité des données et l'exercice de leurs droits par les personnes concernées. L'avis du groupe de travail «Article 29» apportant des contributions supplémentaires au débat sur la réforme de la protection des données[70] met en lumière de nombreux domaines pour lesquels il serait utile que le comité européen de la protection des données fournisse des orientations complémentaires, en particulier en ce qui concerne la sécurité des traitements, les critères à appliquer pour déterminer le degré élevé de risques particuliers visés à l'article 34, paragraphe 2, point a), ainsi que l'application de certaines des exigences des REC aux sous-traitants.

110. De plus, le CEPD est favorable à l'élaboration de codes de conduite applicables à l'informatique en nuage (article 38 du règlement proposé), sous réserve qu'ils respectent pleinement les exigences de protection des données. À cet égard, le CEPD souligne que seule la validation des codes de conduite par les autorités de contrôle peut fournir aux sociétés la certitude juridique qu'elles se conformeront à la législation en vigueur lorsqu'elles appliqueront lesdits codes.

V.2. Programmes de normalisation et de certification

[70] Voir la note de bas de page n° 47.

111. Dans le cadre de l'action essentielle 1, la communication propose la normalisation comme une mesure phare en faveur de l'acceptation des services d'informatique en nuage. La communication indique que d'ici à 2013, une cartographie des normes nécessaires sera établie. Ces normes s'appliqueront notamment à la sécurité, l'interopérabilité, la portabilité des données et la réversibilité.

112. Ces normes pourraient être un facteur de succès essentiel pour permettre la mise en place de modèles de gouvernance et de contrôle à l'échelle internationale. Elles contribueront à garantir que l'ensemble de la chaîne des acteurs concernés par l'architecture de l'informatique en nuage, y compris les intermédiaires, appliquent tous le même niveau d'exigences techniques. Cependant, pour être efficaces en termes de protection des données, le CEPD souligne que ces normes devraient reprendre l'intégralité des exigences de protection des données dès la conception et par défaut établies à l'article 23 du règlement proposé. Ainsi, le CEPD encourage la Commission à redoubler d'efforts pour veiller à ce que les normes et les méthodes de mesure définies à l'échelle internationale couvrent adéquatement les exigences de l'Union européenne.

113. Il conviendrait de veiller en particulier à ce que les normes dans le domaine des services d'informatique en nuage se traduisent effectivement par un niveau élevé de sécurité et de protection des données. Cela concerne en particulier:

- l'interopérabilité, qui peut être définie comme la capacité de différents systèmes à fonctionner ensemble et à échanger des informations. D'un point de vue économique et technique, l'interopérabilité permet d'intégrer différentes sources de données, ce qui peut amener le traitement des données à un nouveau niveau. Le risque potentiel de voir des données à caractère personnel être utilisées pour des finalités non compatibles avec celles pour lesquelles elles ont été collectées devrait être abordé en tenant compte du principe de la limitation de la finalité dès lors que l'interopérabilité s'applique à des données à caractère personnel;

- la portabilité des données, qui est définie à l'article 18 du règlement proposé comme la capacité, pour une personne concernée, d'obtenir auprès du responsable du traitement une copie des données faisant l'objet d'un traitement automatisé dans un format électronique structuré qui est couramment utilisé. Pour mettre ce droit en application, il est important, une fois les données transférées, qu'il n'en reste aucune trace dans le système[71]. En termes techniques, il devrait être possible de vérifier que les données ont été effacées en toute sécurité.

114. Ces normes devraient aider les fournisseurs de services en nuage à garantir leur responsabilité dans les faits. La combinaison de normes avec la certification par des parties indépendantes pourrait accroître la confiance du public à l'égard des services en nuage et aider les responsables du traitement et les sous-traitants à se conformer aux cadres réglementaires.

[71] Voir l'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, paragraphes 150 à 152, et l'avis du groupe de travail «Article 29» sur l'informatique en nuage, page 16.

