COMMISSION
EUROPÉENNE

Bruxelles, le 24.7.2019
COM(2019) 372 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur l'interconnexion des mécanismes automatisés centralisés nationaux (registres centraux ou systèmes électroniques centraux de recherche de données) des États membres concernant les comptes bancaires

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur l'interconnexion des mécanismes automatisés centralisés nationaux (registres centraux ou systèmes électroniques centraux de recherche de données) des États membres concernant les comptes bancaires

1. Introduction

L'article 32 *bis* de la directive anti-blanchiment 2015/849/UE[1] requiert des États membres qu'ils mettent en place au 10 septembre 2020 des mécanismes automatisés centralisés nationaux, tels que des registres centraux ou des systèmes électroniques centraux de recherche de données, permettant l'identification de toute personne physique ou morale qui détient ou contrôle des comptes de paiement, des comptes bancaires et des coffres-forts. La directive anti-blanchiment définit un ensemble minimal d'informations à inclure dans ces mécanismes centralisés. Elle prévoit par ailleurs que les cellules de renseignement financier devraient y avoir accès de manière immédiate et non filtrée, et que les autres autorités compétentes devraient également y avoir accès pour l'accomplissement des missions qui leur incombent au titre de ladite directive. La directive 2019/1153 facilitant l'accès aux informations financières et d'une autre nature[2] oblige les États membres à désigner les autorités nationales chargées de la prévention ou de la détection d'infractions pénales, ou des enquêtes ou des poursuites en la matière qui devraient avoir accès de manière directe, immédiate, et non filtrée à l'ensemble minimal d'informations inclus dans ces mécanismes centralisés. Ces autorités compétentes comprennent au moins les bureaux de recouvrement des avoirs.

L'accès des autorités compétentes aux registres centraux des comptes bancaires ou aux systèmes centraux de recherche de données aura une forte incidence dans la lutte contre le blanchiment de capitaux, les infractions sous-jacentes associées ou le financement du terrorisme et, plus généralement, dans la lutte contre les formes graves de criminalité. Ayant en vue les objectifs de la directive anti-blanchiment et de la directive facilitant l'accès aux informations financières et d'une autre nature, une interconnexion future des registres des comptes bancaires et des systèmes de recherche de données à l'échelle de l'Union faciliterait la coopération transfrontière des autorités compétentes participant à la lutte contre le blanchiment de capitaux, le financement du terrorisme et d'autres formes graves de criminalité.

L'article 32 *bis*, paragraphe 5, de la directive anti-blanchiment exige de la Commission qu'elle évalue les conditions et les spécifications techniques et procédures permettant d'assurer une interconnexion sécurisée et efficace des mécanismes automatisés centralisés. Ainsi, le présent rapport évalue les différentes solutions informatiques à l'échelle de l'Union qui sont déjà opérationnelles ou en cours

[1] 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) 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 (JO L 849 du 9.7.2018, p. 1).

[2] 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 (JO L 186 du 11.7.2019, p. 122).

d'élaboration et qui pourraient servir de modèles pour une interconnexion possible des mécanismes centralisés. Un instrument législatif serait nécessaire pour assurer une telle interconnexion.

Le présent rapport devrait être examiné en liaison avec le rapport de la Commission sur l'évaluation supranationale des risques[3], le rapport de la Commission sur les cellules de renseignement financier[4] et le rapport de la Commission sur l'évaluation des récents cas présumés de blanchiment de capitaux impliquant des établissements de crédit de l'Union européenne[5], qui sont présentés parallèlement.

2. État des lieux

2.1. Registres centralisés ou systèmes électroniques de recherche de données concernant les comptes bancaires dans les États membres

À l'heure actuelle[6], les mécanismes centralisés contenant des informations sur les comptes bancaires sont opérationnels dans 15 États membres[7]. D'après leurs réponses, les États membres ont une légère préférence pour la solution technique du registre centralisé: en effet, ils sont 17 à avoir ou à être sur le point d'avoir des registres centralisés, contre 9 à déclarer avoir ou envisager d'avoir des systèmes centraux de recherche de données[8]. Ils ont également exprimé une préférence pour les systèmes qui contiennent plus de données que l'ensemble minimal d'informations relatives au profil du compte, prévu à l'article 32 *bis*, paragraphe 5, de la 5e directive anti-blanchiment (11 ont répondu y être en faveur contre 6)[9].

[3] Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontières - COM(2019) 370.

[4] Rapport de la Commission au Parlement européen et au Conseil portant évaluation du cadre pour la coopération entre les cellules de renseignement financier - COM(2019) 371.

[5] Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des récents cas présumés de blanchiment de capitaux impliquant des établissements de crédit de l'Union européenne - COM(2019) 373.

[6] Les informations contenues dans cette section sont fondées sur les réponses des États membres à un questionnaire spécifique qui leur a été adressé en mars 2019, sur les informations reçues lors de l'atelier de transposition du 1er avril 2019 organisé par la Commission et sur l'annexe 7 de l'analyse d'impact accompagnant la proposition de directive du Parlement européen et du Conseil fixant les règles facilitant l'utilisation d'informations financières et d'autre nature aux fins de la prévention et de la détection de certaines infractions pénales, et des enquêtes et des poursuites en la matière, et abrogeant la décision 2000/642/JAI du Conseil [SWD(2018) 114 final].

