

DIRECTION GÉNÉRALE DES POLITIQUES INTERNES
DÉPARTEMENT THÉMATIQUE DES DROITS DES CITOYENS ET DES AFFAIRES
CONSTITUTIONNELLES

LIBERTÉS CIVILES, JUSTICE ET AFFAIRES INTÉRIEURES

Interopérabilité des systèmes d'information européens dans le domaine de la justice et des affaires intérieures

ÉTUDE

demandée par la commission LIBE

SYNTHÈSE

Résumé

La présente étude a été commandée par le département thématique des droits des citoyens et des affaires constitutionnelles du Parlement européen à la demande de la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE) du Parlement européen. Elle examine essentiellement les propositions de règlement portant établissement d'un cadre pour l'interopérabilité des systèmes d'information dans le domaine de la justice et des affaires intérieures, présentées par la Commission en décembre 2017. L'étude analyse tout d'abord la relation entre les systèmes d'information existants et proposés, puis examine les principaux éléments des propositions de la Commission, y compris le concept d'interopérabilité utilisé, la définition des problèmes, les objectifs et les propositions de solutions, ainsi que les conséquences sur le plan de la mise en œuvre, des droits fondamentaux et de la protection des données.

À PROPOS DE LA PUBLICATION

Cette étude a été demandée par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen et commandée, contrôlée et publiée par le département thématique des droits des citoyens et des affaires constitutionnelles.

Les départements thématiques fournissent des expertises indépendantes, internes ou externes, dans le but d'aider les commissions du Parlement européen et les autres organes parlementaires à concevoir la législation et à exercer le contrôle démocratique des politiques externes et internes de l'Union.

Pour contacter le département thématique des droits des citoyens et des affaires constitutionnelles ou pour vous abonner à sa lettre d'information, veuillez écrire à l'adresse suivante:

poldep-citizens@ep.europa.eu

Administrateur de recherche responsable

Udo BUX

Département thématique des droits des citoyens et des affaires constitutionnelles

Parlement européen

B-1047 Bruxelles

Adresse électronique: poldep-citizens@ep.europa.eu

Assistante de rédaction

Monika Laura LAZARUK

AUTEURS

Mirja GUTHEIL, Optimity Advisors

Quentin LIGER, Optimity Advisors

James EAGER, Optimity Advisors

Yemi OVIOSU, Optimity Advisors

Daniel BOGDANOVIC, Optimity Advisors

Avec le soutien de la professeure Katrin NYMAN-METCALF de l'Académie pour l'e-gouvernance en Estonie et de l'Université de technologie de Tallinn; Niovi VAVOULA, Université Queen Mary de Londres; Jeremy COLLINS, Optimity Advisors; et Carolin Möller, Optimity Advisors.

VERSIONS LINGUISTIQUES

Original: FR

Rédaction achevée en avril 2018

© Union européenne, 2018

Ce document est disponible sur l'internet à l'adresse suivante:

<http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html>

CLAUSE DE NON-RESPONSABILITÉ

Les opinions exprimées dans le présent document sont celles des auteurs et ne reflètent pas nécessairement la position officielle du Parlement européen.

Reproduction et traduction autorisées, sauf à des fins commerciales, moyennant mention de la source, information préalable de l'éditeur et transmission d'un exemplaire à celui-ci.

SYNTHÈSE

Interopérabilité des systèmes d'information de l'Union dans le domaine de la justice et des affaires intérieures: historique et contexte

Les débats sur l'interopérabilité des systèmes d'information de l'Union dans le domaine de la justice et des affaires intérieures¹ ont commencé au lendemain des attentats du 11 septembre² et se sont poursuivis dans les années 2000. Tout d'abord suscités par les attentats terroristes perpétrés sur le territoire de l'Union (les attentats à la bombe de 2004 à Madrid et de 2005 à Londres), ces débats ont donné lieu à la communication de la Commission de 2005 sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases³. Des critiques formulées par des acteurs de premier plan, comme le Contrôleur européen de la protection des données (CEPD), ont toutefois empêché la poursuite de ces débats. Ces critiques visaient principalement deux éléments: la **définition** de l'interopérabilité et les conséquences possibles sur la **protection des données à caractère personnel**⁴.

