La révision de la quatrième directive anti-blanchiment à la lumière

Maxime Lassalle

ABSTRACT

The Commission's proposal for a directive amending the fourth AML directive raises numerous issues concerning respect of the rights to privacy and to protection of personal data. The main challenges are related to the creation of central and public registries of beneficial ownership information and to the extension of the powers of the financial intelligence units concerning access to financial data. The latter is of utmost concern, as this new power of access to personal data is not balanced with explicit legal guarantees. Financial data, however, are private data deserving adequate protection.

AUTHOR

Maxime Lassalle

Maître de conférences
Université de Bourgogne

CITE THIS ARTICLE

Lassalle, M. (2016). La révision de la quatrième directive anti-blanchiment à la lumière. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2016-023

Published in eucrim 2016, Vol. 11(4) pp 184 – 188

https://eucrim.eu

ISSN:

En 2015, le nouveau système européen de lutte contre le blanchiment de capitaux et le financement du terrorisme était adopté[1]. Quelques mois plus tard voilà que la Commission annonce déjà son intention de l'amender[2]. Ce projet s'explique en partie par les attaques terroristes qui ont touché le territoire européen en 2015 et en 2016. Il avait d'ailleurs été annoncé en février 2016 par la Commission dans son plan d'action pour renforcer la lutte contre le financement du terrorisme[3]. Il s'explique aussi par l'affaire des « panama papers », qui a convaincu la Commission d'agir plus fermement contre l'évasion fiscale et la fraude fiscale. L'analyse d'impact de ce projet soulève plusieurs questions relatives à la protection des droits fondamentaux et l'objectif de cet article est de les analyser. Il se concentrera sur les enjeux en matière de protection des données et de droit à la vie privée au sens de la charte des droits fondamentaux de l'Union européenne.

Le cadre européen de lutte contre le blanchiment de capitaux est basé sur la collecte et le traitement d'une quantité considérable de données personnelles par les entités assujetties et en particulier par les institutions financières[4]. Le nouveau projet présenté par la Commission repose toujours sur la même logique de collecte de données personnelles en l'approfondissant (I). L'un des éléments principaux du nouveau projet est qu'il entend grandement faciliter l'accès à ces données collectées par le secteur privé. L'accès à ces données nécessite un encadrement pour être compatible avec le respect du droit à la vie privée et du droit à la protection des données (II). Si la nécessité d'encadrer l'accès aux données relatives aux bénéficiaires effectifs a été prise en compte dans une certaine mesure par la Commission (III), il n'en va pas de même pour l'accès aux autres données financières collectées par les établissements financiers (IV).

I. Un approfondissement du système existant

Le système préventif de lutte contre le blanchiment de capitaux repose sur un élément essentiel : la collecte et la rétention par les institutions financières de quantités très importantes de données personnelles. Cette obligation est aujourd'hui imposée par l'article 40 de la quatrième directive anti-blanchiment qui prévoit que les institutions financières doivent conserver les données relatives à leurs clients pendant au moins cinq ans. Cette obligation n'est pas modifiée par le nouveau projet de la Commission. En revanche, le projet a bien d'autres incidences sur les droits fondamentaux, et la plupart d'entre eux sont analysés par l'analyse d'impact de la Commission. Ainsi, en souhaitant inclure les établissements d'échange de monnaies virtuelles dans le champ d'application de la directive, le projet augmente automatiquement la quantité de données collectées[5]. De même, le projet accroît le contrôle des instruments prépayés qui avait été mis en place par la quatrième directive, ce qui a pour conséquence un plus grand degré de contrôle de la part des institutions financières[6]. En outre, la proposition modifie la définition de bénéficiaire effectif d'une construction juridique en abaissant le seuil de participation requise dans la structure, augmentant ainsi la quantité d'informations recueillies par les entités assujetties[7]. De la même manière, l'obligation générale de *due diligence* est précisée dans le cas particulier des relations financières avec les pays tiers à haut risque, ce qui accroît le degré de contrôle appliqué par les institutions financières[8]. Pour toutes ces raisons, la quantité de données collectées et l'intensité du contrôle exercé sur leurs clients par les entités assujetties va augmenter. Cela renforce l'atteinte à la vie privée exercée par le système préventif de lutte contre le blanchiment de capitaux. Pour l'ensemble de ces propositions, la Commission renvoie au chapitre V de la quatrième directive anti-blanchiment[9] qui encadre le droit à la protection des données des clients des entités assujetties. Cet encadrement n'est lui-même pas entièrement satisfaisant et certains éléments pourraient être améliorés[10], mais de manière générale la lutte contre le blanchiment de capitaux et le financement du terrorisme justifie ces atteintes au droit à la vie privée et du droit à la protection des données[11].

