

TRANSFERTS DE FONDS

ET PRÉVENTION DU BLANCHIMENT DE CAPITAUX

ET DU FINANCEMENT DU TERRORISME



GUILLAUME BÈGUE

Conseiller stratégique Sentinel Analyses & Solutions Membre du centre de droit financier Université de Paris I (Panthéon-Sorbonne)

La possibilité de remonter la trace de mouvements de fonds est l'un des piliers de la lutte contre la criminalité financière internationale. Les opérations de blanchiment de capitaux mais aussi et surtout de financement de terrorisme s'en trouvent ainsi plus risquées et donc plus difficiles à mettre en œuvre pour leurs auteurs. À cet effet, un règlement vient renforcer l'arsenal normatif européen désormais conforme aux standards internationaux en ce domaine, et consacre les acteurs intervenant dans les circuits de paiements comme douaniers des flux bancaires internationaux. Depuis le 15 décembre 2007, des sanctions peuvent théoriquement être prononcées à l'encontre des assujettis ne respectant pas les obligations prévues. Il semble dès lors primordial de rappeler le contenu de ce règlement qui, s'il n'a eu que peu de retentissement sur le grand public, aura mobilisé la communauté bancaire et financière pendant de longs mois.

INTRODUCTION

Dans certaines conditions, les virements peuvent représenter un outil privilégié pour ceux qui souhaitent, de manière anonyme ou quasi-anonyme, faire évader le produit d'une infraction pénale du territoire d'où il a été tiré. Dans cette

hypothèse, ils sont un formidable moyen de dissimuler l'origine de fonds en brouillant les pistes, surtout quand le nom du donneur d'ordre du transfert n'y apparaît pas. Ainsi, lorsque des fonds d'origine ou à des fins criminelles, sans indication du donneur d'ordre, transitent de comptes bancaires en comptes bancaires, sur trois continents différents et ce, en l'espace d'une semaine, comment exercer une vigilance appropriée et permettre à des enquêteurs de remonter rapidement le circuit emprunté par ces fonds? Même si cette remontée pourra être effectuée, elle se fera inéluctablement moins rapidement que dans le cas où ledit message aurait été renseigné de cette donnée. Pis encore, comment détecter des messages financiers filtrés au regard des listes de présumés terroristes actuellement en vigueur lorsque, justement, aucun nom ni indication alphanumérique intelligible n'apparaissent dans ce message?

Si l'on se cantonne à l'activité de blanchiment de capitaux, nous sommes ici dans la deuxième phase du « cycle de blanchiment ». Communément admis, ce cycle est par ailleurs constitué d'une première phase dite de placement (pénétration du système bancaire et financier afin de convertir les fonds sales) ainsi que d'une troisième appelée phase d'intégration (ancrage dans le tissu économique par le biais d'investissements). La phase intermédiaire, celle de l'empilage, consiste quant à elle à éloigner les fonds de leur source afin de masquer leur origine. Cette deuxième phase peut notamment se concrétiser par de nombreux transferts de fonds initiés par exemple d'un pays ou territoire à la réglementation laxiste sur le fait de mentionner le nom du donneur d'ordre dans les messages financiers. Ces fonds transiteront ensuite par plusieurs pays pour être finalement crédités sur un compte ouvert dans les livres d'un établissement tout à fait respectable. Les multiples jeux d'écritures entre banques correspondantes, alliés à des conversions en devises, parachèveront encore un peu plus le souhait d'effacer toute trace de l'origine véritable des fonds incriminés.

Aussi, l'insertion et la conservation tout au long du circuit emprunté, du nom du donneur d'ordre dans les messages financiers appaurent comme une priorité aux yeux des experts européens en charge de la mise en place d'un

cadre global cohérent de lutte contre le blanchiment de capitaux et le financement du terrorisme. C'est la raison pour laquelle le règlement CE n° 1781/2006 fut adopté le 15 novembre 2006¹.

Tout l'enjeu du présent règlement réside non pas tant à briser l'anonymat qui prévalait jusqu'ici dans de nombreux messages financiers qu'en l'amélioration de la capacité des enquêteurs à remonter la trace de flux à l'origine douteuse ou à la destination maléfique.

Peu de textes auront suscité tant d'efforts et mobilisé tant d'énergies au sein de la communauté des spécialistes des flux bancaires au cours de ces dernières années. A l'instar de la directive européenne sur les services de paiement (« SEPA »), la transposition en droit communautaire de la recommandation spéciale n° 7 du GAFI (ci-après RS VII) aura été un chantier entrepris quelques années auparavant, pour aboutir à une rédaction acceptable aux yeux de protagonistes aux intérêts divergents.

Il s'agira dès lors, préalablement à l'exposé de son champ d'application (II), de s'intéresser à la genèse ainsi qu'au fondement d'un texte qui recèle des débats insoupçonnés (I), pour enfin en détailler les obligations (III). Il conviendra d'aborder pour chacune de ces parties les difficultés rencontrées et de mentionner quelques-unes des multiples conséquences tant opérationnelles que juridiques engendrées par ce règlement.

I. GENÈSE ET FONDEMENT DU RÈGLEMENT

Le règlement ne s'est pas fait en un jour. C'est une évidence pourra-t-on penser de prime abord, mais vraiment, on est loin d'imaginer les turpitudes attachées à son élaboration. Ce texte se distingue tant par la richesse des discussions pré-conceptuelles dont il a fait l'objet durant plusieurs années, que par les nombreuses versions des *guidelines* qui lui sont attachées. Ces dernières, élaborées par les experts du European Payment Council (EPC), sont une véritable balise d'orientation sur la façon de mettre en œuvre juridiquement mais aussi et surtout techniquement les dispositions prévues. On aura l'occasion d'abuser des références à ce document, véritable fil d'Ariane pour des assujettis insatisfaits des réponses données par le seul règlement. Il faut avouer que ce texte et son « mode d'emploi », représentent l'aboutissement d'un long processus de réflexion sur l'adaptation d'une norme internationale qui fait maintenant l'unanimité parmi les acteurs du monde des flux.

1. Origine du règlement et enjeu politique

a. La recommandation spéciale VII du GAFI et sa note interprétative

Le règlement trouve son origine dans la *soft law* (« droit mou ») internationale puisqu'il est directement inspiré d'une

disposition émanant du Groupe d'action financière sur le blanchiment des capitaux (GAFI). En effet, le 30 octobre 2001, le GAFI dévoilait huit recommandations spéciales destinées à la lutte contre le financement du terrorisme, celles-ci étant au nombre de neuf aujourd'hui.

L'une d'entre elles, la RS VII, porte sur les informations qui doivent figurer dans les messages financiers². Considérée comme lacunaire par les professionnels de la banque, elle fut agréementée d'une note interprétative le 14 février 2003 qui s'est elle-même avérée trop imprécise.

Dès lors, des travaux menés de concert avec les institutions bancaires du monde entier furent entrepris par l'instance internationale, pour aboutir à la révision de la note interprétative de la RS VII. Une nouvelle mouture de cette note fut publiée, avec comme principal point d'achoppement la question du seuil en dessous duquel il n'était pas imposé d'inclure les renseignements exacts et pertinents concernant le donneur d'ordre. Ce seuil avait été fixé à 3 000 dollars dans la première note interprétative.

L'instauration d'un tel seuil de minima avait été justifiée, entre autres, par le travail fastidieux qui aurait été de renseigner les très nombreux messages inférieurs à ce montant. Les messages supérieurs à ce montant, eux, devaient être renseignés de manière exhaustive. Mais ce seuil ne recueillait pas tous les suffrages, notamment parmi les banques européennes.

b. L'enjeu des négociations

Ainsi, lorsque l'idée d'un règlement fit son apparition, les banques européennes, par la voie de la commission européenne, ont formulé des avis sur la pertinence de la note interprétative de 2003 afin d'atteindre un certain degré de cohérence et d'harmonisation dans l'interprétation de la note sur la RS VII. En effet, ladite note prévoyait une évaluation de l'efficacité et de la justification du maintien du seuil de 3 000 dollars après un an à compter de sa publication, deux éléments fortement contestés par le camp du vieux continent.

À cet égard, le secteur bancaire européen a toujours tenu une position claire et constante en ce qu'il requerrait la suppression de tout seuil d'exonération quel que soit son niveau. À l'inverse, les États-Unis suivis par le Mexique, le Japon et le Canada justifiaient le maintien d'un tel seuil afin d'éviter que les opérations de leurs migrants (entre le Mexique et les États-Unis notamment) n'empruntent des circuits alternatifs non contrôlés.

Toujours est-il que les négociations entre les instances américaines et la commission européenne ont abouti seulement à la réduction du seuil de 3 000 à 1 000 dollars/

1. Règlement CE n° 1781/2006 du Parlement européen et du Conseil relatif aux informations concernant le donneur accompagnant les virements de fonds du 15 novembre 2006, publié au JOCE le 8 décembre 2006 (JO L 345, p. 1-9).

