28 JANVIER 1981-2021
CONVENTION 108
POUR LA PROTECTION DES DONNÉES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 2 juin 2021 T-PD(2021)4

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

CONVENTION 108

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

par

Eleni Kosta

Direction Générale Droits de l'homme et État de droit

Table des matières

Abréviations et acronymes

4AMLD	4ème directive anti-blanchiment (directive 2015/849)
5AMLD	5e directive anti-blanchiment (directive 2018/843)
ACIP	Partenariat industriel de Singapour en matière de LBC/FT
AEOIAutomatic	Exchange of Information (échange automatique d'informations)
AML	Anti-Money Laundering
AUSTRAC	Centre australien de déclaration et d'analyse des transactions
BO	Propriétaire bénéficiaire
	Accord d'autorité compétente de la CAAC
CDD	Diligence raisonnable du client
CDOTRèglement sur le respect des obligations fiscales internationales des dépendances de la Couronne et des territoires d'outre-mer du Royaume-Uni	
CJUE	Cour de justice de l'Union européenne
CTF	Lutte contre le financement du terrorisme
CoE	Conseil de l'Europe
Convention 108	Convention modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108
CRS	Norme commune de déclaration
CRS MCAA	Common Reporting Standard Multilateral Competent Authority Agreement (Accord multilatéral de l'autorité compétente)
DAC	Directives sur la coopération administrative
ECHRE	Convention européenne des droits de l'homme
CEMHRE	Commission européenne des droits de l'homme
	CEDH-Cour européenne des droits de l'homme
	EDPBEureau européen de la protection des données
CEPD	Contrôleur européen de la protection des données
EOIR	Exchange d'informations sur demande
FATCA	Loi sur la conformité fiscale des comptes étrangers
GAFI	Groupe d'action financière
FFI	Institution financière étrangère
CRF	Unité de renseignement financier
FMLIT Kong	Groupe de travail sur la fraude et le blanchiment d'argent de Hong (Hong Kong Fraud and Money Laundering Intelligence Taskforce)
RGPD	Règlement général sur la protection des données
HIRE	Loi sur les incitations à l'embauche pour restaurer l'emploi
IGA	Mise en œuvre des accords intergouvernementaux
IRSUS	Internal Revenue Service

JMLIT	Joint Money Laundering Intelligence Taskforce du Royaume-Uni
KYC	Connaître son client
LED	La directive sur l'application de la loi
LQDN	Affaires jointes C-511/18, C-512/18 et C-520/18 *La Quadrature du Net et autres c. Premier Ministre et autres* [2020] ECLI:EU:C:2020:791
MACOECD	et Convention multilatérale du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale
OCDE	Organisation de coopération et de développement économiques
PPP	Partenariat public-privé
RIPAUnited	Kingdom Regulation of Investigatory Powers Act 2000 (loi sur la réglementation des pouvoirs d'investigation)
STR/SAR	Déclaration d'opérations suspectes/ Déclaration d'activités suspectes
TEUTraité	sur l'Union européenne
UBO	Propriétaire Bénéficiaire Effectif Ultime
WP29	Groupe de travail Article 29 sur la protection des données

1. Contexte

1.1 Introduction [1]

L'échange d'informations entre diverses entités est la pierre angulaire de la lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi qu'à des fins fiscales. La facilitation de l'échange d'informations dans le secteur financier et à des fins fiscales figurait en bonne place dans l'ordre du jour du Groupe d'examen de la mise en œuvre de la Conférence des États parties à la Convention des Nations unies contre la corruption et a attiré une attention particulière en tant que mesure permettant de dénoncer la corruption lors du Sommet sur la lutte contre la corruption qui s'est tenu à Londres en 2016.[2] Dans le secteur financier, le Groupe d'examen de la mise en œuvre a encouragé « toutes les juridictions, lorsque le droit national applicable le permet, à améliorer le partage d'informations entre les autorités chargées de l'application des lois, les CRF, les régulateurs et les banques, ainsi qu'au sein et entre les participants du secteur privé, tant au niveau national qu'international ».[3] Dans le cadre de leurs efforts pour décourager l'évasion fiscale et d'autres délits fiscaux, ils ont approuvé la mise en œuvre de la Norme commune de déclaration (NCD) sur l'échange automatique de renseignements, qui est essentielle pour la transparence fiscale mondiale.[4]

Le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme implique des échanges complexes de données entre les clients, les entités obligées, les cellules de renseignement financier (CRF) et les autorités chargées de l'application des lois, ainsi que les services de renseignement dans certains cas. En ce qui concerne le domaine de la fiscalité, le principe de l'imposition mondiale des revenus présuppose l'échange d'informations entre différents pays. En d'autres termes, « les pays de résidence qui imposent leurs résidents sur les revenus produits à la fois dans le pays et à l'étranger ont besoin de la coopération des pays de source pour obtenir des informations sur les revenus produits par leurs résidents dans ces pays ». [5]

Traditionnellement, les échanges de données à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme et à des fins fiscales reposent sur la lutte contre la criminalité économique. Cependant, ces échanges englobent généralement des données personnelles dont la protection doit être respectée. La nécessité d'aligner les exigences en matière de LBC/FT sur celles de la protection des données a été reconnue par le Groupe d'action financière (GAFI) qui a recommandé aux pays de renforcer la coopération et la coordination entre les autorités compétentes afin d'assurer la compatibilité des exigences en

[1] Je suis très reconnaissante à Sophie Kwasny et Bohumila Ottova du Conseil de l'Europe pour leur aide à la préparation de ce rapport. Lorena Ungureanu, Igor Nebyvaev, Benjamin Vogel, Magdalena Brewczyńska et Silvia de Conca ont formulé des commentaires très utiles sur les versions antérieures. Je suis également reconnaissante aux membres des délégations qui ont posé des questions et fourni des commentaires sur les versions antérieures présentées lors de la plénière (18-20 novembre 2020) et de la réunion du Bureau (24-269 mars 2021).

[2] UNODC, Sommet sur la lutte contre la corruption : Londres 2016, Communiqué soumis par le gouvernement du Royaume-Uni, septième session du groupe d'examen de la mise en œuvre (20-24 juin 2016) CAC/COSP/IRG/2016/CRP.19. <https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/20-24June2016/V1603744e.pdf> consulté le 25 mai 2021.

[3] Ibid, p.3.

[4] Ibid, p.5.

[5] Carlo Garbarino, *The EU Protection of Tax Data Transferred to Third Countries* (2020) Bocconi Legal Studies Research Paper No. 3730009, p. 1.

matière de LBC/FT avec les règles de protection des données.[6] De même, le Forum mondial sur la transparence et l'échange d'informations à des fins fiscales, un organisme international qui travaille à la mise en œuvre de normes mondiales de transparence et d'échange d'informations dans le monde entier, accorde une grande importance à la protection des données personnelles.

1.2 L'avis de 2014 sur l'échange de données

Le Conseil de l'Europe a adopté la Convention 141 relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et la Convention 198 relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme.

Au niveau de l'UE, le Conseil a adopté en 2011 la première directive, la Directive 2011/16, relative à la coopération administrative dans le domaine fiscal (CAD). En 2012, le GAFI a révisé ses recommandations sur la lutte contre le blanchiment d'argent et le financement du terrorisme recommandant, entre autres, la surveillance et l'enregistrement des données relatives aux transactions et le partage de toute information pertinente avec les autorités requérantes au niveau national.

En réponse à cette "nouvelle tendance" à réglementer les échanges de données, le Conseil de l'Europe a adopté en 2014 un avis sur les implications en matière de protection des données à caractère personnel des mécanismes d'échanges interétatique et automatique de données à des fins administratives et fiscales[7]. L'avis de 2014 ne couvrait que les échanges interétatiques à des fins administratives et fiscales et uniquement ceux qui étaient automatiques. Selon l'Organisation de coopération et de développement économiques (OCDE), « l'échange automatique de renseignements s'entend comme impliquant la transmission systématique et périodique d'informations "en vrac" sur les contribuables par le pays source au pays de résidence concernant diverses catégories de revenus (par exemple, dividendes, intérêts, redevances, salaires, pensions, etc.) [8]» L'échange automatique d'informations est central dans le domaine de l'échange d'informations fiscales, comme expliqué ci-dessous, tandis que l'échange d'informations pour la lutte contre le blanchiment d'argent et le financement du terrorisme, notamment en ce qui concerne l'accès des CRF aux données, peut se faire de diverses manières, comme expliqué ci-dessous.

Le rapport qui accompagnait l'avis de 2014 justifiait le lien entre l'échange automatique de données personnelles entre États à des fins administratives et fiscales et les échanges similaires visant à lutter contre le blanchiment d'argent par deux raisons principales :

[6] GAFI, Quarante recommandations (octobre 2003), recommandation n° 2, www.fatf-gafi.org/media/fatf/documents/FATF Standards - Quarante recommandations rc.pdf, consulté le 25 mai 2021.

[7] Conseil de l'Europe, Avis sur les implications en matière de protection des données à caractère personnel des mécanismes d'échanges interétatique et automatique de données à des fins administratives et fiscales (4 juin 2014) : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064ae584 , consulté le 25 mai 2021.

[8] OCDE, L'échange automatique d'informations - Qu'est-ce que c'est, comment ça marche, les avantages, ce qui reste à faire (2012) p. 7 https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf, consulté le 25 mai 2021.

Tout d'abord, dans le cadre de la révision de ses Recommandations en février 2012, le GAFI a décidé de faire entrer dans le champ du LAB-FT « toutes les infractions graves » ceci comprenant donc bon nombre d'infractions fiscales.

La terminologie « d'infraction graves » employée répond à une volonté d'incrimination du plus grand nombre d'infractions possibles en corrélant le champ d'application de la lutte contre le blanchiment à la peine encourue au titre de l'infraction sous-jacente. […]

Ensuite, il convient de rappeler que dans un rapport1 de 1998 établi aux fins de «mettre au point des mesures pour limiter les distorsions introduites par la compétition fiscale dommageable dans les décisions d'investissement et de financement et leurs conséquences pour la matière imposable au niveau national », l'OCDE avait déterminé quatre facteurs essentiels2 permettant d'identifier les paradis fiscaux : des impôts inexistants ou insignifiants, l'absence d'un véritable échange de renseignements, l'absence de transparence et l'absence d'activités substantielles.

Si les paradis fiscaux ont été depuis largement stigmatisés sur la scène politicomédiatique, il convient de relever que l'objectif primitif de limitation des distorsions introduites par la compétition fiscale internationale s'est aujourd'hui transformé en lutte contre la fraude et l'évasion fiscale. La défiance qui existait sur des pratiques étatiques de compétition fiscale s'est désormais reportée sur les individus. Le développement exponentiel des obligations et diligences fondées sur la notion de « soupçon » est à cet égard remarquable.

Aussi en plein débat européen sur la question des échanges interétatiques et automatiques de données à caractère personnel à des fins administratives et fiscales, l'entrée en vigueur imminente pour bon nombre de pays du Foreign Account Tax Compliant Act3 (FATCA) a précipité la mise en œuvre de traitements automatisés de données personnelles destinés à permettre des échanges automatiques de renseignements fiscaux.

Ainsi, l'échange automatique de renseignements est en passe de devenir la norme internationale comme l'a par ailleurs encore rappelé le Secrétaire général de l'OCDE se félicitant que « l'adhésion politique à l'échange automatique de renseignements sur les revenus de placements n'a jamais été aussi forte. Le Luxembourg a modifié sa position et la législation FATCA (Foreign Account Tax Compliance Act) adoptée par les États-Unis suscite une acceptation rapide de l'échange automatique, et pousse les pays européens à adopter la même approche pour eux-mêmes. L'objectif du mandat du G20 étant que cette pratique devienne désormais la norme, l'OCDE travaille actuellement à mettre en place un système d'échange automatique standardisé, fiable et efficace ». [9]

1.3 Développements dans le domaine de l'échange d'informations

Depuis l'adoption de l'avis de 2014 susmentionné sur les implications pour la protection des données des mécanismes d'échanges automatiques interétatiques de données à des fins administratives et fiscales, le cadre de la protection des données tant au niveau du Conseil de l'Europe que de l'Union européenne a été modifié, avec l'adoption de la Convention 108

[9] Caroline Porasso, Benjamin Aouizerat, Rapport sur les implications pour la protection des données d'un recours croissant à des mécanismes d'échanges interétatiques et automatiques de données à caractère personnel à des fins administratives et fiscales, ainsi que dans le cadre de la lutte contre le blanchiment d'argent, le financement du terrorisme et la corruption (30 janvier 2014) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae586, consulté le 25 mai 2021.

modernisée (ou Convention 108+ du CoE) en 2018[10] et l'adoption du Règlement général sur la protection des données (RGPD)[11] et de la Directive 2016/680 (la directive relative à l'application de la loi ou la LED)[12], qui prévoit des règles spécifiques pour la protection des données à caractère personnel dans le contexte de l'application de la loi. Le champ d'application de la Convention 108+ du CdE a été élargi et comprend « le traitement automatisé et le traitement non automatisé des données à caractère personnel (traitement manuel où les données forment une structure permettant d'effectuer des recherches par personne concernée selon des critères prédéterminés), ce traitement relevant de la juridiction d'une Partie à la Convention».[13] En outre, la Cour de justice de l'Union européenne a rendu un certain nombre d'arrêts fondamentaux[14] qui fixent des garanties pour l'échange de données à caractère personnel qui sont pertinentes pour la question qui nous occupe et qui seront examinées plus loin dans ce rapport.

Dans le même temps, les échanges d'informations dans ce contexte se sont fortement intensifiés et un cadre complexe d'instruments juridiques et réglementaires a été adopté, nécessitant une attention particulière dans les domaines de la lutte contre le blanchiment d'argent et de la fiscalité.

1.4 Objet du présent rapport

Ces évolutions appellent un nouvel avis, une mise à jour qui traiterait des implications des échanges de données en matière de protection des données. Alors que l'avis de 2014 se concentrait sur les données à des fins administratives et fiscales, la référence aux données administratives reste très large. Le présent rapport se concentre plutôt sur les échanges de données à des fins fiscales et de LBC/FT. L'échange de données dans le domaine de la fiscalité est principalement réalisé entre les autorités fiscales compétentes et, dans une large mesure, il a lieu de manière automatique, souvent sans demande préalable. Dans le contexte de la lutte contre le blanchiment de capitaux et le financement du terrorisme en revanche, les données sont échangées entre divers acteurs et de diverses manières. Ne s'intéresser qu'aux

[10] Conseil de l'Europe, Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (2018) STCE n° 223 Détails du résultat (coe.int), consulté le 25 mai 2021.
[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE.
[12] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[13] Conseil de l'Europe, La Convention 108 modernisée : aperçu des nouveautés https://rm.coe.int/la-convention-108-modernisee-appercu-des-nouveautes-fr/16808b07e8, consulté le 25 mai 2021.
[14] Affaires jointes C-293/12 et C-594/12 *Digital Rights Ireland Ltd c. ministre des communications, du milieu marin et des ressources naturelles et autres et Kärntner Landesregierung et autres* [2014] ECLI:EU:C:2014:238 ; Affaires jointes C-2013/15 et C698/15 *Tele2 Sverige AB c. Post- och telestyrelsen* et *Secretary of State for the Home Department c. Watson* [2016] ECLI:EU:C:2016:970 ; Affaire C-362/14 *Maximillian Schrems c. Data Protection Commissioner* [2015] ECLI:EU:C:2015 :650 ; affaire C-311/18 *Commissaire à la protection des données c. Facebook Ireland, Maximillian Schrems* [2020] ECLI:EU:C:2020:559 ; C-623/17 *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs et autres* [2020] ECLI:EU:C:2020 :790 ; Affaires jointes C-511/18, C-512/18 et C-520/18 *La Quadrature du Net et autres c. Premier Ministre et autres* [2020] ECLI:EU:C:2020:791 ; Affaires jointes C-245/19 et C-246/19 *État luxembourgeois c. B* et *État luxembourgeois c. B,C,D,F.C* [2020] ECLI:EU:C:2020:795.

échanges interétatiques "automatiques" laisserait de côté des échanges de données cruciaux, notamment dans le domaine de la LBC/FT. Par conséquent, le rapport couvrira les échanges de données qui ne sont pas nécessairement automatiques. Il convient de souligner qu'il y a un intérêt croissant pour les échanges de données à des fins de LBC/FT et de fiscalité au sein d'un même État, impliquant par exemple des partenariats public-privé en matière de LBC ou la mise en commun de données pour le secteur privé, qui est l'une des initiatives du GAFI sous la présidence allemande.[15] Néanmoins, la nature des problèmes est dans une large mesure différente lorsque l'échange a lieu au sein d'un même pays, de sorte que ce rapport couvre délibérément les échanges interétatiques. Ainsi, il se concentrera sur les implications pour la protection des données des mécanismes d'échanges de données à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme et à des fins fiscales.

L'échange de données à caractère personnel dans les domaines de la lutte contre le blanchiment d'argent et le financement du terrorisme et de la lutte contre la fraude et l'évasion fiscales suscite des inquiétudes quant au traitement légitime de ces données.

Ce rapport présentera d'abord l'échange de données dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme et dans le domaine de la fiscalité. Il examinera ensuite les acteurs impliqués dans ces deux domaines du point de vue de la protection des données. Il éclairera ensuite les droits des personnes concernées en matière de protection des données. Il analysera ensuite la base juridique qui peut légitimer les échanges de données avant d'analyser les principes de protection des données (proportionnalité, loyauté et transparence, limitation de la finalité, minimisation des données, exactitude et limitation de la conservation). La section suivante abordera brièvement les questions de sécurité des données, tandis que la dernière section analysera les flux de données transfrontaliers ce qui revêt une importance particulière étant donné que le rapport se concentre sur les échanges "interétatiques". Le rapport se conclura par quelques recommandations afin que l'échange interétatique de données personnelles à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme et à des fins fiscales respecte les principes et les dispositions du cadre de protection des données du Conseil de l'Europe.

2. Échange de données dans le cadre juridique de la lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT)

2.1 Cadre réglementaire LBC/FT relatif aux échanges de données

En 1990, le GAFI a présenté la première version des Quarante recommandations du GAFI[16]. Elles ont été révisées en profondeur en 2012, intégrant des recommandations spéciales sur le financement du terrorisme aux mesures contre le blanchiment d'argent, afin de constituer un ensemble complet de normes[17]. Le GAFI postule que l'État doit pénaliser le blanchiment de capitaux et le financement du terrorisme et impliquer les institutions financières et autres dans la prévention et la déclaration du blanchiment de capitaux. Les tâches de prévention et

[15] GAFI, Priorités du Groupe d'action financière (GAFI) sous la présidence allemande - Objectifs pour 2020-2022 (2020) https://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf consulté le 25 mai 2021.
[16] GAFI, Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (2020) https://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf consulté le 25 mai 2021.
[17] Ibid.

de déclaration du blanchiment de capitaux par les entités obligées sont réalisées principalement par le biais de la vigilance à l'égard de la clientèle (CDD) [18]. Les obligations imposées aux institutions financières sont exprimées par l'exigence de "connaître son client" (KYC), c'est-à-dire l'identification de tous les clients, la tenue de registres des transactions financières et l'information des cellules de renseignement financier (CRF) de toute activité suspecte par le biais de la déclaration.

