Avis du Contrôleur européen de la protection des données

sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16;

vu le traité sur la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8;

vu la directive (CE) nº 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) nº 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[2], et notamment son article 28, paragraphe 2;

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 5 février 2013, la Commission a adopté deux propositions: une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme[3] («la directive proposée»), et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds[4] («le règlement proposé»), ci-après communément dénommées «les propositions». Les propositions ont été communiquées au CEPD pour consultation le 12 février 2013.

2. Le CEPD se félicite d'être consulté par la Commission et recommande qu'il soit fait référence au présent avis dans le préambule des instruments adoptés.

[1] JO L 281, 23.11.1995, p 31.
[2] JO L 8, 12.1.2001, p. 1.
[3] COM (2013) 45 final.
[4] COM (2013) 44 final.

3. Avant que ces propositions ne soient adoptées, le CEPD a pu faire part d'observations informelles à la Commission. Certaines d'entre elles ont été prises en considération.

1.2. Objectifs et champ d'application des propositions

4. Par «blanchiment de capitaux», on entend généralement la conversion du produit d'activités criminelles en des fonds apparemment licites, habituellement *par l'entremise du système financier*[5]. L'opération consiste à déguiser l'origine de l'argent, en modifiant sa forme ou en déplaçant les fonds à un endroit où ils sont moins susceptibles d'attirer l'attention. Le financement du terrorisme consiste en l'apport ou la collecte de fonds, par quelque moyen que ce soit, directement ou indirectement, dans l'intention de les utiliser afin de commettre des infractions terroristes ou en sachant qu'ils vont servir à ces fins[6].

5. Une législation a été adoptée au niveau de l'Union européenne dès 1991 en vue de prévenir le blanchiment de capitaux et le financement du terrorisme. Ces infractions sont considérées comme une menace pour l'intégrité et la stabilité du secteur financier et, de façon plus générale, comme une menace pour le marché intérieur. La base légale de ces propositions est l'article 114 du TFUE.

6. Les règles européennes conçues pour prévenir le blanchiment de capitaux sont dans une large mesure fondées sur les normes adoptées par le Groupe d'action financière internationale (GAFI)[7]. Les propositions ont pour but de mettre en œuvre au sein de l'Union européenne les normes internationales révisées de lutte contre le blanchiment de capitaux qui ont été introduites par le GAFI en février 2012. La directive actuelle, la troisième directive anti-blanchiment (LBC)[8], est en vigueur depuis 2005 et fournit un cadre européen basé sur les normes internationales du GAFI.

7. La troisième directive LBC s'applique au secteur financier (établissements de crédit et financiers) ainsi qu'à un éventail de professions couvrant notamment les avocats, les notaires, les comptables, les agents immobiliers, les casinos et les prestataires de services aux sociétés. Le champ d'application englobe également les fournisseurs de biens, pour les transactions en espèces d'un montant supérieur à 15 000 euros. Tous ces destinataires sont considérés comme étant des «entités soumises à obligations». La directive exige de ces entités soumises à obligations qu'elles identifient et vérifient l'identité de leurs clients (lesdites obligations de vigilance à l'égard de la clientèle) et des bénéficiaires effectifs, et qu'elles surveillent les transactions financières de leurs clients. Elles ont donc pour obligation, entre autres, de déclarer les soupçons de blanchiment de capitaux ou de financement du terrorisme aux cellules de renseignement financier concernées

[5] Voir article 1, paragraphe 2, de la directive proposée.
[6] Voir article 1, paragraphe 4, de la directive proposée.
[7] Le GAFI est l'instance globale de normalisation qui fixe les mesures de lutte contre le blanchiment de capitaux, le financement du terrorisme et (plus récemment) le financement de la prolifération. Il s'agit d'un organisme intergouvernemental réunissant 36 membres et bénéficiant de la participation de plus de 180 pays. La Commission européenne fait partie des membres fondateurs du GAFI et 15 États membres de l'Union en sont membres de plein droit.
[8] Directive 2005/60/CE du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

(CRF). La directive prévoit également des exigences et des garanties supplémentaires (telles que l'application d'obligations renforcées de vigilance à l'égard de la clientèle) pour les situations présentant un risque majeur.

8. La directive proposée élargit le champ d'application du cadre actuel et vise à renforcer ces obligations, en incluant par exemple les prestataires de services de jeux d'argent et de hasard, de même que les négociants en biens dès le seuil de 7 500 EUR Par ailleurs, elle requiert de plus amples informations sur les bénéficiaires effectifs, resserre les exigences relatives aux «personnes politiquement exposées» et introduit de nouvelles exigences concernant le contrôle des membres de la famille de toutes les personnes politiquement exposées ou des personnes étroitement associées à ces dernières. La liste des infractions principales[9] liées au blanchiment de capitaux a été allongée pour inclure les infractions fiscales pénales liées aux impôts directs et indirects.

9. Le règlement proposé, quant à lui, remplace le règlement (CE) nº 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds (ci-après «le règlement relatif aux virements de fonds»), qui vise à améliorer la traçabilité des paiements. Le règlement relatif aux virements de fonds complète les autres mesures de lutte contre le blanchiment de capitaux, en veillant à ce que les informations de base concernant le donneur d'ordre des virements de fonds soient immédiatement accessibles aux autorités policières ou judiciaires afin de les aider à détecter des infractions, à mener des enquêtes sur celles-ci, à poursuivre des terroristes ou d'autres criminels, et à repérer les avoirs des terroristes.

2. ANALYSE GÉNÉRALE DES PROPOSITIONS

2.1. Remarques liminaires

Nécessité de tenir compte des exigences relatives à la protection des données

10. Le CEPD comprend qu'il est nécessaire de mettre en œuvre la nouvelle série des recommandations du GAFI qui ont été publiées en février 2012[10] , dans le cadre européen de la lutte contre le blanchiment de capitaux. Il reconnaît l'importance des politiques de lutte contre le blanchiment de capitaux pour la réputation économique et financière des États membres, et de manière plus générale en tant qu'instrument de lutte contre les formes graves de criminalité. Il tient cependant à souligner que les normes européennes en matière de protection des données n'ont pas d'équivalent à l'échelle internationale du GAFI, et que la recherche de cohérence entre les politiques de lutte contre le blanchiment de capitaux à l'échelle internationale ne devrait pas ignorer les exigences de l'Union européenne en matière de protection des données. Le CEPD rappelle que le droit d'un individu à la protection de ses données à caractère personnel est garanti par l'article 16 du TFUE et l'article 8 de la charte des droits fondamentaux de l'Union européenne.

[9] Une «infraction principale» est une infraction pénale dont le produit est utilisé pour commettre une autre infraction: dans le présent contexte, par exemple, la fraude, la corruption, le trafic de drogue et les autres crimes graves peuvent constituer des activités criminelles sous-jacentes aux fins du blanchiment de capitaux.

[10] Voir en particulier la recommandation 16.

11. Assurer la transparence des sources de paiements, des dépôts et virements de fonds afin de combattre le terrorisme et le blanchiment de capitaux est un intérêt légitime, mais cet objectif doit être poursuivi dans le respect des exigences en matière de protection des données. Le CEPD insiste dès lors sur le fait qu'il est indispensable de tenir compte de ces exigences lors de la transposition des normes du GAFI dans l'ordre juridique de l'Union européenne.

12. Le CEPD souhaite également attirer l'attention des législateurs sur le fait que les propositions produisent des effets sur la relation entre le prestataire de service et le client, et que la collecte d'information aux fins de la lutte contre le blanchiment de capitaux s'effectue en même temps que la collecte de données à des fins commerciales. Par exemple, les données seront recueillies par les entités soumises aux obligations de vigilance à l'égard de leur clientèle en même temps que les données nécessaires pour établir la relation d'affaires (voir article 10 de la directive proposée), aux fins de vérification, lorsqu'un virement de fonds est envoyé ou reçu par un prestataire de services de paiement établi au sein de l'Union (voir article 3 du règlement proposé). Parfois, les mêmes données (comme l'identité du client) seront recueillies simultanément à des fins commerciales et aux fins de la lutte contre le blanchiment de capitaux.

13. Une des préoccupations du CEPD est que le client n'est pas correctement informé de la finalité de la collecte et du traitement des informations au moment où celles-ci sont recueillies. Ce droit d'être informé est consacré dans la directive 95/46/CE et est nécessaire pour donner effet aux droits d'accès et de rectification prévus à l'article 8 de la charte des droits fondamentaux.

14. Le CEPD souligne également que les propositions accroîtront les volumes de données collectées aux fins de la lutte contre le blanchiment de capitaux et le terrorisme, ce qui multipliera les éventuelles conséquences pour les personnes concernées. Plus particulièrement, la directive proposée prévoit le contrôle des transactions financières des clients des établissements de crédit et financiers, ainsi que celles des clients d'un certain nombre d'autres catégories de prestataires de services dont les activités sont liées aux activités économiques. Cela implique le traitement massif des données à caractère personnel des clients, pouvant mener en fin de compte à des enquêtes policières. En soi, la directive proposée a un impact majeur sur le droit des individus à la protection de leurs données à caractère personnel. Le règlement proposé prévoit l'obligation de recueillir des données à caractère personnel sur le donneur d'ordre et le destinataire des fonds, et parfois même le transfert de ces données vers des organisations ou des filiales établies dans des pays tiers.