[7] Allemagne, Autriche, Belgique, Bulgarie, Croatie, Espagne, France, Grèce, Italie, Lettonie, Lituanie, Portugal, Roumanie, Slovénie, Tchéquie. La Slovaquie dispose d'un système électronique centralisé de recherche de données, cependant, il ne peut à ce jour être consulté que par les officiers ministériels.

[8] La Finlande rentre dans les deux catégories, car elle est sur le point de déployer un système utilisant les deux solutions. Un registre central collecte et conserve les informations pertinentes dans une base de données centrale, alors qu'un système électronique central de recherche de données est un portail informatique central qui récupère des informations issues de différentes bases de données sous-jacentes (actualisées, par exemple, par les institutions financières).

[9] D'après les réponses obtenues des États membres, de telles informations supplémentaires pourraient prendre la forme de données sur les contrats financiers conclus par le titulaire du compte ou sur des opérations réalisées en lien avec le compte.

2.2. Systèmes européens assurant l'interconnexion des bases de données électroniques nationales décentralisées

Plusieurs projets européens assurent l'interconnexion décentralisée à l'échelle de l'Union des bases de données électroniques nationales[10]. Les systèmes informatiques jugés pertinents pour ce rapport sont les suivants:

Le système européen d'information sur les casiers judiciaires (ECRIS) a été mis en service en avril 2012 afin d'améliorer l'échange d'informations sur les casiers judiciaires dans l'ensemble de l'Union[11]. Tous les États membres sont actuellement connectés à l'ECRIS. L'ECRIS garantit que les informations sur les condamnations pénales sont échangées entre les États membres de façon uniforme, rapide et compatible et offre aux juges et aux procureurs un accès aisé à toutes les informations relatives aux antécédents judiciaires des personnes concernées[12].

Le système d'information européen concernant les véhicules et les permis de conduire (EUCARIS) met en contact les États qui en sont membres afin qu'ils puissent partager les informations dont ils disposent sur les véhicules et les permis de conduire ainsi que d'autres données en lien avec les transports. L'EUCARIS est un mécanisme qui met en lien les différentes autorités chargées de l'immatriculation des véhicules et des permis de conduire dans l'Union. Grâce à ce système, les données concernant les propriétaires de véhicules et les assurances automobiles peuvent être échangées entre les points de contact nationaux des États membres[13].

L'interconnexion des registres d'insolvabilité (IRI) à l'échelle de l'Union, qui comprend deux projets différents. La première version du système (IRI 1.0) est accessible sur le portail e-Justice européen[14] depuis juillet 2014. Elle a été élaborée en tant que projet pilote[15] avec la participation volontaire de

---

[10] Les systèmes informatiques centralisés regroupant des bases de données uniques à l'échelle de l'Union, comme le système d'information Schengen ou le système d'information sur les visas, sont exclus de l'évaluation, car ils ne sont pas compatibles avec l'existence préalable de bases de données centralisées à l'échelle nationale.

[11] Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres et décision du Conseil 2009/316/JAI du 6 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2009/315/JAI, actuellement modifiées par la directive (UE) 2019/884 du Parlement européen et du Conseil du 17 avril 2019 en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS).

[12] En avril 2019, un nouveau cadre législatif a été adopté en vue de compléter l'ECRIS par un mécanisme permettant d'échanger efficacement des informations sur les casiers judiciaires des ressortissants de pays tiers condamnés sur le territoire de l'Union. Le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN) sera un système de concordance/non-concordance centralisé contenant uniquement les données d'identification des ressortissants de pays tiers condamnés et l'indication de l'État membre où ces derniers ont été précédemment condamnés. En cas de concordance, l'État membre demandeur devra demander les informations sur la condamnation auprès du ou des État(s) membre(s) indiqué(s) dans l'ECRIS-TCN en passant par le système ECRIS existant.

[13] Les bases juridiques du service Prüm sont la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, et la décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI.

[14] https://beta.e-justice.europa.eu/246/FR/bankruptcy_amp_insolvency_registers__search_for_insolvent_firms_in_the_eu?init=true.

[15] Le projet pilote a été mis en œuvre et appliqué sur la base du plan d'action européen pluriannuel relatif à la justice en ligne 2009-2013 (JO C 75 du 31.3.2009, p. 1) et du plan d'action européen pluriannuel relatif à la justice en ligne 2014-2018 (JO C 182 du 14.6.2014, p. 2).

certains États membres[16]. La seconde version (IRI 2.0) est fondée sur le règlement (UE) 2015/848 relatif aux procédures d'insolvabilité et interconnectera les registres d'insolvabilité nationaux de tous les États membres (à l'exception du Danemark). Tous les États membres doivent assurer ladite interconnexion d'ici juin 2021. L'IRI 1.0 est fondée sur un service de messagerie web sécurisé et normalisé (SOAP sur HTTPS) et l'IRI 2.0 a pour fonctionnalité supplémentaire de favoriser les échanges de données, tirant parti des éléments constitutifs de la transmission électronique de documents (eDelivery) du mécanisme pour l'interconnexion en Europe (MIE)[17].