2. La RS VII est rédigée comme suit : « Les pays devraient prendre des mesures afin d'obliger les institutions financières, y compris les services de remise de fonds, à inclure des renseignements exacts et utiles relatifs au donneur d'ordre (nom, adresse et numéro de compte) concernant les transferts de fonds et l'envoi des messages qui s'y rapportent. Les renseignements devraient accompagner le transfert ou le message qui s'y rapporte tout au long de la chaîne de paiement. Les pays devraient prendre des mesures pour s'assurer que les institutions financières, y compris les services de remise de fonds, mettent en œuvre une surveillance approfondie et un suivi aux fins de détection des activités suspectes des transferts de fonds non accompagnés de renseignements complets sur le donneur d'ordre (nom, adresse et numéro de compte) ». Pour plus d'information, V. le site du GAFI : www.fatf-gafi.org. V. également G. Bègue, Note interprétative de la recommandation spéciale VII du GAFI : un pas de plus dans la lutte contre le financement du terrorisme?, La Lettre Sentinelle n° 27-28, juin-juillet 2005, p. 6.

euros. Pour les virements inférieurs à ce nouveau seuil, la nouvelle note interprétative prévoit que les pays n'ont pas l'obligation d'imposer aux institutions financières d'identifier et de vérifier les données ou de transmettre des informations relatives au donneur d'ordre. Un bémol apparaît en ce que les pays peuvent néanmoins exiger que les virements en réception contiennent des informations précises et complètes sur le donneur d'ordre, les messages non conformes pouvant faire l'objet d'un rejet.

L'enjeu était de taille, dans la mesure où les dispositions de la note interprétative avaient vocation à être transposées, notamment dans le futur règlement. Le problème était alors de les adapter au système bancaire européen et à ses membres que la commission européenne ne voulait pas voir dans une situation passive lors de la réception des virements inférieurs au seuil, ni dans une position trop tranchée d'un rejet systématique des messages non renseignés. Toutes ces préoccupations étaient depuis longtemps discutées au sein des groupes de travail européens en vue de l'adoption du règlement. À cet égard, il est certain qu'une indication plus claire du GAFI aurait été appréciée, au lieu d'une reconduite de seuil agrémentée d'une simple alternative.

c. Une bataille politique

Cela pose plus précisément la question des rapports de force entre pays ou groupe de pays au sein des organisations internationales, et notamment du GAFI. En effet, cette entité est une instance internationale, dont la France et les États-Unis sont des membres influents. Comme dans toute instance collégiale à fort retentissement politique, il est délicat voire difficile de trouver un compromis qui puisse satisfaire tous les participants.

C'est pourtant ce à quoi le GAFI semblait avoir abouti. « Semblait », seulement, car en réalité, le compromis trouvé n'était qu'une victoire de l'Amérique sur l'Europe, et ne réjouissait à l'époque aucunement les banques européennes et en particulier les banques françaises qui devaient s'adapter aux nouveaux critères imposés par leurs homologues anglo-saxonnnes.

Cette énième domination des lobbyistes américains peut paraître surprenante car, nonobstant le degré d'avancement normatif des États-Unis dans ce domaine³, l'Europe et la France sont considérées à juste titre comme des plus en pointes en matière de lutte globale contre le terrorisme et son financement. Pourtant, rien n'y a fait, la voix du lobby bancaire américain aura été plus forte que celle des banques établies de ce côté-ci de l'Atlantique et ce, malgré le relais de la commission européenne ainsi que la présidence française du GAFI durant cette période.

2. Contextes nationaux et modalités d'adoption

À l'échelle internationale, aucune insertion d'information n'était imposée jusqu'en 2001, la fourniture de renseignements devenant une réalité qu'avec l'avènement de la RS VII. Cependant, tel que susmentionné, cette disposition

n'est qu'une norme de *soft law* avec pour seule arme coercitive le poids politique de l'entité qui peut se targuer d'en détenir la paternité. Peu de pays étaient donc enclins à l'appliquer, pour peu qu'ils étaient au courant de l'existence d'une telle norme. Cependant, certains ont incorporé très rapidement une telle obligation dans leur corpus juridique, sans compter ceux ayant une longueur d'avance.

a. État des législations nationales

C'est le cas des États-Unis où une disposition similaire existait déjà avant la rédaction des recommandations spéciales du GAFI : l'article 31 CFR 103.33 du Bank Secrecy Act, entré en vigueur le 28 mai 1996⁴. Cette disposition se révèle être parmi les premières à prévoir une obligation d'insertion de renseignements dans certains messages financiers. Plus connue sous le vocable de *travel rule*, elle préfigure la RS VII du GAFI en fixant un seuil de 3 000 dollars ou l'équivalent en toute autre devise au-delà duquel le nom, l'adresse et le numéro de compte du donneur d'ordre doivent apparaître, hormis quelques exceptions fondées principalement sur la qualité des donneurs d'ordre et des bénéficiaires (établissements de crédit américains). Comme évoqué précédemment, ce seuil est l'illustration de la volonté américaine de ne pas contrôler la grande majorité des autres virements inférieurs à ce seuil.

À l'automne 2001, le gouvernement américain renforcera sensiblement cette disposition avec le Patriot Act et notamment sa section 328 qui prévoit la prise de mesures raisonnables afin d'encourager les gouvernements étrangers à mettre en place des législations similaires⁵.

En Europe, certains pays ont préféré ne pas attendre un texte coercitif tardant à venir et ont en quelque sorte transposé la RS VII en droit interne. Le fait de mentionner le nom d'un donneur d'ordre dans les messages financiers n'est donc pas une totale nouveauté pour certains droits d'États membres de l'Union. C'est par exemple, le cas du Luxembourg. Le point 145 al. 2 de la circulaire CSSF 05/211 du 13 octobre 2005 prévoit « L'obligation d'incorporer aux virements et transferts de fonds ainsi qu'aux messages s'y rapportant, soit le nom soit le numéro de compte du donneur d'ordre. [...] Sont visés tous les virements et transferts, à savoir nationaux, hors UE et intra-UE au départ de l'établissement de crédit ou du PSF luxembourgeois »⁶.

En Suisse, l'ordonnance de la Commission fédérale des banques en matière de lutte contre le blanchiment d'argent en date du 18 décembre 2002 prévoit en son article 15 intitulé « Indication des donneurs d'ordre lors de virement » que « pour tous les virements effectués vers l'étranger, l'intermédiaire financier

4. V. le site du Financial Crime Enforcement Network (FinCEN) : www.fincen.gov.

5. Le texte en langue anglaise se présente comme suit : Sec. 328. *International cooperation on identification of originators of wire transfers.* The Secretary shall—(1) in consultation with the Attorney General and the Secretary of State, take all reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the United States and other countries, with the information to remain with the transfer from its origination until the point of disbursement [...].

6. Contrairement à nombre d'idées reçues, le juris corpus luxembourgeois en matière de prévention des activités de blanchiment de capitaux et de financement du terrorisme est l'un des plus avancés du vieux continent. Pour un aperçu de la récente réglementation luxembourgeoise sur la prévention des activités de blanchiment de capitaux, V. G. Bègue, « Le droit luxembourgeois, nouveau référent dans la lutte contre le blanchiment de capitaux et le financement du terrorisme? », RD Banc. Fin., janvier-février 2006, p. 50.

3. La pléiade de textes législatifs qui ont suivi les attentats du 11 septembre 2001 (Patriot Act, Sarbanes-Oxleys Act,...) en témoigne.

indique le nom, le numéro de compte et le domicile du cocontractant donneur d'ordre ou le nom et un numéro d'identification de celui-ci » sachant que « l'intermédiaire financier peut renoncer à faire figurer ces indications pour des motifs légitimes, notamment en cas d'ordre permanent » devant « clarifier ces motifs et les documenter »⁷. Cette rédaction devrait évoluer d'ici au 1^{er} juillet 2008 étant donné le projet de modification de l'ordonnance précitée. La nouvelle mouture de cette disposition devrait être plus fidèle à la lettre de la RS VII du GAFI.

Mais ce type de législation faisait figure d'exception, par rapport à toutes les autres qui ne prévoyaient absolument rien en ce sens. On ose à peine citer le cas de la France, où aucune disposition similaire n'existait jusqu'au règlement, si ce n'est une simple obligation de se renseigner sur l'origine de fonds dont la transaction remplit les trois critères cumulatifs requis par l'article L. 563-3 al.1 du Code Monétaire et Financier rédigé de la manière suivante : « Toute opération importante portant sur des sommes dont le montant unitaire ou total est supérieur à une somme fixée par décret en Conseil d'État et qui, sans entrer dans le champ d'application de l'article L. 562-2, se présente dans des conditions inhabituelles de complexité et ne paraît pas avoir de justification économique ou d'objet licite, doit faire l'objet de la part de l'organisme financier ou de la personne mentionnés à l'article L. 562-1 d'un examen particulier. En ce cas, l'organisme financier ou la personne mentionnés à l'article L. 562-1 se renseigne auprès du client sur l'origine et la destination de ces sommes ainsi que sur l'objet de la transaction et l'identité de la personne qui en bénéficie ».