15. Par conséquent, le CEPD insiste sur la nécessité de veiller à l'application concrète des garanties en matière de protection des données dans ce domaine spécifique et à leur élaboration dans le texte de manière à sensibiliser le client et à l'informer qu'il/elle bénéficie de la sécurité juridique et de l'entière protection accordée par la législation de l'Union européenne en matière de protection des données. Ces garanties, telles que décrites ci-après, veilleront également à ce que le client ne fasse pas l'objet de décisions fondées sur des données qui n'auraient pas dû être collectées, qui ont été indûment stockées ou qui ne sont pas ou plus correctes. À

cet égard, le CEPD attire l'attention sur l'article 8, paragraphe 2, de la charte des droits fondamentaux qui garantit à tous le droit de faire corriger les données le concernant.

16. Le client ne sera plus le seul à bénéficier des garanties en matière de protection des données. Les professionnels chargés d'exécuter les obligations de vigilance prévues dans la proposition de directive ou la collecte des données et la vérification nécessaires au virement des fonds bénéficieront également d'une protection adéquate contre la publication arbitraire de sanctions et de leurs données dans le cas où ils seraient considérés comme n'ayant pas remplis leurs obligations. La protection des données ne devrait pas être perçue comme un obstacle aux obligations relatives à la lutte contre le blanchiment de capitaux, mais comme une condition essentielle à la réalisation de cet objectif dans le respect du droit fondamental à la protection des données à caractère personnel de chacun.

17. Le CEPD souligne que ni la directive proposée ni le règlement proposé ne clarifient l'application des règles de l'Union en matière de protection des données aux activités de traitement particulières qui y sont associées et qu'aucune disposition de fond n'aborde les problèmes liés à la protection des données. Dans son avis, le CEPD demande l'introduction de garanties qui s'appliquent à chaque fois que des données à caractère personnel sont traitées.

18. Enfin, le CEPD relève que la protection des données a été citée parmi les préoccupations dans l'étude sur l'application du règlement relatif aux informations accompagnant les transferts de fonds [11] réalisée par la Commission. Cette étude recommande également de clarifier les exigences en matière de protection des données lors de l'élargissement du champ d'application du règlement relatif aux virements de fonds. À plusieurs reprises, l'étude d'impact accompagnant la directive proposée met en évidence les difficultés que les parties prenantes privées rencontrent en ce qui concerne «leur capacité à se conformer aux exigences en matière de lutte contre le blanchiment de capitaux, tout en respectant les règles visant à assurer un niveau élevé de protection des données à caractère personnel». Les difficultés recensées incluent le partage d'informations au sein d'un groupe d'entreprises, le consentement de la personne concernée, la conservation des informations, et l'insécurité juridique s'agissant du traitement des données LBC/FT[12] au sein des entités soumises à obligations. De même, le partage d'informations entre les cellules de renseignement financier est également perçu comme problématique.

2.2. Conséquences

Référence à la législation applicable en matière de protection de données

19. Le CEPD insiste sur le fait qu'il est essentiel d'évoquer explicitement dans une disposition de fond des propositions la législation européenne applicable en matière de protection des données. Une simple référence aux principes généraux

[11] DG Marché intérieur et services (MARKT) de la Commission européenne, *Study on the application of the Regulation on information accompanying transfers of funds*, MARKT/2011/054/F (uniquement disponible en anglais).
[12] Lutte contre le blanchiment de capitaux et le financement du terrorisme.

dans les considérants[13] ne saurait être considérée comme suffisante. Cette disposition de fond est nécessaire pour des raisons de sécurité juridique, afin d'éviter tout ambiguïté quant au fait que les propositions ne doivent pas être considérées comme des dérogations au cadre sur la protection des données, qui reste pleinement applicable aux traitements envisagés. Le CEPD recommande donc d'indiquer explicitement que les propositions sont sans préjudice de la législation applicable en matière de protection des données. Par souci de clarté, le CEPD préconise en outre que les références à ladite législation soient regroupées dans une seule disposition de la directive proposée et du règlement proposé respectivement.

20. Il convient de faire référence aux lois nationales mettant en œuvre la directive 95/46/CE, ainsi qu'à l'applicabilité du règlement (CE) nº 45/2001, en raison de la participation des autorités européennes de surveillance.

21. Un bon exemple de disposition de fond figure à l'article 22 de la proposition de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché[14], qui prévoit explicitement une règle générale prévoyant que (les règles nationales mettant en œuvre) la directive 95/46/CE (et le règlement (CE) nº 45/2001) s'applique(nt) au traitement des données à caractère personnel dans le cadre de la proposition.

22. Le CEPD rappelle que le considérant 33 de la directive proposée se réfère à la décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[15]. Cette décision-cadre s'applique, sous réserve de plusieurs exceptions, au traitement des données 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.

23. Le CEPD fait remarquer que les propositions sont fondées sur l'article 114 du TFUE (marché intérieur) et non sur son article 87 (coopération policière). Ce choix de base juridique implique que les activités prévues dans le cadre des propositions n'incluent pas les activités des autorités compétentes dans les États membres au sens de l'article 87 du TFUE, parmi lesquelles figurent la police, la douane et les autres services répressifs spécialisés chargés de la prévention et la détection des infractions pénales ainsi que des enquêtes y afférant.

24. En conséquence de ce choix de base juridique, la décision-cadre du Conseil ne serait pas applicable dans le cadre des propositions. Au contraire, le traitement de données à caractère personnel dans le cadre de la lutte contre le blanchiment de capitaux engloberait les activités des prestataires de services du marché intérieur[16] et non «un traitement de données à caractère personnel ayant pour objet la sécurité

[13] Actuellement les considérants 30 et 34 de la directive proposée et le considérant 7 du règlement proposé.

[14] Proposition de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, présentée par la Commission (COM(2011) 651). Le texte est en cours d'examen par le Parlement européen et le Conseil conformément à la procédure législative ordinaire.

[15] JO L 350, 30.12.2008, p. 60.

[16] Arrêt du 10 février 2009, rendu par la Cour de justice dans l'affaire C-301/06, Irlande/Parlement européen et Conseil de l'Union européenne, Recueil 2009, p. I-00593, point 91.

publique et les activités de l'État relatives à des domaines du droit pénal»[17]. De ce fait, toutes les traitements relèveraient de la directive 95/46/CE et du règlement (CE) nº 45/2001, et la référence faite à la décision-cadre du Conseil dans le considérant perdrait sa raison d'être et devrait être supprimée. Le CEPD saluerait davantage de cohérence à cet égard.

25. Cependant, ce résultat ne peut être obtenu que si «les autorités compétentes» et les «cellules de renseignement financier» mentionnées dans la directive proposée ne constituent pas des autorités au sens de l'article 87 du TFUE et, en tout état de cause, que si leurs activités ne relèvent pas de la coopération policière. La directive 95/46/CE et le règlement (CE) nº 45/2001 ne seraient pleinement applicables que dans ce scénario. Les observations formulées concernant les autorités compétentes et les cellules de renseignement financier (voir les points 29 à 32) doivent être considérés dans ce contexte.

Autres conséquences

26. Le CEPD rappelle qu'il est essentiel de préciser la législation applicable en matière de protection des données, mais que cela ne suffit pas. Les références à cette législation devraient être précisées dans des garanties concrètes qui s'appliqueront à toute situation dans laquelle le traitement de données à caractère personnel est envisagé (à ce sujet, voir les points 62 et suivants).

27. De plus, toutes les spécifications relatives aux principes de protection des données qui seront formulées dans le cadre de la lutte contre le blanchiment de capitaux devront être justifiées. Par exemple, la période de conservation des données qui sera fixée devra correspondre à une nécessité avérée de conserver les données pendant un certain temps. De même, les droits des personnes concernées ne doivent être restreints qu'en vertu d'une exception fondée sur une nécessité décrite et expliquée, et à condition que cette restriction soit strictement limitée par les justifications apportées. Par ailleurs, la proportionnalité de la publication systématique des sanctions administratives n'est pas évaluée.

28. Le CEPD souhaite en outre attirer l'attention sur le fait qu'il est indispensable de respecter le principe de proportionnalité, ce qui signifie dans le présent contexte, qu'il importe d'assurer un juste équilibre entre deux intérêts différents, à savoir la lutte contre le blanchiment de capitaux d'un côté, et la protection des données à caractère personnel d'un individu de l'autre.

2.3. Observations générales communes

2.3.1. Les «autorités compétentes» et les «cellules de renseignement financier»

29. La directive proposée prévoit l'échange d'informations, et éventuellement celui de données à caractère personnel, entre les cellules de renseignement financier (CRF)

[17] Arrêt du 30 mai 2006, rendu par la Cour de justice dans les affaires C-317/04 et C-318/04, Parlement européen/Conseil de l'Union européenne (C-317/04) et Commission des Communautés européennes (C-318/04), Recueil 2006, p. I-04721.

des différents États membres, entre les autorités compétentes et l'ABE, l'AEAPP et l'AEMF[18], ainsi qu'entre les CRF et la Commission (voir articles 46 à 53).