Au cours de la décennie suivante, peu de mesures ont porté l'interopérabilité bien que l'environnement des systèmes d'information de l'Union dans le domaine de la justice et des affaires intérieures ait largement évolué, notamment par la création du système d'information sur les visas (VIS)⁵, du système d'information Schengen de deuxième génération (SIS II)⁶ et du système européen d'information sur les casiers judiciaires (ECRIS)⁷.

À la suite des nouveaux attentats terroristes perpétrés sur le sol de l'Union (à Paris en 2015 et à Bruxelles en mars 2016), les discussions sur l'interopérabilité ont repris de plus belle. Par conséquent, de 2015 à 2017, la pression politique s'est accrue en vue d'une mise en œuvre plus rapide de l'interopérabilité des systèmes d'information dans le domaine de la justice et des affaires intérieures, notamment par la publication de multiples conclusions du Conseil⁸, d'une feuille de route du Conseil⁹, et d'une déclaration commune des ministres européens de la justice et des affaires intérieures en 2016¹⁰.

En se fondant sur ces documents et sur les appels du Conseil, la Commission a publié en 2016 sa communication sur des systèmes d'informations plus robustes et plus intelligents au service des frontières et de la sécurité¹¹, qui présente «quatre dimensions»¹² de l'interopérabilité et crée un groupe d'experts à haut niveau sur les systèmes d'information et l'interopérabilité chargé de se pencher sur les aspects juridiques, techniques et opérationnels de ces quatre dimensions. En

¹ En raison de son emploi fréquent dans les propositions de la Commission, le terme «justice et affaires intérieures» (JAI) remplace celui d'«espace de liberté, de sécurité et de justice» (ELSJ).

² Conseil de l'Union européenne, document n° 13176/01 du 24.10.2001.

³ COM(2005) 597 final du 24.11.2005.

⁴ Observations du CEPD de 2006 relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes.

⁵ Décision 2004/512/CE du Conseil.

⁶ Règlement (CE) n° 1987/2006 (coopération dans le domaine du contrôle aux frontières); décision 2007/533/JAI du Conseil (coopération des services répressifs); règlement (CE) n° 1986/2006 (coopération dans le domaine de l'immatriculation des véhicules).

⁷ Décision-cadre 2009/315/JAI du Conseil; et décision 2009/316/JAI du Conseil.

⁸ Conseil de l'Union européenne, document EUCO 28/15 du 18.12.2015; Conseil de l'Union européenne, document EUCO 34/16 du 15.12.2016.

⁹ Conseil de l'Union européenne, document n° 9368/1/16 du 6.6.2016.

¹⁰ Conseil de l'Union européenne, document n° 158/16 du 24.3.2016.

¹¹ COM(2016) 205 final du 6.4.2016.

¹² Ibid, p. 14.

juin 2017, à la suite du rapport final du groupe d'experts à haut niveau, la **Commission a annoncé son intention de présenter une proposition législative relative à l'interopérabilité**¹³.

Le 12 décembre 2017, la Commission européenne a publié ses propositions de règlement portant établissement d'un cadre pour l'interopérabilité entre les systèmes d'information de l'Union¹⁴. Distinctes mais très étroitement liées, les deux propositions législatives visent à mettre en œuvre quatre solutions principales.

- Le **portail de recherche européen (ESP)** permettrait d'interroger simultanément de multiples systèmes d'information dans le domaine de la justice et des affaires intérieures (le SIS central, Eurodac, le VIS, le futur EES et les systèmes ETIAS et ECRIS-TCN proposés, ainsi que les systèmes d'Interpol pertinents et les données Europol) à l'aide de données d'identité (biographiques et biométriques) (chapitre II).
- Le **service partagé de mise en correspondance de données biométriques (BMS partagé)** permettrait d'interroger et de comparer des données biométriques (empreintes digitales et images faciales) contenues dans plusieurs systèmes d'information de l'Union en créant et en stockant des représentations mathématiques des données biométriques (le SIS, Eurodac, le VIS, le futur EES et les systèmes ETIAS et ECRIS-TCN proposés) (chapitre III).
- Le **répertoire commun de données d'identité (CIR)** serait un élément partagé pour le stockage des données d'identité biographiques et biométriques des ressortissants de pays tiers, englobant Eurodac, le VIS, le futur EES ainsi que les systèmes ETIAS et ECRIS-TCN proposés (chapitre IV).
- Le **détecteur d'identités multiples (MID)** permettrait de vérifier si les données d'identité recherchées existent dans plus d'un système et de mettre en place un mécanisme permettant de rechercher et de vérifier les données d'identité liées (contenues dans le CIR ainsi que dans le SIS) (chapitre V).