Ce n'est pas tant le bénéficiaire final du transfert que le donneur d'ordre bénéficiaire de l'opération qui est visé dans cette dernière phrase, ce qui nous permet de dire que c'était là les prémices d'une obligation générale et autonome telle qu'elle existe dorénavant. Mais son caractère partiel et inachevé est éloquent, sans oublier le fait que la présente situation est totalement différente, puisque s'inscrivant dans le cadre d'une obligation de vigilance, certes spécifique, mais d'une toute autre nature que celle qui a trait uniquement au donneur d'ordre⁸.

b. La nécessité d'élaborer une norme de droit communautaire

Dans la foulée de la vague normative états-unienne et des textes adoptés à l'échelle mondiale ainsi que des attentats (principalement de New York, Madrid et Londres) ou tentatives d'attentats, les communautés européennes ne pouvaient faire l'impasse sur ce sujet. Les avancées normatives en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme au niveau européen avec les trois dernières directives (2^e directive⁹ et 3^e directive¹⁰), la plus

récente étant la directive d'application¹¹ de cette dernière) servirent de catalyseur dans la rédaction du texte.

On peut s'interroger sur le fait de ne pas avoir opté pour l'incorporation de ce sujet dans la 3^e directive, ou à tout le moins sa simple évocation, dans la mesure où c'est dorénavant le texte de référence au sein de l'Union et que le projet du règlement était déjà sur les rails avant la fin du processus d'adoption de ladite directive. Cependant, cette volonté de traiter ce sujet indépendamment et ce, par le biais d'un règlement, n'est pas anodine.

En effet, les directives successives en ce domaine et notamment la 3^e, ne sont pas des textes de pleine harmonisation, laissant ainsi une marge de manœuvre et une certaine liberté aux États membres dans leur manière d'interpréter et de transposer leurs dispositions en droit interne.

À l'inverse, ce nouveau règlement, d'applicabilité directe dans les États membres, ne souffre aucune transposition de complaisance et va permettre ainsi une application coordonnée des dispositions prévues par ce règlement. Ce souci est clairement exprimé par le considérant 2 qui met en avant la nécessité d'une « transposition uniforme dans l'ensemble de l'Union européenne » de la RS VII du GAFI afin d'éviter toute « discrimination entre les paiements nationaux dans un État membre et les paiements transfrontaliers entre États membres ».

Le travail de rédaction du règlement se fit en plusieurs étapes. Les rédacteurs, assistés d'organismes de représentation des professionnels impactés de près ou de loin¹², ont pu présenter le 26 juillet 2005 une proposition de règlement à la Commission européenne¹³.

Un an plus tard, ce fut au tour du Parlement de donner son accord, pour une publication intervenant à la fin de la même année. Parallèlement, l'EPC fut extrêmement actif dans l'élaboration des très utiles *guidelines* précitées, orientant les assujettis dans le processus d'application concrète des dispositions.

3. L'objet du règlement

a. La lutte contre le terrorisme et ses moyens de financement

Initialement, la volonté d'imposer de telles obligations découle d'une considération unique : être capable de prévenir de manière plus efficace des projets d'attentats dont les commanditaires utiliseraient les circuits officiels de transferts de fonds. En témoigne la nature de la RS VII du

du blanchiment d'argent : bilan et préconisations à l'aube de la troisième directive », Bull. Joly Bourse, septembre-octobre 2004, p. 567 ; G. Bègue, « Lutte contre le blanchiment d'argent et le financement du terrorisme : les apports de la 3^e directive européenne », La Lettre Sentinel n° 27-28, juin-juillet 2005, p. 4 ; E. Gastebled, « État du dispositif juridique de lutte contre le blanchiment au lendemain de l'adoption de la troisième directive européenne », Banque & Droit n° 105 – Janvier-Février 2006, p. 3.

7. V. le site de la Commission Fédérale des Banques : www.ebk.admin.ch.

8. Pour plus de précision sur cette disposition, V. G. Bègue, « Lutte contre le blanchiment de capitaux et secret professionnel : extension des obligations de contrôle et de déclaration de soupçon », Revue Lamy Droit des Affaires, avril 2006, n° 4, p. 56.

9. 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 (JO L 344 du 28 décembre 2001, p. 0076-0082).

10. Directive 2005/60/CE du Parlement européen et du Conseil 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 (JO L 309 du 25.11.2005, p. 15). Pour une analyse de ces textes, V. C. Cutajar, « Prévention et répression

11. Directive 2006/70/CE du 1^{er} août 2006 portant mesures de mise en œuvre de la directive 2005/60/CE du Parlement Européen et du Conseil pour ce qui concerne la définition des « personnes politiquement exposées » et les conditions techniques de l'application d'obligations simplifiées de vigilance à l'égard de la clientèle ainsi que de l'exemption au motif d'une activité financière exercée à titre occasionnel ou à une échelle très limitée (JO n° L 214 du 04/08/2006 p. 0029 0034). Pour une étude fouillée de ce texte, V. G. Bègue, « Les conséquences en droit interne de la mise en œuvre de la directive 2005/60/CE relative à la prévention du blanchiment de capitaux et du financement du terrorisme », Revue Trimestrielle de Droit Financier, mars 2007, n° 1, p. 47.

12. Il faut souligner à cet égard le rôle majeur de l'EPC.

13. COM (2005) 343.

GAFI qui a été rédigée peu de temps après les attaques du 11 septembre 2001 et qui porte exclusivement sur le thème du terrorisme et non sur celui du blanchiment.

b. L'élargissement de l'objet initial du texte

Ce n'est qu'avec la réunion des notions de lutte contre le financement du terrorisme et de lutte contre le blanchiment de capitaux – certes différentes non seulement opérationnellement mais aussi juridiquement – que l'idée d'un texte à l'application beaucoup plus large est apparue. C'est ainsi que le règlement vise, à travers divers considérants, tant le blanchiment que le financement du terrorisme¹⁴.

Si cette dernière préoccupation l'emporte largement sur les autres, le texte fait également expressément mention du plan d'action élaboré par le Conseil européen du 21 septembre 2001 et révisé en 2004. Au-delà du seul thème du terrorisme, ce plan vise au renforcement de la coopération policière et judiciaire ainsi qu'à l'amélioration de la sécurité aérienne¹⁵.

C'est donc la stabilité et la réputation du système financier dans son ensemble qui est en jeu. Est plus précisément cité le bon fonctionnement du marché intérieur de l'Union, notamment dans le domaine financier, qui risque d'être compromis si de telles mesures ne sont pas respectées par les assujettis.

Littéralement, l'objet du règlement, défini à l'article 1, est d'établir « les règles relatives aux informations sur le donneur d'ordre qui doivent accompagner les virements de fonds, aux fins de la prévention, de l'enquête et de la détection des activités de blanchiment de capitaux et de financement du terrorisme ».

À première vue, la difficulté n'est pas flagrante et l'on ne peut soupçonner quelconque mise en œuvre d'un chantier pourtant conséquent. Ce n'est qu'au fur et à mesure de la lecture du règlement qu'apparaissent les contours de la somme de difficultés rencontrées. L'étude de son champ d'application nous en fournit les prémices.

II. LE CHAMP D'APPLICATION DU RÈGLEMENT

Bien que le règlement soit applicable aux virements, certains d'entre eux ne sont pas concernés en raison de leur faible exposition au risque de blanchiment ou de financement du terrorisme. Quant à son champ d'application géographique, il est loin d'être figé et à vocation à s'élargir.

1. Les champs d'application matériel et personnel

a. Le champ d'application *rationae materiae*

L'article 3 al. 1 du règlement prévoit qu'il « est applicable aux virements de fonds, en toutes monnaies, qui sont envoyés ou reçus par un prestataire de services de paiement établi dans la communauté ».

Il s'agit donc d'une application multidevises, aux virements de fonds qu'il faut comprendre comme « toute opération effec-

tuée par voie électronique pour le compte d'un donneur d'ordre par l'intermédiaire d'un prestataire de services de paiement (ci-après PSP) en vue de mettre des fonds à la disposition d'un bénéficiaire auprès d'un PSP, le donneur d'ordre et le bénéficiaire pouvant être ou non la même personne »¹⁶. Tant les flux domestiques que les flux internationaux sont impactés.

b. Le champ d'application *rationae personae*

Les assujettis sont les PSP, définis comme « les personnes physiques ou morales dont l'activité professionnelle comprend la fourniture de services de virements de fonds »¹⁷. Cette définition large comprend notamment les établissements de crédit ou les sociétés de transfert de fonds.

Le considérant 8 précise que « les personnes dont l'activité se limite à convertir des documents sous format papier en données électroniques et qui agissent en vertu d'un contrat conclu avec un PSP ne relèvent pas du champ d'application du règlement ». Il en va de même pour celles qui n'offrent que des systèmes de messagerie ou d'autres systèmes de support pour la transmission de fonds ou des systèmes de compensation et de règlement.