Les recommandations du GAFI contiennent un certain nombre d'exigences relatives à l'échange d'informations entre les institutions financières et à la mise en œuvre sans entrave de la CDD et de la déclaration. Plus concrètement, la recommandation 9 demande aux pays de s'assurer que les lois sur le secret des institutions financières n'entravent pas la mise en œuvre des recommandations du GAFI. La recommandation 10 stipule que « Les institutions financières devraient prendre les mesures de vigilance (« due diligence ») à l'égard de la clientèle (CDD) » dans des situations spécifiques. La note interprétative de la Recommandation 10 (Diligence raisonnable à l'égard de la clientèle) précise, en ce qui concerne la CDD renforcée, que : « Les institutions financières devraient examiner, dans la mesure où cela est raisonnablement possible, le contexte et l'objet de toutes les transactions complexes, inhabituelles et de grande ampleur, et de tous les schémas inhabituels de transactions, qui n'ont pas d'objet économique ou licite apparent. Lorsque les risques de blanchiment de capitaux ou de financement du terrorisme sont plus élevés, les institutions financières devraient être tenues d'appliquer des mesures CDD renforcées, en fonction des risques identifiés. En particulier, elles devraient accroître le degré et la nature de la surveillance de la relation d'affaires, afin de déterminer si ces transactions ou activités semblent inhabituelles ou suspectes. » [19]

La recommandation 13 exige que, dans le cadre de relations transfrontalières de correspondance bancaire ou de relations similaires, les institutions financières fournissent des informations les unes sur les autres, au-delà de l'exécution des mesures normales de CDD. La recommandation 16 exige que les entités obligées recueillent des informations précises sur le donneur d'ordre et le bénéficiaire des virements électroniques. La Recommandation 17 établit les exigences pour l'externalisation de la CDD à des tiers (qui peuvent être basés dans un autre pays) des données d'identification du client et des données relatives à l'objet et à la nature prévue de la relation d'affaires. Enfin, la Recommandation 18 établit une obligation pour les groupes financiers de partager des informations au sein du groupe à des fins de LBC/FT. La note interprétative de cette recommandation explique que ces programmes devraient être applicables à toutes les succursales et filiales à participation majoritaire du groupe financier et concerner les informations requises aux fins de la CDD et de la gestion du risque de blanchiment de capitaux et de financement du terrorisme. En outre, elle souligne l'importance de garanties adéquates sur la confidentialité et l'utilisation des informations, et précise que la portée et l'étendue de ce partage d'informations peuvent être déterminées par les pays en fonction de la sensibilité des informations et de leur pertinence pour la gestion du risque de LBC/FT. [20]

Pour renforcer la coopération internationale, le GAFI recommande également de surveiller et de conserver des enregistrements des flux financiers transfrontaliers et de partager les informations pertinentes avec les autorités requérantes. Selon le GAFI, « le partage efficace des informations est l'une des pierres angulaires d'un cadre efficace de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) ».[21] C'est pourquoi le GAFI

[18] Ibid, recommandation n° 10. Pour en savoir plus sur le CDD, voir la section 2.3.1.
[19] Ibid, note interprétative de la Recommandation 10 (Diligence raisonnable du client), Para 20.
[20] Ibid, p.85.
[21] GAFI, *Consolidated FATF Standards on Information Sharing - Relevant excerpts from the FATF Recommendations and Interpretive Notes* (2017).
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/consolidated-fatf-standards-information-sharing.pdf consulté le 25 mai 2021

a compilé les 25 recommandations du GAFI qui définissent les exigences en matière de partage d'informations dans un document intitulé *Consolidated FATF Standards on Information Sharing*.[22]

Au niveau de l'Union européenne, les instruments juridiques les plus importants relatifs à l'échange de données sont la Directive 2015/849 (4eme Directive anti-blanchiment ou 4AMLD)[23] et introduisant des modifications à celle-ci, la Directive 2018/843 (5eme Directive anti-blanchiment ou 5AMLD).[24] La Directive 2019/1153[25] établit des mesures visant à améliorer l'accès aux informations financières et aux informations sur les comptes bancaires et à leur utilisation par les autorités chargées de l'application de la loi compétentes en leur fournissant un accès direct aux informations contenues dans les registres centralisés nationaux. Elle facilite également l'accès des CRF aux informations des services chargés de l'application de la loi et stimule l'accès des autorités d'enquête aux données des CRF. [26]

2.2 Échange d'informations en matière de LBC/FT

L'échange d'informations est important pour la stratégie AM/CFTL. Les données sont collectées par les entités obligées et sont transférées aux CRF puis aux autorités chargées des enquêtes et à d'autres entités obligées. Le cadre juridique de la LBC/FT prévoit un certain nombre de dispositions concrètes sur l'échange d'informations dans le contexte de la LBC/FT (voir figure 1). Les données proviennent directement d'un client, qui peut être une personne physique ou morale, ou de tiers, de sources ouvertes et potentiellement aussi d'informations non ouvertes acquises commercialement. Si une entité obligée considère qu'une transaction ou une activité est suspecte, elle est obligée de soumettre une Déclaration de transaction suspecte (STR) (également connue sous le nom de Déclaration d'activité suspecte (SAR)) à la CRF. C'est généralement le moment où les données franchissent la frontière entre la sphère privée et la sphère publique. Cet échange peut également avoir lieu lorsque la CRF demande à l'entité obligée de fournir des informations. Une fois que la CRF a analysé les informations provenant de la déclaration de soupçon, elle les examine généralement dans un contexte plus large. À cette fin, la CRF peut demander des informations de suivi adressées aux entités obligées déclarantes, à d'autres entités obligées ou même à des CRF étrangères et à d'autres autorités.

Si la CRF conclut que les faits de l'affaire justifieraient à ses yeux l'ouverture d'une enquête pénale, elle partage le résultat de son analyse avec les autorités de justice pénale. D'autres

[22] GAFI, Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (2020) https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-information-sharing.html , consulté le 25 mai 2021.

[23] Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, p. 73-117.

[24] Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, et modifiant les directives 2009/138/CE et 2013/36/UE, p. 43-74.

[25] Directive (UE) 2019/1153 du Parlement européen et du Conseil établissant des règles visant à faciliter l'utilisation d'informations financières et autres pour la prévention, la détection, l'investigation ou la poursuite de certaines infractions pénales, et abrogeant la décision 2000/642/JAI du Conseil.

[26] Ibid, article 1(1).

échanges d'informations peuvent avoir lieu au niveau du partage du renseignement financier avec d'autres autorités, telles que les autorités fiscales ou douanières.

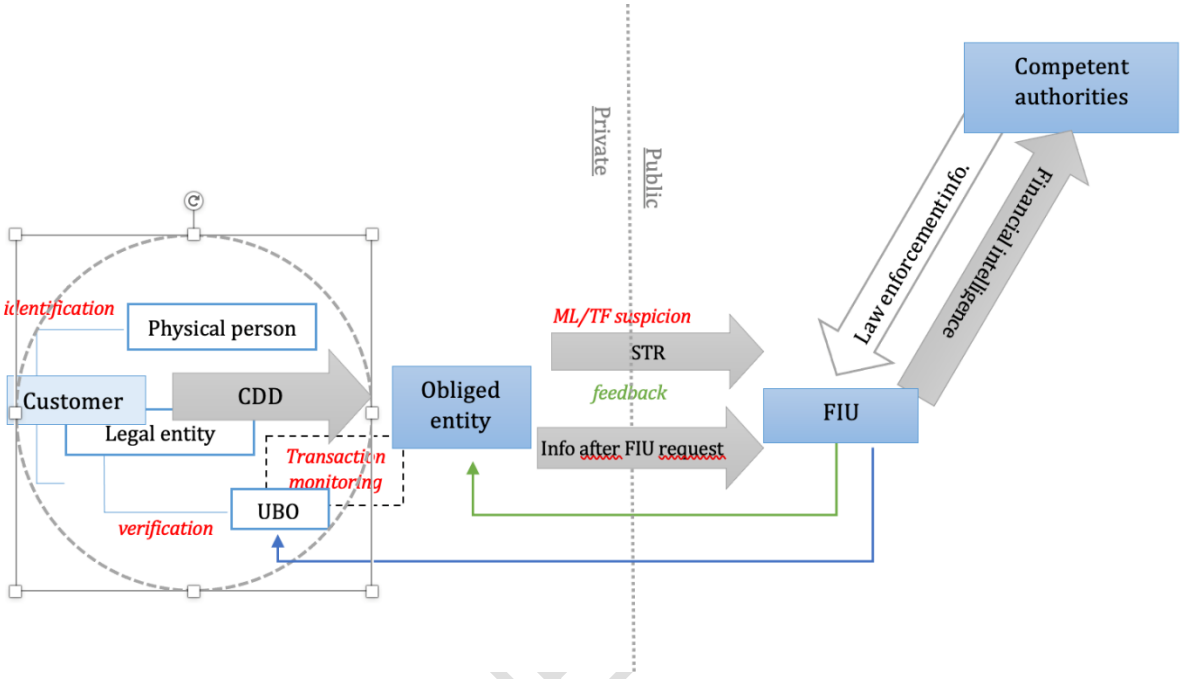

Figure 1: Flux d'informations de base en matière de LBC/FT (Crédit : Magdalena Brewczyńska)

Les évolutions technologiques améliorent les méthodes et techniques de collecte et d'analyse des données. Les institutions financières adoptent progressivement des solutions basées sur l'apprentissage automatique pour compléter et intégrer les outils basés sur les règles. La combinaison de l'approche basée sur les règles et de l'approche basée sur le risque utilise de nombreuses techniques de détection pour simplifier et en même temps améliorer le processus de détection et mettre en œuvre les exigences CDD pour mieux comprendre qui sont les clients, leurs transactions et permettre une identification plus précise du risque client. [27]

Les logiciels d'apprentissage automatique sont capables d'exploiter d'importantes quantités de données pour identifier des modèles, créer des profils, regrouper et catégoriser des clients sur la base de caractéristiques communes, et déduire des données supplémentaires par rapport à celles saisies. Les solutions d'apprentissage automatique peuvent également être utilisées par les entités obligées pour segmenter les clients en fonction de leur catégorie de risque, et effectuer une analyse des modèles pour détecter les anomalies dans le comportement (soit personnalisé sur un client spécifique, soit basé sur les catégories de clients). Elles peuvent également effectuer une [28] analyse des liens pour déduire les relations entre les clients (réseau), ou entre les clients et les éventuelles PPE ou les sujets sous

[27] Tamer Hossam et autres, *Design of a Monitor for Detecting Money Laundering and Terrorist Financing* (2016) 85 Journal of Theoretical and Applied Information Technology 425, 426. 9.

[28] L'analyse des liens est une technique utilisée pour étudier les relations entre un grand nombre d'objets de différents types. Dans le cadre du blanchiment d'argent, les objets peuvent être des personnes, des comptes bancaires, des entreprises, des virements électroniques et des dépôts en espèces. L'examen des associations entre ces divers objets permet d'indiquer les réseaux d'activité, tant légaux qu'illégaux. Cfr. Congrès américain, Office for Technology Assessment, *Information Technologies for the Control of Money Laundering* (US Government Printing Office 1995) 56 https://docplayer.net/28783887-Information-technologies-for-the-control-of-money-laundering-september-ota-itc-630-gpo-stock.html consulté le 26 mai2021.

surveillance, et pour identifier le bénéficiaire effectif (BE) [29] d'une transaction ou d'un nouveau compte.

2.3 Échanges de données entre États dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme.

2.3.1 Diligence raisonnable des clients

Le devoir de vigilance à l'égard de la clientèle (DDC) est un processus dans lequel les informations pertinentes sur le client d'une entité obligée sont recueillies et évaluées du point de vue du risque de blanchiment de capitaux ou de financement du terrorisme. Par conséquent, la réalisation du CDD est une source primaire d'information dans le système de LBC/FT. Les obligations en matière de CDD imposent aux entités obligées de mettre en place des contrôles et des procédures adéquats afin de connaître les clients avec lesquels elles traitent et de comprendre la nature de leurs activités.[30] Dans le cadre des mesures CDD d'identification, les entités obligées identifient généralement, au minimum, leurs clients et vérifient leur identité sur la base de documents, de données ou d'informations obtenus d'une source fiable et indépendante. Elles identifient également l'ayant droit économique et prennent des mesures raisonnables pour vérifier l'identité de cette personne afin que l'entité obligée sache qui est l'ayant droit économique, en particulier en ce qui concerne les personnes morales, les trusts, les sociétés, les fondations et les arrangements juridiques similaires, et qu'elle comprenne la structure de propriété et de contrôle du client. En outre, les entités obligées sont tenues d'obtenir des informations sur l'objet et la nature envisagée de la relation d'affaires.

Lorsqu'une activité ou une transaction comporte un risque plus élevé de blanchiment de capitaux ou de financement du terrorisme (y compris lorsqu'un pays tiers impliqué dans une transaction est considéré comme présentant un risque élevé), les entités soumises à l'obligation de vigilance appliquent des mesures CDD renforcées, notamment l'obtention d'informations sur le client ou le(s) bénéficiaire(s) effectif(s), la nature prévue de la relation d'affaires, l'origine des fonds et l'origine de la richesse du client et du(des) bénéficiaire(s) effectif(s).

2.3.2 Partage d'informations au sein d'un groupe

L'échange interétatique d'informations peut déjà avoir lieu au sein d'un groupe de plusieurs entreprises dont certaines peuvent être établies dans un autre État. Dans ce cas, ces entités obligées sont tenues de mettre en œuvre des politiques et des procédures à l'échelle du groupe pour l'échange d'informations à des fins de LBC/FT au sein du groupe auquel elles appartiennent.[31] Ces règles doivent être effectivement mises en œuvre au niveau des succursales et des filiales à participation majoritaire, tant dans les États membres que dans les pays tiers. Par groupe, on entend « un groupe d'entreprises composé d'une entreprise mère, de ses filiales et des entités dans lesquelles l'entreprise mère ou ses filiales détiennent une participation, ainsi que des entreprises liées l'une à l'autre par une relation au sens de

[29] Selon l'art.3(6) de la directive 2015/849 (AMLD4) : " on entend par "bénéficiaire effectif" toute(s) personne(s) physique(s) qui possède(nt) ou contrôle(nt) en dernier ressort le client et/ou la(les) personne(s) physique(s) pour le compte de laquelle (desquelles) une transaction ou une activité est effectuée ". L'article fournit également une liste de spécifications et d'explications dans le cas, par exemple, de trusts ou d'autres entités commerciales.

[30] Eds. Colin King, Clive Walker et Jimmy Gurulé, *The Palgrave Handbook of Criminal and Terrorism Financing Laws* (Palgrave Macmillan, 2018) p.42.

[31] Directive 2015/849 (4AMLD), art. 45(1).

l'article 22 de la directive 2013/34/UE».[32] La recommandation 18 du GAFI établit l'obligation pour les institutions financières de partager des informations au sein du groupe à des fins de lutte contre le blanchiment et le financement du terrorisme. Une exigence similaire se trouve à l'art. 45 de la 4AMLD. Compte tenu de la possibilité qu'une succursale ou une filiale d'un établissement de crédit ou d'un établissement financier soit située dans un pays tiers, où les exigences minimales en matière de LBC/FT sont moins strictes que celles de l'État membre, et afin d'éviter l'application de normes très différentes au sein de l'établissement ou du groupe d'établissements, les entités obligées doivent appliquer les normes de l'Union ou informer les autorités compétentes de l'État membre d'origine si l'application de ces normes n'est pas possible en raison des lois du pays tiers[33]. Les informations partagées concernent les informations relatives à des soupçons selon lesquels les fonds sont le produit d'une activité criminelle ou sont considérés comme liés au financement du terrorisme et, à ce titre, ont été signalés à la CRF.

2.3.3 Registres des propriétaires de bénéficiaires ultimes

La 4ème AMLD oblige les États membres de l'Union européenne à mettre en place des registres centraux des bénéficiaires effectifs (UBO) [34] et à fournir un accès rapide et illimité aux informations qui y sont stockées, dans tous les cas, aux autorités compétentes et aux CRF, ainsi qu'aux entités soumises à l'obligation de vigilance. Les registres UBO regroupent les informations sur les bénéficiaires effectifs qui sont définis comme « la ou les personnes physiques qui en dernier lieu possèdent ou contrôlent un client et/ou la personne physique pour le compte de laquelle une opération est effectuée. Sont également comprises les personnes qui exercent en dernier lieu un contrôle effectif sur une personne morale ou une construction juridique. »[35]. La 4AMLD prétendait que l'accès aux informations sur la propriété effective devait être accordé à d'autres personnes en mesure de démontrer un intérêt légitime. La 5AMLD a introduit un changement important en ce qui concerne ce dernier point. Conformément à l'article 30, paragraphe 5, modifié de la 4AMLD, les États membres doivent veiller à ce que les informations sur les sociétés ou autres entités juridiques soient accessibles non seulement à une personne ou à une organisation qui peut démontrer un intérêt légitime, mais aussi au grand public. Les membres du grand public doivent être autorisés à accéder au moins aux informations suivantes : le nom, le mois et l'année de naissance, le pays de résidence, la nationalité du bénéficiaire effectif et la nature et l'étendue du droit effectif détenu.[36]

Le CEPD a exprimé ses réserves sur l'Ouverture à l'accès aux registres UBO par le public et a recommandé de « concevoir l'accès aux informations sur les bénéficiaires effectifs dans le respect du principe de proportionnalité, entre autres, en n'octroyant cet accès qu'aux entités chargées de faire respecter la loi.»[37] Cependant, cette proposition n'a pas été reprise par les organes législatifs de l'UE lors de la promulgation de la 5AMLD.

---

[32] Directive 2015/849 (4AMLD), art. 3, tiret 15.
[33] Directive 2015/849 (4AMLD), considérant 48.
[34] Directive 2015/849 (4AMLD), art. 30(3).
[35] GAFI, Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (2020), p. 129 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Recommandations du GAFI 2012.pdf consulté le 25 mai 2021.
[36] Directive 2015/849 (4AMLD), art. 30(5).
[37] CEPD, Avis 1/2017 sur une proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE - Accès aux informations sur la propriété effective et incidences sur la protection des données (2 février 2017) https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_fr.pdf consulté le 25 mai 2021.

Au début de l'année 2021, le Tribunal d'arrondissement de Luxembourg a saisi la Cour de justice de l'Union européenne (CJUE) d'une demande de décision préjudicielle sur l'accès du grand public aux registres UBO.[38] Entre autres, le Tribunal d'arrondissement de Luxembourg a demandé en substance si le fait de rendre les informations sur les bénéficiaires effectifs accessibles au grand public sans qu'il soit nécessaire de démontrer un intérêt légitime est conforme aux droits à la vie privée et à la protection des données et à un certain nombre de principes et d'exigences concrets en matière de protection des données établis dans le RGPD. Elle a également demandé des précisions sur les restrictions d'accès prévues dans des circonstances exceptionnelles.

Aux Pays-Bas, l'ONG Privacy First Dutch a intenté une action en justice pour contester le registre UBO néerlandais pour des raisons de protection des données, en particulier pour non-respect du principe de proportionnalité. Le tribunal de district de La Haye n'a pas fait droit à la demande de désactivation du registre UBO et Privacy First a déposé un recours urgent contre l'intégralité du jugement du tribunal de district de La Haye, demandant notamment à la Cour d'appel de La Haye de soumettre une demande de décision préjudicielle à la CJUE, à l'instar de l'affaire luxembourgeoise mentionnée ci-dessus.

Il convient de prêter attention au fait que la directive 2019/1153[39] établit des registres centralisés de comptes bancaires, qui sont les mécanismes automatisés centralisés, tels que les registres centraux ou les systèmes centraux d'extraction de données électroniques, mis en place conformément à l'article 32a (1) de la 4AMLD, tel que modifié par la 5AMLD. Toutefois, ces registres centralisés de comptes bancaires (qui visent à permettre aux autorités de savoir rapidement où une personne a des comptes afin de pouvoir ensuite contacter l'institution financière concernée pour obtenir des données plus détaillées sur le client) sont des registres complètement différents des registres UBO et ne doivent pas être confondus avec ces derniers.

2.3.4 Accès supplémentaire aux données par les CRF

Lorsque l'entité obligée sait, soupçonne ou à des motifs raisonnables de soupçonner que des fonds, quel que soit le montant en jeu, sont le produit d'une activité criminelle ou sont liés au financement du terrorisme, elle doit en informer la CRF. Toutes les opérations suspectes, y compris les tentatives d'opérations, doivent être déclarées[40] par le biais d'une déclaration d'opérations suspectes, qui est devenue la principale source d'information sur le blanchiment de capitaux ou le financement du terrorisme dont dispose la CRF. Après la soumission d'une déclaration de soupçon avec toutes informations à l'appui, l'entité obligée peut toujours être contactée par une CRF pour toute information supplémentaire nécessaire concernant l'événement déclaré.[41] En outre, depuis l'entrée en vigueur de la loi 5AMLD, les CRF peuvent demander des informations indépendamment du fait que l'entité requise ait déposé une déclaration de soupçon antérieure[42]. Il s'agit d'un changement important, car la déclaration de soupçon n'est plus un filtre servant de condition préalable à l'accès des CRF aux données des entités obligées.