Le système d'interconnexion des registres du commerce (BRIS) interconnecte les registres du commerce; il permet à ces derniers d'échanger des messages transfrontaliers sur des fusions et des succursales, et offre aux utilisateurs du portail e-Justice la possibilité d'obtenir des informations sur des entreprises de l'Union dans plusieurs langues différentes. Le système est opérationnel depuis juin 2017, conformément à la directive (UE) 2012/17 concernant l'interconnexion des registres centraux, du commerce et des sociétés[18]. Le BRIS utilise les éléments constitutifs de la transmission électronique de documents du mécanisme pour l'interconnexion en Europe (MIE) aux fins des échanges de messages normalisés. Le système est décentralisé, mais doté d'une composante centrale (la plateforme centrale européenne) qui stocke et indexe les dénominations sociales et les numéros d'enregistrement des entreprises.

L'interconnexion des registres fonciers (LRI) est un projet volontaire en cours[19] qui vise à fournir un point d'accès unique aux registres fonciers des pays participants de l'UE sur le portail e-Justice européen. Il devrait être opérationnel au cours du deuxième trimestre de l'année 2020.

Le projet EBOCS (Structures européennes de contrôle et de propriété bénéficiaire) est mené par l'Association européenne des registres de commerce avec le soutien financier du Fonds pour la sécurité intérieure - coopération policière, prévention et répression de la criminalité, et gestion des crises (FSI-POLICE) (programmes de travail annuels 2016 et 2018). La plateforme EBOCS offre un accès simplifié et unifié aux données du registre des entreprises sur les structures de contrôle et de propriété bénéficiaire à des fins d'analyse financière et d'enquête. Elle prévoit également l'agrégation des résultats des demandes sur une carte de visualisation. Il convient de noter que l'Union ne détient pas les droits de propriété intellectuelle de ce système.

Le système e-CODEX (communication du portail e-Justice au moyen d'échanges de données en ligne) facilite la mise en place d'une communication sécurisée dans les procédures pénales et civiles en prévoyant un système décentralisé pour l'échange de messages électroniques transfrontaliers dans le domaine de la justice[20]. Actuellement, e-CODEX facilite la communication électronique entre les citoyens et les tribunaux et entre les administrations des États membres en pilotant la procédure

[16] Actuellement, l'Allemagne, l'Autriche, l'Estonie, l'Italie, la Lettonie, les Pays-Bas, la Roumanie, la Slovénie et la Tchéquie y participent.
[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery.
[18] Directive (UE) 2012/17 du Parlement européen et du Conseil du 13 juin 2012 modifiant la directive (CEE) 89/666 du Conseil et les directives (CE) 2005/56 et 2009/101 du Parlement européen et du Conseil en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés (JO L 156 du 16.6.2012).
[19] L'interconnexion n'est fondée sur aucune base juridique, mais elle fonctionne comme un système volontaire auxquels les États membres peuvent choisir de participer.
[20] Le système e-CODEX consiste en un ensemble de produits logiciels (transmission électronique de documents du MIE et connecteur d'e-CODEX), qui peuvent être utilisés pour configurer un point d'accès à l'échelon national aux fins d'une telle communication sécurisée. Il ne s'agit pas d'un système qui interconnecte les bases de données ou registres nationaux, mais d'une infrastructure de communication qui garantit une communication et un échange d'informations sécurisés entre les systèmes d'information nationaux et, à ce titre, il est considéré comme pertinent pour l'évaluation du présent rapport. Le système e-CODEX a été élaboré entre 2010 et 2016 par 21 États membres, avec la participation d'autres pays/territoires et organisations.

européenne d'injonction de payer et la procédure européenne de règlement des petits litiges. En matière pénale, e-CODEX est également la solution de choix pour le système d'échange numérique de preuve électronique[21], permettant des échanges électroniques dans le contexte de la décision d'enquête européenne et des traités d'assistance judiciaire mutuelle.

3. Principaux paramètres

3.1. Condition d'accès par les utilisateurs

Après consultation des systèmes existants, il apparaît que l'accessibilité du système interagissant avec le système informatique interconnecté proposé à l'utilisateur est déterminée par la raison de l'établissement de l'interconnexion. Lorsque l'interconnexion a été établie dans l'objectif d'accroître la transparence des informations pour les entreprises sur le marché intérieur (BRIS, IRI), le système est publiquement accessible. Lorsque l'objectif de l'interconnexion est d'améliorer la coopération transfrontière entre les autorités compétentes en vue de l'application de la loi ou à des fins administratives d'ordre public, comme c'est le cas de l'ECRIS ou du service Prüm de l'EUCARIS[22], l'accès est limité.

La fonctionnalité de recherche d'une entreprise proposée par le système BRIS est disponible à tous dans le portail e-Justice, mais l'infrastructure de messagerie est actuellement limitée par la loi pour les registres nationaux du commerce. En ce qui concerne l'IRI, les informations consultables au moyen de l'interface de recherche sont accessibles publiquement et la possibilité pour les États membres de restreindre l'accès des demandeurs ayant un intérêt légitime n'est accordée que dans le contexte d'une «procédure d'insolvabilité du consommateur». L'ECRIS n'est accessible qu'aux autorités centrales désignées des États membres. De façon semblable, l'accès aux services de l'EUCARIS est ouvert aux pouvoirs publics par l'intermédiaire des points de contact nationaux désignés. Pour l'EBOCS, l'accès est limité aux agences de lutte contre la criminalité participantes.