30. Ni la directive proposée ni la troisième directive relative au blanchiment de capitaux ne définissent le concept d'«autorités compétentes», et les définitions des deux premières directives en la matière ne précisent pas la nature de ces autorités. La première directive relative au blanchiment de capitaux (91/308/CEE)[19] définit les autorités compétentes comme suit: «les autorités nationales habilitées, en vertu d'une loi ou d'une réglementation, à contrôler les établissements de crédit ou les institutions financières». Aux termes de la deuxième directive relative au blanchiment de capitaux (2001/97/CE)[20], le concept d'«autorités compétentes» signifie «les autorités nationales habilitées, en vertu d'une loi ou d'une réglementation, à surveiller l'activité de tout établissement ou personne relevant de la présente directive».

31. La nature des cellules de renseignement financier nécessite également quelques éclaircissements. L'article 31 de la directive proposée indique que la CRF est censée être une cellule nationale centrale chargée de recevoir (et, dans la mesure de ses pouvoirs, de demander), d'analyser et de communiquer aux autorités compétentes les informations concernant un éventuel blanchiment de capitaux ou les infractions principales liées, un éventuel financement du terrorisme ou toute information requise par les dispositions législatives ou réglementaires nationales. L'article 49 ne clarifie pas davantage leur nature en posant que les CRF sont des «autorités répressives, judiciaires ou hybrides». En réalité, la nature des CRF peut varier d'un État membre à l'autre et prendre la forme d'agences d'organes quasi policiers ou de services d'entités simplement chargées d'une mission de surveillance financière[21].

32. Afin de garantir l'homogénéité et l'efficacité de la protection des données, et au regard de la base juridique choisie pour les propositions[22], il ne devrait y avoir aucun doute sur le fait que les activités des autorités compétentes et des CRF relevant de la directive proposée seront exclusivement soumises aux dispositions nationales appliquant la directive 95/46/CE. Le CEPD recommande donc d'insérer dans la directive proposée une définition des concepts d'«autorités compétentes» et de «CRF» qui précisera, à tout le moins, que les «autorités compétentes» visées dans la directive proposée ne doivent pas être assimilées aux «autorités compétentes» au sens de l'article 2, point h), de la décision-cadre 2008/977/JAI[23].

---

[18] Autorité bancaire européenne (ci-après «ABE»), Autorité européenne des assurances et des pensions professionnelles (ci-après «AEAPP») et Autorité européenne des marchés financiers (ci-après «AEMF»).

[19] Directive 91/308/CE du 10 juin 1991 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 166, 28.6.1991, p. 77-83.

[20] Directive 2001/97/CE du Parlement européen et du Conseil, du 4 décembre 2001, modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JO L 344, 28.12.2001, p. 76-82.

[21] Sur la liste des membres du Groupe Egmont, un groupe informel créé en 1999 et réunissant des CRF, figurent par exemple un département de la Banque d'Italie, la CRF britannique (UKFIU) au sein de l'Agence de lutte contre la grande criminalité (SOCA - Serious Organised Crime Agency), TRACFIN au sein du ministère français de l'économie et des finances. Voir www.egmontgroup.org.

22 Voir plus haut points 27 à 30.

[23] Décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350, 30.12.2008, p. 6071.

Même si celles-ci peuvent accomplir des tâches similaires à celles d'autorités répressives, elles ne devraient pas être considérées comme des autorités policières ou judicaires dans le cadre des activités couvertes par la directive proposée.

2.3.2. Base légale du traitement des données et principe de limitation de la finalité

Motifs légitimes de traitement

33. Le CEPD constate que de la directive proposée pose au considérant 32 que la lutte contre le blanchiment de capitaux et le financement du terrorisme est reconnue par tous les États membres comme un intérêt public important. Toutefois, cette reconnaissance ne revêt aucune pertinence pour le motif légitime justifiant le traitement de données visé à l'article 7, point e) de la directive 95/46/CE. Dans le cadre de la directive proposée, il serait plus approprié que le motif légitime justifiant le traitement de données à caractère personnel soit la nécessité de se conformer à une obligation légale pour les entités soumises à obligations, les autorités compétentes et les CRF (à savoir, l'article 7, point c) de la directive 95/46/CE). Dans un souci de sécurité juridique, le CEPD propose d'ajouter cette précision au considérant.

Principe de limitation de la finalité

34. Le CEPD salue le fait que le considérant 31 de la directive proposée s'attache au respect du principe de limitation de la finalité, dans la mesure où il prévoit que la seule finalité du traitement doit être la prévention du blanchiment de capitaux et du financement du terrorisme. Les données ne doivent pas faire l'objet d'un traitement ultérieur à des fins incompatibles. Le CEPD rappelle que la directive 95/46/CE interdit de traiter ultérieurement les données à caractère personnel collectées pour des finalités déterminées, explicites et légitimes, de manière incompatible avec ces finalités (article 6, paragraphe 1, point b). L'avis récemment adopté par le groupe de travail «Article 29» sur la limitation de la finalité[24] explique les critères sur lesquels l'évaluation de la compatibilité de la finalité devrait se fonder. Plus particulièrement, des facteurs tels que les répercussions du traitement ultérieur sur l'individu et leurs éventuelles conséquences négatives concrètes sont considérés comme les signes d'une utilisation probablement incompatible.

[24] Avis 3/2013 du groupe de travail «Article 29» sur la limitation de finalité, adopté le 3 avril 213, p. 26, disponible (en anglais uniquement) à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Concernant l'interdiction du traitement des données collectées aux fins de la lutte contre le blanchiment de capitaux à des fins commerciales

35. Le considérant 31 de la directive proposée et le considérant 7 du règlement proposé prévoient que le traitement des données à caractère personnel à des fins commerciales est interdit[25]. Le CEPD souligne l'existence d'un risque de «détournement de finalité» susceptible de mener à une utilisation ultérieure, à des fins commerciales ou de marketing, des données collectées initialement aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Pour ces raisons, la référence faite dans les considérants ne peut être considérée comme suffisante. À cet égard, le CEPD recommande que l'interdiction spécifique de traiter les données à des fins commerciales soit intégrée dans une disposition de fond de la directive proposée et du règlement proposé.

L'éventuelle intégration des infractions fiscales pénales à la liste des activités criminelles visées par la directive

36. Le CEPD note la proposition d'ouvrir la liste des «activités criminelles» pouvant être considérées comme des infractions principales liées au blanchiment d'argent (article 3, paragraphe 4, point f), de la directive proposée) aux infractions fiscales pénales. Cet ajout a son importance par rapport à l'exigence pour les entités soumises à obligations d'informer les CRF compétentes lorsqu'elles savent, soupçonnent ou ont des motifs raisonnables de soupçonner que des fonds proviennent d'une activité criminelle (article 32). Selon l'exposé des motifs[26], utiliser le fruit d'une activité considérée comme infraction fiscale pénale conformément à la définition de l'article 3, paragraphe 4, point f) devrait également être considéré comme du blanchiment de capitaux. Par conséquent, les entités soumises à obligations devront informer promptement les CRF.

37. Toutefois, le CEPD constate un manque de cohérence flagrant avec les propos ultérieurs de l'exposé des motifs, selon lequel «[l]e renforcement des obligations de vigilance à l'égard de la clientèle dans le cadre de la lutte contre le blanchiment contribuera aussi à la lutte contre la fraude et l'évasion fiscales»[27]. La directive proposée se réfère ici à la communication de la Commission concernant la lutte contre la fraude et l'évasion fiscales[28] qui affirme que le renforcement de l'obligation de diligence à l'égard de la clientèle et l'amélioration de la transparence des informations concernant les bénéficiaires effectifs pourraient également «faciliter le recours à des données utiles aux fins de la fiscalité, par exemple pour accroître l'efficacité du traitement des structures d'investissement offshore au titre de la directive de l'Union sur la fiscalité de l'épargne».

---

[25] À ce sujet, voir: l'étude sur l'application du règlement relatif aux informations accompagnant les virements de fonds (*Study on the application of the Regulation on information accompanying transfers of funds*, MARKT/2011/054/F, uniquement disponible en anglais, p. 97: «toute communication exhaustive d'informations sur le bénéficiaire est susceptible de violer les droits à la protection des données et à la vie privée des clients et pourrait faire l'objet d'abus commis à des fins commerciales par les prestataires de services de paiement qui reçoivent ces informations (ceux-ci pourraient utiliser ces informations pour contacter directement les clients de leurs concurrents».

[26] Exposé des motifs, p. 5.

[27] Exposé des motifs, p. 5.

[28] Communication de la Commission, Plan d'action pour renforcer la lutte contre la fraude et l'évasion fiscales, adoptées par la Commission le 6 décembre 2012, COM(2012)722 final, p. 10.

38. Le CEPD estime que ces mentions dans l'exposé des motifs n'ont pas et ne devraient pas avoir pour effet d'inclure la lutte contre l'évasion fiscale parmi les finalités du traitement de données au titre des propositions. Cet avis procède du principe généralement applicable de limitation de la finalité consacré dans la directive 95/46/CE et expliqué ci-dessus. L'effet juridique de l'intégration des infractions fiscales pénales à la liste des infractions principales élargirait en effet l'obligation d'information aux cas où les entités soumises à obligations savent ou soupçonnent qu'une infraction fiscale est à l'origine d'un transfert de fonds, alors que les objectifs généraux des propositions, à savoir la lutte contre le blanchiment de capitaux et le financement du terrorisme, resteraient inchangés. Afin d'éviter toute ambiguïté et dans un souci de sécurité juridique, le CEPD recommande que cet aspect soit clarifié dans un considérant consacré à cette question.