2. Les transferts exclus du périmètre

a. L'application de l'approche risque

Cependant, de nombreuses exceptions viennent restreindre ce champ d'application. C'est ainsi que le règlement n'est pas applicable :

- aux virements de fonds effectués à l'aide d'une carte de crédit ou de débit, à la double condition qu'ils soient accompagnés d'un identifiant unique, permettant de remonter jusqu'au donneur d'ordre, et que « le bénéficiaire ait passé un accord avec le prestataire de services de paiement permettant le paiement de la fourniture de biens et de services »¹⁸ ;
- aux virements de fonds effectués au moyen de monnaie électronique d'un montant inférieur à 1 000 euros¹⁹ : cela est à mettre en rapport avec l'article 11, 5), d) de la 3^e directive anti-blanchiment qui considère ces opérations comme peu risquées et ne nécessitant dès lors qu'une vigilance simplifiée ;
- aux virements de fonds exécutés au moyen d'un téléphone portable lorsqu'ils sont prépayés et inférieurs à 150 euros²⁰. Il est à noter qu'un lobbying actif a été opéré à Bruxelles par les représentants des PSP « traditionnels » (principalement les établissements de crédit), pour réduire autant que faire se peut l'étendue du champ d'application de l'exonération allouée aux opérateurs de téléphonie mobile qui auraient autrement bénéficié d'un avantage concurrentiel discriminatoire vis-à-vis des premiers ;
- aux virements de fonds exécutés au moyen d'un téléphone portable quand ils sont postpayés et remplissent les trois conditions cumulatives suivantes : le virement doit être accompagné d'un identifiant unique permettant de remonter jusqu'au donneur d'ordre, le bénéficiaire doit

16. Article 2, 7) du règlement.

17. Article 2, 5) du règlement.

18. Article 3, 2) du règlement.

19. Article 3, 3) du règlement.

20. Article 3, 4) du règlement.

14. Considérants 1, 2, 3, 5, 6, 13, 16, 17, 21, 22, 24.

15. Considérant 3.

avoir passé un accord avec le PSP permettant le paiement de la fourniture de biens et de services, et le PSP doit être soumis à la 3^e directive anti-blanchiment²¹ ;

- aux virements de fonds pour lesquels le donneur d'ordre retire des espèces de son propre compte²² ;

- aux transactions de débit direct pour lesquelles il existe une autorisation de prélèvement automatique entre les deux parties, à condition qu'un identifiant unique accompagne la transaction²³. Sur ce point, une interrogation subsistait quant au fait d'exclure de la même façon les prélèvements sans autorisation préalable. Pourtant, par « parties », faut-il comprendre le débiteur et le créancier qui doivent normalement prévoir contractuellement une telle opération. Il est difficile d'imaginer qu'aucun accord, serait-il non spécifique et dès lors intégré dans une autre convention plus générale, n'ait été conclu entre ces deux parties. Mais si cela est avéré en France, il est le cas de pays où il n'existe pas le système de double mandat – un premier mandat entre le débiteur et sa banque appelé « demande de prélèvement » et un second mandat entre le débiteur et son créancier appelé « autorisation de prélèvement » – tel l'Allemagne. C'est d'ailleurs probablement la raison pour laquelle les *guidelines* ne requièrent seulement que « l'autorisation existe entre le donneur d'ordre et le bénéficiaire »²⁴.

En outre, au sens du règlement, celui qui doit être identifié est le donneur d'ordre, sous-entendu celui qui initie « l'entrée » du paiement dans le système de paiement au profit d'un bénéficiaire. Or, dans le cas des prélèvements, le donneur d'ordre qui initie le paiement est le bénéficiaire. D'où l'exclusion des opérations de prélèvement du champ d'application du règlement, exclusion qui doit être considérée, à notre sens, comme applicable à tout type de prélèvement.

- aux virements de fonds effectués au moyen d'images-chèques²⁵. Pour la France, on peut justifier cette exception par l'existence, préalablement à la création des images-chèques, d'un contrôle sur les chèques en vertu du règlement CRBF 2002-01 relatif aux obligations de vigilance en matière de chèques aux fins de lutte contre le blanchiment des capitaux et le financement du terrorisme²⁶.

- aux virements de fonds, au sein d'un État membre, pour le paiement de taxes, amendes ou autres impôts aux autorités publiques, au sein d'un État membre²⁷ ;

- aux virements de fonds pour lesquels le donneur d'ordre et le bénéficiaire sont tous deux des PSP opérant pour leur propre compte²⁸. Cela signifie que les paiements interbancaires sont exclus du champ d'application du règlement, soit toutes les opérations de trésorerie effectuées entre PSP. Les messages SWIFT de type MT 202, qui sont les messages financiers utilisés pour les flux de trésore-

rie interbancaire, ne devraient donc pas être impactés. En revanche, rien n'est moins sûr concernant les messages dissociés faisant intervenir un message principal de type MT 103 ainsi qu'un message de couverture de type MT 202. Si le format des messages de type MT 202 de couverture n'est pas modifié par la société SWIFT, la réponse sera sans nul doute naturellement donnée par l'évolution de la pratique à venir dans le monde des paiements internationaux²⁹.

- Aux virements de fonds effectués au sein d'un État membre et si le PSP du bénéficiaire, en sus d'être soumis aux obligations imposées par la 3^e directive anti-blanchiment, a les moyens de remonter jusqu'au donneur d'ordre grâce à un numéro de référence unique, le montant devant être inférieur ou égal à 1 000 euros³⁰. Cette disposition fait écho à son pendant d'outre-Atlantique, et instaure une simple option conforme au principe de seuil de la RS VII du GAFI. Il sera intéressant d'observer les pays levant cette option qui, in fine, rend la tâche encore plus compliquée pour les PSP en termes de développement informatiques et de paramétrage des outils de filtrage.

Globalement, on peut constater que ces exclusions se justifient par le faible degré d'exposition au risque de blanchiment ou de financement du terrorisme que leurs sous-jacents représentent.

b. Une exonération sujette à critique

Cependant, une dernière exception est nettement plus contestable. Contrairement aux exceptions susmentionnées, cette disposition ne figure pas à l'article 3 mais au chapitre VI du règlement consacré aux dérogations, et plus particulièrement en son article 17, al. 1 rédigé comme suit : « tout État membre peut exempter les prestataires de services de paiement situés sur son territoire des obligations prévues à l'article 5 pour les virements de fonds destinés à des organisations sans but lucratif exerçant des activités à finalité charitable, religieuse, culturelle, éducative, sociale, scientifique ou fraternelle, à condition que ces organisations soient soumises à des obligations d'information et d'audit externe ou à la surveillance d'une autorité publique ou d'un organisme d'autorégulation reconnu en vertu du droit national et que ces virements de fonds soient limités à un montant maximal de 150 euros par virement et effectués exclusivement sur le territoire de cet État membre ». Cette disposition a pour objectif de ne pas décourager les donations à des fins charitables³¹. Si l'on comprend cette disposition, les conditions prévues ainsi que le fait d'être inscrites sur une liste devraient porter ces associations au-delà de tout soupçon.

Si les ONG paraissent naturellement être les bénéficiaires de cette mesure exonératoire, on peut envisager pour la France probablement une assimilation aux associations « loi 1901 » d'une certaine importance, ce qui effectivement ne présente pas d'inquiétudes. En revanche, qu'en serait-il d'autres pays membres aux dispositions plus clémentes à l'égard du statut d'associations ? Quoi qu'il en soit, l'argument avancé peut être sujet à critique.

21. Article 3, 5) du règlement.

22. Article 3, 7), a) du règlement.

23. Article 3, 7), b) du règlement.

24. Partie 1, intitulée « Explanation on payments covered », article 1.1. types of payments : "direct debit transactions when a debit authorization exists between payer and payee as long as a unique identifier accompanies the transaction (art. 2.2.f)"

25. Article 3, 7), c) du règlement.

26. Arrêté du 26 avril 2002 portant homologation dudit règlement, publié au JO n° 104 du 4 mai 2002 page 8303, texte n° 11.

27. Article 3, 7), d) du règlement.

28. Article 3, 7), e) du règlement.

29. On peut observer les prémices d'une telle évolution à travers la récente communication du Comité de Bâle portant sur la nécessaire transparence des messages de couverture, V. http://www.bis.org/publ/bcbs_n12.htm

30. Article 3, 6) du règlement.

31. Considérant 27 du règlement.

3. Le périmètre d'application géographique

a. La création d'une juridiction unique

L'élément phare de ce règlement est d'avoir réussi, dans un domaine qui n'est pas aisé à harmoniser tel celui des paiements, à créer une juridiction unique. Cette « zone domestique » permet d'instituer des règles distinctes selon la provenance et la destination du transfert de fonds, mettant en rapport cette zone et le reste du monde. Ce principe est important dans la mesure où il permet à l'Europe d'adopter une position unique face à d'autres zones aux règles différentes, telle celle des États-Unis.

b. Les pays et territoires concernés

Le texte du règlement est d'applicabilité directe dans tous les pays membres de l'Union européenne mais il a également vocation à s'appliquer à ceux restants de l'Espace économique européen (EEE), savoir l'Islande, la Norvège et le Liechtenstein. Devraient également être considérés comme partie intégrante de la zone domestique les territoires suivants : Guadeloupe, Guyane française, Martinique, réunion, les îles Canaries, Ceuta et Melilla, les Açores, Madères ou encore Gibraltar. Bien évidemment, cette liste n'a pas vocation à rester figée, et devrait évoluer dans les prochaines années.