Outre les DOD et les DRS, d'autres sources d'information cruciales pour les CRF peuvent provenir d'autres bases de données publiques existantes. Étant donné que les connaissances acquises à partir des DOD/SAR peuvent devoir être complétées, les CRF devraient "avoir

[38] Affaire C-601/20 *SOVIM SA c. Luxembourg Business Registers* [2020].
[39] Directive 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 établissant des règles visant à faciliter l'utilisation d'informations financières et autres pour la prévention, la détection, l'investigation ou la poursuite de certaines infractions pénales, et abrogeant la décision 2000/642/JAI du Conseil.
[40] Directive 2015/849 (4AMLD) Art. 33(1).
[41] Directive 2015/849 (4AMLD) Art. 33(1)(b) tel que modifié par la directive 2018/843 (5AMLD)
[42] Directive 2015/849 (4AMLD) Art 32(9), tel que modifié par la directive 2018/843 (5AMLD)

accès, directement ou indirectement, en temps utile, aux informations financières, administratives et policières dont elles ont besoin pour s'acquitter correctement de leurs tâches".[43]

La 4AMLD ne précise toutefois pas à quel type d'informations "financières", "administratives" ou "répressives" les CRF devraient avoir accès, ni dans quelle mesure ces sources d'information devraient être mises à la disposition des CRF dans la pratique. Cela laisse une grande marge de manœuvre aux États membres pour déterminer ces questions.

2.3.5 Partage des données au sein des Partenariats public-privé (PPP)

En plus des modèles existants d'échange d'informations entre les entités obligées, les CRF, les autorités compétentes, les partenariats public-privé (PPP) favorisent l'échange d'informations financières. Les origines du premier PPP d'échange de renseignements financiers remontent à 2015, lorsque la *Joint Money Laundering Intelligence Taskforce* (JMLIT) a été créée au Royaume-Uni. Puis, au tournant des années 2015 et 2016 au Canada, une initiative connue sous le nom de " *Project PROTECT* " a donné lieu à la mise en place d'un PPP unique pour cibler la traite des êtres humains à des fins d'exploitation sexuelle en tenant compte de l'aspect blanchiment d'argent de ce crime.[44] En 2017, le Centre australien de déclaration et d'analyse des transactions (AUSTRAC) a lancé un PPP pour le partage de renseignements financiers nommé "*Fintel Alliance*". La même année, à Singapour, le partenariat de l'industrie de la lutte contre le blanchiment d'argent et le financement du terrorisme (ACIP) a été créé et, à Hong Kong, le groupe de travail sur la fraude et le blanchiment d'argent (FMLIT). Depuis lors, le nombre de PPP dans le monde n'a cessé d'augmenter.

Avec quelques différences dans leur composition et leur mode de fonctionnement exact, les PPP sont des plateformes de collaboration établies principalement dans le but de faciliter la collaboration entre le secteur bancaire et le gouvernement dans la lutte contre la criminalité financière.[45] Grâce à l'expertise et aux ressources collectives des deux secteurs, il est envisagé d'améliorer la détection, la prévention et la neutralisation des menaces graves de criminalité financière et de blanchiment d'argent.

Le terme PPP a évolué au fil du temps et, dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme, il sert à décrire des formes de collaboration public-privé pour le partage d'informations stratégiques et/ou tactiques. Cela signifie qu'au cœur de la collaboration entre les partenaires publics et privés se trouve le renseignement qui peut être généré grâce à la combinaison de plusieurs éléments d'information dispersés entre les membres d'un PPP et qui ne peuvent former une image complète qu'en étant rassemblés. L'image créée par le suivi des transactions peut concerner soit un cas spécifique et permettre ainsi d'enquêter sur certains incidents suspects, soit des modèles plus généraux d'activité criminelle. Ainsi, on peut conclure qu'un PPP dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme peut servir à soutenir les enquêtes des autorités compétentes ou à soutenir la conformité des entités obligées, ou une combinaison des deux.[46] L'objectif principal des PPP d'enquête est de permettre au secteur privé de contribuer aux enquêtes en cours des autorités compétentes. Le principal objectif des PPP de conformité est de permettre au secteur public de contribuer à l'amélioration de la conformité du secteur privé avec les mesures de LBC/FT (en particulier le CDD). Les PPP de conformité, axés sur le développement et le partage de typologies, sont susceptibles d'avoir des exigences moindres

[43] Directive 2015/849 (4AMLD) Article 32(4).
[44] FINTRAC, *Projet PROTECT* (Renouvellement du service public en action) https://www.fintrac-canafe.gc.ca/emplo/psr-eng.pdf, consulté le 25 mai 2021.
[45] Oldrich Bures, Les partenariats public-privé dans la lutte contre le terrorisme ? [2013] 60(4) Crime, Law and Social Change, p. 441.
[46] Benjamin Vogel, Jean-Baptiste Maillart, *National and international anti-money laundering law* (1st edn Insertia 2020), p. 922 ss et 1015 ss.

en matière de renseignement opérationnel et de se concentrer principalement sur le renseignement stratégique. Enfin, les PPP hybrides combinent les objectifs des PPP d'enquête et de conformité.

3. Échanges de données dans le domaine de la fiscalité

3.1 FATCA AMÉRICAIN

Les États-Unis ont élaboré leurs propres politiques en matière d'échange d'informations à des fins fiscales en s'appuyant essentiellement sur la coopération des institutions financières.[47] En 2010, ils ont adopté la loi HIRE (*Hiring Incentives to Restore Employment Act*), qui comprenait la loi FATCA (*Foreign Account Tax Compliance Act*). La FATCA leur a permis de prélever un impôt, en vertu de leur propre législation fiscale, sur tous les comptes détenus à l'étranger par des personnes soumises à l'impôt aux États-Unis. Garbarino résume les principaux points de la FATCA comme suit :

> *La FATCA a établi un principe de base : une institution financière étrangère ("FFI") est soumise à une retenue à la source de 30 % sur tous ses revenus provenant des États-Unis, à moins qu'elle ne se conforme aux obligations de déclaration FATCA en ce qui concerne les informations relatives aux "U.S. Persons" qui sont titulaires de comptes auprès de cette institution ("données FATCA"). La FATCA impose donc aux FFI, où qu'elles soient situées en dehors des États-Unis, un régime étendu de contrôle et de divulgation par des tiers, dans le but d'exposer leurs actifs étrangers non déclarés à l'I.R.S. [International Revenue Service] américain.*
>
> *Plus précisément, la FATCA a introduit unilatéralement un mécanisme complexe de collecte d'informations géré par les intermédiaires financiers et reposant sur quatre éléments : 1) l'identification de la FFI participante, 2) l'obligation de déclaration par cette FFI de certains titulaires américains et non américains de comptes, 3) la menace d'une retenue à la source sur les paiements d'origine américaine en cas de non-conformité, et 4) l'obligation pour les U.S. Persons de déclarer spécifiquement à l'I.R.S. leurs actifs financiers étrangers. [48]*

3.2 Cadre supranational pour l'échange de données dans le domaine de la fiscalité

Au début de la décennie précédente, un certain nombre de documents réglementaires et politiques ont été adoptés concernant l'échange de données à des fins administratives et fiscales. Le Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales, fondé en 2000 et restructuré en septembre 2009, travaille sous les auspices de l'OCDE et du G20.

L'OCDE a adopté un nombre d'instruments qui facilitent l'échange de données dans le domaine de la fiscalité. En 1988, le Conseil de l'Europe et l'Organisation de coopération et de développement économiques (OCDE) ont adopté une convention commune concernant

[47] Carlo Garbarino, *The EU Protection of Tax Data Transferred to Third Countries* (2020) Bocconi Legal Studies Research Paper No. 3730009, p. 2.
[48] Ibid, p.3.

l'assistance administrative mutuelle en matière fiscale[49] qui a été modifiée par un protocole en 2010. Ce traité permet aux parties, les États membres du Conseil de l'Europe et les pays membres de l'OCDE, de développer une coopération administrative étendue couvrant tous les impôts obligatoires, y compris l'échange de renseignements entre les parties.

L'article 6 de la Convention multilatérale concernant l'assistance administrative mutuelle en matière fiscale (MAC) prévoit que deux ou plusieurs parties échangent automatiquement tous les renseignements vraisemblablement pertinents pour l'administration ou l'application de leur législation interne relative à leurs impôts[50], pour les catégories de cas et selon les procédures qui sont déterminées dans un accord mutuel. En vertu de cet article, qui exige que les autorités compétentes des parties à la convention conviennent mutuellement du champ d'application de l'échange automatique de renseignements et de la procédure à suivre, l'accord multilatéral d'autorité compétente CRS (CRS MCAA) a été adopté. Le CRS MCAA est un accord-cadre multilatéral qui précise les détails sur les types d'informations à échanger et le moment où cela sera réalisé.

Les juridictions peuvent également s'appuyer sur des accords bilatéraux pour l'échange d'informations, tels qu'une convention de double imposition ou un accord d'échange d'informations fiscales.[51] Comme nous le verrons plus loin, les échanges de SIR se feront sur la base de la Directive CAD2, des accords entre l'UE et les pays tiers et des accords bilatéraux, tels que les accords UK-CDOT. [52]

Le modèle de convention fiscale de l'OCDE concernant le revenu et la fortune[53] permet de régler sur une base uniforme les questions les plus courantes qui se posent dans le domaine de la double imposition juridique internationale.[54] L'article 26 du modèle de convention fiscale de l'OCDE constitue une base pour toutes les formes d'échange de renseignements entre les autorités compétentes. Les autorités compétentes des États contractants échangent les renseignements vraisemblablement pertinents pour assurer l'application correcte des dispositions de la convention à la législation interne des États contractants relative aux impôts de toute nature. [55]

Le Forum mondial sur la transparence et l'échange d'informations à des fins fiscales soutient à la fois l'échange d'informations sur demande (EOIR) et l'échange automatique d'informations (AEOI) entre autorités fiscales, ainsi que l'échange spontané d'informations. [56]

L'EOIR, s'appuie sur un système d'examens par les pairs sur l'EOIR, au cours duquel le cadre légal et réglementaire d'une juridiction et sa mise en œuvre dans la pratique sont évalués. La norme internationale prévoit l'échange sur demande de renseignements vraisemblablement pertinents pour l'application des dispositions d'une convention fiscale ou pour l'administration ou l'application de la législation fiscale interne d'une partie requérante.

[49] OCDE et Conseil de l'Europe, La Convention multilatérale concernant l'assistance administrative mutuelle en matière fiscale : Amendée par le Protocole de 2010 (Éditions OCDE 2011).
[50] Ibid, article 4.
[51] OCDE, Portail d'échange automatique - Cadre international pour le CRS, <https://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/> consulté le 25 mai 2021.
[52] Ibid.
[53] OCDE, Modèle de convention fiscale concernant le revenu et la fortune : Version condensée (Éditions OCDE 2017)
[54] Ibid, Introduction.
[55] Ibid, commentaire de l'article 26 concernant l'échange d'informations.
[56] OCDE, 'Activités substantielles dans des juridictions fiscales nulles ou seulement nominales : Orientations pour l'échange spontané de renseignements' (2019). https://www.oecd.org/tax/beps/substantial-activities-in-no-or-only-nominal-tax-jurisdictions-guidance-for-the-spontaneous-exchange-of-information.htm 25 mai 2021.

En 2014, l'OCDE, en collaboration avec les pays du G20, a élaboré la Norme d'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale (la Norme AEOI), communément appelée Norme commune de déclaration (NCD), qui a ensuite été approuvée par le Forum mondial. La CRS invite les juridictions à obtenir des informations de leurs institutions financières et à les échanger automatiquement avec d'autres juridictions sur une base annuelle. Il définit les informations sur les comptes financiers à échanger, les institutions financières tenues de faire des déclarations, les différents types de comptes et de contribuables couverts, ainsi que les procédures communes de diligence raisonnable à suivre par les institutions financières.[57] En principe, les échanges ont lieu sur une base réciproque. Le SRC comprend quatre parties : (i) un modèle d'accord de l'autorité compétente (CAA) pour l'échange automatique d'informations CRS ; (ii) la Norme commune de déclaration ; (iii) les Commentaires sur le CAA et le CRS ; et (iv) le Guide d'utilisation du schéma XML CRS, qui est un schéma en langage XML pour l'échange d'informations. Il convient de noter que le CRS s'inspire de l'approche intergouvernementale pour la mise en œuvre de la FATCA :

> *La Norme commune de déclaration (« NCD »), qui vise à optimiser l'efficacité et à réduire les coûts pour les institutions financières, est largement inspirée de l'approche intergouvernementale suivie pour la mise en œuvre de la loi FATCA. Bien que cette approche diffère de la NCD sur certains aspects, les différences tiennent à la nature multilatérale du système NCD et à d'autres facteurs spécifiques aux États-Unis, en particulier le concept d'imposition fondée sur la citoyenneté et l'existence d'une retenue d'impôt à la source significative et libératoire au titre de la loi FATCA. Compte tenu de ces caractéristiques, du fait que l'approche intergouvernementale pour l'application de la loi FATCA est un système préexistant qui présente d'étroites similitudes avec la NCD, et des progrès escomptés vers une large adhésion à la NCD, la démarche des États-Unis qui consiste à ne pas requérir de regarder à travers les entités d'investissement implantées dans des juridictions non-partenaires est compatible et en accord avec la NCD. [58]*

L'article 22 de la MAC sur le secret prévoit des exigences strictes en matière de confidentialité et limite les entités auxquelles les informations peuvent être révélées. Il stipule que toute information protégée par une partie en vertu de La MAC doit être protégée de la même manière que les informations obtenues en vertu du droit interne de la partie et, dans la mesure où cela est nécessaire pour assurer le niveau nécessaire de protection des données personnelles, conformément aux garanties qui peuvent être spécifiées par la partie qui fournit les informations, comme l'exige son droit interne. L'article 22 de La MAC précise également les fins auxquelles les informations peuvent être utilisées. La section 5 de CRS MCAA sur la confidentialité et la protection des données reflète dans une large mesure les dispositions de l'article 22 de la MAC. En particulier, en ce qui concerne la confidentialité et la protection des données, la section 5 du CRS MCAA stipule que « Toutes les informations échangées sont soumises aux règles de confidentialité et aux autres garanties prévues par la Convention, y compris les dispositions limitant l'utilisation des informations échangées et, dans la mesure où cela est nécessaire pour assurer le niveau de protection des données à caractère personnel requis, conformément aux garanties qui peuvent être spécifiées par l'autorité compétente pour la fourniture, conformément à son droit interne, et énumérées à l'annexe C [du CRS MCAA] »[59]. Il convient donc de souligner que l'article 22 de la MAC et la section 5 du CRS MCAA permettent à la juridiction expéditrice de spécifier des exigences supplémentaires spécifiques à la protection des données personnelles qui doivent être respectées par la

[57] OCDE, Norme pour l'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale (2e éd. Éditions OCDE 2017), p.3.
[58] Ibid, p. 10.
[59] OCDE, Norme pour l'échange automatique de renseignements relatifs aux comptes financiers en matière fiscale, Modèle d'accord entre autorités compétentes et norme commune de déclaration, section 5 (2e éd. Éditions OCDE 2017).

juridiction destinataire. Ces exigences sont précisées par l'autorité compétente dans une notification adressée au Secrétariat de l'Organe de coordination et spécifiant toute mesure de sauvegarde éventuelle pour la protection des données à caractère personnel (Annexe C), conformément à la section 7(1)(d) du CRS MCAA.

La section 5(2) du CRS MCAA établit l'obligation pour l'autorité compétente de notifier immédiatement au secrétariat de l'organe de coordination toute violation de la confidentialité ou tout manquement aux garanties, ainsi que toute sanction éventuelle et toute mesure corrective imposée en conséquence. Le non-respect de cette obligation (ou de toute autre obligation établie dans le CRS MCAA) entraîne le droit de suspendre l'échange d'informations avec effet immédiat (section 7 du CRS MCAA).

3.3 Cadre européen pour l'échange de données dans le domaine de la fiscalité

Au niveau de l'Union européenne, l'échange d'informations à des fins fiscales au plan de l'UE et au plan mondial a occupé une place importante dans l'agenda européen au cours des dix dernières années. En 2011, le Conseil a adopté la Directive 2011/16 relative à la coopération administrative dans le domaine fiscal[60], communément appelée DAC1. La DAC1 définit l' " échange automatique " comme « la communication systématique, sans demande préalable, d'informations prédéfinies, à intervalles réguliers préalablement fixés, à un autre État membre. Dans le cadre de l'article 8 [Champ d'application et conditions de l'échange automatique et obligatoire d'informations], les informations disponibles désignent des informations figurant dans les dossiers fiscaux de l'État membre qui communique les informations et pouvant être consultées conformément aux procédures de collecte et de traitement des informations applicables dans cet État membre ». [61]

La DAC1 prévoit trois formes d'échange d'informations, à savoir : sur demande (l'autorité requise doit communiquer à l'autorité requérante toute information pertinente en sa possession ou qu'elle obtient à la suite d'enquêtes administratives) ; spontanément (par la communication non systématique, à tout moment et sans demande préalable, d'informations à un autre État membre) ; et automatiquement (lorsque la communication systématique d'informations prédéfinies à un autre État membre a lieu, sans demande préalable, à intervalles réguliers préétablis). L'article le plus pertinent pour le sujet examiné dans ce rapport est l'article 8 sur la portée et les conditions de l'échange automatique obligatoire d'informations.

La Directive 2014/107 (DAC2) a modifié la DAC1 et a prévu l'échange automatique d'informations sur les comptes financiers à l'art. 8, paragraphe 3a.[62] Le CRS, examiné dans la section précédente, s'applique en Europe en vertu de la DAC2. Le cadre juridique de l'UE en matière de coopération administrative a été complété par la Directive 2015/2376[63] (DAC3) qui a ajouté à la DAC1 l'article 8 bis relatif à la portée et aux conditions de l'échange automatique obligatoire d'informations sur les décisions anticipées transfrontalières et les accords préalables en matière de prix.

[60] Directive 2011/16/UE du Conseil du 15 février 2011 en ce qui concerne la coopération administrative dans le domaine fiscal et abrogeant la directive 77/799/CEE.
[61] Ibid, Art. 3(9).
[62] Directive 2014/107/UE du Conseil du 9 décembre 2014 modifiant la directive 2011/16/UE relative à l'échange automatique obligatoire d'informations dans le domaine fiscal.
[63] Directive (UE) 2015/2376 du Conseil du 8 décembre 2015 modifiant la directive 2011/16/UE relative à l'échange automatique obligatoire d'informations dans le domaine fiscal.

Afin de faciliter la lutte contre le blanchiment de capitaux et le financement du terrorisme, le Conseil a adopté la Directive 2016/2258 (DAC5) en ce qui concerne l'accès des autorités fiscales aux informations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.[64] La Directive 2016/2258 fournit une base permettant aux autorités fiscales d'accéder aux informations, procédures, documents et mécanismes de lutte contre le blanchiment d'argent pour l'exercice de leurs fonctions de contrôle de la bonne application de la Directive 2011/16/UE et pour le fonctionnement de toutes les formes de coopération administrative prévues par cette directive.[65] Enfin, la Directive 2018/822[66] (DAC6) a été adoptée en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal en rapport avec les dispositifs transfrontières devant faire l'objet d'une déclaration.[67] La DAC6 oblige les intermédiaires (tels que les conseillers fiscaux, les comptables, les cabinets d'avocats et les banques) à communiquer certaines informations sur les montages transfrontaliers aux autorités fiscales locales. Il s'applique aux accords impliquant des parties situées dans plusieurs pays, dont l'un au moins est un État membre de l'UE. [68]

La figure 2 donne un aperçu des directives sur la coopération administrative et des principales modifications qu'elles ont apportées à la DAC1.

[64] Directive (UE) 2016/2258 du Conseil du 6 décembre 2016 modifiant la directive 2011/16/UE en ce qui concerne l'accès des autorités fiscales aux informations relatives à la lutte contre le blanchiment de capitaux.
[65] Ibid, Art. 22, paragraphe 1a.
[66] Directive (UE) 2018/822 du Conseil du 25 mai 2018 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal en rapport avec les dispositifs transfrontières devant faire l'objet d'une déclaration.
[67] Ibid, Art. 8ab.
[68] ING, DAC6 : Directive de l'UE contre les arrangements fiscaux agressifs https://www.ing.com/About-us/Compliance/Automatic-Exchange-of-Information-AEOI/DAC6.htm consulté le 25 mai 2021.