2.3.3. Échange de données avec des pays tiers

39. Les deux propositions impliquent d'importants échanges de données à caractère personnel avec des pays tiers qui ne garantissent pas nécessairement un niveau de protection suffisant en la matière.

40. Les règles régissant le transfert de données à caractère personnel vers des pays tiers sont définies aux articles 25 et 26 de la directive 95/46/CE. Ces articles interdisent le transfert de données à caractère personnel lorsque le niveau de protection garanti dans le pays du destinataire n'est pas adéquat et soumettent le recours aux exceptions à des conditions rigoureuses. L'article 26, paragraphe 1, de la directive 95/46/CE, prévoit un nombre limité de motifs pouvant justifier le transfert de données à caractère personnel vers des pays tiers par dérogation au principe d'adéquation prévu à l'article 25.

41. Par ailleurs, l'avis du groupe de travail «Article 29» sur l'interprétation de l'article 26 de la directive 95/46/CE[29] fait valoir qu'une société multinationale ne devrait pas effectuer «des transferts importants de données vers un pays tiers sans prévoir un cadre approprié à cet effet, alors qu'elle a les moyens pratiques d'assurer cette protection (par exemple, un contrat, une règle d'entreprise contraignante, une convention)»[30]. Le groupe de travail «Article 29» recommande que les transferts de données à caractère personnel pouvant être qualifiés de répétés, massifs ou structurels ne soient, dans toute la mesure du possible et justement en raison de ces caractéristiques, effectués que si des garanties adéquates sont prévues, lesquelles pourraient prendre la forme de contrats ou de règles d'entreprise contraignantes.

Transferts au titre de la directive proposée

42. Dans le cadre de la directive proposée, des transferts internationaux de données à caractère personnel peuvent avoir lieu au sein d'entités soumises à obligations qui ont des succursales ou de leurs filiales détenues à majorité dans des pays tiers

[29] Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE, adopté le 25 novembre 2005 (2093-01/05/FR), disponible à l'adresse suivante: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_fr.pdf

[30] Voir note 29, page 9.

(article 42, paragraphe 2). Il se peut, par exemple, que ces entités doivent communiquer à leurs succursales ou filiales des données relatives à l'obligation de vigilance à l'égard de la clientèle afin de partager des informations sur les activités de certains clients.

Transferts au titre du règlement proposé

43. Lorsque le prestataire de services de paiement du bénéficiaire est établi en dehors de l'Union, le prestataire de services de paiement du donneur d'ordre veillera à accompagner tout virement de fonds d'un montant supérieur à 1 000 EUR du nom, du numéro de compte, de l'adresse, du numéro national d'identité du donneur d'ordre, ou de son numéro d'identification de client ou de ses date et lieu de naissance, et du nom et du numéro de compte du bénéficiaire [31]. Ce transfert de données à caractère personnel peut être qualifié de répété (car accompagnant chaque virement de fonds répondant aux critères ci-dessus), massif (la quantité de données potentiellement recueillies est assez considérable), et structurel (le transfert de données est une règle commune et ne peut être considéré comme une exception). De surcroît, les données concernant le donneur d'ordre et le bénéficiaire seront collectées et transférées en plus grand nombre lorsque les fonds sont virés de l'Union vers des pays tiers (informations complètes) que quand le virement est effectué au sein de l'Union (informations simplifiées)[32].

Conséquences

44. Compte tenu du transfert de données à caractère personnel répété, massif et structurel qui sera effectué dans le cadre de la directive et du règlement proposés, le CEPD recommande d'inclure des dispositions de fonds consacrées au transfert des données à caractère personnel en vue de garantir une protection adéquate des personnes concernées lorsque les données sont transférées.

45. Malheureusement, l'article 42 de la directive proposée est très flou sur les transferts de données et laisse, en tout état de cause, une large marge de manœuvre aux entités soumises à obligations qui pourraient toujours faire valoir que l'application des exigences en matière de protection des données dans les pays tiers ne serait pas compatible avec la législation locale.

46. Le problème du manque de garantie quant au niveau de protection adéquat des données à caractère personnel qui font l'objet d'un transfert massif vers des pays

[31] L'article 4 dresse la liste des informations relatives au donneur d'ordre et au bénéficiaire qui doivent accompagner le virement de fonds. L'article 5 limite la quantité des données transférées lorsque les prestataires de services de paiement du donneur d'ordre et du bénéficiaire sont tous deux établis au sein de l'Union mais requiert, à l'inverse, qu'un ensemble complet de données, tel que celui défini à l'article 4, soit communiqué si le prestataire de services de paiement du bénéficiaire est établi en dehors de l'Union, sauf dans le cas des exceptions figurant à l'article 6.

[32] Ces propos figurent dans les considérants 11 et 12. Voir également l'étude sur l'application du règlement relatif aux informations accompagnant les transferts de fonds, p. 88: «dans le cas de virements de fonds dans des pays qui n'offrent pas ou peu de garanties contre l'utilisation ou l'abus des informations ou leur transfert à des tiers par l'institution destinataire, le risque pour la personne concernée pourrait être considérable. Comme environ 85 % des transactions traitées par la société de services de transfert d'argent et de valeurs A sont destinées à des pays hors Union, y compris des pays dotés de systèmes juridiques faibles, cet aspect est une véritable préoccupation pour elle».

tiers n'est abordée qu'au considérant 32 de la directive proposée, qui souligne que la lutte contre le blanchiment de capitaux et le financement du terrorisme est reconnue par tous les États membres comme un intérêt public important. De même, le considérant 7 du règlement proposé souligne que le transfert de données à caractère personnel est nécessaire pour des raisons importantes d'intérêt public. Les deux propositions suggèrent donc que si ces transferts poursuivent un intérêt public important, ils relèveraient des dérogations prévues à l'article 26, paragraphe 1, point d), de la directive 95/46/CE et seraient donc conformes à la législation en matière de protection des données.

47. Le CEPD estime qu'on ne peut justifier le recours à la dérogation prévue à l'article 26, paragraphe 1, point d), en affirmant que le transfert s'effectuera en vertu d'un intérêt public important. Les transferts effectués au titre d'un intérêt public important ne peuvent être autorisés qu'au terme d'une évaluation minutieuse au cas par cas[33]. Le CEPD recommande donc d'insérer une disposition de fond dans la directive proposée, ainsi que dans le règlement proposé, offrant une base légale appropriée aux transferts intragroupes/entre prestataires de services de paiement qui respecte l'esprit et la lettre de l'article 26 de la directive 95/46/CE.

2.3.4. Publication des sanctions administratives

48. Aux termes de l'article 56, paragraphe 2, point a), de la directive proposée, et de l'article 18, paragraphe 2, point a) du règlement proposé, les États membres devraient au moins inclure dans la liste des sanctions prévues en cas de certains manquements[34] «une déclaration publique qui précise l'identité de la personne physique ou morale et la nature de l'infraction».

49. Les deux textes prévoient également la publication automatique dans les meilleurs délais des sanctions ou des mesures appliquées à la suite d'infractions, y compris l'identité des personnes responsables (article 57 de la directive proposée et article 19 du règlement proposé). Cette publication peut être évitée si elle est «de nature à compromettre sérieusement la stabilité des marchés financiers». Si cette publication risque de causer «un préjudice disproportionné aux parties en causes», les sanctions devraient également être publiées sous une forme anonyme. Cette obligation s'appliquera aux personnes physiques, mais les catégories de données qui devront être collectées et publiées ne sont pas précisées.

50. Comme le CEPD l'a souligné à plusieurs reprises[35], la publication obligatoire et automatique des sanctions, telle qu'elle est formulée actuellement, ne satisfait pas

[33] Comme le CEPD l'a déjà fait valoir dans son avis du 7 mars 2012 sur le paquet de mesures pour une réforme des règles en matière de protection des données, points 225 à 227.
[34] Relatifs aux règles en matière de vigilance à l'égard de la clientèle, de signalement des transactions suspectes, de conservation des informations, et de contrôles internes.
[35] Voir par exemple, l'avis du contrôleur européen de la protection des données sur les propositions de la Commission relatives à une directive du Parlement européen et du Conseil concernant les marchés d'instruments financiers abrogeant la directive 2004/39/CE du Parlement européen et du Conseil et à un règlement du Parlement européen et du Conseil concernant les marchés d'instruments financiers modifiant le règlement sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux, disponible sur le site Internet du CEPD à l'adresse:

aux normes de la législation en matière de protection des données telles qu'elles ont été clarifiées par le jugement de la Cour de justice dans l'affaire *Schecke*. Il convient de garder à l'esprit que, pour évaluer la conformité aux normes de protection des données d'une disposition imposant la divulgation publique d'informations personnelles, il est crucial que la publication concernée serve une finalité claire et bien définie. Seule une finalité claire et bien définie permet d'apprécier si la publication de données à caractère personnel envisagée est effectivement nécessaire et proportionnée. Dans ce contexte, la clause habituelle présente à l'article 17, paragraphe 1, qui prévoit que les États membres arrêtent des sanctions «efficaces, proportionnées et dissuasives» n'est pas suffisante. La Cour de justice a insisté sur le fait que les institutions devraient explorer différentes méthodes afin de trouver celle qui serait cohérente avec l'objectif de la publication, tout en compromettant le moins possible le droit des personnes concernées de voir leur vie privée respectée et la protection de leurs données à caractère personnel.