En plus de cet approfondissement du système préexistant, d'autres bases de données sont créées. La Commission entend en effet faciliter et accélérer l'identification des détenteurs de comptes bancaires et de comptes de paiement. Il n'existe à l'heure actuelle pas d'obligation pour les Etats membres de mettre en place des systèmes centralisés permettant un accès rapide des autorités compétentes à ces données. Au niveau des Etats membres, on retrouve trois situations différentes. Soit (i) il existe un registre central permettant d'identifier directement les détenteurs de comptes bancaires et de paiement[12], soit (ii) il existe un système d'extraction de données qui permet d'accéder directement aux registres des comptes bancaires et de paiements enregistrés auprès des banques et des établissements de paiement[13], soit (iii) il est nécessaire de contacter l'ensemble des établissements bancaires et de paiement afin de leur demander de vérifier dans leurs registres s'ils ont ouvert un compte au nom d'une personne précise. Pour la Commission, ce dernier cas n'est pas satisfaisant car il empêche un accès rapide à ces données[14]. De ce fait, elle suggère de demander aux Etats membres de choisir entre un registre central et un système centralisé d'extraction de ces données[15]. La Commission est consciente de l'encadrement nécessaire afin de garantir le droit à la protection des données des personnes concernées par ces mécanismes de rétention des données[16]. Cependant, d'autres propositions visent à renforcer les possibilités d'accès aux bases de données financières et c'est ici que se situe le véritable enjeu pour les droits fondamentaux.

II. La nécessité d'encadrer l'accès aux données financières

L'accès aux données financières devrait tenir compte des exigences qui existent en matière d'encadrement de l'accès aux données personnelles par les autorités chargées de l'application de la loi. Dans son fameux arrêt *Digital Rights Ireland Ltd* [17], la Cour de justice de l'Union européenne avait fermement critiqué la rétention de données de toute personne « de manière généralisée »[18], sans que les personnes concernées se trouvent « même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales »[19]. L'obligation de rétention s'appliquait même « à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves » et sans prévoir d'exceptions pour les personnes protégées par le secret professionnel[20]. Ce qui est important ici, c'est que la rétention massive et indiscriminée de données personnelles n'est pas en tant que telle disproportionnée pourvu qu'elle soit accompagnée de « garanties strictes concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données »[21]. Outre la durée de rétention et la sécurité des données, l'encadrement de l'accès à ces données est une garantie primordiale pour la Cour. En particulier, elle exige la présence d'un « critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données »[22] et de « conditions matérielles et procédurales »[23] relatives à cet accès. La Cour souhaite également la présence d'un « critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès » et, surtout, d'un contrôle préalable permettant de limiter « l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi »[24]. Comme les métadonnées de communications, les obligations de rétention des données financières sont très générales et concernent l'ensemble des personnes qui font usage des services bancaires et financiers. Il n'existe pas d'exception, y compris pour les personnes soumises au secret professionnel, par exemple pour les avocats. L'accès à ces données doit donc aussi être strictement encadré.