Les propositions de règlements visent également à mettre en œuvre:

- **une approche en deux étapes de l'accès des services répressifs aux systèmes d'information à finalité non répressive** aux fins de la prévention et de la détection du terrorisme et d'autres infractions pénales graves, ou d'enquêtes et de poursuites en la matière (article 22):
 - la «fonctionnalité d'indicateur de concordance» du CIR permettrait aux services répressifs de déterminer quels systèmes d'information contiennent des données enregistrées sur une personne, sans que soient révélées des données sous-jacentes.
 - Les autorités répressives auraient dès lors la possibilité d'émettre des demandes individuelles d'accès à chaque système contenant des données, dans le respect des règles et des procédures fixées par les règlements relatifs à chaque système d'information.
- **Le répertoire central des rapports et statistiques (CRRS):** ce répertoire permettrait de créer et d'échanger des rapports contenant des données statistiques anonymisées issues de plusieurs systèmes d'information aux fins des politiques menées, des exigences opérationnelles et de la qualité des données (article 39).

¹³ COM(2017) 261 final du 16.5.2017.

¹⁴ Propositions de règlement portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union: COM(2017) 794 final, Bruxelles, 12.12.2017 et COM(2017) 793 final, Strasbourg, 12.12.2017.

- **Le format universel pour les messages (UMF):** il s'agirait d'un langage technique normalisé permettant de décrire et de relier des éléments de données, facilitant ainsi l'intégration et l'interopérabilité des systèmes d'information de l'Union et des États membres (article 38).

Les propositions introduisent également le concept de **mécanismes automatisés de contrôle de la qualité des données** (article 37). Ces mécanismes comprennent l'application de règles de validation automatique lors de la saisie de données et la mise en place d'indicateurs communs de qualité des données et de normes de qualité minimales. Si l'article 37 prévoit leur création et détaille leurs fonctions et responsabilités associées, le contenu de ces mécanismes reste encore à définir.

Systèmes d'information existants et proposés dans le domaine de la justice et des affaires intérieures

En ce qui concerne la mise en œuvre actuelle, il est essentiel de souligner que **chacun des systèmes d'information dans le domaine de la justice et des affaires intérieures a été créé (ou proposé) à des fins spécifiques** dans un cadre institutionnel déterminé. Bien que les objectifs principaux de chaque système restent distincts, ils présentent clairement des caractéristiques communes concernant:

- i. **l'élargissement du champ d'application des systèmes au fil du temps.** À titre d'exemple, les finalités d'Eurodac ont été élargies au domaine des migrations et de l'application des lois
- ii. avec un **chevauchement croissant des objectifs accessoires des systèmes**, essentiellement dans le domaine de l'accès des services répressifs. À titre d'exemple, l'identification des «ressortissants de pays tiers en séjour irrégulier» est désormais commune à Eurodac, au SIS II, au VIS et à l'EES.

Les ajouts de fonctions et d'objectifs aux différents systèmes d'information sont susceptibles de **rendre plus floues les limites entre le contrôle à l'immigration et la sécurité intérieure.**

Pour ce qui est des **données collectées par chaque système, elles concernent principalement, sans toutefois s'y limiter, les ressortissants de pays tiers.** Cette situation peut avoir des conséquences sur les propositions en matière d'interopérabilité, dès lors que certaines solutions s'adressent uniquement aux ressortissants de pays tiers mais utilisent des bases de données englobant les ressortissants de l'Union. Par ailleurs, il existe un **chevauchement important des systèmes s'agissant des données d'identité biographiques et biométriques collectées.** Outre les données d'identité, ce chevauchement vaut également pour les données collectées par le VIS et l'EES, et par l'EES et l'ETIAS. Les données de nombreux voyageurs étant susceptibles d'être enregistrées dans l'EES et dans au moins un autre de ces systèmes d'information, l'interopérabilité entre ces systèmes a été intégrée aux propositions législatives les concernant.

En ce qui concerne les difficultés que rencontrent les systèmes existants, se posent **plusieurs problèmes transversaux** dont les plus importants sont les suivants:

- la fragmentation de l'architecture des données de l'Union,
- l'efficacité de la gestion des risques et de la protection des données des personnes concernées,
- la piètre qualité des données et
- des usages très variables selon les États membres.