51. Le CEPD considère par exemple que la finalité, la nécessité et la proportionnalité de la publication automatique des sanctions ne sont pas évaluées comme il le faudrait. En tout état de cause, des garanties adéquates protégeant contre les risques qui pèsent sur les droits des personnes auraient dû être prévues. Dans ce contexte, le CEPD relève que, même si les sanctions peuvent être publiées dans la plupart des États membres, cette publication n'est jamais automatique[36]. Par ailleurs, l'analyse d'impact n'indique pas si des méthodes moins intrusives que l'obligation de publier toute sanction ou mesure auraient pu garantir le même résultat par rapport à l'objectif poursuivi, tout en compromettant moins le droit à la vie privée des personnes concernées.

52. En outre, comme l'article 56, paragraphe 2, point a), de la directive proposée confère déjà aux autorités compétentes, parmi leurs pouvoirs de sanction, celui de publier une déclaration publique dénonçant la personne responsable et la nature de l'infraction, on ne voit pas très bien comment l'obligation de publication prévue à l'article 57 est liée au pouvoir de publier une déclaration publique au titre de l'article 56, paragraphe 2, point a).

53. La possibilité d'évaluer la nécessité d'une publication au cas par cas, à la lumière des circonstances spécifiques (par exemple la gravité et le type d'infraction), constituerait une approche plus proportionnée et, dès lors, une option préférable par rapport à la publication obligatoire et automatique dans tous les cas. Le texte de la directive proposée devrait donc être modifié en ce sens.

54. Des garanties sont également nécessaires en matière de droit des prévenus de contester une décision devant l'autorité compétente, ainsi qu'en ce qui concerne leur droit à la présomption d'innocence. Le texte de la directive proposée devrait préciser que les autorités compétentes sont tenues de prendre des mesures

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-10_Financial_instruments_FR.pdf.

[36] Analyse d'impact, pages 92 et 93, et annexe VIII, page 123 et sv. Il est également mentionné à la page 128 que presque toutes les parties prenantes du secteur public ont fait savoir que les sanctions disponibles sont suffisantes et proportionnées à la gravité du manquement.

appropriées pour préserver ces deux droits lorsque la décision est susceptible d'appel et qu'elle est finalement annulée par l'autorité compétente.

55. De plus, en cas de publication sur l'internet, la question particulière de savoir comment s'assurer que les informations ne sont pas maintenues en ligne plus longtemps que nécessaire et que les données ne peuvent être manipulées ou modifiées se pose. En outre, l'utilisation de moteurs de recherche externes comporte le risque que les informations puissent être sorties de leur contexte et diffusées sur et en dehors du web d'une façon difficilement contrôlable.

56. Au vu des considérations qui précèdent, le CEPD recommande d'évaluer d'autres options moins intrusives que l'obligation générale de publication et, en tout état de cause, de préciser dans la directive proposée:
    - la finalité de cette publication, si elle devait être maintenue;
    - les données à caractère personnel qui devraient être publiées;
    - que les personnes concernées doivent être informées avant la publication de la décision et se voir garantir le droit d'introduire un recours contre la décision avant qu'elle ne soit publiée;
    - qu'en vertu de l'article 14 de la directive 95/46/CE, les personnes concernées ont le droit de s'opposer pour des raisons légitimes de force majeure.

57. Les propositions devraient également prévoir que les autorités chargées de la publication doivent veiller à ce que les données à caractère personnel des personnes concernées ne sont maintenues en ligne que pendant une durée raisonnable, au terme de laquelle ces informations doivent être systématiquement effacées. Les textes devraient également faire le nécessaire pour que ces données soient actualisées régulièrement et que ces autorités veillent à ce que des mesures de sécurité et de protection adéquates soient mises en place, notamment pour protéger les personnes concernées contre les risques liés à l'utilisation de moteurs de recherche externes.

2.3.5. Conservation des données

58. La manière dont la question des périodes de conservation des données est abordée dans les propositions suscite quelques préoccupations.

59. Conformément à la directive 95/46/CE, les données échangées doivent seulement être conservées pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées[37] et être automatiquement supprimées une fois la période de conservation arrivée à expiration. Cette durée doit être justifiée et motivée.

60. L'article 39 de la directive proposée fixe à cinq ans la durée pendant laquelle les données à caractère personnel collectées au titre de l'obligation de vigilance à l'égard de la clientèle devront être conservées. De même, l'article 16 du règlement proposé prévoit que la période de conservation des données sera de cinq ans après l'exécution du paiement. Les deux articles ajoutent également que la législation

[37] Voir article 6, point d), de la directive 95/46/CE.

nationale des États membres ne peut prolonger la conservation des données «qui si cela est nécessaire à la prévention ou à la détection du blanchiment de capitaux et du financement du terrorisme ou aux enquêtes en la matière. La période de conservation maximale après la fin de la relation d'affaires ne dépasse pas dix ans».

61. Le CEPD constate que la période de conservation maximale de dix ans est trop générale. Il recommande donc que:
   - le critère de la nécessité de toute prolongation de la période de conservation soit précisé et/ou que des garanties procédurales soient ajoutées afin de s'assurer que les périodes de conservation de plus de cinq ans ne seront appliquées que dans des situations exceptionnelles et que la prolongation sera au maximum de cinq années supplémentaires;
   - les propositions prévoient que les données ne pourront être conservées au-delà de la fin de la période de conservation, indépendamment de la législation nationale;
   - la durée de la période de conservation choisie soit justifiée au cas par cas. Un considérant devrait préciser que, s'il appert que la période de conservation semble avoir été choisie de façon arbitraire, sans lien évident avec les obligations professionnelles ou pratiques, elle ne sera pas conforme aux exigences de la directive 95/46/CE.

3. OBSERVATIONS PARTICULIÈRES SUR LES PROPOSITIONS

3.1. Observations particulières sur la directive proposée

3.1.1. Limitation des droits des personnes concernées

62. Vu la nature potentiellement très intrusive des obligations prévues dans le cadre de la lutte contre le blanchiment d'argent, le droit des personnes concernées d'être informées, et les modalités des éventuelles restrictions de leurs droits devraient être clairement définies par la directive proposée. En outre, toute limitation des droits fondamentaux doit être justifiée et proportionnée. Le CEPD rappelle que le droit d'accès est un élément essentiel du droit fondamental à la protection des données, qui est expressément mentionné à l'article 8 de la charte des droits fondamentaux de l'Union européenne. Les exceptions doivent donc être interprétées de manière restrictive.

63. Le CEPD suggère de compléter la directive proposée par une disposition spécifiant qui sera chargé d'informer les personnes concernées et préconise d'introduire l'obligation pour les entités soumises à obligations d'informer le client à ce sujet en même temps que sur les conditions générales régissant la relation client/fournisseur.

64. Par ailleurs, l'article 38, paragraphe 1, de la directive proposée prévoit une dérogation générale au droit d'accès. Le CEPD relève que la seule justification est apportée au considérant 34, qui se réfère à la limitation des droits des personnes concernées conformément à l'article 13 de la directive 95/46/CE, laquelle est nécessaire ici afin d'éviter le risque de nuire gravement à l'efficacité de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Ajoutons que le libellé de l'exception relative aux déclarations de transactions suspectes prévue à l'article 38, paragraphe 1, est très large.

65. Du reste, l'article 38, paragraphe 1, ne contient pas les garanties requises. La disposition comporte une interdiction générale d'informer les personnes concernées, qui n'est aucunement circonscrite dans le temps. En raison des conséquences éventuelles que les enquêtes menées dans le cadre de la lutte contre le blanchiment de capitaux peuvent entraîner pour les personnes concernées, dont l'impossibilité d'établir une relation commerciale et de ce fait d'ouvrir un compte bancaire, cette interdiction générale sans limite de temps est disproportionnée. Par ailleurs, il semble également disproportionné de limiter des droits d'accès relativement aux déclarations de transactions suspectes qui seraient considérées comme non fondées ou non pertinentes ultérieurement. Il paraît difficile de justifier la limitation des droits d'accès des personnes concernées une fois qu'il a été établi que la déclaration de transaction suspecte est non pertinente ou non fondée, dans la mesure où la divulgation n'entraverait aucune espèce de prévention, de détection, d'enquête ou de poursuites d'éventuelles infractions pénales. Enfin, il est difficile de déterminer comment les entités soumises à obligations, les directeurs et les employés sont censés savoir si une enquête «pourrait être ouverte» par les autorités compétentes, les enquêtes menées par les services répressifs étant supposées rester secrètes et confidentielles. La disposition

ne précise pas quelle personne ou entité est chargée de déterminer si une enquête «pourrait être ouverte».

66. Le CEPD recommande que la directive proposée détaille davantage dans une disposition de fond y consacrée, les conditions dans lesquelles les droits des personnes concernées pourraient être limités ainsi que l'objectif poursuivi. Par ailleurs, il préconise l'introduction des délais et conditions suivants: si, au terme d'une période donnée après la déclaration à la CRF il a été décidé de ne pas mener d'enquête ou que l'alerte donnée ne s'est pas avérée pertinente, et à condition que la personne concernée n'éveille aucun soupçon, celle-ci devrait être informée qu'une vérification a été effectuée et pouvoir exercer ses droits d'accès et de rectification. Le CEPD prône également l'ajout d'une obligation pour les CRF d'avertir les entités soumises à obligations quand une déclaration ne sera pas suivie d'une enquête.