V.3. Élaborer des clauses et des conditions contractuelles types

115. Le CEPD reconnaît entièrement la nécessité d'aider les parties prenantes à définir des clauses contractuelles types étant donné le déséquilibre significatif habituellement constaté en termes de pouvoir de négociation entre les fournisseurs de services en nuage et leurs clients. Ainsi qu'indiqué supra, les fournisseurs de services en nuage se trouvent souvent dans une position qui leur permet d'imposer des clauses contractuelles non négociables à leurs clients. Le CEPD est donc satisfait que l'action essentielle 2 de la communication prévoie l'élaboration de clauses et de conditions contractuelles types par la Commission, ce qui devrait contribuer à une meilleure prise en compte des obligations en matière de protection des données et des droits des personnes concernées dans les propositions commerciales des fournisseurs de services en nuage aux clients (dans les accords sur le niveau de service) et aux consommateurs (dans les clauses et conditions contractuelles).

116. Ces clauses et conditions contractuelles types visent à fournir des clauses types qui seront incluses dans les propositions commerciales faites aux clients des services en nuage. Elles sont distinctes des clauses contractuelles types utilisées aux fins de fournir des garanties adéquates lors des transferts internationaux de données. Même si l'action essentielle 2 n'a pas pour principal domaine d'action les clauses contractuelles types pour les transferts internationaux, le CEPD salue le fait que la communication prévoit que ces clauses types seront également révisées et adaptées à l'environnement de l'informatique en nuage, ainsi que suggéré au point IV.4 ci-dessus.

117. La communication signale plusieurs questions de protection des données qui doivent être réglées dans les clauses et conditions contractuelles types, telles que la préservation des données après l'expiration du contrat, la divulgation et l'intégrité des données, la localisation et le transfert des données, la modification du service par les fournisseurs et la sous-traitance. Le groupe de travail «Article 29» a également formulé des suggestions concernant les points qui doivent être spécifiquement abordés dans les contrats[72]. Outre les points énumérés par la communication et par le groupe de travail «Article 29», le CEPD souligne qu'il est particulièrement important que les contrats types et les clauses et conditions contractuelles types comportent également des dispositions appropriées concernant les aspects suivants:

    - supprimer les clauses abusives par lesquelles les fournisseurs de services en nuage déclinent toute responsabilité s'agissant de garantir la confidentialité et la sécurité des données de leurs clients ou en cas de perte ou de corruption de ces données. En outre, les contrats devraient également contenir des clauses adéquates concernant le droit applicable et la résolution des conflits, qui permettent aux personnes concernées d'obtenir réparation devant une autorité chargée de la protection des données et/ou le tribunal national d'un État

[72] Voir l'avis 05/2012 du groupe de travail «Article 29», pages 12 à 14. Ces recommandations concernent, notamment, les mesures de sécurité, la confidentialité, la sous-traitance, les modalités de restitution ou de destruction des données après la prestation du service, les notifications de violation des données à caractère personnel, l'audit et la gestion des demandes d'accès émanant d'autorités répressives.

membre dans des affaires impliquant une violation de la législation de l'Union européenne relative à la protection des données (par exemple en cas de violation ou de perte de données);

- informer les clients s'il est possible de conserver les données dans un espace en nuage national ou régional, et leur indiquer les conditions applicables;

- concernant les modifications contractuelles ultérieures, garantir que des informations appropriées sont fournies et que le consentement des clients de services en nuage est obtenu avant toute modification ou suppression de clause et condition;

- inclure des clauses appropriées concernant la conservation des données après l'expiration du contrat, en particulier définir des bonnes pratiques en ce qui concerne la période maximale de conservation des données et leur suppression ultérieure;