Système	Accès public	Accès limité	Observations
BRIS	Oui		La fonctionnalité de recherche d'une entreprise proposée par le système BRIS est disponible à tous dans le portail e-Justice, mais l'infrastructure de messagerie est actuellement limitée par la loi pour les registres nationaux du commerce.
IRI	Oui		
ECRIS		Oui	Pour les autorités centrales des États membres nommées spécifiquement à cette fonction.
EUCARIS		Oui	Pour les points de contact nationaux de l'EUCARIS, par l'intermédiaire desquels les pouvoirs publics peuvent obtenir un accès, selon la base juridique de la coopération.
EBOCS		Oui	Pour les agences de lutte contre la criminalité participant au projet.
LRI	Oui*		Les fonctionnalités avancées ne seront accessibles qu'aux professionnels du droit certifiés.

[21] Établi conformément aux conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace du 9 juin 2016.
[22] Plusieurs autorités peuvent accéder à l'EUCARIS, mais le service Prüm de ce système régule l'accès aux autorités répressives.
* n'est pas encore opérationnel

Tableau 1: accessibilité du système interagissant avec le système d'information interconnecté proposé aux utilisateurs

Au titre de la directive anti-blanchiment, l'objectif des mécanismes centralisés concernant les comptes bancaires est d'améliorer la lutte contre le blanchiment de capitaux et le financement du terrorisme, et leur accès est limité à certains pouvoirs publics. La directive facilitant l'accès aux informations financières et d'une autre nature élargit le but de l'utilisation des informations contenues dans les mécanismes centraux aux infractions graves et élargit les droits d'accès aux autorités compétentes désignées. Enfin, la capacité d'action des autorités nationales ayant un accès direct aux registres nationaux revient aux États membres exploitant les registres. De telles règles peuvent entraîner des disparités, car certains types d'autorités peuvent avoir accès aux données dans un État membre et pas dans un autre. Dans le contexte d'un échange transfrontière au moyen du système d'interconnexion à l'échelle de l'Union, cela pourrait mener à une situation où une autorité demande des informations provenant du registre d'un autre État membre alors que cette recherche a été refusée à une autre autorité semblable.

Une possibilité serait que les mêmes autorités, se voyant accorder un accès direct aux mécanismes centralisés conformément à la directive anti-blanchiment et à la directive facilitant l'accès aux informations financières et d'une autre nature, bénéficient d'un accès à la plateforme d'interconnexion. Une autre option serait que les droits d'accès au système d'interconnexion soient accordés aux mêmes types d'autorités dans tous les États membres, ce qui pourrait être réalisé au moyen d'une liste harmonisée et fermée à l'échelon de l'UE des types d'autorités spécifiés en accord avec l'objectif de l'accès aux informations.

Si l'interconnexion est élargie à toutes les autorités bénéficiant actuellement d'un accès au titre de lois nationales, des dispositions détaillées sur les conditions d'accès et de recherche par les autorités nationales compétentes seraient nécessaires. À cet égard, il est important de souligner que la directive sur l'utilisation d'informations financières et d'une autre nature établit des conditions strictes concernant l'accès et les recherches sur les informations relatives aux comptes bancaires contenues dans les mécanismes automatisés centralisés par les autorités compétentes désignées à l'échelon national. De telles conditions comprennent, par exemple, la fourniture d'un accès aux registres et aux systèmes de recherche de données uniquement aux personnes autorisées et spécifiquement désignées de chaque autorité compétente. Une autre mesure visant à atténuer les risques générés par l'extension des droits d'accès aux autorités nationales désignées pourrait être la restriction de la portée des informations consultables dans le système d'interconnexion à l'ensemble minimal d'informations relatif au profil du compte, conformément à l'article 32 *bis*, paragraphe 3, de la directive anti-blanchiment.

En ce qui concerne le champ d'application, l'article 32 *bis*, paragraphe 3, de la directive anti-blanchiment définit les informations que tous les systèmes centralisés doivent contenir, comme le titulaire du compte, les comptes bancaires identifiés par un numéro IBAN et les coffres-forts détenus par un établissement de crédit sur le territoire national. Néanmoins, l'article 32 *bis*, paragraphe 4, de la directive prévoit la possibilité que les États membres incluent d'autres informations dans les registres, jugées essentielles aux cellules de renseignement financier et aux autorités compétentes pour l'accomplissement des obligations qui leur incombent en vertu de la directive. Du point de vue de la protection des données à caractère personnel, il semble nécessaire de restreindre la portée des informations consultables via la plateforme d'interconnexion à l'ensemble minimal obligatoire d'informations tel que défini à l'article 32 *bis*, paragraphe 3, de la directive anti-blanchiment. Conformément aux règles de protection des données, l'accès aux données à caractère personnel

devrait être proportionné à ce qui est nécessaire à la réalisation des objectifs définis dans la directive anti-blanchiment. Une approche semblable est adoptée par la directive concernant l'utilisation d'informations financières et d'une autre nature. L'article 4, paragraphe 2, de cette directive précise que les informations supplémentaires que les États membres incluent dans les mécanismes centralisés ne sont pas accessibles aux autorités compétentes et que celles-ci ne peuvent y effectuer des recherches.

3.2. Fonctionnalité de recherche

Les critères de recherche applicables sont extrêmement importants pour garantir que l'interconnexion des mécanismes centralisés automatisés apporte une valeur ajoutée aux utilisateurs. Les critères de recherche devraient être conçus de manière à renforcer la capacité des autorités concernées à effectuer leurs tâches et à réaliser des enquêtes plus efficacement, tout en garantissant la proportionnalité et en respectant les exigences applicables en matière de protection des données.