Aujourd'hui, le système prévoit seulement que les entités assujetties sont chargées de détecter des comportements suspects et d'effectuer des déclarations d'opérations suspectes auprès des cellules de renseignement financier. Ces dernières se doivent alors d'analyser ces déclarations et peuvent pour cela accéder aux données financières nécessaires à leurs analyses avant de déterminer si l'ouverture d'une enquête pénale

est pertinente[25]. Avec le système actuel, l'accès aux données en l'absence de déclaration d'opération suspecte n'est pas encadré au niveau européen. Il est possible d'accéder à ces données dans le cadre d'une enquête pénale et les conditions de cet accès sont prévues par le droit national. L'encadrement de cet accès au niveau national laisse parfois à désirer[26] et a récemment retenu l'attention de la CEDH. En effet, l'accès à ces données doit faire l'objet d'une procédure susceptible de prévenir les abus, par exemple pour l'accès aux données bancaires des avocats ou aux données relatives à des personnes non visées par une enquête pénale[27]. Si la procédure d'accès en matière pénale relève des Etats membres et ne constitue pas l'objet de la proposition de la Commission, les pouvoirs d'accès aux données financières par les cellules de renseignement constituent bien, eux, l'objet de la proposition. Or, étendre ces pouvoirs via une Directive ne peut se faire sans respecter les conditions strictes prévues par l'arrêt *Digital Rights Ireland Ltd*. Cela est fait en ce qui concerne l'accès aux données relatives aux bénéficiaires effectifs.

III. L'identification des bénéficiaires effectifs

La quatrième directive anti-blanchiment avait été très innovante en imposant la création de registres centralisés pour faciliter l'accès aux informations relatives aux bénéficiaires effectifs des sociétés et autres entités juridiques[28] ainsi que des trusts et fiducies[29]. Cette nouvelle forme de collecte des données était justifiée par l'existence de preuves selon lesquelles ces structures étaient utilisées pour couvrir des activités illicites[30]. Les règles relatives à l'accès aux deux types de registres sont actuellement différentes. Contrairement au registre des sociétés et autres entités juridiques, l'accessibilité des données relatives aux trusts et fiducies n'est pas rendue obligatoire pour « toute personne ou organisation capable de démontrer un intérêt légitime »[31]. Cette différence de traitement est justifiée par le fait que les sociétés et autres entités juridiques ne sont utilisées que pour des fins strictement économiques, alors que les trusts peuvent aussi être utilisés pour d'autres raisons, par exemple en relation avec la gestion d'un patrimoine familial[32].

La Commission, motivée en cela par la récente affaire des « panama papers », entend désormais permettre un accès public à ces registres, non limité aux personnes pouvant démontrer un intérêt légitime[33]. La démonstration d'un intérêt légitime ne serait nécessaire que pour les trusts qui ne sont pas utilisés dans le cadre d'une activité purement économique[34]. Cette modification qui prévoit le principe d'un accès public a plusieurs objectifs, à savoir renforcer la transparence de l'information vis-à-vis des tierces personnes souhaitant engager une activité commerciale avec une certaine société ou structure juridique[35], faciliter l'accès de la presse et de la société civile à ces informations, renforcer la confiance dans l'intégrité du système financier et supprimer tout obstacle à l'accès aux données par les institutions financières et par les autorités compétentes y compris depuis des pays tiers[36]. La Commission estime que cette transparence peut contribuer à combattre l'abus de constructions juridiques. Cette proposition répond à une revendication de longue date de la société civile[37].

La Commission reconnaît que cette solution est risquée et mérite de plus amples analyses en ce qui concerne sa compatibilité avec la Charte des droits fondamentaux de l'Union européenne[38]. Cette crainte est justifiée. Le Conseil constitutionnel français vient de rendre une décision illustrant le risque de créer une base de données personnelles relative aux trusts et accessible librement. Le Conseil constitutionnel a estimé que constituait une ingérence dans le droit à la vie privée le fait de fournir dans un registre public des « informations sur la manière dont une personne entend disposer de son patrimoine »[39]. Bien qu'il reconnaisse que la mesure poursuit « l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscale »[40], il estime que l'atteinte est manifestement disproportionnée[41]. En effet, le législateur n'a pas « précisé la qualité ni les motifs justifiant la consultation du registre, n'a pas limité le cercle des personnes ayant