- s'assurer que des informations adéquates sont fournies aux clients des services en nuage en matière de traitement des données à caractère personnel, conformément aux exigences de protection des données. On devrait également envisager d'inclure des informations complémentaires essentielles dans le contexte de l'utilisation de services d'informatique en nuage dans ces clauses et conditions contractuelles types (par exemple, le droit applicable, le(s) lieu(x) de traitement des données, la conformité avec des programmes/normes de certification, la mise en œuvre de garanties appropriées à tous les niveaux de l'infrastructure et à tous les endroits où les données sont transférées ou stockées, les mesures de protection spécifiques mises en place pour les données sensibles, l'identification de l'organisme de contrôle compétent, etc.);

- s'assurer que les personnes concernées sont informées de leurs droits, conformément aux exigences de protection des données, et que les clauses et conditions types fournissent des moyens effectifs d'exercer ces droits. Dans l'environnement de l'informatique en nuage, il est particulièrement important de s'assurer que les personnes ont un droit d'accès effectif à leurs données et le droit à la portabilité des données;

- concernant l'accès aux données par les autorités répressives dans des pays tiers, il conviendrait de s'assurer que les clients des services en nuage sont au moins informés des implications juridiques liées à la juridiction dont dépend ou peut dépendre le traitement, et de garantir qu'en règle générale, ces clients sont informés de toute demande d'accès émanant d'autorités répressives. Ces informations devraient figurer dans les clauses contractuelles des fournisseurs de services en nuage ainsi que dans les garanties produites pour le transfert de données à caractère personnel vers des pays situés hors de l'UE/EEE (par exemple, les clauses contractuelles types, les REC).

118. En outre, dans le contexte du partenariat européen en faveur de l'informatique en nuage, la Commission travaillera à l'élaboration de clauses spécifiques aux marchés pour le secteur public en définissant des exigences communes en matière de passation de marchés pour les organismes publics utilisateurs de services

d'informatique en nuage. Le CEPD souligne que ces exigences communes en matière de passation de marchés devraient inclure des exigences relatives à la protection des données (y compris des mesures de sécurité appropriées), lesquelles devraient être définies en fonction des risques spécifiques liés au traitement de données du secteur public dans un environnement d'informatique en nuage, sur la base d'une analyse d'impact minutieuse relative à la protection des données, en fonction du type et du degré de sensibilité du traitement réalisé (par exemple, en différenciant les traitements, par le secteur public, de données concernant la santé, les délits pénaux, les données confidentielles, etc.). Ainsi, les exigences contenues dans les clauses relatives à la passation de marchés devront être distinguées en fonction du degré de sensibilité des données traitées, ce qui devrait conduire à la définition de plusieurs ensembles d'exigences communes.

V.4. Dialogue international

119. Dans son avis, le CEPD souligne la nécessité d'établir une coopération plus globale entre les autorités de contrôle (point IV.6) et l'importance de répondre à des questions spécifiques concernant l'informatique en nuage au niveau international (points IV.5 et IV.7). Il salue donc le fait que la communication sur l'informatique en nuage prend dûment en compte la nature mondiale de ces services et qu'elle prévoit des mesures visant à favoriser l'émergence de normes de gouvernance mondiale et la mise en œuvre de pratiques de coopération plus efficaces.

120. Il est important qu'une place essentielle soit accordée à la protection des données dans le dialogue international sur l'informatique en nuage. Ce dialogue doit être abordé: au niveau technologique, pour créer des solutions et des normes garantissant un niveau adéquat de protection des données (par exemple, en intégrant la protection par défaut et dès la conception, et la sécurité); au niveau commercial, pour créer des solutions fondées sur des mécanismes de responsabilité et de gouvernance; et au niveau politique, pour déterminer les moyens dont disposent la Commission et les pays tiers pour permettre l'interopérabilité à l'échelle mondiale des différents cadres juridiques en ce qui concerne des points essentiels, tels que la compétence juridictionnelle et les demandes d'accès émanant d'autorités répressives.

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 élargirait 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

(**signed**)

Peter HUSTINX
Contrôleur européen de la protection des données