3.1.2. Évaluation des risques

67. La directive proposée crée l'obligation pour les États membres d'effectuer des évaluations des risques afin de leur permettre de détecter, comprendre et atténuer leurs propres risques (voir considérants 15, 16 et 17, ainsi les articles 7 et 8 à la section 2 de la proposition de directive).

68. Cependant, nonobstant la légitimité et la nécessité de ces évaluations des risques, le texte ne précise pas si ces évaluations porteront également sur les données à caractère personnel ou non. Cette ambiguïté est particulièrement patente à l'article 8, paragraphe 1, qui précise que les évaluations des risques réalisées par les entités soumises à obligation doivent tenir compte «de facteurs de risques tels que les *clients*, les pays ou les zones géographiques, les produits, les *services*, les *transactions* ou les canaux de distribution». Cette liste semble suggérer que le traitement des données à caractère personnel ne peut être catégoriquement exclu au moment de la préparation des évaluations des risques.

69. Dès lors, le CEPD recommande d'indiquer clairement si les évaluations des risques effectuées par l'autorité désignée et les entités soumises à obligations peuvent ou non comporter le traitement de données à caractère personnel.

70. Si le traitement de données personnelles est prévu, la directive proposée devrait exiger des États membres qu'ils introduisent les garanties nécessaires en matière de protection des données dans leurs législations nationales respectives. Les États membres devront notamment définir la finalité du traitement et les utilisations compatibles, identifier et limiter rigoureusement les entités qui auront accès aux évaluations des risques (la Commission, l'ABE, l'AEMF et l'AEAPP sur demande), garantir le droit d'accès et d'être informé à toutes les personnes concernées dont les données à caractère personnel pourraient être traitées, et enfin définir et limiter la période minimale de conservation des données à caractère personnel nécessaire à la réalisation de la finalité susvisée. La conservation ultérieure des évaluations des risques serait par exemple possible après qu'elles auraient été rendues complètement anonymes.

71. Conformément à l'article 7, paragraphe 5, les résultats des évaluations des risques effectuées par l'autorité désignée doivent être mis à la disposition de la Commission, de l'ABE, de l'AEMF et l'AEAPP à leur demande. Dans ce cas aussi, si ces rapports comportent le traitement de données à caractère personnel, leur traitement serait soumis au règlement (CE) nº 45/2001.

3.1.3. Obligation de vigilance à l'égard de la clientèle

Définir les données pouvant être collectées pour le respect de l'obligation de vigilance à l'égard de la clientèle afin de prévenir les décisions arbitraires et la discrimination

72. Les considérants 19, 20, 23 et 47, ainsi que le chapitre II (articles 9 à 28) de la directive proposée abordent la question de l'obligation de vigilance à l'égard de la clientèle, qui peut être simplifiée, renforcée ou remplie par des tiers.

73. Ce sujet est abordé de façon assez détaillée et les circonstances entourant l'obligation de vigilance à l'égard de la clientèle sont clairement définies (articles 9 et 10). Il est demandé à toutes les entités soumises à obligations [les établissements de crédit et financiers, les auditeurs, les membres de professions juridiques, les agents immobiliers, les prestataires de services de jeux de hasard, par exemple (article 2)] de soumettre leurs clients à ce contrôle rigoureux. Cependant, la directive proposée ne définit pas suffisamment le contenu concret dudit contrôle et les données à collecter sur le client dans le cadre de l'obligation de vigilance (il en va de même si cette dernière est renforcée ou simplifiée) et laisse une large marge de manœuvre aux entités qui opèrent ce contrôle, ce qui pourrait déboucher sur le traitement arbitraire ou excessif des données personnelles, voire sur le traitement de données sensibles.

74. Les résultats de ce contrôle peuvent priver certaines personnes de la possibilité, par exemple, d'ouvrir un compte bancaire ou d'établir une relation commerciale. Le CEPD est donc satisfait de la référence faite, au considérant 47, au principe de non-discrimination consacré à l'article 21 de la charte des droits fondamentaux de l'Union. Néanmoins, cette référence ne permet pas de cibler le type de données pouvant faire l'objet d'un traitement dans le cadre de l'obligation de vigilance à l'égard de la clientèle[38].

75. Le CEPD estime qu'il est important d'insérer dans le texte de la directive proposée une liste précise des informations qui doivent et ne doivent pas être prises en considération pour l'application des obligations de vigilance à l'égard de la clientèle (et notamment si le traitement doit ou non porter sur des données sensibles, comme on l'explique plus loin). Par ailleurs, le CEPD préconise l'utilisation de modèles de réponses à donner aux questions à choix multiple car cela empêcherait de prendre des décisions subjectives et assurerait une application uniforme de l'obligation à travers l'Union européenne. Les spécifications de ces modèles pourraient être précisées dans des arrêtés d'application ou dans des orientations.

[38] Les annexes II et III recensent uniquement les facteurs de risque en général.

76. Si cette approche ne peut être suivie, la directive proposée devrait au moins prévoir l'obligation pour les États membres de définir les données qui doivent et ne doivent pas être collectées par les entités soumises à obligations quand elles se conforment à l'obligation de vigilance à l'égard de la clientèle. Cependant, le CEPD souhaite attirer l'attention sur les risques d'insécurité juridique et d'incohérence entre États membres qui pourraient découler de l'absence de règles harmonisées au niveau européen.

Données sensibles

77. Il convient de souligner que le traitement de données sensibles décrit à l'article 8, paragraphe 1, de la directive 95/46/CE ne semble pas nécessaire aux fins de la directive proposée. Le texte lui-même ne mentionne pas la nécessité d'un tel traitement, mais, vu la définition de la notion d'«activité criminelle» formulée à l'article 3, on ne peut exclure que dans le cadre de l'obligation de vigilance, les entités soumises à obligations traitent des données sensibles concernant les clients, par ex. des données concernant des infractions, réelles ou soupçonnées, des condamnations pénales ou des mesures de sûreté au sens de l'article 8, paragraphe 5, de la directive 95/46/CE[39], auquel cas, la directive précitée exige que le traitement ne puisse être «effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national […]». Toujours est-il que la directive proposée n'aborde pas cette question.

78. Par ailleurs, les circonstances dans lesquelles l'obligation de vigilance doit être exécutée peuvent mener à une discrimination, si des données sensibles sont traitées sans réserve. Laisser aux entités soumises à obligations la possibilité de décider si elles ont besoin ou non de données sensibles pour se conformer à l'obligation de vigilance comporte le risque que celles-ci prennent des décisions arbitraires, comme priver les clients d'une certaine origine ethnique, qu'elles considèrent suspecte, ou des clients ayant différentes opinions politiques ou religieuses du droit d'effectuer des transactions.

79. Le CEPD estime qu'il est indispensable de clarifier dans la directive proposée si, oui ou non, des données sensibles au sens de l'article 8, paragraphe 1 de la directive 95/46/CE doivent être collectées aux fins des obligations de vigilance à l'égard de la clientèle. Si ce genre de traitement est nécessaire, les États membres devraient s'assurer qu'il est effectué sous le contrôle de l'autorité publique et que le droit national prévoit des garanties appropriées et précises.

Mesures de vigilance renforcées

[39] À cet égard, le CEPD tient à rappeler qu'il estime que les données relatives aux infractions soupçonnées sont considérées comme des données sensibles au sens de l'article 8 de la directive 95/46/CE, parce que ces informations peuvent mener les personnes devant les tribunaux civils, voire pénaux. Voir notamment l'avis sur les agences de notation de crédit https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-02-09_EU_US_Joint_Customs_FR.pdf, et en particulier le point 22, ainsi que l'avis sur l'ACAC, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf, point 32(ii).

80. Dans les cas définis aux articles 17 à 23 de la directive proposée et dans d'autres cas de risques plus élevés identifiés par les États membres ou les entités soumises à obligations, des mesures renforcées de vigilance à l'égard de la clientèle devront être appliquées. Sont visés en particulier les cas où la relation d'affaires est nouée ou la transaction conclue avec un établissement client situé dans un pays tiers, une personne locale ou étrangère exposée politiquement[40] ou une personne à qui sont ou ont été confiées des fonctions publiques importantes au sein d'une organisation internationale. L'obligation de vigilance renforcée est définie à l'article 16, paragraphe 2, comme l'obligation «*d'examiner, dans la mesure de ce qui est raisonnablement possible, le contexte et la finalité de toute transaction complexe d'un montant inhabituellement élevé ainsi que tout schéma inhabituel de transaction n'ayant pas d'objet économique ou licite apparent*». Les articles 18 et 19 prévoient la mise en place de «*procédures adéquates fondées sur les risques*», l'obtention «*d'un niveau élevé de leur hiérarchie l'autorisation de nouer et de maintenir une relation d'affaires*» et «*un suivi renforcé continu de la relation d'affaires*».

81. Le texte précise qu'en cas de mesures renforcées de vigilance, les membres de la famille immédiate et les personnes connues pour être étroitement associées aux personnes politiquement exposées pourraient également faire l'objet de ce contrôle (article 21). Le CEPD souligne que l'article 21 pourrait donner lieu à un examen approfondi des activités d'affaires et financières des membres de la famille ou des personnes connues pour être étroitement associées. Il recommande dès lors de limiter plus clairement les situations dans lesquelles les risques sont si importants qu'ils justifient des mesures de vigilance renforcée, et d'inclure des garanties procédurales contre les abus.