accès aux données de ce registre »[42]. On aurait pu estimer que les données disponibles, limitées aux noms de l'administrateur, du constituant, du bénéficiaire et à la date de la constitution du trust, étaient suffisamment limitées pour justifier la faible ingérence dans le droit à la vie privée. Cela étant, il est vrai que le système français allait plus loin que ce que propose la Commission. En l'espèce il s'agissait d'un trust purement privé et le Conseil d'Etat, dans sa décision de transmission de la question prioritaire de constitutionnalité, expliquait que la personne concernée faisait « valoir que la publication dans le registre litigieux de données personnelles la concernant, se rapportant notamment aux bénéficiaires des trusts qu'elle a constitués aux Etats-Unis en vue d'organiser la dévolution de ses biens après son décès, est susceptible de permettre à des personnes de son entourage d'avoir accès à des informations devant rester confidentielles jusqu'à l'ouverture de sa succession, et de les inciter à exercer sur elle des pressions en vue d'obtenir qu'elle modifie ces dispositions successorales, le cas échéant en reconsidérant la liste des bénéficiaires des trusts ainsi constitués »[43]. Cette décision du Conseil constitutionnel ne fait pas ressortir la spécificité des trusts « privés » et il est possible que la même décision serait prise dans le cas de ce que la Commission appelle les « business-type trusts » dont la transparence ne pourrait avoir de conséquences sur la vie privée. Malgré cela, il nous apparaît que le choix de la Commission est justifié et équilibré dans la mesure où il distingue les trusts qui, en raison de leur spécificité et de leur caractère privé, familial, ne peuvent être totalement transparents[44]. Plus problématique, la Commission ne s'est pas intéressée à l'encadrement de l'accès par les cellules de renseignement financier aux autres données financières collectées par les institutions financières.

IV. L'accès aux autres données financières

Selon le système actuel, les Etats membres sont libres de permettre aux cellules de renseignement financier d'accéder aux données financières détenues par les établissements financiers en l'absence de déclaration préalable par les entités assujetties[45]. En principe, les cellules policières ou judiciaires disposent de cette possibilité[46]. En effet, dans ces cas, le pouvoir d'accéder aux données financières étant déjà attribué à la police et/ou au parquet, il n'y a pas de raison pour que les cellules de renseignement financier n'en bénéficient pas. Ce pouvoir d'accès pour les cellules de renseignement financier de nature administrative est moins systématique, c'est ce qui manque dans le système actuel. Cela pose problème par exemple en matière de coopération internationale, lorsque des cellules administratives refusent d'accéder à des données dans le cadre d'une demande émanant d'une cellule judiciaire ou policière, par exemple. C'est cette situation que la Commission entend améliorer en exigeant de tout Etat membre qu'il accorde des pouvoirs d'accès plus large à sa cellule de renseignement financier, quelle que soit sa nature. La Commission entend ainsi « passer d'un système de divulgation fondé sur des suspicions à un système de divulgation davantage basé sur le renseignement »[47]. La Commission précise que la mesure peut être justifiée par une suspicion préalable issue de la propre analyse des cellules, de renseignements fournis par les autorités compétentes ou d'informations détenues par des cellules étrangères[48]. C'est un changement significatif[49]. Notons qu'une telle extension avait été envisagée en 2014 en France, afin de transformer la cellule de renseignement financier française en « un service de renseignement financier de plein exercice»[50].