Il est mentionné à l'article 17 que des accords avec des territoires ou des pays ne faisant pas partie du territoire de la Communauté peuvent être conclus « afin de permettre que les virements de fonds entre ce pays ou territoire et l'État membre concerné soient traités comme des virements de fonds à l'intérieur de cet État membre ». Cependant, des conditions à ce processus d'accord bilatéral se voient imposées, notamment l'existence d'une union monétaire entre le pays ou territoire requérant et l'État membre.

Concernant le choix des pays et territoires, l'EPC apparaît comme étant l'organisme compétent dans la mesure où il avait déjà été en charge de la composition de la liste des pays et territoires soumis au règlement CE n° 2560/2001 du Parlement européen et du Conseil du 19 décembre 2001 concernant les paiements transfrontaliers en euros³².

D'autres territoires « poussières d'Empire » ont vocation à intégrer la zone domestique et bénéficieront ainsi d'une passerelle bienvenue. Mais l'extension prévisible aura des impacts non négligeables pour tous les PSP européens. En effet, il s'agira au moment venu de réactualiser leurs systèmes d'information internes à mesure qu'un nouvel entrant fait son apparition.

III. LES OBLIGATIONS EN FONCTION DU STATUT DES PSP

Les obligations des assujettis vont varier selon le statut que détient un PSP assujetti lorsqu'il traite un transfert de fonds, ce statut étant déterminé par la place du PSP dans la « chaîne » de paiement. Mais abordons préalablement l'apport fondamental du texte qu'est la coexistence de deux régimes.

1. L'instauration de régimes

Il existe dorénavant deux types de régime de renseignements : l'un normal, l'autre simplifié.

a. Le principe : le régime normal dit « d'informations complètes »

Ce régime consiste à intégrer dans les messages financiers « les informations complètes sur le donneur d'ordre » tel que formulé en titre de l'article 4. Cet article prend place au début du chapitre II du règlement portant sur les obligations de PSP du donneur d'ordre. Cela peut paraître surprenant dans la mesure où cette disposition institue un régime qui n'est pas spécifique à ce type de PSP puisqu'il s'applique également aux deux autres. Il eut été dès lors plus judicieux de l'intégrer dans l'article 2 consacré aux définitions dans la mesure où il définit les trois critères constituant le régime normal d'information.

Oubliée cette remarque de pure forme, on peut ainsi lire que :

1. Les informations complètes sur le donneur d'ordre consistent en son nom, son adresse et son numéro de compte.
2. L'adresse du donneur d'ordre peut être remplacée par sa date et son lieu de naissance, son numéro d'identification de client ou son numéro national d'identité.
3. En l'absence de numéro de compte du donneur d'ordre, le prestataire de services de paiement du donneur d'ordre le remplace par un identifiant unique permettant de remonter jusqu'au donneur d'ordre.

Ce régime est applicable si l'un des deux PSP situés en bout de chaîne est localisé dans la zone domestique. Le fait que l'un de ces deux PSP au moins soit situé dans la zone domestique est la condition sine qua non de l'application du règlement (principe du *one leg in, one leg out*). En revanche, si aucun de ces deux PSP n'est situé dans la zone domestique, aucune des dispositions prévues au règlement ne devraient s'appliquer, y compris dans le cas où le PSP intermédiaire est situé dans la zone.

b. L'exception : le régime simplifié

Ce second régime est applicable lorsque le virement est exécuté entre deux PSP (celui du donneur d'ordre et celui du bénéficiaire) établis au sein de la zone domestique. Dans ce cas, le virement doit « seulement être accompagné du numéro de compte du donneur d'ordre ou d'un identifiant unique permettant de remonter jusqu'au donneur d'ordre »³³.

Il est néanmoins également indiqué à l'article 6 al.2 que « toutefois, à la demande du prestataire de services de paiement du bénéficiaire, le prestataire de services de paiement du donneur d'ordre met à la disposition du prestataire de services de paiement du bénéficiaire les informations complètes sur le donneur d'ordre, dans les trois jours ouvrables suivant la réception de cette demande », ce qui ne sera pas sans poser de problèmes.

Il est à noter que ce régime simplifié, s'il n'est pas pour déplaire à une certaine catégorie de Français qui s'adonnent aux jeux, loteries et autres paris sur la toile, ne saurait satisfaire l'État français. En effet, celui-ci veut lutter contre toutes les sociétés de jeux et paris en ligne considérées comme illégales au sens de la législation nationale,

32. Publié au JO L 344/13 du 28 décembre 2001.

33. Article 6 al. 1 du règlement.

et accusées d'être un vecteur d'activités de blanchiment de capitaux.

Ainsi, la loi du 5 mars 2007 relative à la prévention de la délinquance³⁴ impose aux établissements assujettis l'application de mesures de restriction à l'encontre des transferts de fonds initiés par des sociétés répertoriées sur une « liste noire » (qui d'ailleurs se fait toujours attendre), basées sur la pratique du filtrage des flux financiers et la détection du nom du donneur d'ordre. Cependant, ce nouveau corpus juridique mort-né va faire montre d'une inefficacité sans précédent pour deux motifs. Tout d'abord, en raison du régime simplifié qui n'exige pas que figure systématiquement le nom du donneur d'ordre pour les transferts intra-zone et ensuite, parce que nombre de sociétés potentiellement vouées aux gémonies sont implantées dans des pays ou territoires intra-zone (ex : Angleterre, Malte, Autriche,...)³⁵

En dehors de la question de la faible efficacité d'un système connexe, et par là même de celle du nouveau règlement européen, il convient de détailler les obligations pesant sur les PSP assujettis – c'est-à-dire ceux localisés à l'intérieur de la zone domestique – selon qu'ils agissent en qualité de PSP du donneur d'ordre, PSP du bénéficiaire ou PSP intermédiaire.

2. Le statut de PSP du donneur d'ordre

Tout PSP dont les clients souhaitent passer un ordre de virement sont dorénavant astreints à réaliser plusieurs contrôles.

a. La notion de donneur d'ordre

Le donneur d'ordre est défini comme « soit la personne physique ou morale qui est le titulaire d'un compte et qui autorise un virement de fonds à partir dudit compte, soit, en l'absence de compte, la personne physique ou morale qui donne l'ordre d'effectuer un virement de fonds ».

Si l'application de cette définition ne pose pas de problème pour les particuliers titulaires individuels d'un compte³⁶, qu'en est-il du cas où c'est un mandataire qui passe l'ordre en leur nom et pour leur compte? Les *guidelines* indiquent que doit être considéré comme donneur d'ordre également celui qui a le droit d'ordonner des transferts à partir d'un compte, soit le mandataire. Mais cette rédaction sibylline ne nous dit pas si c'est son nom ou celui du titulaire du compte qui doit figurer dans les messages. Il semble que l'esprit du texte milite pour l'incorporation du nom de ce dernier plutôt que celui du mandataire, l'essentiel étant de pouvoir remonter la trace du « véritable » donneur d'ordre.

De la même façon, mais dotée d'une sensibilité moindre, la question des filiales financières des grands groupes de sociétés qui se chargent de gérer les mouvements finan-

ciers de l'ensemble des entités regroupées sous le nom de la société-mère, est réelle. Bien souvent, ces filiales holdings financières portent un nom totalement différent de celui de leur maison mère pour le compte de laquelle elles agissent et qui est le véritable titulaire du compte. Dès lors, quel nom indiquer dans le message financier? L'argument précité pourrait encore une fois trouver à s'appliquer en l'espèce.

Dans les deux cas, les contraintes techniques auront raison de l'imprécision des textes. Les informations indiquées dans le message de paiement seront très probablement celles extraites de la base de données clients préalablement renseignée lors de l'entrée en relation, laissant apparaître en premier lieu le nom du titulaire du compte. Des champs d'informations libres prévus dans certains types de message pourront toujours être complétés de renseignements jugés utiles par le PSP.

Si l'on aborde le domaine des fonds d'investissement, il semble logique d'insérer le nom du fonds en tant que donneur d'ordre et non pas celui de l'entité agissant en tant que banque dépositaire ou encore celui de souscripteurs, qui certes ordonnent le remboursement de leurs parts, mais n'initient pas en lui-même le virement dont ils seront bénéficiaires.

b. Des obligations particulières selon la destination du transfert

Dans l'hypothèse où le transfert est opéré à destination d'un bénéficiaire dont le PSP est situé en France ou dans la zone domestique, le régime simplifié s'applique, savoir l'incorporation du numéro de compte du donneur d'ordre ou d'un identifiant unique qui permettra de remonter la trace de ce dernier³⁷.

