Projet de lignes directrices sur les implications pour la protection des données des mécanismes d'échanges interétatiques de données pour la lutte contre le blanchiment d'argent et le financement du terrorisme, et à des fins fiscales.

Section I.

Règles et principes de protection des données

1. Introduction

Objet : *Ces lignes directrices visent à fournir des orientations sur la manière d'intégrer les règles et normes internationales de protection des données dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme, et à des fins fiscales, afin d'assurer un niveau de protection approprié tout en facilitant la libre circulation des informations, notamment en mettant en évidence les zones grises dans les questions liées à la lutte contre le blanchiment d'argent et le financement du terrorisme, où les exigences en matière de protection des données devraient être renforcées.* Le partage des données est essentiel pour lutter contre le blanchiment de capitaux et le financement du terrorisme, qui implique souvent des systèmes transfrontaliers et de multiples institutions par lesquelles les produits du crime sont blanchis. La lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT) sont deux intérêts publics importants, qui ne sont ni opposés, ni intrinsèquement exclusifs l'un de l'autre (voir le rapport du GAFI sur la mise en commun des données). Par conséquent, il faut tenir compte à la fois des intérêts de la LBC/FT et des principes, obligations et droits de la protection des données personnelles, conformément aux obligations des États membres en vertu du droit international, y compris les droits de l'homme. En vertu de ces lois, l'existence d'une base juridique valide pour le traitement des données à caractère personnel est une condition préalable dont la justification sous-jacente doit être soigneusement analysée et articulée par les parties prenantes internationales du domaine de la LBC/FT, de la protection des données et des droits de l'homme.

Champ d'application : les lignes directrices couvriront le traitement des données personnelles par les entités publiques et privées.

Définitions (données personnelles, traitement des données, personne concernée, contrôleur des données, processeur des données et destinataire) appliquées à la LBC/FT. Plus précisément, il convient d'expliquer la partie la plus difficile : qui serait considéré comme personne concernée, responsable du traitement et sous-traitant du point de vue de la LBC/FT.

* Échanges interétatiques de données dans le domaine (a) de la lutte contre le blanchiment d'argent et le financement du terrorisme et (b) de la fiscalité.
* Interaction entre la protection des données et (a) la lutte contre le blanchiment d'argent et le financement du terrorisme et (b) le domaine fiscal
* Référence à l'avis de 2014

2. Principes de base pour la protection des données à caractère personnel

(i) Équité et transparence

(ii) Limitation de la finalité

- Les législateurs sont incités à définir concrètement les finalités pour lesquels l'échange d'informations est requis, afin d'éviter que les données personnelles soient échangées pour d'autres finalités qui peuvent être légitimes, mais qui sont trop larges ou pas du tout compatibles avec les finalités initiales.

(a) LBC/FT

- Des dispositions claires et détaillées sont établies en ce qui concerne les partenariats public-privé créés pour le partage d'informations opérationnelles sur les renseignements concernant les suspects, empêchant les entités obligées participant à ces partenariats d'intégrer dans leurs propres bases de données les informations partagées par les services répressifs.

(iii) Proportionnalité

- En particulier lorsque l'IA est utilisée, le respect des droits fondamentaux doit être prévu (référence aux Lignes directrices sur l'IA et la protection des données
- Le droit de la propriété intellectuelle pourrait entraver la divulgation d'informations importantes sur la logique et la formation des algorithmes : comment y remédier ?

4. Base juridique (article 5)

(i) Défis liés à l'application de l'article 5(2) de la Convention 108+ du Conseil de l'Europe

(a) LBC/FT

(ii) Le traitement/l'échange de données ne doit être autorisé que sur le fondement d'une base juridique valide : cette considération peut être pertinente pour toutes les entités (législateur, CRF, entités privées et LEA).

b) La fiscalité

(iii) Minimisation des données

- Les entités qui envoient des données doivent être en mesure de justifier, dans chaque cas de partage de données personnelles, pourquoi ces données spécifiques étaient nécessaires pour la finalité spécifique. Autant que faire se peut, la législation doit être aussi concrète que possible en ce qui concerne les données qui peuvent être collectées par une entité et les données qui peuvent être partagées à des fins spécifiques.

(a) Le domaine fiscal

- Les États veillent à ce que la minimisation des données soit respectée et à ce que les autorités fiscales compétentes mettent en balance l'intérêt public qui sous-tend la demande d'échange de données et les droits et intérêts des personnes concernées et, le cas échéant, des prestataires de services qui doivent être atteints.