3.1.4. Confidentialité et protection des données

82. L'article 43 demande aux États membres d'imposer aux entités soumises à obligation d'adopter des mesures appropriées afin que les employés aient connaissance des dispositions en vigueur, y compris des exigences applicables en matière de protection des données. Ces mesures devraient inclure des programmes spéciaux de formation (article 43). L'article 45, paragraphe 2, exige que les États membres veillent à ce que le personnel des autorités compétentes nationales respecte des exigences professionnelles élevées en matière de confidentialité et de protection des données. Le CEPD se réjouit de ces dispositions qui mettent en exergue le devoir des employés travaillant avec des informations à caractère personnel relatives au blanchiment d'argent de respecter les principes de la protection des données et suggère que l'article 42 fasse également référence à la confidentialité, étant donné que les employés concernés seront associées aux procédures relatives à l'obligation de vigilance à l'égard de la clientèle.

[40] L'article 3, paragraphe 7, point a), définit les «personnes politiquement exposées étrangères» comme «les personnes physiques qui sont ou ont été chargées de fonctions publiques importantes par un pays tiers», et l'article 3, paragraphe 7, point b), définit «les personnes politiquement exposées nationales» comme «les personnes physiques qui sont ou ont été chargées de fonctions publiques importantes par un État membre».

3.1.5. Informations concernant le bénéficiaire effectif

83. L'article 29 prévoit que «[l]es États membres veillent à ce que les sociétés ou les entités juridiques établies sur leur territoire obtiennent et détiennent des informations adéquates, exactes et actuelles sur leurs bénéficiaires effectifs». D'autre part, l'article 30, traitant des fiduciaires, prévoit le traitement des données suivantes: l'identité du constituant, du ou des fiduciaires, du protecteur (le cas échéant), des bénéficiaires ou de la catégorie de bénéficiaires et de toute autre personne physique exerçant un contrôle effectif sur la fiducie. La seule indication (très générale) apportée par la directive proposée concernant les données à recueillir pour le respect de cette obligation figure au considérant 10, qui rappelle qu'il «est nécessaire d'identifier toute personne physique qui possède ou exerce le contrôle sur une personne morale».

84. Comme les données qui permettent d'identifier une personne physique peuvent être le nom, ainsi que les données biométriques ou un numéro d'identification, il est indispensable d'apporter plus de précisions à ce sujet. Le CEPD préconise donc d'insérer une disposition de fond dans la directive proposée, qui dresserait la liste des données d'identification qui doivent être collectées sur le bénéficiaire effectif, y compris lorsqu'il n'est pas question de fiducie, ou à tout le moins d'introduire l'obligation pour les États membres de définir des règles précises concernant les données relatives au bénéficiaire effectif que les entités soumises à obligations doivent collecter ou non.

3.1.6. Coopération et échange d'informations entre les CRF

85. La proposition de directive encourage la coopération et la communication entre les CRF (sous-section III, articles 48 à 54). La coopération mutuelle implique nécessairement des échanges d'informations, et dès lors, de données à caractère personnel éventuellement importantes sur les clients soupçonnés de blanchiment de capitaux ou de financement du terrorisme. Les considérants 39 et 40 prônent une amélioration de la coordination et de la coopération entre les CRF des États membres, notamment au moyen de dispositifs sécurisés pour l'échange d'informations, comme le réseau informatique décentralisé «FIU.net» et les techniques offertes par cet outil.

86. Vu la nature des données à caractère personnel concernées par les échanges envisagés (surtout si l'on considère que les données relatives à des infractions soupçonnées[41] seront collectées), il convient de prévoir des garanties spécifiques en matière de sécurité et de respect de la vie privée. Le CEPD salue le fait que l'article 52 exige des États membres qu'ils veillent à ce que les CRF prennent toutes les mesures nécessaires, notamment des mesures de sécurité, et fassent en sorte qu'aucune autre autorité, agence ou département n'ait accès aux informations échangées entre les CRF, sauf accord préalable de la CRF ayant fourni ces informations.

87. Le CEPD apprécie également qu'il soit spécifiquement exigé des États membres qu'ils veillent à ce que les CRF appliquent des «technologies sophistiquées» qui

[41] Voir point 87 ci-dessus et note de bas de page 45.

leur permettent de comparer leur données à celles des autres CRF, de façon anonyme, en assurant pleinement la protection des données à caractère personnel (article 53, paragraphe 2). Néanmoins, il suggère de remplacer les mots «technologies sophistiquées» par «technologies de pointe appliquant le principe de respect de la vie privée dès la conception». Le CEPD préconise également que la période de conservation des données échangées soit précisée et limitée au strict nécessaire au regard de la finalité du traitement; que l'actualisation des données soit assurée en désignant des agents chargés de cette tâche au sein des CRF, et que les moyens garantissant la sécurité des données traitées soient précisés.

3.2. Observations particulières sur le règlement proposé

3.2.1. Informations recueillies sur le donneur d'ordre et le bénéficiaire

88. Conformément à l'article 4 du règlement proposé, les prestataires de services de paiement doivent généralement accompagner tous les virements du nom et du numéro de compte du donneur d'ordre et du bénéficiaire, ainsi que l'adresse du domicile du donneur d'ordre. Chaque fois qu'un individu vire de l'argent depuis l'Union européenne vers un pays étranger, les données à caractère personnel de ce dernier seront envoyées au prestataire de services de paiement du bénéficiaire, y compris son nom complet, l'adresse de son domicile, ou ses lieu et date de naissance, ou son numéro national d'identité, ainsi que le numéro de la transaction.

89. Le CEPD se réjouit que l'article 4 précise les données à collecter sur le donneur d'ordre et le bénéficiaire, conformément au principe de réduction au minimum des données traitées décrit à l'article 6, point c), de la directive 95/46).

90. Il s'interroge toutefois sur la présence dans cette liste du numéro national d'identité et rappelle que l'article 8, paragraphe 7, de la directive 95/46/CE prévoit que «*[l]es États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement*». Le CEPD souligne que le traitement du numéro national d'identité est soumis à des restrictions et/ou des garanties particulières dans plusieurs États membres, et recommanderait par conséquent d'utiliser le numéro de transaction en lieu et place. Si cette option n'est pas envisageable, il convient de préciser à l'article 4 du règlement proposé que l'adjonction du numéro national d'identité aux données communiquées au prestataire de services de paiement du bénéficiaire est possible sous réserve d'une législation nationale plus stricte mettant en œuvre l'article 8, paragraphe 7, de la directive 95/46/CE.

91. Le principe d'exactitude des données décrit à l'article 6, point d), de la directive 95/46/CE requiert de vérifier que les données traitées sont correctes et ne contiennent aucune faute d'orthographe ou confusion. En outre, le vol d'identité est une préoccupation récurrente en matière de blanchiment d'argent. Par conséquent, le CEPD tient à insister sur le caractère essentiel de la vérification par le prestataire de services de paiement des informations concernant le bénéficiaire

d'une transaction avant de les communiquer[42] et se réjouit dans ce contexte de la précision apportée au considérant 14. Compte tenu du risque élevé d'inexactitude des données et le fait qu'il incombe au prestataire de services de paiement de s'assurer que les informations qu'il communique sont correctes, le CEPD salue également le fait que l'article 4, paragraphe 3, l'article 4, paragraphe 4, ainsi que les articles 7 et 12 instaurent une procédure de vérification visant à garantir que les données sont non seulement complètes, mais aussi correctes.

3.2.2. Accès aux informations / confidentialité

92. Les articles 16 et 17 de la directive 95/46/CE exigent que des garanties soient prévues afin d'assurer la confidentialité et la sécurité des données. Ainsi, les personnes qui accèdent aux données ne doivent pas les traiter, sauf sur instruction du responsable du traitement, et des mesures techniques et d'organisation appropriées doivent être mises en œuvre pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, etc. La confidentialité implique également l'application du principe du besoin d'en connaître, à savoir que seules les personnes qui doivent accéder aux données pour exercer leurs responsabilités professionnelles devraient y être autorisées.

93. À cet égard, le CEPD attire l'attention sur le fait que la confidentialité des données n'est pas mentionnée dans le règlement proposé. Compte tenu du volume considérable des données qui seront traitées du fait du règlement proposé, et compte tenu de l'extrême sensibilité du contexte, le CEPD préconiserait l'introduction d'une disposition prévoyant que «les informations sont uniquement accessibles aux personnes ou catégories de personnes désignées». Il recommande que celle nouvelle disposition exige des États membres qu'ils précisent dans le droit national la fonction que la personne doit occuper au sein de l'organisation pour pouvoir accéder aux données.

94. Le CEPD constate également qu'aucune disposition n'impose aux entités soumises à obligations de prendre des mesures appropriées pour garantir que le personnel a connaissance des normes applicables en matière de protection des données, et en particulier des normes de confidentialité et de sécurité (à l'instar de ce qui est prévu à l'article 42 et à l'article 45, paragraphe 2, de la directive proposée). Le CEPD recommande donc que soit introduite une disposition qui mette en lumière l'obligation pour le personnel travaillant avec des données à caractère personnel concernant le donneur d'ordre et le bénéficiaire de respecter la confidentialité des données traitées, ainsi que les normes applicables en matière de protection des données. En plus de cela, cette disposition devrait exiger des États membres qu'ils fassent en sorte qu'une formation spécifique soit dispensée au personnel régulièrement chargé de collecter des données à caractère personnel, et que des orientations lui rappelant ce qu'il peut ou ne peut pas faire - notamment quelles données peuvent ou ne peuvent pas être traitées dans ce contexte -, soient diffusées.