Toutefois, le PSP du donneur d'ordre doit, en contrepartie de cet « allègement » dans la fourniture automatique d'information, mettre « à la disposition du prestataire de services de paiement du bénéficiaire les informations complètes sur le donneur d'ordre, dans les trois jours ouvrables suivant la réception de cette demande ».

À l'inverse, dans l'hypothèse où le transfert est opéré à destination d'un bénéficiaire dont le PSP est situé en dehors de la zone domestique, celui-ci doit être accompagné des informations complètes sur le donneur d'ordre. C'est l'application combinée des articles 5 al.1³⁸ et 7 al.1, certes peu facile à établir, qui impose cette obligation phare.

Echappent à cette obligation les virements individuels groupés dans des lots, pour peu que chaque virement individuel porte le numéro de compte du donneur d'ordre ou un identifiant unique, les fichiers comprenant lesdits lots devant, eux, être complètement renseignés³⁹.

c. Les obligations générales

Dans tous les cas et quelle que soit la destination des fonds, les informations complètes sur le donneur d'ordre qui accompagnent les virements doivent être conser-

34. Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, publiée au JO le 7 mars 2007 (NOR : INTX0600091L).

35. Pour une étude approfondie de cette problématique, V. G. Bègue, « L'impact de la problématique des jeux d'argent en ligne sur le domaine bancaire », JCP Entreprise, 2 août 2007, n°31-34, p. 9.

36. Concernant l'hypothèse d'un compte collectif, joint ou pas, on pourrait aussi se poser la question du co-titulaire à indiquer selon que c'est l'un ou l'autre qui passe l'instruction. Aucune réponse n'est fournie par les textes. Encore une fois, les considérations techniques guideront les assujettis.

37. Article 6 al.1 du règlement.

38. Cet article se lit ainsi : « Les prestataires de services de paiement veillent à ce que les virements de fonds soient accompagnés des informations complètes sur le donneur d'ordre ».

39. Article 7 al.2 du règlement.

vées pendant cinq ans, période classique de conservation en la matière.

Il est également indiqué que, préalablement à ces diligences, le PSP du donneur d'ordre doit opérer les vérifications d'identité de son client « sur la base de documents de données ou de renseignements obtenus auprès d'une source fiable et indépendante »⁴⁰. Ces vérifications sont considérées comme ayant eu lieu si l'identité du donneur d'ordre a été vérifiée lors de l'entrée en relation et/ou de l'ouverture du compte conformément aux obligations prévues en la matière par la 3^e directive anti-blanchiment⁴¹.

En revanche, concernant les virements de fonds qui ne sont pas effectués à partir d'un compte, l'article 5 al.4 précise que le PSP du donneur d'ordre « ne vérifie les informations concernant le donneur d'ordre que si le montant est supérieur à 1 000 euros, à moins que la transaction ne soit effectuée en plusieurs opérations qui semblent être liées et excèdent conjointement 1 000 euros ». Cela permet aux établissements de crédit de ne pas alourdir leur tâche en matière de vérification de « KYC » documentaire. Quant aux PSP spécialisés uniquement dans le service de transfert de fonds, ils échappent à une vérification pesante concernant des clients qui ne souhaitent émettre que des ordres de petits montants.

Des critiques peuvent être prononcées à cet égard dans la mesure où, de toutes les analyses sur le financement des actes terroristes, il ressort que dans la très grande majorité des cas les sommes transférées sont de petits montants, inférieurs au seuil de 1 000 euros. C'est une faille supplémentaire dans ce dispositif à visées préventives.

d. Autres diligences à accomplir

Le simple respect des obligations gravées dans le texte du règlement ne suffit pas à une application sereine et sans heurts du règlement. Ainsi, certaines précautions devront être prises par les PSP assujettis. Entre autres, la communication des PSP vers leurs clients donneurs d'ordres est un élément primordial. Elle est principalement de deux ordres.

Tout d'abord, le fait d'informer par quelconque moyen tous les clients, tant personnes physiques que personnes morales, afin de les « éduquer » au nouveau précepte. Cela est particulièrement vrai pour les clients *corporate* d'une certaine importance. Certains d'entre eux, en dépôt d'avoir un accès direct à un réseau de paiement (ex : accès au réseau SWIFT par le système MaCUG), utilisent la plateforme de traitement des ordres de leur PSP (qui reste responsable de la conformité du contenu des messages financiers) et n'indiquent parfois que le nom dudit PSP, voire même omettent d'insérer quelconque donnée. Un tel comportement devra être corrigé.

De la même façon, il faudra inclure dans les modèles de conventions de compte une clause explicitant brièvement les changements à venir sur le contenu de l'information relative à des données nominatives confidentielles qui seront amenées à circuler (pour les conventions existantes, prévoir une communication écrite faisant office d'avenant)⁴².

Comme le soulignent les *guidelines*, cet aspect contractuel n'est pas à négliger. Il évitera probablement des litiges au cas où un bénéficiaire, en relation d'affaires avec le donneur d'ordre, ne reçoit pas les fonds attendus en raison du refus de sa banque de créditer son compte au motif d'un message incomplet.

3. Le statut de PSP du bénéficiaire

a. L'obligation principale : la détection des messages non-conformes

La principale obligation incombant à un PSP assujetti est de « détecter que les champs relatifs aux informations concernant le donneur d'ordre prévus dans le système de messagerie ou de paiement et de règlement utilisés pour effectuer un virement de fonds ont été complétés à l'aide de caractères ou d'éléments compatibles avec ce système de messagerie ou de paiement et de règlement »⁴³.

Le PSP devra ainsi disposer de procédures efficaces et de moyens techniques développés afin de détecter toute information manquante au regard du contenu obligatoire des virements. Ce contenu sera bien évidemment variable car attaché à la provenance des virements et/ou à ses caractéristiques techniques (hors zone/intra-zone, virement individuel/virements par lots).

En clair, la responsabilité de la conformité des messages repose essentiellement sur le PSP du bénéficiaire dont le comportement est prévu en conséquence. Cependant, les solutions apportées par le règlement ne sont pas des plus réalistes.

b. Le comportement à adopter lors de la réception de messages non conformes

Si les informations concernant le donneur d'ordre sont manquantes ou incomplètes, le PSP doit, lors de la réception du message financier, rejeter le virement ou demander des informations complètes sur le donneur d'ordre, sans préjudice de l'application des « disposition légale ou administrative relative au blanchiment de capitaux et au financement du terrorisme, notamment aux règlements (CE) n° 2580/2001 et (CE) n° 881/2002 et à la directive 2005/60/CE, ainsi qu'à toute mesure d'exécution nationale »⁴⁴.

Il est également précisé à l'article 9 al.2 que « lorsqu'un prestataire de services de paiement omet régulièrement de fournir les informations requises sur le donneur d'ordre, le prestataire de services de paiement du bénéficiaire prend des dispositions qui peuvent, dans un premier temps, comporter l'émission d'avertissements et la fixation d'échéances, avant soit de rejeter tout nouveau virement de fonds provenant de ce prestataire de services de paiement, soit de décider, s'il y a lieu ou non, de restreindre sa relation commerciale avec ce prestataire de services de paiement ou d'y mettre fin ».

Ces réponses préconisées par les experts de Bruxelles n'ont, de toute évidence, pas été conçues pour faciliter les relations entre les acteurs internationaux du monde des

40. Article 5 al.2 du règlement.

41. Article 5 al.3 du règlement.

42. En pratique, une clause parapluie figure déjà dans la majeure partie des

conventions de compte proposées par les établissements de crédit, celle-ci prévoyant un consentement exprès du titulaire du compte quant au transfert ou à la communication des données personnelles le concernant dans le cadre des obligations relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme.

43. Article 8 du règlement.

44. Article 9 al.1 du règlement.

flux! Sans évoquer les conséquences désastreuses – non seulement commerciales mais également politiques – de l'application stricte de cette disposition, le rejet paraît dès lors être une solution pour trop radicale qui, dans l'hypothèse où elle serait appliquée à la lettre, ne manquerait pas de créer des situations de conflits inédites.

Certes, le considérant 16 indique qu'il faut « permettre au PSP du bénéficiaire d'éviter ou de corriger de telles situations » et qu'une « certaine souplesse devrait être autorisée, en fonction du risque, en ce qui concerne l'étendue des informations à fournir », mais cela ne résout pas le blocage de fonds. Et jusqu'alors, les autorités nationales qui ont pu être interrogées à ce sujet n'ont pas trouvé mieux à faire que de renvoyer la responsabilité de la prise de décision sur les épaules des assujettis, celle-ci devant être justifiée au regard de leur propre jugement fondé sur le risque.

Ainsi, on pourrait imaginer, relativement au fait de savoir si l'on peut ou pas créditer le compte du bénéficiaire, une gradation du risque selon certains critères pré-déterminés. Par rapport au pays d'origine dans lequel est implanté le PSP du donneur d'ordre (par la devise), ou au secteur d'activités principal du bénéficiaire voire du donneur d'ordre (certes plus difficile à déterminer!), au montant, etc. Cela serait cependant bien compliqué à réaliser.