Le système proposé par la Commission se rapproche dans une certaine mesure de ce qui a été mis en place aux Etats-Unis via le PATRIOT ACT. La section 314 (a) du PATRIOT Act permet à la cellule de renseignement financier américaine d'accéder aux données financières sur demande d'autres autorités enquêtant sur des faits soit de blanchiment de capitaux, soit de financement du terrorisme[51]. Cette disposition permet de contourner deux obstacles : l'absence de déclaration d'opération suspecte de la part des entités assujetties et les obstacles procéduraux à l'accès aux données financières via les voies classiques en matière de procédure pénale[52]. Avant d'en revenir à la proposition de la Commission, deux éléments du système améri-

cain méritent d'être précisés. Le premier élément est constitué par le fait que les Etats-Unis appliquent un système de protection de la vie privée en matière d'enquête qui est très différent du système européen. Les données financières ne bénéficient pas d'une protection constitutionnelle sur le fondement du quatrième amendement de la Constitution américaine[53]. De ce fait, le Congrès est absolument libre de permettre un accès à ces données qui ne soit pas enserrés dans des conditions strictes. Le deuxième élément important est que la section 314 (a) ne permet qu'un accès limité aux données financières. La cellule de renseignement financier américaine ne peut que demander aux établissements financiers de lui signaler si une certaine personne, celle qui fait l'objet de l'enquête, détient des comptes auprès de cet établissement, et si ces comptes ont permis d'effectuer des transactions dans les six derniers mois avec d'autres comptes dont l'identité sera, elle aussi, divulguée. Autrement dit, il ne s'agit d'accéder qu'à des « lead information » qui ne font qu'indiquer dans quelle direction les enquêteurs doivent diriger leur attention. Pour accéder aux informations relatives à toutes les transactions, en particulier aux relevés de compte enregistrés par les banques, il faudra alors passer par les procédures normales qui, elles, sont plus encadrées[54].

La proposition de la Commission ne s'embarrasse pas de limiter les pouvoirs qu'elle attribue aux cellules de renseignement financier. Elle renvoie purement et simplement au droit national qui doit encadrer ces mesures et se contente de rappeler les exigences très générales qui devront être respectées au niveau national, en particulier que l'ingérence doit être prévue par la loi[55]. Aurait-elle pu faire autrement ? Le problème vient du fait que les pouvoirs d'enquête tant des autorités compétentes en matière pénale que des cellules de renseignement financier dans le champ du renseignement relèvent en principe des prérogatives des Etats membres. Cependant, la Commission entend étendre les pouvoirs des cellules de renseignement financier via une Directive et doit en tirer les conséquences. De plus, comme l'a affirmé récemment l'avocat général Henrik Saugmandsgaard Øe « la raison d'être d'une obligation de conservation de données est de permettre aux autorités répressives d'accéder aux données conservées, de sorte que les problématiques de la conservation et de l'accès ne sauraient être complètement dissociées »[56]. En matière de données financières, l'obligation de rétention étant organisée dans une large mesure par la quatrième directive anti-blanchiment, n'aurait-il pas été pertinent d'accompagner la nouvelle proposition de lignes directrices en matière de garanties devant encadrer les pouvoirs des cellules de renseignement financier ?[57]

En guise de conclusion, une première garantie pourrait être proposée. Les nouveaux pouvoirs des cellules s'appliqueraient tant en matière de blanchiment de capitaux qu'en matière de financement du terrorisme[58], autrement dit il n'y aurait pas de limitation quant aux raisons qui peuvent justifier l'accès aux données. Or, cette nouvelle mesure étant justifiée par le besoin de coopération accru entre les cellules de renseignement financier en matière de lutte contre le financement du terrorisme, n'aurait-il pas été préférable de la limiter aux cas de financement du terrorisme, en écartant le blanchiment de capitaux ? Il est en effet peu discutable qu'en matière de financement du terrorisme, les entités assujetties soient bien moins à même de détecter des faits suspects dans la mesure où les capitaux utilisés sont généralement d'origine légale, alors qu'un tel problème ne se pose pas en matière de blanchiment de capitaux[59].

Plutôt que d'ignorer le problème en renvoyant à la responsabilité des Etats membres dans la transposition de la Directive, n'aurait-il pas été préférable de « rouvrir des débats fondamentaux »[60] en matière de lutte contre le financement du terrorisme afin de proposer un nouveau système ambitieux mais précisément encadré ? Cela aurait aussi permis de ne pas assimiler lutte contre le financement du terrorisme et lutte contre l'évasion fiscale, des objectifs différents qui appellent des réponses adaptées et donc vraisemblablement différenciées.