Une attention particulière devrait être accordée aux parties habilitées à effectuer la recherche (parties privées ou publiques) et aux données qui peuvent ou ne peuvent pas être censées être connues de la personne réalisant la recherche. Exiger que la recherche contienne des données ayant peu de chances d'être connues de la personne effectuant la demande peut rendre difficile voire impossible la réalisation de recherches de façon efficace. Il convient également de noter qu'il se peut qu'une cellule de renseignement financier ou que l'autorité répressive d'un État membre ne connaisse pas la date de naissance ou le numéro d'identification national d'un citoyen d'un autre État membre. Si l'interconnexion est ouverte à de telles informations supplémentaires dans les systèmes centralisés, il sera important de déterminer s'il sera possible d'effectuer les recherches sur la base de telles informations supplémentaires.

Les types d'informations constituant l'ensemble minimal harmonisé d'informations prévu à l'article 32 *bis*, paragraphe 3, de la directive anti-blanchiment pourraient être envisagés comme critères de recherche. De cette façon, le système d'interconnexion répondrait aux objectifs originaux des mécanismes centralisés. De nouvelles mesures de protection permettant de vérifier les concordances (en particulier lorsqu'une recherche génère plusieurs réponses) seraient nécessaires.

Les conditions relatives aux modalités de recherche applicables sont décisives pour l'efficacité d'utilisation des bases de données interconnectées. La possibilité d'effectuer des «recherches approximatives», c'est-à-dire des recherches qui génèrent des plages de résultats plus larges même si un terme est mal orthographié ou incomplet, élargira les résultats de concordances, augmentant partant la probabilité que les informations demandées soient consultées grâce à la recherche, mais cela pourrait aussi soulever des préoccupations en matière de protection des données, car risquant de dévoiler des données à caractère personnel qui n'étaient pas véritablement concernées par la recherche. Inversement, une exigence de «correspondance exacte» atténuerait le risque de divulgation inutile de données à caractère personnel, mais augmenterait la probabilité que les informations demandées soient négligées par le moteur de recherche (en cas de différence dans l'orthographe de l'entrée ou d'utilisation de différentes règles de translittération).

La possibilité d'effectuer des «recherches approximatives» réduirait le recours aux procédures de validation automatiques et éviterait ou réduirait ainsi le volume de correspondances erronées, mais elle réduirait également la valeur opérationnelle du système. Si le choix de «recherches approximatives» est validé, il conviendrait d'envisager d'utiliser d'autres outils pour réduire le risque de rechercher des renseignements à l'aveuglette, comme c'est par exemple le cas dans l'IRI où le nombre maximal de résultats affichés est limité.

3.3. Structure de gouvernance, responsabilité de maintenance

Pour ce qui est du BRIS, de l'IRI, de la LRI et de l'ECRIS, les différents services de la Commission européenne sont *responsables de la maintenance du système informatique*, c'est-à-dire qu'ils doivent garantir la disponibilité de l'élément d'interconnexion et assumer les coûts découlant de sa mise en place et de sa maintenance. Pour le moment, e-CODEX est entretenu par un consortium d'États membres (la transmission électronique de documents du MIE relève des attributions de la Commission européenne). Dans l'EUCARIS, la responsabilité est assumée par les 28 États membres et les pays tiers participants, alors que dans l'EBOCS, le système est détenu par l'Association européenne des registres du commerce (EBRA). Puisque ces systèmes informatiques interconnectent des bases de données nationales, la responsabilité de maintenir les bases de données nationales et de garantir leur disponibilité revient aux États membres.

Concernant la *structure de gouvernance* d'un système qui interconnecte des bases de données, les compétences nécessaires pour la prise de décisions politiques et opérationnelles devraient être bâties d'une façon servant les intérêts des composantes nationales.

S'agissant du BRIS, son comité de pilotage agit en qualité de forum interne de la Commission pour les décisions politiques, la supervision et la gestion du BRIS, alors que le groupe d'experts en droit des sociétés - Registres de commerce (CLEG-BRIS) agit en qualité de forum pour la collaboration à l'échelon politique entre les acteurs concernés. Une distinction semblable peut être constatée entre le processus d'élaboration des politiques et les structures de fonctionnement dans EUCARIS, car l'assemblée générale composée de hauts représentants des agences gouvernementales détermine la politique à appliquer, gère le budget et les contributions annuelles, et prend des dispositions pour la gestion du système.

3.4. Contrôle des données

La responsabilité de la maintenance du système informatique diffère de la question de la *responsabilité du point de vue de la protection des données*. Au titre du règlement général sur la protection des données[23], le responsable du traitement est la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel, et assume la responsabilité du traitement des données à caractère personnel. La question du contrôle est complexe et de multiples facteurs entrent en jeu dans l'évaluation du responsable du traitement, notamment, mais sans s'y limiter, la question de savoir qui stocke les données et à quel endroit.