Une autre classification pourrait consister en l'attribution d'un degré de risque intrinsèque à chaque donnée devant figurer dans un message financier. Par exemple, pour les virements en provenance de pays hors zone domestique, le nom serait considéré comme la donnée à laquelle il faut attacher la plus grande importance, son absence empêchant tout crédit en compte des fonds reçus. En revanche, l'adresse se verrait attribuer un coefficient de risque moins élevé, permettant ainsi d'envisager un crédit en compte en attendant des informations complémentaires.

En l'état actuel des réflexions, le plus sage des comportements serait, lors de la réception d'un message non conforme, ni de rejeter automatiquement le message, ni de créditer le compte du bénéficiaire, mais d'isoler les fonds (sur un compte d'attente), dans l'attente des informations idoines de la part du PSP du donneur d'ordre. Sans réponse passé un délai fixé lors de la requête par le PSP du bénéficiaire, un rejet serait alors inéluctable.

Mais, de la même manière, quels sont les critères à privilégier pour fixer un tel délai? Et surtout, de quelle manière et à quels interlocuteurs le PSP du bénéficiaire peut-il s'adresser? Doit-il respecter l'ordre des intervenants dans la chaîne de transmission de la communication financière (il interrogerait alors son correspondant direct, qui, en tant que PSP intermédiaire, répercuterait la demande d'information soit à un autre PSP intermédiaire, soit au PSP du donneur d'ordre), ou peut-il s'adresser directement au PSP du donneur d'ordre?

Les solutions, on peut aisément le constater, ne sont pas des plus évidentes. Des réponses à ces interrogations seraient les bienvenues de la part des autorités, avec si possible la fourniture d'une procédure d'escalade raisonnable et des précisions quant à celle relative à la communication.

c. L'obligation de déclaration

Il est imposée une double obligation de déclarer aux autorités nationales compétentes, soit l'état de faits constaté au travers de messages financiers peu ou mal renseignés et

prévue au dernier paragraphe de l'article 9⁴⁵, soit les soupçons qui pourraient émerger de l'appréciation du risque faite par les PSP conformément à l'article 10 du règlement intitulé « Évaluation des risques »⁴⁶. Est-ce à dire que nous sommes en présence d'un ou plusieurs nouveaux cas de déclaration de soupçon?

S'il s'agit assurément d'un nouveau fondement juridique de déclaration qui pourra être invoqué lors de la transmission d'un dossier à la cellule de renseignement financier nationale, au même titre que les déclarations déjà effectuées sur le fondement de l'article L. 562-2 du CMF, on ne peut affirmer que l'on est en présence d'un nouveau cas de déclaration à proprement parler, sauf à considérer que cette obligation soit un nouveau cas de déclaration automatique, identique à celle instituée par l'article L. 563-3 du CMF. La déclaration prévue à l'article 9 s'inscrirait dans ce cadre.

En revanche, il en est autrement concernant le possible nouveau cas de déclaration prévu par l'article 10 qui, s'il en est, devra être fondé sur une approche risque laissant part à la subjectivité des déclarants. Il entrerait donc dans le cadre général de la déclaration volontaire, subjective, prévu à l'article L. 562-2 du CMF. Ce qui infirme, concernant l'article 10, l'hypothèse d'un nouveau cas de déclaration.

d. Autres diligences à prévoir

Certaines diligences sont à opérer, notamment le fait de conserver pendant cinq ans les données relatives au donneur d'ordre⁴⁷, ce qui aura des impacts en terme de capacité d'archivage.

Concernant les diligences extra-légales, la communication est là encore gage de bonne application des présentes dispositions. De manière similaire à celle évoquée pour les PSP des donneurs d'ordre, la communication des PSP vers leurs contreparties bancaires ou de transferts de fonds doit être claire. Il convient ici de prévoir, par l'envoi de messages individualisés ou par l'utilisation du procédé des broadcast, certes coûteux mais efficace, la diffusion à tous ses correspondants de sa propre politique de traitement des messages.

Ainsi informés, les correspondants bancaires situés hors de la zone domestique (et plus particulièrement ceux qui n'accordent pas nécessairement une attention aux recommandations du GAFI) sauront s'adapter. Globalement, cela permettra une meilleure assimilation des nouvelles règles.

4. Le statut de PSP intermédiaire

Si un statut devait être distingué comme étant le moins précisément déterminé, celui du PSP intermédiaire rem-

45. On peut lire que « le prestataire de services de paiement du bénéficiaire déclare ce fait aux autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme ».

46. Article rédigé de la manière suivante : « Le prestataire de services de paiement du bénéficiaire considère les informations manquantes ou incomplètes sur le donneur d'ordre comme un facteur à prendre en compte dans l'appréciation du caractère éventuellement suspect du virement de fonds ou de toutes les opérations liées à ce virement et, le cas échéant, de la nécessité de déclarer, conformément aux obligations prévues au chapitre III de la directive 2005/60/CE, aux autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme ».

47. Article 11 du règlement.

porterait sans conteste la palme. À l'instar d'autres textes spécifiques au contrôle de flux qui n'ont jamais été véritablement clairs et précis sur cette question⁴⁸, le présent règlement ne fixe pas de manière satisfaisante les modalités de contrôle afférentes au contenu des messages ni ne pose un cadre net en terme de responsabilité.

a. La conservation des données

La principale obligation d'un PSP intermédiaire est de veiller à l'intégrité du contenu des messages qu'il reçoit et route ensuite vers le PSP du bénéficiaire. L'article 12 prévoit que « les prestataires de services de paiement intermédiaires veillent à ce que toutes les informations reçues sur le donneur d'ordre qui accompagnent un virement de fonds soient conservées avec ce virement ». De prime abord, cette obligation semble simple à réaliser. Il en est pourtant tout autrement en réalité.

Si les contours sont certes déterminés par le règlement, seules les *guidelines* peuvent nous donner une esquisse d'orientation lorsqu'il s'agit d'aborder les situations concrètes.

b. L'obstacle des systèmes nationaux de paiement

Ce précepte serait aisément applicable si les réseaux de paiements domestiques étaient au diapason, c'est-à-dire comportant des formats de messages uniformisés, permettant ainsi la conservation des données tout au long de la chaîne de paiement. Ce n'est malheureusement pas le cas, et certains réseaux de paiements nationaux ne prévoient pas le renseignement complet comme indiqué dans le règlement (en France, c'est le cas du système interbancaire de télécompensation – SIT).

Or, parmi les PSP intermédiaires, certains n'ont pas le choix du canal de transmission. L'unique ou les peu nombreux systèmes d'un pays ne permettent parfois pas la transmission fidèle des données telles qu'ils peuvent les recevoir. Les messages sont dès lors tronqués et l'information parvenant au PSP du bénéficiaire n'est que partielle. Si une telle incertitude ne devrait pas perdurer⁴⁹ – de nombreux systèmes nationaux étant en pleine phase de mutation vers des systèmes permettant le renseignement complet – ce problème sera d'actualité pour quelque temps encore.

c. Une obligation implicite de contrôle matériel

D'aucuns estiment que le PSP intermédiaire n'a, à la lecture du règlement, aucune obligation de contrôle à sa charge. Cela ne nous apparaît exact qu'à l'aune de contrôles d'une nature spécifique, savoir les contrôles intellectuels : cela signifie qu'il n'a pas à vérifier l'exactitude des informations contenues dans un message.

Cependant, il est loisible de considérer qu'il doit effectuer

un contrôle matériel portant sur la présence ou l'absence des informations requises selon la provenance du message (PSP de pays dans ou hors zone domestique). L'article 13, en ses alinéas 2 et 3, révèle implicitement cette obligation de contrôle, certes purement matérielle, mais bel et bien présente à travers le verbe « constater ».

Dans l'hypothèse d'informations incomplètes reçues du PSP du donneur d'ordre, il doit informer le PSP du bénéficiaire de cet état de fait, seulement lorsque le système domestique utilisé empêche, pour des raisons techniques, la transmission de toutes les informations au dit PSP du bénéficiaire. C'est dans le cas présent l'interprétation a contrario dudit article 13⁵⁰. Cela est logique pour deux raisons :

- dans un tel cas, le PSP du bénéficiaire n'a aucune autre possibilité de savoir si le PSP intermédiaire a reçu ou non les informations complètes ;
- la responsabilité du contrôle de la présence des informations complètes revient, au final, au PSP du bénéficiaire qui pourra adopter l'un ou l'autre comportement.

La responsabilité d'un PSP intermédiaire devrait donc être limitée aux éléments suivants :

- la transmission intègre au PSP du bénéficiaire de toutes les informations qu'il a reçues du PSP du donneur d'ordre ;
- la conservation des informations qu'il a reçues du PSP du donneur d'ordre (pendant 5 ans), et notamment celles qui ne sont pas transmises à celui du bénéficiaire en raison de contraintes techniques⁵¹ ;
- implicitement, l'information au PSP du bénéficiaire du caractère incomplet des informations qu'il a reçues du PSP du donneur d'ordre, le cas échéant.