Propositions relatives à l'interopérabilité: définition de l'interopérabilité

Le **concept d'interopérabilité est considéré comme positif par la grande majorité des parties prenantes, pour peu qu'il soit correctement appliqué.** La mise en relation de systèmes d'information distincts dans le but d'améliorer l'efficacité des opérations pour les utilisateurs finaux ainsi que la stricte réglementation des droits d'accès et le plein respect de la protection des données à caractère personnel sont des initiatives qui peuvent présenter de nombreux avantages. En revanche, l'interopérabilité n'a pas vocation à instaurer de nouveaux modes de stockage, un nouveau traitement des données à caractère personnel outrepassant les finalités de chaque système ou de nouveaux droits d'accès.

Toutefois, dans les propositions législatives de la Commission portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union, **la définition associée au concept d'interopérabilité n'est pas explicitement formulée ni suffisamment développée, point sur lequel le CEPD a lourdement insisté.** La définition s'inspire manifestement au domaine de l'administration en ligne, mais elle devrait dans la pratique être bien plus claire quant à la manière dont le concept d'interopérabilité (en particulier, les notions d'interopérabilité juridique, sémantique, opérationnelle et technique) a été appliqué à la création et à la conception des solutions.

Par conséquent, la **plus grande difficulté découlant des propositions est qu'en réalité, elles n'instaurent pas de cadre pour l'interopérabilité, mais proposent plutôt des solutions techniques, dont certaines seulement sont compatibles avec le concept d'interopérabilité.** En outre, l'interprétation de l'interopérabilité semble être fondée sur des solutions clé sur porte, et non sur des solutions élaborées sur la base d'une compréhension claire, transparente et commune de l'interopérabilité. Cependant, il est nécessaire de proposer une définition claire de l'interopérabilité, y compris ses limites extérieures, sans quoi il pourrait s'agir d'un concept flou assorti d'un objectif incertain.

Par ailleurs, les propositions gagneraient à être plus claires et transparentes sur les questions transversales suivantes:

- **l'utilisation d'une terminologie péremptoire** affirmant constamment la nécessité des propositions sans les étayer de suffisamment de preuves.
- **le recours limité à la consultation**, en particulier en ce qui concerne les conséquences des propositions en matière de protection des données et de droits fondamentaux.

Définition du problème et besoins

D'une part, la définition du problème montre que la situation actuelle se heurte aux deux principaux écueils suivants:

- i. les informations sur les bases de données existantes ne sont pas toujours complètes, précises et fiables,
- ii. et les utilisateurs finaux ne disposent pas toujours d'un accès rapide et systématique à toutes les informations nécessaires pour s'acquitter de leurs tâches. Dans certains cas, les droits d'accès existants aux différents systèmes dans le respect des

instruments juridiques de l'Union ne sont pas pleinement exercés en raison d'un «manque de moyens techniques et pratiques à l'échelle nationale»¹⁵.

Il est évident que l'interopérabilité peut répondre au second problème, mais il est nécessaire de préciser comment ce concept permettrait de disposer de données plus exhaustives, plus précises et plus fiables. Les mesures proposées en vue d'améliorer la qualité des données et le fonctionnement du CIR, du BMS partagé et du MID pourraient apporter un début de réponse au premier problème, mais elles mettent en place de nouveaux droits et modes d'accès ainsi qu'un nouveau traitement des données à caractère personnel.

D'autre part, la définition met en lumière deux aspects principaux du problème. Les **différences entre ces aspects ne sont pas expliquées clairement, et ils laissent entendre que les lacunes en matière d'interopérabilité aggravent les problèmes en question**. En réalité, ce sont les personnes chargées de saisir les données qui déterminent pour chaque système si les données sont exhaustives, précises et fiables.

En outre, les différents systèmes d'information ont été volontairement élaborés séparément, en fonction des objectifs spécifiques à chaque système et conformément au principe de limitation des finalités en matière de protection des données¹⁶. Par ailleurs, les besoins formulés dans les propositions sont rarement étayés par des preuves.

Objectifs

Les **propositions fixent plusieurs ensembles d'objectifs, dont les liens ne sont pas clairement expliqués**. L'exposé des motifs présente les objectifs généraux, les objectifs fondés sur le traité ainsi que les objectifs spécifiques, et l'article 2 du texte législatif présente les autres objectifs.