S'agissant de l'IRI, la plateforme de l'UE interconnecte uniquement les bases de données nationales décentralisées et toutes les données affichées dans la plateforme centrale ne sont que des «données transitoires», car elles n'y sont pas stockées, tout comme les journaux issus des requêtes envoyées par les utilisateurs au moyen du service web, qui sont enregistrés ou conservés au centre. La situation est quelque peu différente pour ce qui est du BRIS: ce service a innové avec une fonctionnalité particulière de stockage des principales données de profil des entreprises dans une base centrale à l'échelle de la Commission, que les registres nationaux continuent de mettre à jour régulièrement. La requête initiale est envoyée à cette base de données centrale, générant une liste de correspondances indiquant les noms des entités. Le demandeur peut obtenir des renseignements détaillés sur une entité

[23] 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) (JO L 119 du 4.5.2016).

en particulier en choisissant le nom de cette entité dans la liste de correspondances, ce qui génère une interconnexion directe avec les informations contenues dans la base de données nationale.

En ce qui concerne une possible interconnexion des mécanismes centralisés, il conviendrait de s'attacher à élaborer un système informatique où l'élément de routage central ne stocke aucune donnée à caractère personnel et où toutes les décisions sur les finalités et les moyens du traitement des données sont prises à l'échelon national. L'objectif du service d'interconnexion serait simplement de faciliter le traitement des données pour le compte des mécanismes centralisés, qui continueraient d'être les responsables du traitement de leurs ensembles de données respectifs.

3.5. Coûts d'établissement et de maintenance

La mise en place d'un système interconnectant les mécanismes centraux nationaux va générer des coûts d'établissement et de maintenance du système, que l'Union et ses États membres devraient se partager. S'agissant du partage des coûts dans les exemples de modèle, en règle générale, les coûts liés à la composante de l'UE (l'élément de routage centralisé, la plateforme européenne) ont été financés sur le budget général de l'Union, alors que les États membres ont assumé les coûts nécessaires à l'ajustement de leurs systèmes nationaux pour rendre ces derniers interopérables avec le système européen d'interconnexion. Pour ce qui est du BRIS, la mise au point de sa première version, qui a été mise en ligne en juin 2017 et comprenait la plateforme européenne centralisée, a requis environ 1,7 million d'EUR. Quant à l'IRI, dont l'architecture est plus simple, les coûts de développement du système pilote de recherche centralisée (IRI 1.0) étaient d'environ 280 000 EUR, mais l'adaptation de l'application de recherche centralisée en vue de l'établissement d'IRI 2.0 coûtera approximativement 170 000 EUR. En ce qui concerne l'ECRIS, le coût total du déploiement du logiciel «application de référence», qui sert à échanger les données concernant les casiers judiciaires entre États membres, a atteint 2 050 000 EUR. Le coût de maintenance annuel du système s'est élevé à 150 000 EUR. Concernant l'EUCARIS, une somme forfaitaire générale d'environ 20 000 EUR est demandée à chaque pays participant à des fins de maintenance.

Au regard des chiffres fournis ci-dessus, il semble que les coûts d'établissement et de maintenance d'un système d'interconnexion à l'échelle de l'Union sont relativement bas en comparaison avec les avantages qu'un tel projet apporte à l'Union. Les coûts pourraient être optimisés en réutilisant les capacités existantes (comme les points d'accès de la transmission électronique de documents, les éléments constitutifs du mécanisme pour l'interconnexion en Europe, les vocabulaires de base de la direction générale de l'informatique de la Commission européenne, etc.).

4. Spécifications techniques du système, notamment la sécurité des données

4.1. Réseau utilisé et sécurité des données

Le service Prüm de l'EUCARIS et l'ECRIS utilisent les services télématiques transeuropéens entre administrations (TESTA), qui consistent en un réseau privé complètement séparé du réseau internet public. Les points de contact nationaux désignés ont accès à ce réseau privé. Le service du réseau TESTA est opéré par la Commission et offre une performance garantie et un niveau de sécurité élevé. En ce qui concerne l'EUCARIS, son utilisation au moyen du réseau internet public est possible, mais actuellement indisponible. Il est connecté à toutes les institutions européennes et à tous les réseaux nationaux, et ce service est privilégié dans le contexte de la coopération des services répressifs, qui utilisent des informations sensibles. D'autres réseaux sécurisés ont également été mis au point par les

institutions européennes, comme le réseau commun de communications/interface commune des systèmes (CCN/CSI), qui est employé dans le domaine des politiques douanières et de la fiscalité.

Le BRIS, l'IRI, la LRI et l'EBOCS utilisent le réseau internet public (associé à une technique de cryptage appropriée pour les données consultables sur le web). En ce qui concerne l'échange sécurisé d'informations sur le réseau internet public, les éléments constitutifs de la transmission électronique de documents permet aux entreprises et aux administrations publiques d'échanger des données électroniques et des documents au format numérique d'une façon interopérable, sécurisée, fiable et en toute confiance avec d'autres organisations. Ces échanges suivent la définition des services d'envoi recommandé électronique inscrite à l'article 3, paragraphe 36, du règlement eIDAS[24].

Pour l'interconnexion possible des systèmes centralisés, qui incluent vraisemblablement des informations à caractère sensible, l'utilisation du réseau TESTA pourrait être envisagée. Néanmoins, des solutions employant le réseau internet public pourraient également être prises en considération. La quasi-totalité des systèmes centralisés nationaux utilisent le réseau internet public. Du point de vue de la sécurité et de l'intégrité des données, le fait que le système sera composé de bases de données décentralisées va atténuer les risques possibles, car la décentralisation et les technologies distribuées sont, en soi, plus résistantes aux cyberattaques puisqu'il est beaucoup plus difficile de corrompre des données de façon générale et beaucoup plus aisé de restaurer les données après un incident.