---

1. Directive 2015/849/EU relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et du financement du terrorisme (« la quatrième directive anti-blanchiment »), J.O. L 141/73, 5.6.2015.↩

2. Proposition de Directive modifiant la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme et la directive 2009/101/CE (la "proposition de directive"), COM (2016) 450 final↩
3. Communication de la Commission relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final.↩
4. Plutôt que de parler d'entités assujetties, nous limiterons nos propos aux établissements financiers.↩
5. Commission Staff Working Document, Impact Assessment accompanying the Proposal for a Directive of the European Parliament and the Council amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC ("l'analyse d'impact"), SWD(2016) 224 final, publié en anglais, p. 53; proposition de directive, p. 11.↩
6. Analyse d'impact, p. 60; proposition de directive, p. 11.↩
7. Analyse d'impact, p. 69-96.↩
8. Analyse d'impact, p. 46-47.↩
9. Ce chapitre est intitulé « Protection des données, conservation des documents et pièces et données statistiques.↩
10. G. Butterelli, Opinion off the European Data Protection Supervisor on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds, Bruxelles, 4 juillet 2013, p. 13, para. 65.↩
11. S. De Vido, « Anti-money laundering measures versus European Union fundamental freedoms and human rights in the recent jurisprudence of the European Court of Human Rights and the European Court of Justice », in *German Law Journal*, n° 5, vol. 16, 2015, p. 1271-1291; J. Böszörmenyi, E. Schweighofer, « A review of tools to comply with the Fourth EU anti-money laundering directive », in *International Review of Law, Computers and Technology*, n° 1, vol. 29, 2015, p. 63-77.↩
12. C'est le cas par exemple en France avec le fichier FICOBA.↩
13. C'est le cas par exemple en Allemagne : Voir l'analyse d'impact, p. 38.↩
14. Analyse d'impact, p. 22-24.↩
15. Proposition de directive, p. 14-15.↩
16. Analyse d'impact, p. 103.↩
17. CJUE, C-293/12 et C-594/12, *Digital Rights Ireland Ltd*, 8 avril 2014.↩
18. *Digital Rights Ireland Ltd*, para. 57.↩
19. *Digital Rights Ireland Ltd*, para. 58.↩
20. *Digital Rights Ireland Ltd*, para. 58.↩
21. Conclusions de l'avocat général Henrik Saugmandsgaard Øe, présentées le 19 juillet 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, para. 195.↩
22. *Digital Rights Ireland Ltd*, para. 60.↩
23. *Digital Rights Ireland Ltd*, para. 61.↩
24. *Digital Rights Ireland Ltd*, para. 62.↩
25. Ou éventuellement de transférer les informations à une autre autorité compétente.↩
26. J. Tricot, A. Nieto Martin, « Monitoring of Banking Transactions and Traffic Data, in K: Ligeti (ed.), *Toward a Prosecutor for the European Union*, Vol. II, Hart Publishing, 2016 (à paraître); M. Simonato et M. Lassalle, "A Fragmented Approach to Asset Recovery and Financial Investigations: a Threat to Effective International Judicial Cooperation, in Z. Durdević, E. Ivičević Karas (eds.), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, Croatian Association of European Criminal Law, 2016.↩
27. CEDH, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, 1er décembre 2015, n°69436/10.↩
28. Article 30 (3) de la quatrième directive.↩
29. Article 31 (3) de la quatrième directive.↩
30. Money Laundering Using Trust and Company Service Providers, FATF, 2010.↩
31. Article 30 (5) c) de la quatrième directive.↩
32. Proposition de directive, p. 17.↩
33. Proposition de directive, p. 16.↩
34. Le système proposé est assez complexe et passe par une modification de l'article 31 de la quatrième directive et par une modification de la directive 2009/101/CE.↩
35. Considérant 22 de la proposition de directive.↩
36. Considérant 23 de la proposition de directive.↩
37. Fifty shades of tax dodging, Eurodad, 2015, p. 38.↩
38. Analyse d'impact, p. 103.↩
39. Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.↩
40. Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para 5.↩
41. Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.↩
42. Conseil constitutionnel français, *Mme Helen S.*, Décision n°2016-591 QPC, 21 octobre 2016, para. 6.↩
43. Décision de renvoi du Conseil d'Etat, para. 9.↩
44. La dernière version du texte, négociée au Conseil, semble toutefois revenir sur l'aspect public au profit d'un accès limité aux personnes prouvant un intérêt légitime. La dernière version est accessible en ligne http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14884_2016_INIT&from=EN.↩
45. Voir à ce sujet : MONEYVAL, *The postponement of financial transactions and the monitoring of bank accounts*, Research report of the Council of Europe, April 2013.↩