En l'espèce, le paradoxe sous-jacent se matérialisait dans le fait d'imposer des obligations de contrôle au PSP intermédiaire alors que personne ne souhaitait voir ce dernier assumer une quelconque responsabilité corollaire. Le résultat s'avère être une responsabilité limitée à certains points bien spécifiques, mais nombreuses sont les questions en suspens.

d. Le cas des transferts par lots : une responsabilité mal définie

L'un des points les plus épineux reste celui des transferts par lots, autrement appelés dans le jargon bancaire « *batch transfers* ». En effet, les PSP offrant un service d'enrichissement des messages individuels issus d'un fichier comprenant des lots sont parfois confrontés à des difficultés.

Il s'agit des situations où les informations qui doivent initialement figurer dans le fichier (et/ou dans les messages qu'il contient) n'y apparaissent finalement pas, que

48. C'est le cas du règlement CRBF N°2002-01 relatif aux obligations de vigilance en matière de chèques aux fins de lutte contre le blanchiment des capitaux et le financement du terrorisme.

49. En lien direct avec ces très probables évolutions technologiques, l'article 19, 2, b) institue une clause de révision rédigée comme suit : « l'application de l'article 13 en ce qui concerne les limites techniques susceptibles d'empêcher la transmission, au prestataire de services de paiement du bénéficiaire, des informations complètes sur le donneur d'ordre. Au cas où il serait possible de passer outre à ces limites techniques compte tenu de nouveaux développements dans le secteur des paiements, et eu égard aux coûts connexes à la charge des prestataires de services de paiement, la Commission présente une proposition visant à modifier le présent règlement ».

50. L'article 13 al.2 est rédigé ainsi : « À moins que le prestataire de services de paiement intermédiaire ne constate, au moment de la réception du virement de fonds, que les informations requises sur le donneur d'ordre en vertu du présent règlement sont manquantes ou incomplètes, il peut utiliser, pour transmettre les virements de fonds au prestataire de services de paiement du bénéficiaire, un système de paiement avec des limites techniques qui empêche les informations sur le donneur d'ordre d'accompagner le virement de fonds » tandis que l'alinéa 3 du même article prévoit que « lorsque le prestataire de services de paiement intermédiaire constate, au moment de la réception du virement de fonds, que les informations sur le donneur d'ordre requises en vertu du présent règlement sont manquantes ou incomplètes, il n'utilise un système de paiement avec des limites techniques que s'il peut informer le prestataire de services de paiement du bénéficiaire de ce fait, soit dans le cadre d'un système de messagerie ou de paiement qui prévoit la communication de ce fait, soit par une autre procédure, à condition que le mode de communication soit accepté ou convenu entre les deux prestataires de services de paiement ».

51. Article 13 al.4 du règlement.

ce fait relève d'une impossibilité technique ou d'un tout autre ordre. Des données préalablement recueillies peuvent néanmoins venir enrichir les messages incomplets. Mais qu'en est-il alors de la responsabilité du PSP intermédiaire au titre de cette action, autrement dit de sa protection? D'où les requêtes pressantes des professionnels auprès de l'EPC afin d'inclure une disposition en ce sens dans la partie consacrée au PSP intermédiaire⁵².

En tout état de cause, il conviendra pour les assujettis de bien définir le cadre contractuel de ce type de services, savoir l'incorporation dans les contrats de *cash clearing* d'une clause ad hoc, prévoyant une ventilation des responsabilités.

CONCLUSION

Après inventaire, ce texte soulève quelques obstacles juridiques mais aussi et surtout des difficultés techniques relatives à l'application concrète de ses dispositions.

Entre autres difficultés juridiques pouvons nous citer la traduction française aléatoire de certaines notions du texte, originellement rédigé en langue anglaise. Les *guidelines* seront alors un outil pratique aux fins d'interprétation de la version française.

Par ailleurs, rien ne figure à propos de la levée du secret bancaire face au principe du règlement. Certains auraient soulevé le problème de l'adéquation d'un tel texte, permettant la circulation de données nominatives à caractère confidentiel, aux dispositions existantes en matière de secret professionnel. On pense notamment aux pays à secret bancaire affirmé tel celui qui prévaut au Luxembourg.

Il est vrai que ce point n'est pas expressément mentionné. Délibérément peut-être, tant il paraît logique aux yeux des rédacteurs qu'un texte portant sur le thème impérieux de la lutte contre le financement du terrorisme prévale sur toute autre règle même pénalement couverte.

On en déduit que ce texte de droit communautaire directement applicable et obligatoire dans tous ses éléments s'impose aux législations nationales sur le secret qui doivent dès lors s'effacer, fussent-elles d'ordre public. Dans ce contexte, comment refuser de respecter les dispositions du règlement au motif que l'on craint de voir sa responsabilité pénale engagée au titre de la violation du secret?

Quant aux difficultés d'ordre technique, elles sont légion, sans parler des procédures internes à mettre en place. Ce texte créé, il est vrai, des contraintes fortes et engendre un coût non négligeable pour les PSP qui se voient obligés d'investir de manière conséquente pour assurer des développements adéquats.

Cependant, ce coût pourrait être amoindri par l'exploitation à bon escient des transgressions opérées par les PSP au regard des dispositions du règlement. Par quel moyen? En facturant les messages non conformes : c'est une manne financière qui pourrait s'avérer non négligeable⁵³.

52. Chapitre 5 des Guidelines intitulé « Role and Responsibility of the Intermediary Bank ».

53. Les commissions trouveraient justification dans le temps passé par un agent de back-office à opérer la suspension du message, créditer les fonds sur un compte d'attente, à questionner le correspondant sur le caractère incomplet et le besoin

Quoi qu'il en soit, il est patent que ce règlement instaure un mécanisme lourd et recèle des failles que certains individus ne manqueront pas d'exploiter. L'efficacité de telles mesures n'est pas évidente. En effet, les terroristes ont compris depuis fort longtemps les avantages en termes de confidentialité et de sécurité de certains systèmes informels de transferts de fonds (Hawalas, Hundi...) ⁵⁴.

Ce constat fait, de considérables efforts pour une once d'efficacité étaient-ils nécessaires? Oui, répondent les spécialistes, car en dépit de son impact limité, il viendra compléter encore un peu plus la tâche des terroristes.

Enfin, le plus étonnant en dehors de ces considérations d'efficacité, est que ce règlement a un impact fort dans le monde des flux. Par-delà son essence et sa mécanique d'application, ce texte est en passe d'avoir des conséquences internationales loin d'être négligeables. Les sanctions attachées aux obligations imposées aux PSP européens lorsqu'ils sont PSP du bénéficiaire sont tellement fortes qu'il est difficile d'imaginer l'absence d'un effet extra-territorial.

En effet, alors que les transferts en provenance de PSP situés dans un pays hors de la zone domestique doivent renfermer les informations complètes sur le donneur d'ordre et ce, dès le premier centime, les mêmes PSP ne se voient pas imposer de telles obligations par leurs propres réglementations nationales. Et contrairement à l'Union européenne qui a fait fi de tout seuil à orientation externe dans l'élaboration du règlement, certains pays se contentent d'appliquer strictement la RS VII du GAFI qui les autorise à ne pas renseigner les messages inférieurs à 1 000 euros/dollars de l'information complète.

À cet égard, quelles vont être les réactions des PSP européens qui reçoivent des virements non conformes au regard du droit communautaire mais tout à fait respectueux de la réglementation américaine? Les PSP étrangers à la zone domestique vont-ils s'adapter à cette nouvelle réglementation qui leur est indirectement mais réellement imposée? Car, au risque de mécontenter certains de leurs clients, tous ces PSP seront obligés de se plier à cette règle afin de ne pas perturber l'actuel système international de communication financière.

Une fois n'est pas coutume, c'est bien l'Europe qui cette fois-ci imposera ses canons juridiques aux pays et territoires extérieurs à la zone domestique et non pas les États-Unis. Voilà peut-être une nouvelle arme – de nature financière mais aux desseins géopolitiques – dont s'est doté le vieux continent⁵⁵. ■

d'obtenir des informations complémentaires, effectuer le suivi de la requête, etc.).

54. De tels systèmes parallèles (dits informels par opposition au système bancaire formel) sont particulièrement développés dans les pays du Maghreb, du Moyen-Orient ou encore d'Asie et sont sans doute aucun des canaux faciles d'utilisation pour des personnes mal intentionnées. Dès lors, il ne s'agit plus de deviner quelles mesures seront adoptées relativement à des circuits de paiements officiels de moins en moins utilisés par les mafias et autres nébuleuses terroristes, mais bel et bien d'aborder la question des systèmes informels de transferts de fonds et de leur utilisation crapuleuse. Cela vaut en particulier pour la France qui, contrairement à ses voisins d'Outre-Atlantique par exemple, ne reconnaît pas ces officines de l'ombre.

55. Voir à ce sujet la pertinente étude de L. Sanchez sur l'utilisation détournée des embargos financiers internationaux, « Embargo financier international : la face cachée du Patriot Act », La Lettre Sentinel n° 45, avril-mai 2007, p. 16.