Figure 2Directives de l'UE sur la coopération administrative (DAC) [69]

En 2019, la Directive 2019/1153 a été adoptée, établissant des règles facilitant l'utilisation d'informations financières et autres pour la prévention, la détection, l'enquête ou la poursuite de certaines infractions pénales.[70]

3.4 Échanges de données à des fins fiscales

Les sections précédentes ont clairement montré que le cadre juridique et réglementaire de l'échange d'informations entre États régit principalement l'échange d'informations entre autorités compétentes. Dans le cadre de ce rapport, l'accent est mis, dans le domaine de la fiscalité, sur l'échange automatique d'informations étant donné qu'il s'agit non seulement de l'objet de l'attention de l'OCDE et des législateurs nationaux, mais aussi parce qu'il couvre la part du lion en matière d'échange d'informations entre États.

[69] Commission européenne, Coopération administrative en matière de fiscalité (directe) dans l'UE - Directives de l'UE sur la coopération administrative (CAD) https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en , consulté le 25 mai 2021.

[70] Directive (UE) 2019/1153 du Parlement européen et du Conseil du 20 juin 2019 fixant les règles facilitant l'utilisation d'informations financières et d'une autre nature aux fins de la prévention ou de la détection de certaines infractions pénales, ou des enquêtes ou des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil.

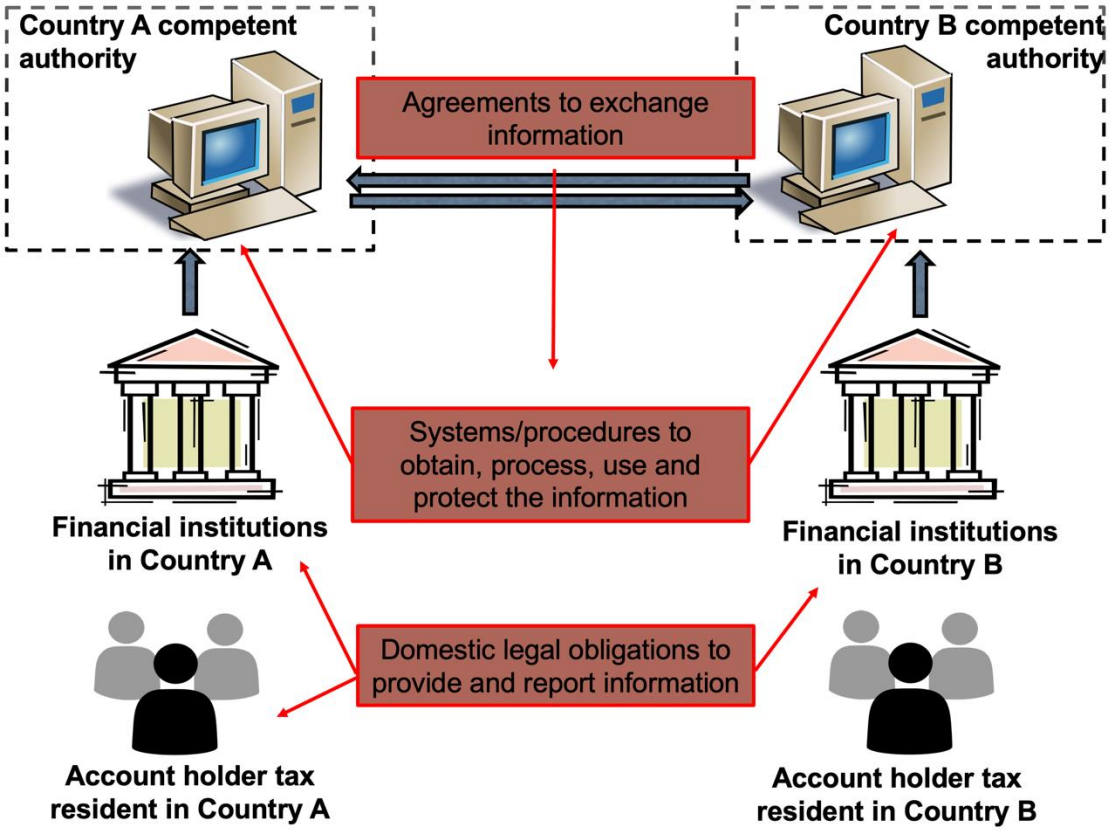

Figure 3Cadre de base du SIR [71]

4. Acteurs impliqués

La Convention 108+ reconnaît quatre grandes catégories d'acteurs : les personnes concernées, les responsables du traitement, les sous-traitants les autorités de contrôle. La répartition correcte des rôles entre les acteurs impliqués dans le traitement des données est essentielle pour attribuer les droits et obligations correspondants aux acteurs pertinents. Dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme ainsi que dans celui de la fiscalité, il existe des zones d'incertitude quant aux catégories de personnes concernées et cette question est aggravée dans le cas d'échanges automatiques de données personnelles. La distinction entre personnes concernées, responsables du traitement et sous-traitants permet de séparer leurs rôles et responsabilités. Alors que les personnes concernées bénéficient d'un ensemble de droits, un ensemble d'obligations est imposé aux responsables du traitement et aux sous-traitants. Les autorités de contrôle, quant à elles, sont chargées de veiller au respect du cadre juridique de la protection des données et de faciliter son efficacité.

[71] South African Revenue Service, *'How does CRS reporting work'* https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/how-does-crs-reporting-work/ (Figure modifiée par l'auteur).

4.1 Contexte LBC/FT

Dans le contexte de la lutte contre le blanchiment d'argent et le financement du terrorisme, l'identification et la vérification de l'identité constituent l'une des mesures CDD les plus importantes et la pierre angulaire de la stratégie. Cela signifie que les principales personnes concernées dans le contexte de la LBC/FT sont les clients qui sont des personnes physiques ou morales, des trusts et des structures similaires (dans le cas de ces dernières, les bénéficiaires effectifs ultimes). En ce qui concerne les personnes physiques, il ne fait aucun doute qu'elles sont des individus (déjà) identifiés ou identifiables, et donc certainement des personnes concernées. En ce qui concerne les personnes morales, en principe, les données d'une société ne sont pas en soi des données à caractère personnel, à moins qu'il ne s'agisse de données concernant une personne physique. Cela peut être le cas des sociétés détenues par une seule personne, c'est-à-dire des entités pour lesquelles il est impossible de considérer séparément la société et le propriétaire, par exemple lorsque le nom de la société est celui du propriétaire. Toutefois, les Parties à la Convention 108+ « peuvent prévoir dans leur droit interne une extension de la protection aux données relatives aux personnes morales afin de protéger les intérêts légitimes de celles-ci ».[72]

En ce qui concerne les trusts (et équivalents), la définition du bénéficiaire effectif est plus large que pour les personnes morales. Par conséquent, presque toutes les personnes concernées peuvent être qualifiées de bénéficiaires effectifs ultimes, c'est-à-dire le constituant, le ou les trustees, le protecteur (le cas échéant), les bénéficiaires, ou toute autre personne physique exerçant un contrôle ultime sur le trust par le biais d'une propriété directe ou indirecte ou par d'autres moyens.[73] L'identification des bénéficiaires effectifs ultimes est essentielle pour identifier correctement les personnes concernées par l'échange de données.

L'attribution des rôles de responsables du traitement et de sous-traitant aux entités concernées est plus compliquée. Les entités obligées et les CRF sont les principaux acteurs concernés dans ce contexte, tandis que les tierces parties qui appliquent des mesures de CDD sont également impliquées.

Les entités obligées semblent correspondre le mieux à la définition des responsables du traitement. Ce sont des entités juridiques qui ont un pouvoir de décision en ce qui concerne le traitement des données.[74] Le contrôle peut être défini par la loi.[75] Les entités obligées peuvent sous-traiter l'exécution des mesures CDD à des tiers. Du point de vue de la protection des données, la question est de savoir si ces entités doivent être considérées comme des responsables du traitement ou des sous-traitants. Le facteur décisif semble être lié à la question de savoir qui a le pouvoir de décision en ce qui concerne le traitement des données en question. Or, la question est de savoir quel est le traitement en cause. Si l'on considère que c'est le traitement qui vise à faire respecter les mesures CDD par l'entité obligée, le tiers peut être considéré comme agissant pour le compte de cette entité obligée et donc être un sous-traitant. Si le tiers traite les mêmes ensembles de données, mais à d'autres fins que celles déterminées dans les instructions de traitement par le responsable du traitement,

[72] Conseil de l'Europe, Rapport explicatif sur le Protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (2018) para. 30 : https://rm.coe.int/16808ac91b , consulté le 25 mai 2021.
[73] Directive 2015/849 (4AMLD), art. 3 alinéa 6 (ii).
[74] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 223, Art. 2(d).
[75] Contribution du Contrôleur européen de la protection des données, Groupe parlementaire mixte d'Europol - 7eme réunion, 28 septembre 2020, paragraphe 19 https://www.europarl.europa.eu/cmsdata/211695/EDPS_letter_23092020.pdf consulté le 26 mai 2021.

obtenant ainsi un pouvoir de décision, alors pour cette activité de traitement, ce tiers serait considéré comme responsable du traitement.

L'attribution des rôles de responsable du traitement ou de sous-traitant en cas de traitement par un groupe d'entreprises, qui peut être constitué d'une entreprise mère, de ses filiales et des entités auxquelles l'entreprise mère ou ses filiales participent, est une tâche difficile. Selon le raisonnement de l'EDPB, il est plus important de prendre en compte la relation factuelle entre les parties prenantes impliquées dans le traitement. Dans le cas de groupes, plusieurs scénarios semblent possibles. Étant donné que les membres du groupe sont étroitement liés par des entités distinctes sur le plan organisationnel, chacun d'entre eux peut être un responsable du traitement indépendant dans la mesure où il dispose d'un pouvoir de décision sur le traitement des données. Les régimes LAB/CFT prévoient toutefois la possibilité de partager des informations au sein d'un groupe, y compris des données personnelles. Dans ce cas, un contrôle conjoint peut être envisagé. Cela suppose toutefois que tous les responsables du traitement, c'est-à-dire tous les membres du groupe impliqués dans la même activité de traitement, aient un pouvoir de décision sur le traitement des données. Si tel est le cas, le groupe peut être considéré comme des responsables conjoints du traitement.

Les CRF collectent et analysent les informations dans le but assez clair d'identifier les raisons de suspecter le blanchiment de capitaux, des infractions sous-jacentes associées ou un financement du terrorisme[76] et de diffuser ensuite les analyses et informations pertinentes aux autorités compétentes. Une telle finalité du traitement est déterminée par la loi, ce qui signifie que le rôle de responsable du traitement peut en fait être défini par la loi[77], ce qui lui confère un pouvoir de décision. Le législateur désigne les CRF comme responsables du traitement en raison de leur réelle capacité à exercer un contrôle.[78] La 4AMLD ne prévoit que les compétences des CRF pour accéder aux informations provenant de diverses sources. Les détails de la collecte d'informations, ainsi que de l'analyse, doivent être déterminés par chaque CRF.

L'attribution des rôles de protection des données aux entités participant à un PPP de LBC/FT pose de sérieux problèmes, principalement en raison du manque *de facto* de transparence des dispositions régissant le PPP (voir section 2.3.5). Compte tenu des diverses structures que peuvent avoir ces PPP et des divers objectifs qu'ils poursuivent principalement, il n'existe pas de modèle unique applicable à la protection des données personnelles lorsque celles-ci sont échangées entre les entités impliquées dans un PPP. L'analyse doit toujours se faire au cas par cas. Il est conseillé, lors de la mise en place d'un PPP, de répartir clairement les rôles entre les entités participantes et de délimiter les droits et obligations en matière de traitement des données personnelles.

4.2 Domaine de la fiscalité

La définition précise des personnes concernées dont les données sont impliquées dans l'échange d'informations est cruciale afin d'éviter la collecte et le transfert en masse de données personnelles. Les autorités compétentes qui ont le pouvoir de décision en ce qui concerne l'échange de données sont les responsables du traitement. Cependant, le rôle des entités qui sont autorisées à utiliser les données échangées sera défini en fonction de leurs pouvoirs, et en particulier s'ils ont un pouvoir de décision. Lorsqu'elles établiront des règles

[76] Directive 2015/849 (4ALMD), article 32.
[77] Conseil européen de la protection des données, Lignes directrices 07/2020 sur les concepts de contrôleur et de sous-traitant dans le RGPD, version 1.0,02 septembre 2020, paragraphe 19 https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf consulté le 26 mai 2021.
[78] Ibid, paragraphe 21.

impliquant l'échange de données, les parties à la Convention veilleront à prévoir une répartition claire des rôles en matière de protection des données, accompagnée de droits et d'obligations concrets.

5. Droits des personnes concernées

La Convention 108+ établit un certain nombre de droits pour les personnes concernées à l'article 9 :

- le droit de ne pas être soumises à une décision les affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que [leur] point de vue soit pris en compte (article 9, paragraphe 1, point *a*), de la Convention 108+ du Conseil de l'Europe), [à moins qu'une telle décision ne soit] autorisée par une loi […] qui prévoit également des mesures appropriées pour la sauvegarde des droits, des libertés et des intérêts légitimes de la personne concernée (article 9, paragraphe 2, de la Convention 108+ du Conseil de l'Europe) ;
- le droit d'obtenir à [leur] demande, à intervalles raisonnables et sans délais ou frais excessifs, la confirmation du traitement des données [les] concernant (article 9, paragraphe 1, point *b*) de la Convention 108+ du Conseil de l'Europe) ;
- le droit de recevoir communication sous une forme intelligible des données traitées, et toute information disponible sur leur origine, sur la durée de leur conservation ainsi que de toute autre information que le responsable du traitement est tenu de fournir au titre de la transparence des traitements conformément à l'article 8, paragraphe 1 de la Convention 108+ du Conseil de l'Europe, [qui précise les informations minimales à fournir (article 9, paragraphe 1, point *b*), de la Convention 108+ du Conseil de l'Europe)] ;
- le droit d'obtenir, à [leur] demande, connaissance du raisonnement qui sous-tend le traitement des données, lorsque les résultats de ce traitement lui sont appliqués (article 9, paragraphe 1, point *c*), de la Convention 108+ du Conseil de l'Europe) ;
- le droit de s'opposer à tout moment, pour des raisons tenant à [leur] situation, à ce que des données à caractère personnel les concernant fassent l'objet d'un traitement, à moins que le responsable du traitement ne démontre des motifs légitimes justifiant le traitement qui prévalent sur les intérêts, ou les droits et libertés fondamentales [des] personnes concernées (article 9, paragraphe 1, point *d*), de la Convention 108+ du Conseil de l'Europe) ;
- le droit d'obtenir, à [leur] demande, sans frais et sans délai excessif, la rectification de [leurs] données ou le cas échéant, leur effacement lorsqu'elles sont ou ont été traitées en violation des dispositions de la […] convention (article 9, paragraphe 1, point *e*), de la Convention 108+ du Conseil de l'Europe) ;
- le droit de disposer d'un recours conformément à l'article 12 , lorsque [leurs] droits prévus par la […] convention ont étés violés (article 9, paragraphe 1, point *f)*, de la Convention 108+ du Conseil de l'Europe) ;
- le droit de bénéficier, quelle que soit [leur] nationalité ou [leur] résidence, de l'assistance d'une autorité de contrôle au sens de l'article 15 pour l'exercice de [leurs] droits prévus par la […] convention (article 9, paragraphe 1, point *g*) de la Convention 108+ du Conseil de l'Europe).

Chaque partie à la Convention 108+ du Conseil de l'Europe doit aider toute personne concernée, quelle que soit sa nationalité ou sa résidence, à exercer les droits susmentionnés (article 18, paragraphe 1, de la Convention 108+ du Conseil de l'Europe).

5.1 Restrictions dans le cadre de la Convention 108+

Plusieurs des droits susmentionnés peuvent être difficiles à satisfaire lorsqu'il y a des intérêts prépondérants à servir. C'est pourquoi la Convention 108+ du Conseil de l'Europe prévoit un certain nombre de cas dans lesquels les droits de la personne concernée peuvent être restreints, certains pouvant être pertinents pour la restriction des droits de la personne concernée dans le cas d'échange de données personnelles à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme ou à des fins fiscales.

L'article 11 de la Convention 108+ permet des exceptions aux dispositions de l'article 5, paragraphe 4 (principes de protection des données), de l'article 7, paragraphe 2 (notification des violations de données), de l'article 8, paragraphe 1 (transparence du traitement) et de l'article 9 (droits des personnes concernées), lorsqu'elles sont prévues par la loi, respectent l'essence des droits et libertés fondamentaux et constituent une mesure nécessaire et proportionnée dans une société démocratique pour les raisons suivantes :

a. la protection de la sécurité nationale, de la défense, de la sûreté publique, des intérêts économiques et financiers importants de l'État, de l'impartialité et de l'indépendance du pouvoir judiciaire ou de la prévention, de l'instruction et de la poursuite des infractions pénales et de l'exécution des sanctions pénales, ainsi que d'autres objectifs essentiels d'intérêt public général ;

b. la protection de la personne concernée ou des droits et libertés fondamentales d'autrui, notamment la liberté d'expression.[79]

Des exceptions supplémentaires peuvent être autorisées pour des activités de traitement à des fins de sécurité nationale et de défense, par la loi et uniquement dans la mesure où elles constituent une mesure nécessaire et proportionnée dans une société démocratique pour atteindre un tel objectif, à l'article 4, paragraphe 3 (évaluation de l'efficacité des mesures par le comité de la convention), à l'article 14, paragraphes 5 et 6 (information de l'autorité de contrôle sur les transferts de données) et à l'article 15, paragraphe 2, points *a), b), c)* et *d).*

5.2 Restrictions en vertu de l'article 23 du RGPD

Des restrictions similaires aux droits des personnes concernées, mais encore plus larges, sont prévues à l'article 23 du RGPD, qui donnent la possibilité de restreindre les droits des personnes concernées et l'application de tous les principes de base du traitement des données personnelles (à l'exception de la responsabilité), c'est-à-dire les droits établis dans « les articles 12 à 22 et l'article 34, ainsi que l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22 ». Étant donné que le droit fondamental à la protection des données ne peut être assuré sans le respect des droits des personnes concernées et l'adhésion aux principes du traitement par les responsables du traitement, il est crucial de souligner que les restrictions prévues à l'article 23 doivent être considérées comme des exceptions. Ces exceptions aux règles générales peuvent donc être appliquées de manière restrictive et uniquement dans des circonstances spécifiquement prescrites.[80]

[79] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, article 11(1).
[80] EDPB, Lignes directrices 10/2020 sur les restrictions en vertu de l'article 23 du RGPD (15 décembre 2020) para. 3
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf consulté le 25 mai 2021.

En conséquence, l'article 23 du RGPD exige que les restrictions puissent être introduites « par voie **de mesure législative »**, qu'elles **respectent « l'essence des droits et libertés fondamentaux » et qu'elles constituent « une mesure nécessaire et proportionnée dans une société démocratique »** pour sauvegarder l'un des objectifs suivants :

a) la sécurité nationale ;

b) la défense ;

c) la sécurité publique ;

d) la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la protection contre les menaces à la sécurité publique et leur prévention ;

e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris les questions monétaires, budgétaires et fiscales, la santé publique et la sécurité sociale ;

f) la protection de l'indépendance de la justice et des procédures judiciaires ;

g) la prévention, les enquêtes, la détection et la poursuite des infractions à la déontologie pour les professions réglementées ;

h) une fonction de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique dans les cas visés aux points a) à e) et g) ;

i) la protection de la personne concernée ou des droits et libertés d'autrui ;

j) l'exécution des demandes de droit civil.

La formulation de l'article 23 du RGPD ressemble à celle de l'article 52(1) du CFR, à la différence qu'elle fait explicitement référence à une "mesure législative", qu'elle relie les exigences de nécessité et de proportionnalité à une société démocratique (comme c'est le cas à l'article 8(2) de la CEDH) et qu'elle fournit une liste exhaustive d'objectifs à la poursuite desquels le législateur peut établir une restriction.