46. Sur la typologie des cellules de renseignement financier, voir par exemple V. Mitsilegas, 'New Forms of Transnational Policing : The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights' in Journal of Money Laundering Control, vol.3, no.2, 1999, pp.147-160 and vol.3, no.3, 2000, pp. 250-259.↩
47. Communication de la Commission relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, COM (2016) 50 final, p. 8.↩
48. Considérant 4 de la directive proposée.↩
49. V. Mitsilegas et N. Vavoula, "The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law", *Maastricht journal of European and comparative law*, no. 2, 2016, p. 292.↩
50. Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014 de la délégation parlementaire au renseignement, Assemblée Nationale, 2014, p.49.↩
51. E. J. Gouvin, "Are There Any Checks And Balances On The Government's Power to Check Our Balances? The Fate Of Financial Privacy In The War On Terrorism", *Temple Political & Civil Rights Law Review*, Vol. 14, 2005, p. 517., E. J. Gouvin, "Bringing Out the Big Guns : The USA PATRIOT Act, Money Laundering, and the War on Terrorism", *Baylor Law Review*, Vol. 55, no. 3, 2003, p. 955.↩
52. En matière de procédure pénale, la protection des données bancaires est très importante aux Etats-Unis. Voir le Right to Financial Privacy Act, Titre XI du Financial Institutions Regulatory and Interest Rate Control Act adopté le 10 novembre 1978. Le Right to Financial Privacy Act est codifié au 12 U.S. Code chapitre 35, para. 3401 et s.↩
53. Miller v. United States, 425 U.S. 435 (1976).↩
54. E. J. Gouvin, "Are There Any Checks And Balances On The Government's Power to Check Our Balances? The Fate Of Financial Privacy In The War On Terrorism", Temple Political & Civil Rights Law Review, Vol. 14, 2005, p. 517, s. p. 535-537.↩
55. Analyse d'impact, p. 53; proposition de directive, p. 63.↩
56. Conclusions de l'avocat général Henrik Saugmandsgaard Øe, présentées le 19 juillet 2016, C-203/15 et C-698/15, *Tele2 Sverige AB*, para. 125.↩
57. CCBE comments on the proposal of 5 July 2016 to amend Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, Conseil des barreaux européens, 2016, p. 3.↩
58. La version issue des négociations au Conseil permet de confirmer cela, alors que la proposition de la Commission ne visait que le blanchiment de capitaux. La dernière version est accessible en ligne http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14884_2016_INIT&from=EN.↩
59. T. Krieger, D. Meirrieks, "Terrorism: causes, effects and the role of money laundering", in B. Unger, D. van der Linde (eds.), Research Handbook in Money Laundering, Cheltenham, Northampton, Edward Elgar, 2013, p. 78; GAFI, Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme, 24 avril 2002, p. 3, point 9.↩
60. M. Wesseling, Evaluation of EU measures to combat terrorism finance, In-depth analysis for the LIBE Committee, Parlement européen, Bruxelles, p. 32.↩

COPYRIGHT/DISCLAIMER
© 2018 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union