En outre, les objectifs généraux énoncés dans l'exposé des motifs associent les objectifs en matière de migration et de sécurité intérieure. Comme le CEPD l'a souligné précédemment, cette situation peut donner lieu à une **confusion entre la gestion des migrations et celle de la sécurité intérieure, rendre plus floues les limites entre les deux domaines d'action**, les termes relatifs aux systèmes d'information dans le domaine de la justice et des affaires intérieures devenant presque interchangeables. Par ailleurs, il convient de préciser que, pour la plupart des systèmes d'information concernés par les propositions (ce qui n'est pas le cas du SIS II ou de l'ECRIS-TCN), les objectifs relatifs à la sécurité sont également accessoires.

Dans l'exposé des motifs à l'appui des propositions, quatre objectifs spécifiques sont également définis. Ces **objectifs dotent l'environnement actuel des systèmes d'information dans le domaine de la justice et des affaires intérieures de nouvelles finalités significatives**. La détection des identités multiples et les contrôles d'identité plus aisés des ressortissants de pays tiers sur le territoire d'un État membre, par exemple, constituent deux nouveaux objectifs importants des systèmes d'information existants et prévus dans le domaine de la justice et des affaires intérieures. De plus, deux de ces nouveaux objectifs mettent nettement l'accent sur la sécurité et présentent une pertinence limitée à l'égard des objectifs des systèmes d'information existants et prévus en la matière.

¹⁵ Analyse d'impact accompagnant la proposition de règlement portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union, p. 9.

¹⁶ Article 5, paragraphe 1, du règlement général sur la protection des données (RGPD).

Les objectifs du texte législatif sont présentés dans l'article 2 des propositions. Le paragraphe 1 énumère simplement les objectifs généraux des systèmes d'information existants et prévus, et met ainsi **sur un pied d'égalité les différents systèmes et leurs objectifs**.

Finalités et conception des solutions

Le **portail de recherche européen (ESP) est une innovation susceptible de présenter d'excellents résultats et d'améliorer vraisemblablement l'efficacité opérationnelle**. Par ailleurs, aucune agrégation significative des données n'est possible et aucun système d'information supplémentaire n'est développé. En tant que tel, l'ESP contribuera à atteindre le premier objectif spécifique (c'est-à-dire, fournir aux autorités un accès rapide, continu, systématique et contrôlé) et pourrait être mis en œuvre sans incidence sur la protection des données. En revanche, la protection des données à caractère personnel pourrait s'avérer problématique lors de l'élaboration des actes délégués relatifs aux profils d'utilisateurs et à la maintenance des droits d'accès existants. Il convient d'élaborer ces actes en tenant mieux compte de la protection des données.

Enfin, il est nécessaire de préciser dans quelle mesure les propriétaires des données d'Interpol seront avertis des recherches concernant leurs données. Rien ne permet par exemple d'affirmer que le propriétaire des données d'Interpol sera averti du déroulement d'une recherche.

Le **service partagé de mise en correspondance de données biométriques (BMS partagé)** contribuera vraisemblablement à atteindre les objectifs qu'il vise grâce au stockage et à l'utilisation de représentations mathématiques de données biométriques, dans le but de soutenir l'ESP, le CIR et le MID. Toutefois, le BMS partagé est une nouvelle base de données et ne répond dès lors pas à une définition adéquate de l'interopérabilité. Il est par ailleurs nécessaire de préciser si les représentations mathématiques (c'est-à-dire, les modèles biométriques) stockées par le BMS partagé constituent des données à caractère personnel.

Cependant, qu'elles le soient ou non, il est évident que le BMS partagé peut apporter une valeur ajoutée à l'identification des identités multiples dans les différents systèmes d'information. Sachant que les possibilités examinées dans l'analyse d'impact sont limitées, il n'est cependant pas certain que le BMS partagé aura la même valeur sans les autres éléments d'interopérabilité. **Il permettra toutefois de détecter des identités multiples dans l'ensemble des systèmes, sauf l'ETIAS, à condition que la détection se fonde sur la comparaison et la consultation de données biométriques**. Au vu des conséquences de la mise en œuvre du CIR et du MID, il s'agit d'une autre possibilité éventuelle de mise en œuvre.

Le **répertoire commun de données d'identité (CIR)** contribuera vraisemblablement à réaliser sa finalité et les objectifs associés. Il facilitera grandement, en particulier, l'identification des ressortissants de pays tiers présents sur le territoire de l'Union, permettra un meilleur fonctionnement du MID en matière de détection et de vérification des identités multiples dans les différents systèmes, et simplifiera l'accès des services répressifs aux bases de données à finalité non répressive. Toutefois, la mise en place du CIR constitue la dimension la plus invasive de l'interopérabilité (telle que conçue par la Commission) et soulève des inquiétudes en matière de respect de la vie privée et de protection des données à plusieurs égards.