5.3 Restrictions des droits dans les cas d'échanges de données à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme et à des fins fiscales.

Lorsque des données à caractère personnel sont échangées à des fins de LBC/FT et de fiscalité, les droits de la personne concernée peuvent être limités dans trois cas principaux : (a) au nom de la prévention, des enquêtes et des poursuites pénales, (b) au nom de la sécurité nationale ou (c) au nom d'autres objectifs importants d'intérêt public général.

5.3.1 Restrictions au nom de la prévention, de la recherche et de la poursuite d'infractions pénales

Alors que la Convention 108+ du CdE autorise les restrictions au nom de la prévention, l'investigation et la poursuite des infractions pénales, l'article 23 du RGPD autorise une telle restriction également pour la détention de ces infractions pénales. L'EDPB a récemment publié des lignes directrices sur l'interprétation de l'article 23. [81] Il a reconnu que dans certains cas, comme par exemple dans le cadre de la lutte contre le blanchiment d'argent et le

[81] Ibid.

financement du terrorisme, la fourniture d'informations aux personnes concernées qui font l'objet d'une enquête peut compromettre l'enquête elle-même. [82] Toutefois, les personnes concernées doivent être notifiées lorsque cela ne compromet plus l'enquête (voir section 5.4 ci-dessous).

5.3.2 Restrictions au nom de la sécurité nationale

L'article 4, paragraphe 2, du Traité de l'Union européenne (TUE) prévoit explicitement que la sécurité nationale reste de la seule responsabilité de chaque État membre.[83] La Cour européenne des droits de l'homme (CEDH) a traité de restrictions au nom de la sécurité nationale, elle n'a jamais défini la portée du terme sécurité nationale. Dans le même ordre d'idées, la CJUE ne fournit pas de définition de la sécurité nationale. Dans l'affaire *Esbester*, la Commission européenne des droits de l'homme (CmEDH) a déclaré que « le terme "sécurité nationale" ne se prête pas à une définition exhaustive et [qu'elle le considère comme satisfaisant lorsque] des indications suffisantes sont données sur la portée et les modalités d'exercice des fonctions du service de sécurité. (…). »[84] Dans l'affaire *Liberty* [85], la Cour s'est appuyée sur la définition de la sécurité nationale donnée par le commissaire britannique désigné en vertu du *British Interception of Communications Act* de 1985.[86] Dans son rapport de 1986, le commissaire a défini les menaces à la sécurité nationale comme des activités : « qui menacent la sécurité ou le bien-être de l'État et qui visent à saper ou à renverser la démocratie parlementaire par des moyens politiques, industriels ou violents. »[87] Plus tard, la Cour a de nouveau mentionné cette définition dans l'affaire *Kennedy* [88] lorsqu'elle a indiqué comment appliquer ce terme aux activités de surveillance secrète au Royaume-Uni. Dans la législation britannique actuelle, la RIPA ne contient pas de définition de la sécurité nationale. Toutefois, la notion de sécurité nationale est définie de manière très large, allant du « concept classique de menaces directes (internes ou externes) pour la sécurité du royaume aux menaces indirectes ». [89],[90] .

5.3.3 Autres objectifs essentiels d'intérêt public général

L'article 11, paragraphe 1, point *b*, de la Convention 108+ du Conseil de l'Europe permet de restreindre les droits des personnes concernées pour d'autres objectifs essentiels d'intérêt public général. L'article 23, paragraphe 1, point *e*, du RGPD, dans les dispositions correspondantes de l'article 11, paragraphe 1, point *b*, mentionnait comme autres objectifs importants d'intérêt public général « un intérêt économique ou financier important de l'Union ou d'un État membre, y compris les questions monétaires, budgétaires et fiscales... ». [91]

---

[82] Ibid, paragraphe 24
[83] Traité sur l'Union européenne (traité de Lisbonne), article 4, paragraphe 2.
[84] *Esbester c. Royaume-Uni* App no 18601/91 (CEDH, 2 avril 1993).
[85] *Liberty and Others v United Kingdom* App no 58243/00 (CEDH, 1 octobre 2008), paragraphe 20.
[86] La loi britannique sur l'interception des communications de 1985 était le prédécesseur de la loi britannique sur la réglementation des pouvoirs d'investigation (RIPA) de 2000.
[87] Le commissaire britannique désigné en vertu de la loi britannique de 1985 sur l'interception des communications, Rapport du commissaire britannique de 1986 sous la référence de *Liberty and Others v United Kingdom* App no 58243/00 (ECtHR, 1 octobre 2008), para 20.
[88] Kennedy c. Royaume-Uni*,* App no 26839/05 (18 août 2010), paragraphe 159.
[89] Eric Metcalfe, *Terror, reason and rights* dans Esther D. Reed et al. (eds) *Civil Liberties, National Security and Prospects for Consensus : Legal, Philosophical and Religious Perspectives* (Cambridge University Press 2012) 155.
[90] Eleni Kosta, *Surveilling Masses and Unveiling Human Rights - Uneasy choices for the Strasbourg Court*, Tilburg Law School Research Paper n° 2018-10, p 32.
[91] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - RGPD), article 23, paragraphe 1, point *e*).

5.3.4 Garanties lors de l'application de restrictions

Dans sa jurisprudence récente, la CJUE a apporté quelques précisions sur les limitations et restrictions établies pour la sécurité nationale. Dans l'affaire *Privacy International*, la CJUE a examiné une législation nationale permettant à une autorité étatique d'exiger des fournisseurs de services de communications électroniques qu'ils transmettent des données relatives au trafic et des données de localisation aux agences de sécurité et de renseignement dans un but de sauvegarde de la sécurité nationale. Un certain nombre de gouvernements européens ont fait alors valoir que « les activités des agences de sécurité et de renseignement [nationales] sont des fonctions essentielles de l'État liées au maintien de l'ordre public et à la sauvegarde de la sécurité nationale et de l'intégrité territoriale et, par conséquent, relèvent de la seule responsabilité des États membres » et que, par conséquent, les mesures nationales pour la sauvegarde de la sécurité nationale ne peuvent être considérées comme relevant du champ d'application de la directive « vie privée et communications électroniques ». [92]

Toutefois, la CJUE a fait valoir qu'il ressort de l'article 23, paragraphe 1, points *d*) [93] et *h*) [94], du RGPD que le traitement des données personnelles par des personnes physiques à ces mêmes fins entre dans le champ d'application du RGPD.[95] La CJUE a conclu que « s'il appartient aux États membres de définir leurs intérêts essentiels de sécurité et d'adopter les mesures appropriées pour assurer leur sécurité intérieure et extérieure, le **seul fait qu'une mesure nationale ait été prise dans le but de protéger la sécurité nationale ne saurait rendre le droit de l'UE inapplicable et dispenser les États membres de leur obligation de respecter ce droit »**. En d'autres termes, la CJUE a clairement établi que les mesures nationales prises dans le but de protéger la sécurité nationale ne peuvent pas rendre le droit communautaire inapplicable en tant que tel et exempter les États membres de leur obligation de se conformer à ce droit. [96] Une conclusion similaire a été tirée dans l'arrêt *LQDN* où la CJUE a conclu que « la législation nationale qui impose aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et à la localisation aux fins de la protection de la sécurité nationale et de la lutte contre la criminalité ... relève du champ d'application [de la législation de l'Union européenne ; en l'espèce] de la directive 2002/58.[97] Suivant le raisonnement de la CJUE, les entités privées impliquées dans l'échange de données à caractère personnel à des fins fiscales ou, de manière peut-être plus importante, à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme, restent dans le champ d'application du RGPD, même lorsque l'échange a été demandé par une autorité compétente (qui pourrait également être une CRF dans le cas de la lutte contre le blanchiment d'argent et le financement du terrorisme). Il est donc essentiel d'examiner attentivement le régime selon lequel l'échange de données est réalisé, en particulier lorsque des entités privées sont impliquées, afin de restreindre les droits des personnes concernées.

---

[92] Affaire C-623/17 *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs et autres* [2020] ECLI:EU:C: 2020:790, paragraphes 32-33.
[93] Article 23, paragraphe 1, point *d*), du RGPD sur la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la sauvegarde et la prévention des menaces pour la sécurité publique.
[94] RGPD 23(1)(*h*) sur une fonction de surveillance, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique dans les cas visés aux points *a*) [sécurité nationale] à *e*) et g).
[95] Affaire C-623/17 *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs et autre*s [2020] ECLI:EU:C: 2020:790, para. 47.
[96] Ibid, para. 44.
[97] Affaires jointes C-511/18, C-512/18 et C-520/18 *La Quadrature du Net et autres c. Premier Ministre et autres* [2020] ECLI :EU:C:2020:791, para. 102.

5.4 Notification des personnes concernées

La notification des personnes concernées est probablement le droit le plus important qui est souvent en contradiction avec les objectifs de la lutte contre le blanchiment d'argent et le financement du terrorisme et la fraude/évasion fiscale. Le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme ne prévoit pas d'obligation d'informer les personnes dont les transactions ont fait l'objet d'une surveillance à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme ou ont été communiquées aux CRF ou aux autorités chargées de l'application de la loi, même lorsqu'il n'y a aucun risque de compromettre les opérations en cours. En fait, il y a même une interdiction de notifier ces personnes qui peut aller jusqu'à la non-divulgation dans le cadre d'une procédure judiciaire.[98] De même, le cadre relatif à l'échange de données à des fins fiscales ne contient pas non plus une telle obligation. Toutefois, dans ces deux cadres, la notification lorsque des données personnelles sont échangées est un droit des personnes concernées. Ce droit ne peut être restreint, comme décrit ci-dessus, que dans des circonstances spécifiques et en offrant des garanties concrètes aux personnes concernées. La Cour européenne des droits de l'homme et la CJUE ont fourni des orientations sur cette question.

Il ressort d'une jurisprudence constante de la CtEDH dans le contexte de l'interception des communications que la notification des personnes concernées est « inextricablement liée à l'efficacité des recours devant les tribunaux » [99] et que les personnes concernées doivent être informées « dès que la notification peut être effectuée sans compromettre l'objectif de la restriction après la fin de la mesure de surveillance ».[100] Cela a également été réitéré dans la jurisprudence ultérieure sur la surveillance secrète : « après la fin de la surveillance, la question de la notification ultérieure des mesures de surveillance est inextricablement liée à l'efficacité des recours devant les tribunaux et donc à l'existence de garanties efficaces contre l'abus des pouvoirs de surveillance ». [101]

La question de la notification des personnes concernées était cruciale dans l'affaire *Tele2/Watson* et la CJUE a déclaré que « les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé doivent notifier les personnes concernées, selon les procédures nationales applicables, dès que cette notification n'est plus susceptible de compromettre les enquêtes menées par ces autorités. Cette notification est, en effet, nécessaire pour permettre aux personnes concernées d'exercer, entre autres, leur droit à un recours juridique ».[102] Cette position est reprise dans l'avis 1/15 de la CJUE sur l'accord PNR UE-Canada. [103]

Bien que le droit des personnes concernées d'être informées du traitement de leurs données personnelles puisse être restreint dans le cadre de la lutte contre le blanchiment d'argent et la fraude fiscale, cela ne doit pas être fait de manière générale. Sur la base de la jurisprudence

---

[98] Ajouter une source

[99] Voir, entre autres, *Roman Zakharov c. Russie* App no 47143/06 (CEDH, 4 décembre 2015), paragraphe 234.

[100] *Roman Zakharov c. Russie*, requête n° 47143/06 (CEDH, 4 décembre 2015), paragraphe 287, avec une référence à *Klass et autres c. Allemagne*, requête n° 5029/71 (CEDH, 6 septembre 1978), paragraphe 58, et *Weber et Saravia c. Allemagne*, requête n° 54934/00 (CEDH, 29 juin 2006), paragraphe 135. Des réflexions similaires ont été formulées par la Cour dans l'affaire *Szabó et Vissy c. Hongrie*, requête n° 37138/14 (CEDH, 12 janvier 2016), paragraphe 86.

[101] *Roman Zakharov c. Russie*, requête n° 47143/06 (CEDH, 4 décembre 2015), paragraphes 233-234.

[102] Affaires jointes C-2013/15 et C698/15, *Tele2 Sverige AB c. Post-och telestyrelsen et Secretary of State for the Home Department c. Watson* [2016] ECLI:EU:C:2016:970, point 121.

[103] Avis 1/15 (accord PNR UE-Canada) du 26 juillet 2017, EU:C:2017:592, paragraphes 222 et 224 https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5512101 consulté le 25 mai 2021.

de la CJUE et de la Cour européenne des droits de l'homme, les autorités compétentes peuvent s'abstenir d'informer les personnes concernées du traitement de leurs données personnelles. Toutefois, ces autorités doivent notifier les personnes concernées, selon les procédures nationales applicables, dès que cela n'est plus susceptible de compromettre les enquêtes. Les autorités de contrôle ont le pouvoir d'examiner si la notification aux personnes concernées est effectivement réalisée.

Dans l'affaire *La Quadrature du Net*, la CJUE a proposé des garanties supplémentaires concernant le droit à la notification en cas d'analyse "automatisée" des données. Selon la CJUE, lorsque 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 avoir à 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'approfondir l'analyse des données la concernant, il est nécessaire de la notifier individuellement. Cette notification ne doit toutefois avoir lieu que dans la mesure où et dès qu'elle n'est plus susceptible de compromettre les tâches dont ces autorités sont chargées ».[104]

La Quadrature du Net était une affaire concernant les autorités françaises qui collectaient des données de trafic et de localisation. La CJUE a établi une obligation générale pour les autorités nationales compétentes de publier des informations de nature générale relatives à l'analyse automatisée des données, sans avoir à notifier individuellement les personnes concernées. Toutefois, la CJUE a établi une obligation plus stricte lorsque 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 concernant ces personnes. Dans ce cas, la CJUE estime qu'il est nécessaire de notifier cette personne individuellement. Conformément à sa jurisprudence constante, la CJUE conclut que la notification ne doit intervenir que dans la mesure où et dès qu'elle n'est plus susceptible de mettre en péril les missions dont ces autorités sont chargées.

Cette position de la CJUE est d'une grande importance lorsque l'analyse automatisée des données intervient à la fois dans le contexte de la fraude/évasion fiscale et dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Il n'est pas clair si l'objectif de la CJUE était d'imposer une telle obligation de notifier individuellement les personnes concernées lorsqu'elles ont été identifiées sur la base d'une analyse automatisée uniquement aux autorités nationales ou si une telle obligation devrait être étendue aux entités privées également. Cette dernière préoccupation aurait un impact important sur les entités obligées dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme qui utilisent déjà l'IA pour effectuer des opérations d'exploration de données et de profilage.

5.5 Réflexion sur les restrictions des droits dans la lutte contre le blanchiment d'argent et le financement du terrorisme.

Comme il a déjà été mentionné ci-dessus, lorsque des données à caractère personnel sont échangées aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, les droits de la personne concernée peuvent être restreints dans trois cas principaux : (a) au nom de la prévention, des enquêtes et des poursuites en matière de criminalité, (b) au nom de la sécurité nationale ou (c) au nom d'autres objectifs importants d'intérêt public général.

[104] Ibid, para. 191.

On peut toutefois se demander quel serait le motif le plus approprié pour justifier les restrictions aux droits des personnes concernées. L'objectif premier du cadre LAB/CFT est de détecter les transactions financières susceptibles d'impliquer des actifs illicites ou de contribuer au financement du terrorisme, mais pas de s'en protéger en soi. Par conséquent, il serait peut-être plus approprié de justifier une ingérence en vue de poursuivre un autre objectif important d'intérêt public général de l'Union ou d'un État membre, ce qui en l'espèce, comme il ressort de nombreux considérants de la directive LAB, serait la protection du système financier.

La loi 4AMLD établit une règle pour la limitation du droit d'accès. L'article 39 établit un secret général sur les politiques de lutte contre le blanchiment d'argent et le financement du terrorisme et interdit la divulgation des demandes de déclaration de soupçon ou d'information. L'art. 41(4) de la 4AMLD stipule que « dans le cadre de l'application de l'interdiction de divulgation prévue à l'article 39, paragraphe 1, les États membres adoptent des mesures législatives restreignant, en tout ou en partie, le **droit d'accès** de la personne concernée **aux données à caractère personnel** la concernant**,** dans la mesure où cette restriction partielle ou totale constitue une mesure nécessaire et proportionnée dans une société démocratique, dans le respect des intérêts légitimes de la personne concernée, pour : a) permettre à l'entité obligée ou à l'autorité nationale compétente de s'acquitter dûment de ses missions aux fins de la présente directive ; ou b) éviter de faire obstacle aux enquêtes, analyses, investigations ou procédures officielles ou légales aux fins de la présente directive et garantir que la prévention, l'investigation et la détection du blanchiment de capitaux et du financement du terrorisme ne sont pas compromises »[105] (soulignement ajouté).

5.6 Réflexion sur les restrictions de droits à des fins fiscales

Il existe un conflit intrinsèque entre les droits des personnes concernées, dont les données personnelles sont échangées, et les objectifs du système de fraude/évasion fiscale. Dans l'Union européenne, la DAC1 prévoit des limitations aux droits spécifiques de protection des données des personnes concernées lorsque leurs données sont échangées à des fins fiscales : « Tout échange d'informations en vertu de la présente directive est soumis aux dispositions d'application de la Directive 95/46/CE. Toutefois, les États membres limitent, aux fins de la bonne application de la présente directive, la portée des obligations et des droits prévus à l'article 10, à l'article 11, paragraphe 1, et aux articles 12 et 21 de la Directive 95/46/CE dans la mesure nécessaire à la sauvegarde des intérêts visés à l'article 13, paragraphe 1, point *e*), de ladite directive »[106]. La Directive 1995/46 (directive sur la protection des données) a été remplacée par le Règlement 2016/679 (Règlement général sur la protection des données - RGPD) et les références à la directive sur la protection des données doivent être interprétées comme des références au RGPD.[107] La DAC1 oblige (" *shall* ") les États membres à restreindre le droit des personnes concernées à recevoir des informations dans les cas où les données sont collectées auprès de la personne concernée ou d'une autre source et le droit d'accès et restreint la publicité des opérations de traitement. Ces limitations sont apportées dans la mesure nécessaire à la sauvegarde d'objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment d'un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale. [108]

[105] Directive 2015/849 (4AMLD) Art. 41(4).
[106] Directive 2011/16/, article 25, paragraphe 1.
[107] Article 94 du RGPD.
[108] Article 23(1)(e) du RGPD.

Récemment, la CJUE, dans l'arrêt *Luxemburg State*, a jugé que l'article 47 CFR s'oppose à la législation d'un État membre mettant en œuvre la procédure d'échange d'informations sur demande établie par la Directive 2011/16 qui empêche une personne détenant des informations d'introduire un recours contre une décision par laquelle l'autorité compétente de cet État membre ordonne à cette personne de lui fournir ces informations, en vue de donner suite à une demande d'échange d'informations formulée par l'autorité compétente d'un autre État membre. L'article 47 CFR doit également être interprété en ce sens qu'il ne s'oppose pas à ce qu'une telle législation empêche le contribuable concerné, dans cet autre État membre, par l'enquête ayant donné lieu à cette demande d'échange d'informations et les tiers concernés par les informations en question d'introduire des recours contre cette décision.[109] Cet arrêt confirme que l'échange d'informations fiscales ne fonctionne pas dans un univers parallèle et que les règles et principes de protection des données s'appliquent à tous les autres domaines du droit. En ce qui concerne le droit à un recours effectif, la CJUE l'a interprété comme exigeant que les personnes qui détiennent des informations qui sont demandées par l'administration nationale dans le cadre d'une procédure de coopération entre États membres, doivent pouvoir introduire une action directe contre une telle demande.