4.2. Élément de routage centralisé

Il existe deux types principaux d'architecture pour les systèmes informatiques: les systèmes purement décentralisés et ceux employant une plateforme ou un élément de routage centralisé déployé à l'échelle de l'Union, qui sert de «liant» entre les bases de données nationales décentralisées.

Les systèmes «purement distribués» ne comportent aucune plateforme ni aucun élément à l'échelle de l'Union, mais tous les pays communiquent directement entre eux, avec l'aide de normes admises d'un commun accord qui permettent des échanges directs entre pairs entre les points connectés des États membres. Dès lors, quand une requête est envoyée, elle est expédiée individuellement à chaque autre système national et les réponses reçues sont collectées et affichées sur l'interface web du demandeur. L'EUCARIS, l'ECRIS et e-CODEX appliquent cette technologie (qui repose sur une application élaborée conjointement).

Les «systèmes distribués comprenant un élément de routage centralisé» utilisent une plateforme centralisée à l'échelle de l'Union: un service web unique et centralisé, maintenu et exploité à l'échelle de l'Union, qui est connecté à tous les systèmes nationaux. Les utilisateurs lancent des requêtes sur le service web centralisé, qui collecte les informations demandées dans les bases de données nationales. Le BRIS, l'EBOCS et l'IRI utilisent cette technologie[25].

[24] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

[25] Des solutions de rechange à un élément centralisé existent. Par exemple, le Service Metadata Publisher (SMP) utilisé pour la transmission électronique de documents du MIE permet aux participants d'une infrastructure de messagerie de découvrir de façon dynamique les capacités (juridiques, organisationnelles et techniques) des uns et des autres. Du fait de cette architecture distribuée, chaque participant doit avoir un identifiant unique. Un élément centralisé, appelé Service Metadata Locator (SML), se sert de ces identifiants pour créer des URL qui, une fois traduits, dirigent les points d'accès de la transmission électronique de documents vers les informations spécifiques concernant le participant.

Une solution comprenant un élément de routage centralisé est peut-être plus facile à mettre en œuvre du point de vue de la connectivité. S'il existe une unique plateforme, chaque État membre ne doit créer et maintenir qu'une seule connexion entre le système national et cette plateforme centralisée. En l'absence de «véritable» plateforme centralisée, néanmoins, chaque État membre devra établir, tester et maintenir des connexions avec tous les autres systèmes nationaux des États membres (par exemple, le service Prüm de l'EUCARIS compte actuellement près de 756 connexions). Un système purement distribué est confronté à la difficulté d'un nombre bien plus élevé de connexions, ce qui peut accroître les problèmes de gestion, de contrôle et d'audit. Cependant, des solutions technologiques existent pour résoudre la difficulté de gérer un nombre important de connexions possibles. Dans le même temps, le fait que, dans un système de routage centralisé, l'élément central puisse devenir un point individuel de défaillance pour l'intégralité du système mérite que l'on y prête l'attention requise.

4.3. Protocole d'échange de données

Le BRIS et e-CODEX utilisent la solution de transmission électronique de documents du MIE alors que l'IRI 2.0 utilisera, en plus de cette solution de transmission, le protocole de communication SOAP[26]. Le service Prüm de l'EUCARIS et l'EBOCS utilisent des interfaces fondées sur SOAP. La LRI applique le service web RESTful[27].

L'élément constitutif de la transmission électronique de documents du MIE aide les utilisateurs à échanger des données électroniques entre eux de façon sécurisée, fiable et en toute confiance. La solution de la transmission électronique de documents du MIE est fondée sur un modèle distribué appelé «modèle à 4 coins» où les systèmes dorsaux des utilisateurs n'échangent pas directement de données entre eux, mais via les points d'accès. Ces points d'accès sont conformes aux mêmes spécifications techniques et, partant, capables de communiquer entre eux. Un autre avantage de la transmission électronique de documents est qu'elle assure la sécurité des données échangées entre les différents points d'accès, sans nécessiter de développement sur mesure. En conséquence, les utilisateurs qui adoptent la transmission électronique de documents du MIE peuvent échanger des données facilement et en toute sécurité même si leurs systèmes informatiques ont été développés indépendamment les uns des autres. Autrement, les multiples fonctionnalités du modèle de transmission électronique de documents – qui s'avère très utile, car il peut servir d'interface lorsque plusieurs systèmes dorsaux sont utilisés – peuvent être centralisées. En utilisant cette solution technologique, les États membres (et, éventuellement, la Commission au cas où un élément de routage centralisé serait utilisé) devraient déployer un portail de transmission électronique de documents à leur échelle respective. Ils peuvent réutiliser leurs portails existants qui avaient été élaborés aux fins d'autres services (ce qui contribue à la rentabilité de la solution). Une solution logicielle compatible élaborée par la direction générale de l'informatique de la Commission européenne existe, proposée gratuitement dans le cadre d'une licence publique de l'Union européenne (EUPL). Toutefois, une certaine personnalisation et une part de développement sont généralement nécessaires. Le modèle de transmission électronique de documents permet une communication asynchrone, qui génère implicitement certaines latences de performance (de généralement 3 à 10 secondes). Il existe une politique européenne générale concernant les éléments constitutifs du MIE qui vise la convergence des divers systèmes élaborés au titre des différents domaines politiques de l'Union.