(iv) Qualité des données, exactitude

a) LBC/FT

- L'entité soumise à l'obligation reçoit ou vérifie des informations sur les clients via des sources externes. Les entités soumises à l'obligation s'assurent de l'exactitude et de la qualité des données qu'elles obtiennent de sources externes
- Il est nécessaire d'harmoniser le cadre réglementaire relatif aux échanges d'informations entre les Cellules de renseignement financier des parties contractantes et d'autres pays tiers.
- Recommandation sur l'importance de l'exhaustivité et de la qualité de l'entrée, car cela est important pour la précision du résultat, en particulier lorsque l'IA est utilisée : "Dans le cas d'un logiciel d'apprentissage automatique, la précision de ses résultats dépend de manière significative de l'exhaustivité et de la qualité de l'entrée, c'est-à-dire des données utilisées pour évaluer un client potentiel ou une transaction. Outre les données, la précision des résultats dépend également de la manière dont le logiciel a été entraîné et du type de modèles et de corrélations qu'il a détectés : si le logiciel présente des biais ou des corrélations inexactes, les prédictions qu'il fait peuvent ne pas être fiables" (extrait du rapport). Faire une référence à la Recommandation du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.

(v) Limitation de la conservation

- Pour que le principe de limitation de la conservation soit respecté, il est essentiel que la législation mentionne clairement les périodes de conservation des données après leur échange. La détermination de la période de conservation doit respecter le principe de proportionnalité et de limitation de la finalité.
- Inclure une section avec des lignes directrices pour la période/situation où il n'y a pas de législation de ce type.

- Sécurité des données (article 7)

Le respect du principe de sécurité des données nécessite des mesures techniques et organisationnelles telles que le cryptage des données et des règles de traçabilité complète des échanges, notamment par la mise en place de journaux d'accès.

3. Les principales parties prenantes

- Une attention accrue au secteur privé, à la fois pour le partage de données de privé à public, mais aussi pour la zone grise que constitue le partage de données de privé à privé.
- Clarifier qui serait un responsable du traitement / un sous-traitant et qui porterait la responsabilité finale.
- Expliquez la difficulté d'identifier la personne d'intérêt par rapport aux bénéficiaires effectifs.
- Suggérer une catégorisation des personnes concernées (suspect, victime, témoin, etc.) et expliquer quel régime de protection des données (régime d'exception fondé sur l'article 11 ou régime normal) utiliser à quel moment de la procédure (au début, après l'établissement d'un soupçon fondé ou d'une cause probable, pendant et après une enquête, etc.)
- Éviter un modèle unique et identifier les acteurs au cas par cas.
- Importance d'identifier les bénéficiaires effectifs pour identifier correctement les personnes concernées par l'échange de données
- Clarifier le rôle des tiers auxquels les entités obligées sous-traitent l'exécution des mesures de due diligence des clients (CDD).
- Clarification des rôles des Partenariats public-privé en matière de LBC/FT dès leur création

4. Types de données (accent sur les données sensibles) - Article 6

- Données transactionnelles et financières (y compris les métadonnées et autres types de données personnelles non conventionnelles telles que les données de géolocalisation)
- Données sensibles :
    - Lorsque le traitement des données à caractère personnel relatives à des procédures et condamnations pénales est autorisé aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, les législateurs et les responsables politiques veillent à ce que ce traitement ne soit autorisé que lorsque des garanties appropriées complétant celles déjà en place sont établies par la loi.
    - Toutes les entités impliquées dans la lutte contre le blanchiment d'argent et le financement du terrorisme, y compris les parties privées, les Cellules de renseignement financier et les autorités chargées de l'application des lois, doivent former leur personnel, en particulier lorsqu'il traite des données personnelles sensibles.
    - Des mesures correctives, y compris des sanctions, sont établies pour l'application effective des mesures de sauvegarde.

5. Transparence

Article 8 de la Convention 108+ et rapport explicatif

y compris

- la notification est requise dans le cadre d'une analyse automatisée (des données de trafic et de localisation, dans ce cas précis) "l'autorité nationale compétente est tenue de publier des informations de nature générale relatives à cette analyse sans devoir notifier individuellement les personnes concernées. Toutefois, si les données correspondent aux paramètres spécifiés dans la mesure autorisant l'analyse automatisée et que cette autorité identifie la personne concernée afin d'analyser de manière plus approfondie les données la concernant, il est nécessaire de la notifier individuellement. Cette notification ne doit toutefois intervenir que dans la mesure et dès qu'elle n'est plus susceptible de mettre en péril les missions dont ces autorités sont chargées" [sera modifié en une recommandation basée sur l'arrêt La Quadrature du Net].

6. Droits des personnes concernées (article 9)

- Développer comment chacun des droits de l'article 9 pourrait/devrait être exercé dans le contexte des lignes directrices, éventuellement avec des recommandations spécifiques ?
- l'obligation de notification :
  - Par exemple, la notification/la fourniture d'informations à la personne concernée. Les personnes concernées sont notifiées lorsque la notification ne compromet plus les enquêtes. Les autorités de contrôle ont le pouvoir d'examiner si la notification aux personnes concernées est effectivement réalisée.
- Examen attentif des cas où les restrictions sont applicables

(a) LBC/FT

- Les restrictions reposeront très probablement sur "l'intérêt public général".