6. Base juridique pour l'échange de données à caractère personnel

Le principe de licéité signifie que le traitement des données à caractère personnel repose sur au moins une des bases licites appropriées. L'article 5, paragraphe 2, de la Convention 108+ prévoit que les données sont traitées « sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi ».[110] Le rapport explicatif de la Convention 108+[111] précise que la notion de « fondement légitime prévu par la loi » « englobe notamment le traitement des données nécessaire à l'exécution d'un **contrat** (ou de mesures précontractuelles à la demande de la personne concernée) auquel la personne concernée est partie ; à la protection des **intérêts vitaux** de la personne concernée ou d'une autre personne ; à la mise en conformité avec une **obligation légale à laquelle** le responsable du traitement est soumis ; ainsi que le traitement de données réalisé pour des motifs d'**intérêt public** ou pour des **intérêts légitimes** prédominants du responsable du traitement ou d'un tiers ».[112] Dans ce contexte, il est intéressant de noter que le rapport explicatif précise que « [l]e traitement de données effectué pour des motifs d'**intérêt public** doit être prévu **par la loi**, notamment lorsqu'il s'agit d'un traitement à des fins **monétaires, budgétaires et fiscales**, à des fins de santé publique et de sécurité sociale, à des fins de prévention, d'investigation, de détection et de répression des infractions pénales et d'exécution des sanctions pénales, à des fins de protection de la sécurité nationale, de défense, de prévention, d'investigation, de détection et de répression des violations de la déontologie en ce qui concerne les professions réglementées, et à des

[109] Affaires C-245/19 et C-246/19 *État luxembourgeois contre B et État luxembourgeois c. B, C, D, F.C* [2020] ECLI :EU :C :2020 :795.
[110] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, article 5(2).
[111] Conseil de l'Europe, Rapport explicatif sur le Protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (2018) <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> consulté le 25 mai 2021.
[112] Ibid, paragraphe 46.

fins d'exécution des décisions civiles et de protection de l'indépendance de la magistrature et de la procédure judiciaire ».[113]

6.1 Échanges de données à des fins fiscales

L'échange de données à caractère personnel à des fins fiscales repose généralement sur le motif que le traitement des données est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. La principale base juridique de l'échange de données à caractère personnel à des fins fiscales est généralement une convention bilatérale en matière d'impôt sur le revenu ou un accord multilatéral d'assistance mutuelle ou d'échange de renseignements. Il s'agit par exemple de :

- La Convention multilatérale conjointe Conseil de l'Europe/OCDE concernant l'assistance administrative mutuelle en matière fiscale ;
- Directive 2011/16/UE du Conseil relative à la coopération administrative dans le domaine fiscal, (abrogeant la Directive 77/799/CE) ;
- Directive 2018/822/UE du Conseil en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal en rapport avec les dispositifs transfrontières devant faire l'objet d'une déclaration.

6.2 Échanges de données pour la LBC/FT

La base juridique de l'échange de données est plus complexe dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme, où plusieurs acteurs sont impliqués. En ce qui concerne le traitement par les entités obligées dans le cadre de l'application des mesures CDD, tel que réglementé dans la 4AMLD, on peut convenir que le RGPD devrait s'appliquer. En effet, le RGPD, en tant que régime général, s'applique à toute opération de traitement, sauf si les conditions de l'une des exceptions énoncées à l'article 2, paragraphes 2 et 3, du RGPD sont remplies.[114] Considérant que l'entité obligée n'est pas une autorité compétente au sens de la LED[115] et ne traite pas de données à caractère personnel à des fins répressives, ou du moins pas directement, et qu'aucune autre exception n'est pertinente, le RGPD en tant que *lex generalis* est le régime applicable. La situation peut être différente en ce qui concerne les CRF. La 4AMLD établit des règles de base pour le fonctionnement et les tâches des CRF. Compte tenu du rôle des CRF dans le système juridique de lutte contre le blanchiment d'argent et le financement du terrorisme et de la nature des CRF, et en particulier de celles qui sont chargées de l'application de la loi, on peut faire

[113] Ibid, paragraphe 47.

[114] L'article 2, paragraphe 2, du RGPD exclut l'application du RGPD pour le traitement des données à caractère personnel : a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ; b) par les États membres lorsqu'ils exercent des activités qui relèvent du champ d'application du titre V, chapitre 2, du TUE ; c) par une personne physique dans le cadre d'une activité purement personnelle ou domestique ; d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la sauvegarde et la prévention des menaces pour la sécurité publique. L'article 2, paragraphe 3, du RGPD prévoit une exception au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union.

[115] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (directive sur l'application de la loi - LED).

valoir que ce n'est pas le RGPD, mais la LED qui devrait être le cadre juridique applicable.[116] Il convient donc de conclure que, malgré le libellé de l'article 43 de la 4AMLD, le RGPD ne s'applique pas nécessairement à toutes les opérations de traitement de données aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme qui sont prévues dans la 4AMLD.

Au niveau de l'Union européenne, la 4AMLD, tel que modifié par la 5AMLD, stipule dans son article 43 que « le traitement des données à caractère personnel sur la base de la présente directive aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme, tel que visé à l'article 1er**, est considéré comme une question d'intérêt public au titre** [du RGPD]. »[117] Le considérant 42 de la 4AMLD ajoute que « [l]a lutte contre le blanchiment de capitaux et le financement du terrorisme est reconnue comme un motif d'intérêt public important par tous les États membre »".

Lorsqu'il s'agit du traitement des données effectué par les CRF, la base légale sera dans la plupart des cas que le traitement des données est nécessaire pour le respect d'une obligation légale des CRF. Lorsqu'il s'agit de l'échange de données à caractère personnel au sein d'un groupe (avec des succursales et des filiales dans des pays tiers), il peut être réalisé sur la base de différents motifs juridiques. Le traitement peut se fonder sur une obligation légale, lorsque les données sont échangées pour le respect des obligations de vigilance. Toutefois, l'article 43 de la loi 4AMLD peut être interprété comme autorisant les entités obligées à traiter davantage de données que celles qui sont absolument nécessaires pour se conformer aux obligations de la CDD. Dans ces cas, les entités obligées pourraient éventuellement invoquer l'intérêt légitime, soit de l'entité obligée, soit d'un tiers. Les entités obligées pourraient traiter les données personnelles en arguant que celles-ci sont nécessaires à l'exécution d'une tâche effectuée dans l'intérêt public. Cependant, le CEPD a fait valoir que « le motif légitime pertinent pour le traitement des données à caractère personnel devrait plutôt être la nécessité de se conformer à une obligation légale des entités obligées, des autorités compétentes et des CRF (c'est-à-dire l'article 7(c) [maintenant 6(1)c)] ».[118]

Il est conseillé aux entités privées qui échangent des données à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme de préciser la base juridique de cet échange.

7. Principes de protection des données

L'article 5 de la Convention 108+ du Conseil de l'Europe stipule un certain nombre de principes pour la légitimité du traitement des données et la qualité des données, qui doivent être respectés chaque fois que des données personnelles sont échangées. Les principes établis à l'article 5, paragraphe 4, c'est-à-dire la loyauté et la transparence, la limitation de la finalité, la minimisation des données, l'exactitude des données et la limitation du stockage, peuvent

---

[116] Teresa Quintel, *Follow the Money, If You Can - Possible Solutions for Enhanced FIU Cooperation Under Improved Data Protection Rules* (2019) University of Luxembourg Law Working Paper No. 001-2019, <https://doi.org/10.2139/ssrn.3318299> consulté le 25 mai 2021.

[117] Directive 2015/849 (4AMLD) relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiée par la directive 2018/843 (5AMLD), article 43.

[118] Voir CEPD, Avis sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil relatif aux informations sur le payeur accompagnant les virements de fonds (4 juillet 2013), para. 33 < https://edps.europa.eu/sites/default/files/publication/13-07-04_money_laundering_en.pdf> consulté le 25 mai 2021.

être restreints conformément à l'article 11 de la Convention 108+ du Conseil de l'Europe (voir section 5.1 ci-dessus).

7.1 Proportionnalité

L'article 5, paragraphe 1, de la Convention 108+ dispose que « [l]e traitement des données est proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et libertés en jeu ». Dans le cadre de l'échange de données à caractère personnel, le principe de proportionnalité doit déjà être respecté au stade de la décision sur la nécessité ou non d'un tel échange.[119]

La CJUE a appliqué le test de proportionnalité à la directive sur la conservation des données[120] dans la célèbre affaire *Digital Rights Ireland.*[121] La directive sur la conservation des données obligeait les fournisseurs d'accès à Internet (FAI) à conserver pendant deux ans maximum toutes les données relatives au trafic de chaque utilisateur afin de les communiquer avec les autorités dans le cadre d'éventuelles enquêtes. La directive sur la conservation des données n'a pas passé le test de proportionnalité. Selon la Cour, le type de surveillance exercé par les fournisseurs d'accès à Internet était particulièrement intrusif. Malgré cela, la directive sur la conservation des données ne prévoyait aucune garantie pour la protection des personnes surveillées, qui n'étaient en fait ni conscientes, ni informées de la collecte de leurs données de trafic et de leur utilisation. Elle ne limitait pas non plus le nombre de personnes pouvant avoir accès à ces données. En outre, la directive sur la conservation des données a été jugée insuffisamment spécifique dans sa formulation, en raison de l'absence de lien entre les activités de surveillance et un ou plusieurs délits spécifiques et du manque de preuves de l'efficacité réelle de la mesure.

À la lumière de ce qui précède, il est raisonnable d'émettre des doutes quant à l'utilisation des technologies axées sur les données pour la lutte contre le blanchiment d'argent et le financement du terrorisme.[122] L'affaire *Digital Rights Ireland* présente plusieurs similitudes avec le type d'activités menées dans le cadre de la LBC/FT. Les technologies basées sur les données utilisées dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme impliquent une intrusion importante dans les droits fondamentaux des personnes (en raison de la surveillance indiscriminée et de la collecte et de la conservation des données de tous les clients des banques[123]), elles comprennent également une évaluation

[119] Conseil de l'Europe, Rapport explicatif sur le Protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (2018) para. 40 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> consulté le 25 mai 2021.

[120] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, (directive sur la conservation des données).

[121] Affaires jointes C-293/12 et C-594/12 *Digital Rights Ireland Ltd/Ministre des communications, du milieu marin et des ressources naturelles et autres et Kärntner Landesregierung et autres* [2014] ECLI:EU:C:2014:238. Voir également : Affaires jointes C-2013/15 et C698/15 *Tele2 Sverige AB c. Post- och telestyrelsen et Secretary of State for the Home Department c. Watson* [2016] ECLI:EU:C:2016:970.

[122] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, Les systèmes anti-blanchiment basés sur l'IA sont-ils compatibles avec les droits fondamentaux ? . (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647420> consulté le 25 mai 2021.

[123] Le considérant 44 de la directive AMLD4 établit, pour éviter un effet d'entraînement de la décision *Digital Rights Ireland*, que la durée de conservation doit être supérieure à cinq ans, et que des

des risques et ne prévoient pas de garantie (les personnes ne savent pas qu'elles sont signalées par le système et qu'elles font l'objet d'une enquête, il n'y a pas de procédure permettant de s'opposer au traitement ou à ses résultats, le logiciel est opaque).

Les points suivants semblent problématiques, en particulier du point de vue de la non-discrimination, sur la base du principe de proportionnalité et de la manière dont il a été appliqué par la CJUE.[124] Si les activités de dépistage en matière de LBC/FT sont soutenues par la loi (les recommandations du GAFI, 4AMLD et 5AMLD), on peut se demander si cette dernière est suffisamment spécifique ; la liberté de manœuvre laissée aux entités obligées, ainsi que l'absence de garanties spécifiques, pourraient laisser penser que la loi n'est pas suffisamment spécifique.[125] Le considérant 43 de la 4AMLD, affirmant que la 4AMLD est conforme à la Charte de l'UE, et les considérants 65 et 66 de la 4AMLD, établissant que les États membres doivent assurer le respect du droit à la non-discrimination, semblent difficiles à appliquer dans la pratique. En outre, le manque de transparence, ainsi que le manque d'informations données aux individus qui sont signalés par un logiciel, et l'absence de procédure au sein des entités obligées pour s'opposer à la procédure/au résultat représentent des problèmes importants en termes de manque de garanties pour les droits fondamentaux des individus. L'effet boîte noire peut être aggravé par le fait que les logiciels sont généralement des technologies propriétaires et que leur utilisation au sein d'une organisation peut être protégée par des secrets commerciaux. Le droit de la propriété intellectuelle peut empêcher la divulgation d'informations importantes sur la logique et la formation des algorithmes.

7.2 Équité et transparence

Selon l'article 5, paragraphe 4, point *a*), de la convention 108+, « les données à caractère personnel faisant l'objet d'un traitement sont traitées loyalement et de manière transparente ».

7.3 Limitation de l'objet

L'article 5, paragraphe 4, point *b*), de la Convention 108+ exige que les données à caractère personnel faisant l'objet d'un traitement soient « collectées pour des finalités explicites, déterminées et légitimes et ne so[ie]nt pas traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins d'archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques est compatible avec ces fins, à condition que des garanties complémentaires s'appliquent ». Les finalités doivent donc être clairement définies et précises et un traitement ultérieur ne peut être autorisé à des fins incompatibles avec les finalités initiales.

Le principe de limitation de la finalité se compose de deux éléments : (1) le responsable du traitement ne doit collecter des données que pour des finalités déterminées, explicites et

---

garanties appropriées doivent être mises en place. Il n'est pas certain que cette formulation soit suffisamment précise.

[124] Gloria González Fuster, Serge Gutwirth et Erika Ellyne, Le profilage dans l'Union européenne : Une pratique à haut risque(2010) INEX Policy Brief no. 10 <http://aei.pitt.edu/14984/1/INEX_PB10_Fuster_et_al._on_Profiling_in_the_EU_e-version.pdf> Accédé le 25 mai 2021

[125] Astrid Bertrand, Winston Maxwell, Xavier Vamparys, *Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?* , 17 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3647420> consulté le 25 mai 2021.

légitimes ; et (2) une fois les données collectées, elles ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Le premier élément exige que la finalité soit clairement établie. L'existence d'une finalité spécifique et explicite est la première exigence du principe de limitation de la finalité, suivie par la garantie de la légitimité de cette finalité. Le deuxième élément concerne ce que l'on appelle le traitement ultérieur, c'est-à-dire le traitement dans un but différent de celui pour lequel les données ont été initialement collectées. Un tel traitement ne peut avoir lieu qu'à condition qu'il ne soit pas "incompatible" avec la finalité initiale.

Le rapport explicatif de la Convention 108+ a précisé certains critères qui peuvent être utilisés pour évaluer si un traitement ultérieur peut être considéré comme compatible avec les finalités initiales : « Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelle les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, doit tenir compte, entre autres : de tout lien entre ces finalités et les finalités du traitement ultérieur prévu ; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier des attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données ; de la nature des données à caractère personnel ; des conséquences du pour les personnes concernées du traitement ultérieur prévu ; et de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu ».[126] Les législateurs sont invités à définir concrètement les finalités pour lesquelles l'échange d'informations est requis, afin d'éviter les échanges de données pour d'autres finalités qui peuvent être légitimes, mais qui ne sont pas compatibles avec les finalités initiales.

7.3.1 Échanges de données à des fins fiscales

En ce qui concerne le principe de limitation de la finalité, si certains des États signataires de la convention prévoient dans leur droit interne que le traitement automatisé peut être effectué pour plusieurs finalités différentes, d'autres ont opté pour le principe de l'unité de finalité. Il devrait être clair qu'en tout état de cause, lorsque des données à caractère personnel sont échangées, le principe de limitation de la finalité devrait être clairement respecté.

La limitation de la finalité est un sujet de préoccupation majeur dans le domaine de l'échange de données à des fins fiscales, car souvent les autorités compétentes souhaiteraient utiliser les informations disponibles à d'autres fins également, si elles le jugent utile. Il est frappant de constater que, même dans la législation existante, les finalités pour lesquelles les données à caractère personnel sont échangées ne sont pas toujours clairement spécifiées, ce qui laisse la place à des échanges de données qui ne seraient pas conformes aux exigences en matière de protection des données.

L'article 26 du Modèle de convention fiscale de l'OCDE, tel que mis à jour, illustre clairement ce cas de figure : « Nonobstant ce qui précède, les renseignements reçus par un État contractant peuvent être utilisés à d'autres fins lorsque cette possibilité résulte des lois des deux Etats et lorsque l'autorité compétente de l'État qui fournit les renseignements autorise cette utilisation ».[127] La justification de cet amendement à l'article 26 du Modèle de convention fiscale de l'OCDE était qu'il prenait « en compte les développements récents et précisait

[126] Conseil de l'Europe, Rapport explicatif sur le Protocole portant amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (2018) para. 49 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> consulté le 25 mai 2021.

[127] OCDE, Mise à jour de l'article 26 du modèle de convention fiscale de l'OCDE et de ses commentaires, approuvés par le Conseil de l'OCDE le 17 juillet 2012, <https://www.oecd.org/ctp/exchange-of-tax-information/120718_Article%2026-ENG_no%20cover%20(2).pdf> consulté le 25 mai 2021.

l'interprétation de certaines dispositions de cet article ». Le paragraphe 2 de l'article a été modifié pour permettre aux autorités compétentes d'utiliser les renseignements reçus à d'autres fins, à condition que cette utilisation soit permise par la législation des deux États et que l'autorité compétente de l'État fournisseur autorise cette utilisation.[128] L'élément important de cet amendement est que l'utilisation ultérieure « résulte des lois des deux États et (…) l'autorité compétente de l'État qui fournit les renseignements autorise cette utilisation ». Toutefois, une évaluation stricte de la compatibilité du traitement ultérieur doit être effectuée conformément aux règles de protection des données.

7.3.2 Echanges de données pour la LBC/FT

La recommandation 3 du GAFI sur la définition de l'infraction de blanchiment de capitaux exige que « les pays devraient appliquer l'infraction de blanchiment de capitaux à toutes les infractions graves afin de couvrir la gamme la plus large d'infractions sous-jacentes ». La note interprétative de la recommandation 3 précise que « 2 (…) Les infractions sous- jacentes peuvent être définies par rapport à l'ensemble des infractions, par rapport à un seuil lié soit à une catégorie d'infractions graves, soit à la peine privative de liberté dont est passible l'infraction sous-jacente (méthode du seuil), par rapport à une liste d'infractions sous-jacentes ou par une combinaison de ces méthodes. 3. Dans les pays qui adoptent la méthode du seuil, les infractions sous-jacentes devraient au minimum comprendre toutes les infractions relevant de la catégorie des infractions graves en vertu de leur droit interne ou inclure les infractions passibles d'une peine maximale de plus d'un an d'emprisonnement ou, pour les pays qui ont établi dans leur système juridique un seuil minimum pour les infractions, les infractions sous-jacentes devraient comprendre toutes les infractions passibles d'une peine minimale de plus de six mois d'emprisonnement. » [129] La recommandation 3 du GAFI doit être lue de manière restrictive en ce qui concerne le principe de limitation de l'objet, en veillant à ce que toutes les procédures soient intrinsèquement liées aux infractions de LBC/FT.

Le CEPD a identifié un danger pour le principe de limitation de la finalité qui peut potentiellement survenir en relation avec les PPP créés pour le partage d'informations opérationnelles sur des personnes suspectées de renseignement. Le CEPD est préoccupé par le fait que « [e]n particulier, les entités obligées participant aux PPP pourraient être tentées d'intégrer les informations partagées par les autorités répressives par le biais de cette plateforme **dans leurs bases de données globales, afin de les réutiliser plus tard, dans le cadre de leurs profils de clients**. Cela pourrait conduire à une discrimination à l'égard de certains clients, par exemple ceux qui offrent une faible rentabilité pour la banque et présentent un niveau de risque important, ce qui pourrait entraîner l'exclusion financière de personnes et de communautés vulnérables (ce que l'on appelle le "dé-risquage" des entités financières, par lequel les relations avec les clients qui peuvent présenter des risques sont interrompues ou restreintes) ».[130]

---

[128] Ibid, paragraphe 4.3.

[129] GAFI, Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération (2020) note interprétative de la recommandation 3, p. 38-39 < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> consulté le 25 mai 2021.

[130] CEPD, Avis 5/2020 sur le plan d'action de la Commission européenne pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme (23 juillet 2020), para. 46 <https://edps.europa.eu/sites/default/files/publication/20-07-23_edps_aml_opinion_en.pdf> consulté le 25 mai 2021.