Quand un protocole SOAP synchrone – permettant la communication sur une couche sécurisée – est utilisé, la plupart du temps, une architecture plus simple est choisie, afin d'optimiser la performance.

[26] Simple Object Access Protocol.

[27] Representational State Transfer est un style d'architecture pour les logiciels qui définit un ensemble de contraintes à utiliser pour la création de services web.

Le style architectural RESTful représente une solution plus récente en comparaison avec le protocole SOAP, de plus, une nouvelle tendance se dégage, où SOAP est supplanté par la technologie REST. Tant lors de la transmission électronique de documents qu'avec les approches fondées sur SOAP ou REST, la confiance est généralement fondée sur un certificat numérique et plusieurs contrôles sont réalisés.

En ce qui concerne l'interconnexion future des mécanismes centralisés, il est noté que la transmission électronique de documents du MIE est utilisée quand des échanges bilatéraux entre les bases de données nationales décentralisées ont lieu, alors que dans les systèmes où la communication s'effectue uniquement à l'égard d'une base de données nationale et de la plateforme centralisée, l'interface fondée sur SOAP (ou RESTful) suffit.

4.4. Travailler dans un environnement multilingue et interopérabilité sémantique

Tous les systèmes évalués fonctionnent dans un environnement multilingue, à l'exception de l'EBOCS qui fonctionne actuellement dans trois langues, mais prévoit à long terme de fonctionner dans toutes les langues. Dans le BRIS, la translittération est menée à l'échelon de l'Union, alors que dans l'IRI, la LRI et l'EUCARIS, elle l'est à l'échelon national. En ce qui concerne l'interopérabilité sémantique (glossaires), une interconnexion future des mécanismes centralisés ne requiert pas de vocabulaire spécifique, car l'ensemble minimal d'informations ne concerne pas des concepts nationaux, mais des données à caractère personnel, comme le nom, l'identifiant unique (par exemple, le numéro d'identification national) et le numéro IBAN. Une interprétation commune dans tous les systèmes nationaux est essentielle, en particulier parce que les mécanismes nationaux centralisés ne contiennent pas d'informations sur les entités de l'Union ou de pays tiers. Les règles de translittération du système d'information Schengen pourraient s'avérer un exemple utile dans ce contexte.

D'après le cadre d'interopérabilité européen, l'aspect sémantique fait référence à la signification des éléments de données et aux relations entre eux. Il inclut la création de vocabulaires et de schémas pour décrire les échanges de données et garantit que les éléments de données sont interprétés de la même façon par toutes les parties communicantes.

Le système utilisé pour interconnecter les registres bancaires devra échanger des données entre différentes bases de données, chacune ayant ses propres modèles de données et normes sémantiques. Des normes sémantiques communes devront être établies, soit de façon native dans les systèmes ou en tant que couche de définition entre les différentes normes dans les États membres. Toutefois, avant de créer une nouvelle norme sémantique, la réutilisation de normes existantes doit être envisagée.

Les vocabulaires de base (pour les entreprises, l'emplacement, les personnes, etc.) créés par le programme ISA2 sont des modèles de données simplifiés, réutilisables et extensibles qui peuvent être utilisés à cette fin. Les différentes solutions pour les interconnexions des registres de base, à l'instar du BRIS, réutilisent déjà une partie de ces normes (par exemple, le vocabulaire de base pour les entreprises).

5. Les prochaines étapes

Le présent rapport établit un ensemble d'éléments qu'il convient de prendre en compte pour pouvoir interconnecter les registres et les systèmes de recherche de données concernant les comptes bancaires, et illustre le fait que l'interconnexion de ces mécanismes centralisés est techniquement possible. Un tel système pourrait être un système décentralisé sur une plateforme commune à l'échelle de l'Union.

La technologie déjà développée par la Commission européenne dans le contexte des différents modèles analysés pourrait être employée.

Ces dernières années, différents systèmes ont suivi la réutilisation des éléments constitutifs communs. Ces éléments constitutifs sont par essence un ensemble de normes et de spécifications techniques bien connus qui peuvent être appliquées aux difficultés récurrentes telles que l'échange sécurisé d'informations. Le recours constant à ces éléments constitutifs est une approche prônée par la politique numérique actuelle de la Commission, envers laquelle les États membres se sont engagés dans la déclaration de Tallinn sur l'administration en ligne[28]. Une interconnexion future des mécanismes automatisés centralisés nationaux pourrait tirer parti de l'utilisation des mêmes éléments constitutifs pour accélérer sa création et son alignement avec les règlements européens pertinents tels que le règlement eIDAS.

Étant donné qu'une future interconnexion à l'échelle de l'Union des mécanismes centralisés accélérerait l'accès aux informations financières et faciliterait la coopération transfrontalière des autorités compétentes, la Commission prévoit de consulter également les parties prenantes pertinentes, les pouvoirs publics, ainsi que les cellules de renseignement financier, les autorités répressives et les bureaux nationaux de recouvrement, car ils pourraient être les «utilisateurs finaux» d'un possible système d'interconnexion.

[28] Tous les États membres de l'Union européenne et les pays de l'AELE ont signé la déclaration de Tallinn sur l'administration en ligne le 6 octobre 2017. Le texte de la déclaration est consultable à l'adresse http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.