Tout d'abord, dans le **texte relatif à son architecture, il n'est pas clairement précisé s'il s'agira d'une base de donnée séparée**. De plus, les propositions disposent explicitement que le CIR n'est pas une nouvelle base de données, tout en la qualifiant de «répertoire» et en utilisant des termes

comme «stocké» et «stockage»¹⁷. Le texte législatif accentue cette confusion en présentant le CIR sous le même jour que les systèmes d'information actuels et prévus (voir, par exemple, les articles 9, 11 et 14). Au vu de ce qui précède, le **CIR ne semble pas être une solution d'interopérabilité et, si c'est le cas, il devrait être déclaré et traité comme tel.**

En outre, le **CIR fera office de base de données** pour faciliter les contrôles, par les services répressifs, de l'identité des ressortissants de pays tiers sur le territoire. Cette opération s'apparente en elle-même à la création d'une nouvelle base de données qui confère de nouveaux droits d'accès aux données à caractère personnel collectées par les différents systèmes d'information, met sur un pied d'égalité tous les ressortissants de pays tiers quels qu'ils soient et modifie fondamentalement la principale finalité des données à caractère personnel collectées par l'ensemble des systèmes. De plus, ce changement de finalité est lié aux objectifs accessoires des systèmes, et remet d'autant plus en question sa proportionnalité. Enfin, les propositions ne précisent et ne démontrent pas de manière suffisante les difficultés et les problèmes actuels qui rendraient cette nouvelle finalité nécessaire.

Les mécanismes existants en matière d'accès des services répressifs au VIS ont fait l'objet de critiques. Il a été conclu dans les arrêts *Digital Rights Ireland* et *Watson* que des autorités indépendantes ou judiciaires devraient être responsables de la vérification des conditions d'accès au VIS, plutôt que des points d'accès centraux ou des autorités de vérification, lesquels peuvent faire partie de la même organisation à laquelle l'accès au VIS est accordé. Compte tenu de ce qui précède, il ressort clairement que l'approche en deux étapes présentée dans les propositions relatives à l'interopérabilité assouplit encore ces conditions, ce qui pose les difficultés exposées ci-après.

- Une recherche pourra être effectuée par les services répressifs sans aucune autorisation, l'absence d'une donnée dans l'ensemble des systèmes d'information (c'est-à-dire, l'absence d'indicateur sur une identité) constituant un résultat.
- Les informations fournies par la fonctionnalité d'indicateur de concordance (c'est-à-dire, la base de données dans laquelle une personne est enregistrée) le sont en violation des conditions d'accès actuelles, donnent aux services répressifs un accès à de nouvelles informations, et mettent sur un pied d'égalité tous les ressortissants de pays tiers dans l'ensemble des différents systèmes.

En tant que tel, le **CIR introduit les modifications les plus profondes par rapport à la mise en œuvre actuelle** et représente en l'occurrence la plus grande menace pour la protection des données à caractère personnel et le droit au respect de la vie privée.

Le **détecteur d'identités multiples (MID)** aidera vraisemblablement à réaliser les finalités et les objectifs prévus. Ce système ne constitue toutefois pas une solution d'interopérabilité conforme à une définition appropriée de l'interopérabilité. Il crée en effet de nouvelles données sous la forme de liens et de dossiers de confirmation d'identité, et confère de nouveaux droits d'accès aux personnes qui trouvent un lien jaune.

De plus, la finalité du MID relative à la lutte contre la fraude à l'identité n'est pas étayée par la base légale d'Eurodac. L'inclusion de données d'Eurodac nécessiterait de modifier à nouveau la finalité du système d'information.

Les autres éléments avancés dans les propositions ne constituent pas non plus des solutions d'interopérabilité. Toutefois, la mise en œuvre cohérente du format universel pour les messages

¹⁷ Proposition de règlement portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union, 2017/0352 (COD) et 2017/0351 (COD), p. 7, paragraphe 3.

(UMF) ainsi que l'élaboration d'un répertoire central des rapports et statistiques (CRRS) représentent des initiatives valables et avantageuses sans pour autant engendrer de nouveaux effets.