7.4 Minimisation des données

L'article 5, paragraphe 4, point *c*) de la Convention 108+ établit le principe de minimisation des données, selon lequel les données à caractère personnel faisant l'objet d'un traitement doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ».[131] Les entités qui envoient les données doivent être en mesure de justifier, dans chaque cas de partage de données à caractère personnel, pourquoi les données spécifiques étaient nécessaires pour la finalité spécifique. La législation, dans la mesure du possible, 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.

7.4.1 Échanges de données à des fins fiscales

Comme nous l'avons déjà mentionné dans l'introduction, l'article 26 du Modèle de convention fiscale de l'OCDE fournit une base pour toutes les formes d'échange de renseignements entre les autorités compétentes, établissant que « les autorités compétentes des États contractants échangent les renseignements vraisemblablement pertinents pour appliquer les dispositions de la présente Convention ou pour l'administration ou l'application de la législation interne relative aux impôts de toute nature ou dénomination perçus pour le compte des États contractants, de leurs subdivisions politiques ou de leurs collectivités locales, dans la mesure où l'imposition qu'elles prévoient n'est pas contraire à la Convention ».[132]

Le critère de la "pertinence prévisible", mentionné à l'article 26 du modèle de convention fiscale de l'OCDE, vise à permettre l'échange de renseignements en matière fiscale dans la **plus large mesure possible** et, en même temps, à préciser que les États contractants ne sont pas libres de se livrer à des "expéditions de pêche" ou de demander des renseignements dont il est peu probable qu'ils soient pertinents pour la situation fiscale d'un contribuable donné ».[133] (accentuation ajoutée) On peut douter que le principe de minimisation des données puisse être respecté dans les cas où les informations échangées sont "vraisemblablement pertinentes" pour la finalité pour laquelle les données sont échangées. Les États doivent veiller à ce que le principe de minimisation des données soit respecté et que les autorités fiscales compétentes mettent en balance les données à échanger avec les objectifs à atteindre.

7.5 Précision

L'article 5, paragraphe 4, point *d*), de la Convention 108+ exige que les données à caractère personnel faisant l'objet d'un traitement soient « exactes et, si nécessaire, mises à jour ».[134]

---

[131] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, article 5(4)(*c*).
[132] OCDE, Modèle de convention fiscale concernant le revenu et la fortune : Version condensée (Éditions OCDE 2017), art.26(1).
[133] OCDE, Mise à jour de l'article 26 du modèle de convention fiscale de l'OCDE et de ses commentaires, approuvés par le Conseil de l'OCDE le 17 juillet 2012, <https://www.oecd.org/ctp/exchange-of-tax-information/120718_Article%2026-ENG_no%20cover%20(2).pdf> consulté le 25 mai 2021.
[134] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, article 5(4)(*d*).

7.5.1 Échange de données en matière de LBC/FT

Le CEPD a relevé que la communication de la Commission européenne sur le plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme[135] souligne « le manque de réglementation des échanges d'informations entre les CRF des États membres et les CRF de pays tiers, qui a conduit à une approche non harmonisée de ces échanges. **Ces obstacles juridiques et pratiques ont inévitablement une incidence sur l'exactitude et l'information actualisée de FIU.net**, et constituent donc un risque pour la protection des droits au respect de la vie privée et à la protection des données à caractère personnel ».[136]

Afin d'établir un profil client précis, les entités obligées déduisent des informations précieuses du comportement du client à l'aide de techniques d'apprentissage automatique et d'exploration de données.[137] Dans le cas des logiciels basés sur des règles, les problèmes de précision sont principalement liés au mécanisme même de ces règles, qui peut conduire à une inclusion excessive. Par exemple, un logiciel moins sophistiqué basé sur des règles pourrait signaler toute transaction dépassant un certain seuil, ou des clients potentiels en raison de leur pays d'origine. Cela génère un nombre très élevé d'alertes, dont seulement 1 à 10 % correspondent à des cas réellement suspects.[138] Ce nombre élevé d'alertes doit être vérifié avec un personnel et un temps limités, ce qui crée un effet de goulot d'étranglement.[139] En outre, en raison de la rigidité du système basé sur des règles, il peut être plus facile pour le crime organisé de créer des réseaux de faux noms, de fausses sociétés et de transactions en chaîne qui ne sont pas détectés par le logiciel.

Dans le cas d'un logiciel d'apprentissage automatique, la précision de ses résultats dépend largement de l'exhaustivité et de la qualité des données d'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.

7.6 Limitation du stockage

Les données doivent également être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités

---

[135] Commission européenne, Communication du 7 mai 2020 relative à un plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme, C(2020)2800 final (le " Plan d'action ") <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:C(2020)2800&from=FR> consulté le 25 mai 2021.

[136] CEPD, Avis 5/2020 sur le plan d'action de la Commission européenne pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme (23 juillet 2020), para. 31 <https://edps.europa.eu/sites/default/files/publication/20-07-23_edps_aml_opinion_en.pdf> consulté le 25 mai 2021.

[137] Hossein Hassani, Xu Huang et Emmanuel Silva, Digitalisation et extraction de données massives dans le secteur bancaire (2018) 2 Big Data and Cognitive Computing 18.

[138] Arin Ray, *DAWN OF A NEW ERA IN AML TECHNOLOGY* (2018) ; Antoinette Verhage, *Between the Hammer and the Anvil ? The Anti-Money Laundering-Complex and Its Interactions with the Compliance Industry* (2009) 52 Crime, Law and Social Change 9.

[139] Araliya Samme, *Automated Financial Crime Technology Can Fix the Bottleneck of AML Transaction Monitoring* (*Featurespace*) <https://www.featurespace.com/newsroom/automated-financial-crime-technology-can-fix-the-bottleneck-of-aml-transaction-monitoring/> consulté le 26 mai 2021.

pour lesquelles elles sont traitées ».[140] Pour que le principe de limitation de la conservation soit respecté, il est essentiel que la législation mentionne clairement les périodes de conservation pendant lesquelles les données doivent être conservées après leur échange.

8. Sécurité des données

L'article 7 de la Convention 108+ du Conseil de l'Europe exige que les Parties à la Convention prévoient que le responsable du traitement et, le cas échéant, le sous-traitant, prennent des mesures de sécurité appropriées contre les risques tels que l'accès accidentel ou non autorisé, la destruction, la perte, l'utilisation, la modification ou la divulgation de données à caractère personnel. Des obligations similaires, bien que plus élaborées, sont établies à l'article 32 du RGPD. Lorsque des données à caractère personnel sont échangées, les destinataires des données sont clairement identifiés et des mesures appropriées sont mises en place afin de permettre l'accès aux données uniquement à ces destinataires spécifiés.

Le respect du principe de sécurité des données nécessite le cryptage des données et des règles de traçabilité complète des échanges, notamment par la mise en place de journaux d'accès.[141]

9. Flux transfrontaliers de données à caractère personnel

Compte tenu de la nature multilatérale des mécanismes d'échanges interétatiques de données à caractère personnel à des fins fiscales, de lutte contre le blanchiment de capitaux et le financement du terrorisme, la question de la protection adéquate se pose dans tous les cas où l'échange de données à caractère personnel concerne un pays qui ne dispose pas d'un niveau de protection adéquat.[142] La Convention 108 modernisée du Conseil de l'Europe contient des règles spécifiques sur les transferts transfrontaliers de données établissant les règles selon lesquelles les États membres qui sont parties à la Convention ne doivent pas, « aux seules fins de la protection des données à caractère personnel, interdire ou soumettre à une autorisation spéciale le transfert de ces données à un destinataire relevant de la juridiction d'une autre partie à la Convention ».[143] Des exceptions à cette règle peuvent être justifiées s'il existe un risque réel et sérieux que le transfert ultérieur conduise à contourner les dispositions de la Convention. En ce qui concerne les transferts transfrontaliers de données à des destinataires établis en dehors des pays parties à la Convention 108+, le

[140] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, article 5(4)(e).
[141] Conseil de l'Europe, Avis sur les implications pour la protection des données des mécanismes d'échanges automatiques interétatiques de données à des fins administratives et fiscales (4 juin 2014) p. 4 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806945a0> consulté le 25 mai 2021.
[142] Caroline Porasso, Benjamin Aouizerat, Rapport sur les implications pour la protection des données du recours croissant aux mécanismes d'échanges automatiques interétatiques de données à caractère personnel à des fins administratives et fiscales, ainsi qu'en matière de blanchiment de capitaux, de financement du terrorisme et de corruption (30 janvier 2014) < https://rm.coe.int/bureau-of-the-consultative-committee-of-the-convention-for-the-protect/168073dc57> consulté le 25 mai 2021.
[143] Conseil de l'Europe, Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel STE n° 108, Art 14(1).

transfert n'est autorisé que si un niveau approprié de protection des données à caractère personnel est assuré.[144] Ce niveau de protection approprié peut être assuré (a) par le droit de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables, ou (b) par des garanties standardisées ad hoc ou approuvées, prévues par des instruments juridiquement contraignants et exécutoires adoptés et mis en œuvre par les personnes concernées par le transfert et le traitement ultérieur.[145] Le transfert de données vers un pays tiers qui ne garantit pas un niveau de protection adéquat peut également avoir lieu dans l'une des circonstances suivantes :

a. la personne concernée a donné son consentement explicite, spécifique et libre, après avoir été informée des risques découlant de l'absence de garanties appropriées ; ou

b. les intérêts spécifiques de la personne concernée l'exigent dans le cas particulier ; ou

c. les intérêts légitimes prévalant, notamment les intérêts publics importants, sont prévus par la loi et ce transfert constitue une mesure nécessaire et proportionnée dans une société démocratique ; ou

d. elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression.[146]

Des règles similaires existent dans le RGPD sur les transferts de données personnelles vers des pays tiers.[147] La CJUE a publié un certain nombre d'arrêts relatifs aux transferts transfrontaliers de données à caractère personnel qui peuvent être pertinents pour les échanges de données à des fins fiscales et dans le contexte de la lutte contre le blanchiment d'argent et le financement du terrorisme. Dans l'affaire *Schrems I*, la CJUE a invalidé les *Safe Harbour Privacy Principles* (décision 2000/520).[148] Dans cet arrêt, la CJUE a établi un certain nombre de garanties qui doivent être respectées lorsque des transferts de données personnelles ont lieu vers un pays qui n'assure pas un niveau de protection adéquat des données personnelles. La CJUE a estimé qu'il était essentiel que les personnes dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers aient la possibilité d'introduire une réclamation auprès des autorités nationales chargées de la protection des données[149], lorsqu'elles prétendent que la législation et les pratiques en vigueur dans le pays tiers n'assurent pas un niveau de protection adéquat.[150] L'accès aux données transférées est autorisé lorsqu'il est strictement nécessaire et proportionné à la protection de la sécurité nationale.[151] Sur ce point, la CJUE a précisé qu'une législation permettant aux autorités publiques d'avoir accès de manière généralisée au contenu des communications électroniques doit être considérée comme portant atteinte à l'essence du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte.[152] En outre, la personne concernée dispose d'un droit de recours, permettant notamment d'accéder aux données la concernant et, le cas échéant, de les rectifier ou de les effacer.[153] La CJUE a fait valoir qu'une législation ne prévoyant aucune possibilité pour un individu d'exercer des voies de recours afin d'avoir accès aux données à caractère personnel le concernant, ou d'obtenir la

[144] Ibid, Art. 14, (2).
[145] Ibid, Art. 14(3).
[146] Ibid, Art. 14(4).
[147] Principalement les articles 45, 46 et 49 du RGPD.
[148] Affaire C-362/14 *Maximillian Schrems c. le commissaire à la protection des données* [2015] ECLI:EU:C:2015:650.
[149] Ibid, para. 53.
[150] Ibid, para. 66.
[151] Ibid, para. 90.
[152] Ibid, para. 94.
[153] Ibid, para. 90.

rectification ou l'effacement de ces données, ne respecte pas l'essence du droit fondamental à une protection juridictionnelle effective.[154]

Suite à l'affaire *Schrems I*, un nouvel accord a été adopté pour les transferts de données de l'UE vers les États-Unis, le *Privacy Shield.*[155] Cependant, la CJUE a également invalidé cet accord. L'invalidation du *Privacy Shield* par la Cour se fonde sur les motifs suivants. Premièrement, la primauté des exigences américaines en matière d'application de la loi sur celles du *Privacy Shield*[156], deuxièmement, l'absence de limitations et de garanties nécessaires quant au pouvoir des autorités en vertu de la loi américaine, notamment à la lumière des exigences de proportionnalité[157], troisièmement, l'absence de recours effectif aux États-Unis pour les personnes concernées situées l'UE[158] et quatrièmement, les déficiences du mécanisme de[159] médiation du *Privacy Shield.*[160]

Les arrêts *Schrems I* et *Schrems II* établissent des garanties qui doivent être respectées lorsque des données à caractère personnel sont transférées vers un pays tiers et qui doivent être prises en compte lorsque des échanges de données interétatiques ont lieu à des fins fiscales mais aussi pour la lutte contre le blanchiment d'argent et le financement du terrorisme. En particulier, les garanties établies par la CJUE soulèvent des questions quant à la compatibilité des échanges de données interétatiques sans garanties adéquates. Il est donc recommandé aux États de veiller à ce que les échanges de données à des fins fiscales et de lutte contre le blanchiment et le financement du terrorisme soient assortis de garanties supplémentaires, conformément à la jurisprudence de la CJUE.

À la suite de l'arrêt de la CJUE dans l'affaire *Schrems II*, le Conseil européen de la protection des données (CEPD) a publié les recommandations 1/2020 sur les mesures qui complètent les outils de transfert pour assurer le respect du niveau de protection des données personnelles de l'UE[161] et les recommandations 2/2020 sur les garanties européennes essentielles pour les mesures de surveillance.[162] Ensemble, ces deux documents décrivent un processus d'évaluation de la suffisance des protections étrangères en vertu du droit européen lorsque des données personnelles sont transférées à l'étranger, ainsi qu'un ensemble de garanties approuvées par l'UE que les entreprises peuvent mettre en œuvre même lorsque les protections étrangères sont jugées insuffisantes par rapport aux normes juridiques européennes. Selon le CEPD, les « garanties européennes essentielles, qui doivent

---

[154] Ibid, para. 95.
[155] Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par le bouclier de protection de la vie privée UE-États-Unis (notifiée sous le document C(2016) 4176) < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN> consulté le 25 mai 2021.
[156] Affaire C-311/18 *Commissaire à la protection des données c. Facebook Ireland, Maximillian Schrems* [2020] ECLI:EU:C:2020:559, para. 164
[157] Ibid, paras. 168-185.
[158] Ibid, paras. 191-192.
[159] Ibid, paras. 193-197.
[160] Christopher Kuner, L'arrêt *Schrems II* de la Cour de justice et l'avenir du règlement sur le transfert des données, 17 juillet 2020 < https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/> consulté le 26 mai 2021.
[161] CEPD, Recommandations 1/2020 sur les mesures qui complètent les outils de transfert pour assurer la conformité avec le niveau de protection des données personnelles de l'UE (10 novembre 2020) <https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf > consulté le 25 mai 2021.
[162] CEPD, Recommandations 2/2020 sur les garanties essentielles européennes pour les mesures de surveillance (10 novembre 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf> consulté le 25 mai 2021.

être respectées pour s'assurer que les interférences avec les droits à la vie privée et à la protection des données personnelles, par le biais de mesures de surveillance, lors du transfert de données personnelles, ne vont pas au-delà de ce qui est nécessaire et proportionné dans une société démocratique ».[163] Ces garanties européennes essentielles sont résumées comme suit :

A - le traitement doit être basé sur des règles claires, précises et accessibles ;

B - nécessité et proportionnalité par rapport aux objectifs légitimes poursuivis doivent être démontrées ;

C - mécanisme de contrôle indépendant ;

D - des remèdes efficaces doivent être disponibles pour l'individu.[164]

Le CEPD a reconnu que la décision finale quant à la justification des ingérences dans les droits de l'homme appartient à la CJUE. Toutefois, il a admis que « en l'absence d'un tel jugement et conformément à la jurisprudence actuelle, les autorités chargées de la protection des données sont tenues d'évaluer les cas individuels, soit d'office, soit à la suite d'une plainte, et de renvoyer l'affaire devant une juridiction nationale si elles soupçonnent que le transfert n'est pas conforme à l'article 45 [RGPD] dans le cas d'une décision d'adéquation, ou de suspendre ou d'interdire le transfert si elles estiment qu'il n'est pas possible de respecter l'article 46 du RGPD et que la protection des données transférées que requiert le droit de l'UE ne peut être assurée par d'autres moyens ».[165] De cette façon, le CEPD reconnaît le pouvoir des autorités de protection des données de renvoyer des cas individuels devant les tribunaux nationaux. Cependant, les autorités de protection des données n'ont pas encore renvoyé de cas potentiels devant une juridiction nationale.[166] La Recommandation 2/2020 présente une feuille de route en six étapes afin d'appliquer le principe de responsabilité aux transferts de données dans la pratique. Elle décrit les mesures techniques, contractuelles et organisationnelles supplémentaires à prendre lorsque l'outil utilisé pour le transfert des données n'est pas suffisant.

À la suite de ces recommandations, le 13 avril 2021, le Conseil européen de la protection des données a invité les États membres à évaluer et, le cas échéant, à réexaminer leurs accords internationaux qui impliquent des transferts internationaux de données à caractère personnel, tels que ceux relatifs à la fiscalité (par exemple, à l'échange automatique de données à caractère personnel à des fins fiscales), à la sécurité sociale, à l'entraide judiciaire, à la coopération policière, etc. ayant été conclus avant le 24 mai 2016 (pour les accords concernant le RGPD) ou le 6 mai 2016 (pour les accords concernant la LED). Cet examen devrait être effectué afin de déterminer si, tout en poursuivant les intérêts publics importants couverts par les accords, un alignement plus poussé sur la législation et la jurisprudence actuelles de l'Union en matière de protection des données, ainsi que sur les orientations du CEPD, pourrait être nécessaire.[167] Un tel examen peut s'avérer très pertinent en matière d'échange interétatique de données à caractère personnel dans les domaines de la fiscalité et de la lutte contre le blanchiment d'argent et le financement du terrorisme ; il permet par exemple aux autorités européennes chargées de la protection des données de saisir les

[163] Ibid.
[164] Ibid, pp. 8-15.
[165] Ibid, para. 6
[166] Voir par exemple l'ICO britannique qui n'a pas examiné la compatibilité de la FATCA avec la CEDH et le CFR et qui n'a pas non plus renvoyé l'affaire devant une juridiction nationale : Information Commissioner's Office, Freedom of Information Act 2000 (FOIA) Decision notice, 1er mars 2019, Ref : FS50751683, para. 33, para. 38-47.
[167] EDPB, Déclaration 04/2021 sur les accords internationaux, y compris les transferts (13 avril 2021) <https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf> consulté le 25 mai 2021.

tribunaux nationaux de cas individuels afin d'examiner la compatibilité des systèmes étrangers avec les garanties européennes, comme la FATCA, pour lequel des préoccupations ont déjà été exprimées concernant sa conformité avec les normes européennes de protection des données. L'accès aux données par les autorités américaines, qui était une préoccupation majeure dans les affaires *Schrems I* et *Schrems II*, affecte tous les échanges de données, y compris ceux qui relèvent de la FATCA (plus d'analyse sur la FATCA dans la section 9.2).

9.1 Échange de données pour la LBC/FT

Dans le contexte de la lutte contre le blanchiment d'argent et le financement du terrorisme, des informations sont transférées, dans plusieurs cas, vers des pays qui n'assurent pas un niveau adéquat de protection des données. Le cas le plus fréquent est l'échange de données d'une CRF vers un homologue étranger établi dans un pays n'ayant pas un niveau de protection adéquat. Lorsque les CRF sont membres du Groupe Egmont, elles suivent les principes d'Egmont pour l'échange d'informations entre les cellules de renseignement financier.[168]

La Recommandation 18 du GAFI invite les fonctions LAB/CFT au niveau du groupe et les succursales des institutions financières à partager les déclarations de soupçon entre elles.[169] Lorsque les succursales ou filiales sont établies dans un pays tiers, les exigences pertinentes en matière de protection des données sont appliquées. La 4AMLD, tenant compte de la possibilité qu'une succursale ou une filiale d'un établissement de crédit ou d'un établissement financier soit située dans un pays tiers où les exigences en matière de LBC/FT sont moins strictes que celles de l'État membre, et afin d'éviter l'application de normes très différentes au sein de l'établissement ou du groupe d'établissements, a établi la règle selon laquelle les entités obligées doivent appliquer les normes de l'Union ou notifier les autorités compétentes de l'État membre d'origine si l'application de ces normes n'est pas possible.[170]

L'article 53 de la 4AMLD oblige les États membres à assurer le libre échange d'informations entre les CRF européennes.[171] L'article 53, paragraphe 3, ne permet de refuser l'échange d'informations que dans des circonstances exceptionnelles, lorsque l'échange pourrait être contraire aux principes fondamentaux de son droit national.