[42] L'importance de ce contrôle d'exactitude est mise en évidence dans l'étude sur l'application du règlement relatif aux informations accompagnant les virements de fonds (*Study on the application of the Regulation on information accompanying transfers of funds*, MARKT/2011/054/F, uniquement disponible en anglais), p. 97.

3.2.3. Obligations de coopération

95. L'article 15 prévoit l'obligation pour les prestataires de services de paiement de donner suite sans délai aux demandes d'informations qui leur sont adressées par les autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme de l'État membre et le considérant 20 souligne la nécessité de s'y conformer. Compte tenu de la nature des données à caractère personnel concernées par les échanges envisagés, il convient de prévoir des garanties. Celles-ci comprennent des normes de sécurité et de respect de la vie privée que les autorités auxquelles les données seront communiquées sont tenues de respecter. Il convient également de rappeler aux autorités que les informations échangées ne doivent pas être accessibles à d'autres autorités, agences ou départements qui n'y seraient pas autorisés. Le CEPD suggère donc d'ajouter une phrase à l'article 15 qui pourrait s'énoncer comme suit: «Des garanties spécifiques doivent être mises en place afin d'assurer que ces échanges d'informations respectent les normes applicables en matière de protection des données».

96. Le CEPD constate que l'article 15 associe les autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme des États membres aux tierces parties qui peuvent accéder aux données collectées, sur présentation d'une demande à cet effet. Il recommande de compléter l'article 15 afin de garantir qu'aucune autre autorité ou partie extérieure n'ayant aucun intérêt dans la lutte contre le blanchiment de capitaux et le financement du terrorisme n'accède aux données stockées.

3.2.4. Signalement des infractions

97. Le CEPD note que l'article 21 exige que les États membres mettent en place des mécanismes efficaces pour encourager le signalement des infractions aux dispositions du règlement proposé. Il apprécie l'article 21, paragraphe 2, point c), qui prévoit que les mécanismes précités comprennent la protection des données à caractère personnel, tant pour la personne qui signale les infractions que pour la personne mise en cause, conformément aux principes énoncés dans la directive 95/46/CE. Toutefois, le CPED suggère de compléter cette disposition en précisant à quelle autorité les infractions doivent être signalées et en exigeant l'application de mesures techniques et d'organisation appropriées afin de protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération ou la diffusion non autorisée.

4. CONCLUSIONS

98. Le CEPD reconnaît l'intérêt des politiques de lutte contre le blanchiment de capitaux pour la réputation économique et financière des États membres. Néanmoins, il souligne que l'objectif légitime d'assurer la transparence des sources de paiements, des dépôts et transferts de fonds afin de combattre le terrorisme et le blanchiment de capitaux doit être poursuivi dans le respect des normes applicables à la protection des données.

99. Les questions suivantes devraient être abordées dans les deux propositions:

- il faudrait insérer une référence explicite à la législation européenne applicable en matière de protection des données dans les deux propositions, au moyen d'une disposition de fond y consacrée qui mentionnerait en particulier la directive 95/46/CE et les législations nationales mettant en œuvre cette dernière, ainsi que le règlement (CE) nº 45/2001 s'agissant du traitement des données à caractère personnel par les institutions et les organes de l'Union européenne. Cette disposition devrait aussi indiquer explicitement que les propositions sont sans préjudice de la législation applicable en matière de protection des données. La référence à la décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, faite au considérant 33 devrait être supprimée;
- une définition des concepts d'«autorités compétentes» et de «CRF» devrait être intégrée à la directive proposée. Cette définition devrait constituer une garantie que les «autorités compétentes» ne seront pas assimilées aux «autorités compétentes» au sens de l'article 2, point h) de la décision-cadre 2008/977/JAI;
- il conviendrait de clarifier au considérant 32 que le motif légitime justifiant le traitement de données à caractère personnel devrait être la nécessité de se conformer à une obligation légale pour les entités soumises à obligations, les autorités compétentes et les CRF (article 7, point c) de la directive 95/46/CE);
- il faudrait rappeler que la seule finalité du traitement doit être la prévention du blanchiment de capitaux et du financement du terrorisme et que les données ne peuvent faire l'objet d'un traitement ultérieur à des fins incompatibles;
- l'interdiction particulière de traiter les données à des fins commerciales, qui est actuellement mentionnée au considérant 31 de la directive proposée et au considérant 7 du règlement proposé, devrait être inscrite dans une disposition de fond;
- il convient d'ajouter un considérant qui précise que la lutte contre l'évasion fiscale n'est incluse qu'en tant qu'infraction principale;
- s'agissant des transferts internationaux, il convient d'introduire des dispositions de fond consacrées aux transferts de données à caractère personnel qui offrent une base légale appropriée aux transferts intragroupes/entre prestataires de services de paiement dans le respect de l'esprit et de la lettre de l'article 26 de la directive 95/46/CE, une option soutenue par le groupe de travail «Article 29» sur la protection des données. Le CEPD préconise que l'on réévalue le caractère proportionnel de l'exigence de transfert massif de données à caractère personnel et d'informations sensibles vers des pays étrangers aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme et prône une approche plus proportionnée;
- s'agissant de la publication des sanctions, le CEPD recommande d'évaluer d'autres options moins intrusives que l'obligation générale de publication et, en tout état de cause, de préciser dans la directive proposée:
  - la finalité de cette publication, si elle devait être maintenue;
  - les données à caractère personnel qui devraient être publiées;

- que les personnes concernées doivent être informées avant la publication de la décision et se voir garantir le droit d'introduire un recours de la décision avant qu'elle ne soit publiée;
- qu'en vertu de l'article 14 de la directive 95/46/CE, les personnes concernées ont le droit de s'opposer pour des raisons légitimes de force majeure;
- des restrictions supplémentaires en ce qui concerne la publication en ligne;

- s'agissant de la conservation des données, il convient d'insérer une disposition de fond qui définira une période de conservation maximale que tous les États membres devront respecter, avec quelques spécifications supplémentaires.

100. En ce qui concerne la directive proposée, le CEPD recommande en outre:
- d'ajouter une disposition particulière rappelant le principe d'information des personnes concernées concernant le traitement de leurs données à caractère personnel (conformément aux articles 10 et 11 de la directive 95/46/CE) et précisant qui sera responsable d'informer les personnes concernées;
- de respecter le principe de proportionnalité quand les droits des personnes viennent à être restreints, en conséquence de quoi il convient d'ajouter une disposition particulière précisant les modalités selon lesquelles les droits des personnes concernées peuvent être limités;
- d'indiquer clairement si les évaluations des risques effectuées par l'autorité désignée et les entités soumises à obligations peuvent inclure ou non le traitement de données à caractère personnel. Le cas échéant, il convient d'assortir la directive proposée des garanties nécessaires en matière de protection des données;
- d'ajouter une liste précise des informations qui doivent ou ne doivent pas être prises en considération dans l'application des mesures de vigilance à l'égard de la clientèle. Il convient de préciser si oui ou non les données sensibles au sens de l'article 8, paragraphe 1, de la directive 95/46/CE doivent être collectées à cette fin. Si ce type de traitement s'avère nécessaire, les États membres devraient s'assurer que ce traitement sera effectué sous le contrôle de l'autorité publique et que le droit national prévoit des garanties appropriées et précises;
- de modifier l'article 21 afin de limiter plus clairement les situations dans lesquelles les risques sont à ce point importants qu'ils justifient des mesures de vigilance renforcée, et d'introduire des garanties procédurales contre les abus;
- de modifier l'article 42 pour qu'il fasse référence à la confidentialité, laquelle devrait être respectée par tous les employés associées aux procédures relatives à l'obligation de vigilance à l'égard de la clientèle;
- d'introduire une disposition de fond dressant la liste des types de données d'identification à collecter sur le bénéficiaire effectif, y compris lorsqu'il n'est pas question de fiducie.

101. En ce qui concerne le règlement proposé, le CEPD recommande en outre:

- de ne pas utiliser le numéro national d'identité en tant que référence sans réserves et/ou garanties, mais d'utiliser le numéro de transaction en lieu et place;
- de garder à l'esprit qu'il est important de respecter le principe d'exactitude des données décrit à l'article 6, point d) de la directive 95/46/CE, dans le cadre des procédures relatives à la lutte contre le blanchiment de capitaux;
- d'ajouter une disposition précisant que «les informations sont uniquement accessibles aux personnes ou catégories de personnes désignées»;
- d'ajouter une disposition relative au respect de la confidentialité et des obligations en matière de protection des données par le personnel qui travaille avec des informations personnelles concernant le donneur d'ordre et le bénéficiaire;
- de clarifier à l'article 15 qu'aucune autre autorité ou partie extérieure qui n'a aucun intérêt dans la lutte contre le blanchiment de capitaux ou le financement du terrorisme ne devrait accéder aux données stockées;
- de compléter l'article 21 en précisant à quelle autorité les infractions au règlement seront signalées et en exigeant l'application de mesures techniques et d'organisation appropriées afin de protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération ou la diffusion non autorisée.

Fait à Bruxelles, le 4 juillet 2013

(signé)

Giovanni BUTTARELLI