7. Exceptions et restrictions (article 11)

- Des restrictions pertinentes peuvent être établies pour les données personnelles échangées à des fins de la lutte contre le blanchiment d'argent et le financement du terrorisme ;

(1) au nom de la prévention, de l'investigation et de la poursuite de la criminalité
- par exemple, la notification/fourniture d'informations à la personne concernée.
- Faire une recommandation

(2) au nom de la sécurité nationale, telle qu'interprétée dans la jurisprudence de la Cour européenne des droits de l'homme, ou

(3) au nom d'autres objectifs importants d'intérêt public général. Cette dernière catégorie peut couvrir les objectifs de lutte contre le blanchiment d'argent et le financement du terrorisme (art. 11(1)(*a)* Convention 108+).

8. Flux transfrontaliers de données à caractère personnel (article 14)

- Compte tenu de la nature multilatérale des mécanismes d'échanges interétatiques de données à caractère personnel à des fins fiscales et de lutte contre le blanchiment de capitaux et le financement du terrorisme, la question du niveau de protection approprié se pose dans tous les cas où l'échange de données à caractère personnel concerne un pays qui ne dispose pas d'un niveau (essentiellement) équivalent de protection des données à caractère personnel.
- Les autorités de contrôle sont habilitées à traiter ces questions conformément à l'article 15, paragraphe 2, point *b*), de la Convention 108+ et, le cas échéant, à saisir les tribunaux nationaux de cas individuels de transferts transfrontaliers de données.
- Les États contractants examinent les accords internationaux qui impliquent des transferts transfrontaliers de données à caractère personnel afin de s'assurer que les principes et les exigences de la Convention 108+ sont respectés.

(a) LBC/FT

- Faire une recommandation sur les Cellules de renseignement financier qui échangent des données avec un homologue étranger établi dans un pays ne disposant pas d'un niveau de protection adéquat (réflexions existantes pour résoudre ce problème au sein du CoE : https://rm.coe.int/t-cy-2020-7-fr-pdp-protocol-v3t-approuve-par-le-tcy-/1680a2bb10 (article 14) et https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee (Point 3.4)
- Les autorités nationales de contrôle aident les autorités des parties signataires à assurer le respect de la Convention 108+.
- Les transferts de données ne sont autorisés que dans les limites géographiques des pays qui offrent un niveau de protection adéquat ou des garanties appropriées (art. 14 (4) de la Convention 108+ et para. 109 à 112 du rapport explicatif). Sans cela, la mise en commun des données entre institutions financières, notamment au-delà des frontières nationales et avec des tiers, soulève un certain nombre de préoccupations.
- Le droit du Conseil de l'Europe autorise les transferts de données vers des territoires qui ne disposent pas d'un niveau approprié de protection des données, sur la base de garanties ad hoc ou normalisées approuvées, prévues par des instruments juridiquement contraignants et exécutoires, adoptés et mis en œuvre par tous les acteurs impliqués dans le transfert et le traitement ultérieur.

9. Une supervision et un contrôle indépendants efficaces (article 15)

- Recommander que l'autorité de protection des données soit compétente pour superviser le traitement des données dans ces domaines.
- Proposer des outils et un *modus operandi* pour une supervision efficace.

10. Coopération et assistance mutuelle (articles 16 et 17)

- Recommander d'utiliser le potentiel de la coopération internationale et, le cas échéant, de l'application de la loi.

Section II.

Les zones grises dans les questions liées à l'AML/CFT où les exigences de la protection des données devraient être renforcées, telles que :

- Les questions liées au partage de données entre particuliers nécessitant une analyse minutieuse des implications en matière de LBC/FT et de protection des données personnelles (lien vers le rapport du GAFI sur le partage des données, l'analyse collaborative et la protection des données)
- les questions liées aux technologies nouvelles et émergentes de renforcement de la protection de la vie privée pour le partage de données entre acteurs du secteur privé et la nécessité de garantir et de renforcer à la fois la protection des données et la protection de la vie privée (lien vers le rapport du GAFI sur la mise en commun des données, l'analyse collaborative et la protection des données).

Section III.

Questions et recommandations prospectives

- Récupérer l'analyse de la voie à suivre sur la manière dont les autorités de protection des données sont invitées à traiter les questions de LBC/FT au fur et à mesure de leur évolution.
- Recommandations de politique générale sur la coopération entre les autorités de lutte contre le blanchiment d'argent et le financement du terrorisme et les autorités de protection des données.
- L'indépendance des autorités de protection des données doit être soulignée et de nouveaux modèles pour une meilleure application de la loi doivent être recommandés. Par exemple, une forme importante de coopération nationale entre les autorités chargées de la protection des données et les autorités chargées de la lutte contre le blanchiment d'argent et le financement du terrorisme consisterait à assurer un contrôle efficace de la protection des données sur les entités du secteur privé impliquées dans le partage des données.