9.2 Échange de données à des fins fiscales

Les États veillent à ce que, lorsque des échanges ont lieu vers un pays tiers qui n'assure pas un niveau de protection adéquat, les garanties établies dans la législation sur la protection des données soient respectées. Tous les accords SIR conclus avec des pays tiers doivent respecter les garanties en matière de protection des données établies dans la Convention 108+ du Conseil de l'Europe.

Les échanges interétatiques de données collectées à des fins fiscales et notamment en ce qui concerne la FATCA ont été au centre de l'attention du Groupe de travail Article 29 sur la protection des données (G29), le prédécesseur du Conseil européen de la protection des

---

[168] Groupe Egmont des cellules de renseignement financier, Principes d'échange d'informations entre cellules de renseignement financier (juillet 2013) <https://egmontgroup.org/en/filedepot_download/1658/79> consulté le 25 mai 2021.

[169] Benjamin Vogel, Jean-Baptiste Maillart, *National and international anti-money laundering law* (1st edn Insertia 2020) p. 858

[170] Directive 2015/849 (4AMLD), considérant 48 et art. 45(5)

[171] Voir également le considérant 58 de la 4AMLD.

données. Le G29 a adressé en 2012 deux lettres à M. Zourek, alors directeur général de la fiscalité et de l'union douanière, concernant le *Foreign Account Tax Compliance Act* (FATCA).[172] Déjà dans la lettre de juin 2012, le G29 soulignait que « la FATCA doit être mutuellement reconnu comme nécessaire d'un point de vue européen. Pour ce faire, il faut s'assurer que le traitement repose sur une base légale en évaluant soigneusement l'équilibre entre les objectifs de la FATCA et le droit fondamental de l'UE inscrit à l'article 8 de la Charte des droits fondamentaux - le droit à une vie privée et familiale, c'est-à-dire en démontrant la nécessité en prouvant que les données requises sont le minimum nécessaire par rapport à la finalité. Un transfert en bloc et le filtrage de toutes ces données ne constituent pas le meilleur moyen d'atteindre un tel objectif. Il convient donc d'envisager des mesures plus sélectives et moins larges afin de respecter la vie privée des citoyens respectueux de la loi, en particulier ; un examen des moyens alternatifs, moins attentatoires à la vie privée, doit être effectué pour démontrer la nécessité de la FATCA ».[173] En 2012 déjà, le G29 soulignait que « en l'absence d'une base légale pour légitimer le traitement requis, le G29 ne voit pas comment la conformité de la FATCA et de la directive pourrait être réalisée simultanément ».[174] Le G29 a constaté qu'à ce moment-là (en 2012), il n'y avait pas de base légale dans le droit communautaire ou national d'un État membre pour assurer le traitement légal des données dans le cadre de la FATCA. Si cela reste le cas lors de l'entrée en vigueur de la FATCA, les autorités de protection des données (APD) de l'UE/EEE peuvent envisager d'interdire le traitement des données en question ».[175]

En 2015, le G29 a publié une déclaration sur les échanges automatiques interétatiques de données à caractère personnel à des fins fiscales[176] et, en 2016, il a publié des lignes directrices à l'intention des États membres sur les critères permettant de garantir le respect des exigences en matière de protection des données dans le cadre de l'échange automatique de données à caractère personnel à des fins fiscales.[177]

La même année, le G29 a envoyé une lettre au collectif des "Américains accidentels" européens sur les questions de protection des données soulevées par la FATCA, les informant que, bien qu'il ne puisse se prononcer sur l'exclusion potentielle des Américains accidentels du champ d'application de la FATCA, ces derniers pouvaient déposer une plainte auprès de leur APD nationale ou de leur tribunal national.[178] La même année, le Parlement européen s'est penché sur les effets négatifs de la FATCA sur les citoyens de l'UE et en particulier sur les "Américains accidentels", c'est-à-dire les personnes « qui, par accident de naissance, ont hérité de la citoyenneté américaine, mais qui n'entretiennent aucun lien avec les États-Unis, n'ayant jamais vécu, travaillé ou étudié aux États-Unis et ne possédant pas de

---

[172] Lettre du groupe de travail Article 29 sur la protection des données à M. Zourek, alors directeur général de la fiscalité et de l'union douanière, concernant le Foreign Account Tax Compliance Act (FATCA), 21.06.2012, < https://ec.europa.eu/justice/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf> consulté le 26 mai 2021

[173] Ibid. Para. 8.3.

[174] Ibid. Para. 8.4.

[175] Ibid .Para. 1.5.

[176] Groupe de travail Article 29 sur la protection des données, Déclaration du WP29 sur les échanges automatiques interétatiques de données personnelles à des fins fiscales, WP230, 04 février 2015 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf> consulté le 26 mai 2021.

[177] Groupe de travail Article 29 sur la protection des données, Lignes directrices à l'intention des États membres sur les critères permettant de garantir le respect des exigences en matière de protection des données dans le cadre de l'échange automatique de données à caractère personnel à des fins fiscales, WP234, 16 décembre 2015 < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp234_en.pdf> consulté le 26 mai 2021.

[178] Lettre du groupe de travail Article 29 sur la protection des données à la Commission européenne, 21.06.2012,

numéro de sécurité sociale américain ».[179] Le Parlement européen a souligné « l'importance d'assurer un niveau adéquat de protection des données personnelles transférées aux États-Unis dans le cadre de la FATCA, dans le plein respect de la législation nationale et européenne en matière de protection des données ; [il a demandé] aux États membres de réexaminer leurs [accords intergouvernementaux de mise en œuvre -] (IGA) et de les modifier, si nécessaire, afin de les aligner sur les droits et principes du RGPD ; a invité] la Commission et le Conseil européen de la protection des données à enquêter sans délai sur toute violation des règles de l'UE en matière de protection des données par les États membres dont la législation autorise le transfert de données à caractère personnel à l'Internal Revenue Service (IRS) des États-Unis aux fins de la FATCA, et à engager des procédures d'infraction contre les États membres qui n'appliquent pas correctement les règles de l'UE en matière de protection des données ».[180] Dans sa récente résolution sur *Schrems II,* le Parlement européen s'est dit préoccupé par le niveau inefficace d'application du RGPD, notamment dans le domaine des transferts internationaux.[181] Il a demandé à la Commission européenne d'analyser l'impact des arrêts *Schrems I et II* sur les échanges de données avec les États-Unis [182], et en particulier la FATCA et les accords intergouvernementaux mettant en œuvre la FATCA. Dans sa résolution de 2018, le Parlement européen a souligné « l'importance de fournir un niveau de protection adéquat pour les données à caractère personnel transférées aux États-Unis dans le cadre de la FATCA, dans le plein respect de la législation nationale et européenne en matière de protection des données ; invite les États membres à réexaminer leurs IGA et à les modifier, le cas échéant, afin de les aligner sur les droits et les principes du RGPD » ; demande instamment à la Commission et au Conseil européen de la protection des données d'enquêter sans délai sur toute violation des règles de l'UE en matière de protection des données par les États membres dont la législation autorise le transfert de données à caractère personnel à l'IRS américain aux fins de la FATCA, et d'engager des procédures d'infraction contre les États membres qui n'appliquent pas correctement les règles de l'UE en matière de protection des données ».[183] Le Parlement européen a également conseillé les actions suivantes :

« 6. Demande à la Commission de réaliser une analyse exhaustive de l'impact de la FATCA et de la pratique extraterritoriale de l'imposition fondée sur la citoyenneté appliquée par les États-Unis à l'encontre des citoyens de l'Union, les établissements financiers de l'Union et les économies de l'Union, en tenant compte des efforts déployés actuellement en France et dans d'autres États membres, et d'expliquer si un écart majeur existe entre les citoyens de l'Union et/ou les résidents de l'Union dans différents États membres, en particulier eu égard aux

[179] Parlement européen, Résolution du Parlement du 5 juillet 2018 sur les effets négatifs de la loi américaine sur le respect des obligations fiscales relatives aux comptes étrangers (FATCA) sur les citoyens de l'UE et en particulier les "Américains accidentels" (2018/2646(RSP), JO C 118/141 (8 avril 2020) point D <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC> consulté le 25 mai 2021.

[180] Ibid, paragraphe 5.

[181] Parlement européen, Résolution du 20 mai 2021 sur l'arrêt de la CJUE du 16 juillet 2020 - *Commissaire à la protection des données c. Facebook Ireland Limited et Maximillian Schrems* ("Schrems II"), affaire C-311/18 (2020/2789(RSP)) para. 5 <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.pdf.> consulté le 25 mai 2021.

[182] Ibid, paragraphe 24.

[183] Parlement européen, Résolution du Parlement du 5 juillet 2018 sur les effets négatifs de la loi américaine sur le respect des obligations fiscales relatives aux comptes étrangers (FATCA) sur les citoyens de l'UE et en particulier les "Américains accidentels" (2018/2646(RSP), JO C 118/141 (8 avril 2020) para. 5 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC> consulté le 25 mai 2021.

règles de l'Union en matière de protection des données et aux normes en matière de droits fondamentaux en lien avec la FATCA et les «indices d'américanité»; invite la Commission à évaluer en détail le degré de réciprocité ou de non-réciprocité de la FATCA dans l'ensemble de l'Union et à vérifier scrupuleusement que les États-Unis respectent les obligations qui leur incombent en vertu des divers accords intergouvernementaux signés avec les États membres;

7. invite la Commission à évaluer et, si nécessaire, à prendre des mesures pour veiller à ce que les droits fondamentaux et les valeurs de l'Union européenne consacrés dans la charte des droits fondamentaux et dans la convention européenne des droits de l'homme, comme le droit à la protection de la vie privée et le principe de non-discrimination, ainsi que les règles de l'Union en matière de protection des données soient respectés dans le contexte de la FATCA et de l'échange automatique d'informations fiscales avec les États-Unis;

8. déplore le manque de réciprocité inhérent aux accords intergouvernementaux de mise en œuvre signés par les États membres, en particulier en ce qui concerne l'étendue des informations à échanger, qui est plus vaste pour les États membres qu'elle ne l'est pour les États-Unis; demande à tous les États membres de suspendre collectivement l'application de leurs accords intergouvernementaux de mise en œuvre (ou le partage d'informations autres que celles relatives à des comptes financiers détenus dans l'Union européenne par des citoyens américains résidant aux États-Unis) jusqu'à ce que les États-Unis consentent à adopter une approche multilatérale de l'échange automatique d'informations, soit en abrogeant la FATCA et en intégrant la norme commune de déclaration, soit en renégociant la FATCA à l'échelle de l'Union européenne avec les mêmes obligations de réciprocité en matière de partage des deux côtés de l'Atlantique;

9. invite la Commission et le Conseil à présenter une approche commune de l'Union relative à la FATCA afin de protéger de manière suffisante les droits des citoyens européens (en particulier les «Américains accidentels») et à améliorer la réciprocité dans l'échange automatique d'informations de la part des États-Unis;

10. demande au Conseil de charger la Commission d'ouvrir des négociations avec les États-Unis en vue d'un accord FATCA UE–États-Unis afin de garantir la pleine réciprocité de l'échange d'informations et de faire respecter les principes fondamentaux du droit de l'Union ainsi que la directive sur les comptes de paiement, et de permettre aux «Américains accidentels» de se défaire de leur citoyenneté américaine non souhaitée gratuitement, sans enregistrement de leurs données et sans sanctions ».[184]

Quelques mois plus tard, le CEPD a publié une déclaration sur la FATCA, annonçant qu'il avait déjà commencé à préparer des lignes directrices sur les outils de transfert fondées sur l'article 46 du RGPD (garanties appropriées).[185] Les recommandations correspondantes ont été publiées en novembre 2020. [186]

---

[184] Parlement européen, Résolution du Parlement du 5 juillet 2018 sur les effets négatifs de la loi américaine sur le respect des obligations fiscales relatives aux comptes étrangers (FATCA) sur les citoyens de l'UE et en particulier les "Américains accidentels" (2018/2646(RSP), JO C 118/141 (8 avril 2020) paras. 6-10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2020.118.01.0141.01.ENG&toc=OJ%3AC%3A2020%3A118%3ATOC consulté le 25 mai 2021.

[185] Conseil européen de la protection des données, EDPB Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA), 25 février 2019 < https://edpb.europa.eu/our-work-tools/our-documents/statements/edpb-statement-012019-us-foreign-account-tax-compliance-act_sv> consulté le 26 mai 2021.

[186] Conseil européen de la protection des données, Recommandations 01/2020 sur les mesures qui complètent les outils de transfert pour assurer la conformité au niveau de protection des données

Toutes les entités qui transfèrent des données vers des pays tiers, et en particulier vers les États-Unis, doivent veiller à respecter le cadre de protection des données établi dans la Convention 108+ du Conseil de l'Europe. De même, les Parties à la convention, éventuellement par l'intermédiaire de leurs autorités de contrôle nationales, doivent examiner la compatibilité des accords qui facilitent l'échange de données à des fins fiscales vers des pays tiers avec le cadre de protection des données de la Convention 108+ du CdE.

10. Conclusions et recommandations

Le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme ainsi que les règles de lutte contre la fraude fiscale et l'évasion fiscale sont appliqués en même temps que les dispositions du cadre de protection des données. Ce rapport présente les principes les plus importants, ainsi que les droits et obligations qui doivent être respectés dans ce contexte. Une attention particulière doit être accordée aux questions suivantes, telles que discutées dans le rapport :

Un point important à clarifier, tant dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme que dans le domaine fiscal, concerne l'attribution des rôles de protection des données aux entités concernées. En particulier lorsque des PPP sont établis, ce qui est plus pertinent pour la lutte contre le blanchiment et le financement du terrorisme, une attribution claire des rôles aux entités qui participent au PPP et une délimitation des droits et obligations en matière de traitement des données personnelles doivent être établies, idéalement déjà dans la loi établissant le PPP. En ce qui concerne le domaine de la fiscalité, les parties à la Convention doivent veiller à inclure une attribution claire des rôles en matière de protection des données, qui s'accompagne de droits et d'obligations concrets, lors de l'établissement de règles impliquant l'échange de données.

Il est essentiel que tous les échanges de données par des entités privées, qui ont généralement lieu à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme, se fassent sur une base juridique claire.

La Convention 108+ du Conseil de l'Europe établit un certain nombre de droits pour les personnes concernées. La jurisprudence récente de la CJUE a renforcé la protection de ces droits. En suivant le raisonnement de la CJUE, il doit être accepté que les entités privées impliquées dans les échanges de données à caractère personnel, soit à des fins fiscales, soit - et c'est peut-être plus important - à des fins de lutte contre le blanchiment d'argent et le financement du terrorisme, restent dans le champ d'application du cadre européen de protection des données (en particulier, le RGPD), même lorsque l'échange a été demandé par une autorité compétente (qui pourrait également être une CRF dans le cas de la lutte contre le blanchiment d'argent et le financement du terrorisme). En tant que tel, un examen attentif du régime sous lequel l'échange de données est réalisé, en particulier lorsque des entités privées sont impliquées, est essentiel, avant de restreindre les droits des personnes concernées. Une attention particulière est accordée au droit des personnes concernées d'être informées du traitement de leurs données personnelles. Bien que le droit des personnes concernées d'être informées du traitement de leurs données personnelles puisse être restreint dans le cadre de la lutte contre le blanchiment d'argent et la fraude fiscale, cela ne doit pas être fait de manière générale. Sur la base de la jurisprudence de la CJUE et de la CtEDH, les autorités compétentes peuvent s'abstenir d'informer les personnes concernées du traitement de leurs données personnelles. Toutefois, ces autorités doivent notifier les personnes

personnelles de l'UE, adoptées le 10 novembre 2020 < https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf> consulté le 26 mai 2021.

concernées, selon les procédures nationales applicables, dès que cette notification n'est plus susceptible de compromettre les enquêtes. Les autorités de contrôle ont le pouvoir d'examiner si la notification aux personnes concernées est effectivement réalisée. Dans l'arrêt *La Quadrature du Net*, la CJUE a établi de nouvelles règles concernant la notification des personnes concernées lors d'une analyse automatisée. Cet arrêt est d'une grande importance lorsque l'analyse automatisée des données a lieu à la fois dans le contexte de la fraude fiscale/évasion fiscale et dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Si l'objectif de la CJUE était d'imposer une telle obligation, il n'est pas évident de savoir si l'obligation de notifier individuellement les personnes concernées lorsque ces personnes ont été distinguées sur la base d'une analyse automatisée uniquement aux autorités nationales ou si une telle obligation devrait être étendue aux entités privées également. Cette dernière préoccupation aurait un impact important sur les entités obligées dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme, qui utilisent déjà l'IA pour effectuer des opérations d'exploration de données et de profilage.

L'article 5 de la Convention 108+ du Conseil de l'Europe stipule un certain nombre de principes pour la légitimité du traitement des données et la qualité des données, qui doivent être respectés chaque fois que des données personnelles sont échangées. Les principes établis à l'article 5, paragraphe 4, c'est-à-dire la loyauté et la transparence, la limitation de la finalité, la minimisation des données, l'exactitude des données et la limitation du stockage, peuvent être restreints conformément à l'article 11 de la Convention 108+ du Conseil de l'Europe. Les échanges interétatiques de données à caractère personnel doivent toujours avoir lieu dans le respect de ces principes, et les restrictions prévues par l'article 11 de la convention 108+ du Conseil de l'Europe doivent être clairement justifiées.

Le principe de proportionnalité exige une utilisation prudente de l'IA dans les domaines de la lutte contre le blanchiment d'argent et le financement du terrorisme et de la fiscalité, afin de s'assurer que le traitement respecte le cadre de la protection des données.

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 et le financement du terrorisme, la question de la protection adéquate se pose dans tous les cas où l'échange de données à caractère personnel concerne un pays qui ne dispose pas d'un niveau de protection adéquat. La CJUE a publié un certain nombre d'arrêts relatifs aux transferts transfrontaliers de données à caractère personnel qui peuvent être pertinents pour les échanges de données à des fins fiscales et dans le contexte de la LBC/FT. Les arrêts *Schrems I* et *Schrems II* établissent des garanties qui doivent être respectées lorsque des données à caractère personnel sont transférées vers un pays tiers et qui doivent être prises en compte lorsque des échanges de données interétatiques ont lieu à des fins fiscales mais aussi pour la lutte contre le blanchiment d'argent et le financement du terrorisme. En particulier, les garanties établies par la CJUE soulèvent des questions quant à la compatibilité des échanges de données interétatiques sans garanties adéquates. L'accès aux données par les autorités américaines, qui était une préoccupation majeure dans les affaires *Schrems I* et *Schrems II*, affecte tout échange de données, y compris ceux relevant de la FATCA. Il est donc recommandé aux États de veiller à ce que les échanges de données à des fins fiscales et de lutte contre le blanchiment de capitaux et le financement du terrorisme soient assortis de garanties supplémentaires, conformément à la jurisprudence de la CJUE.

Toutes les entités qui transfèrent des données vers des pays tiers, et en particulier vers les États-Unis, doivent veiller à respecter le cadre de protection des données établi dans la Convention 108+ du Conseil de l'Europe. Les parties à la Convention, éventuellement par l'intermédiaire de leurs autorités de contrôle nationales, examinent la compatibilité des accords qui facilitent l'échange de données à des fins fiscales vers des pays tiers avec le cadre de protection des données de la Convention 108+ du Conseil de l'Europe. En outre, les parties à la Convention doivent permettre à leurs autorités de protection des données de saisir les tribunaux nationaux de cas individuels afin d'examiner la compatibilité des systèmes

étrangers avec les garanties européennes, comme la FATCA pour lequel des préoccupations ont déjà été soulevées, en ce qui concerne sa conformité avec les normes européennes de