Avis du Comité économique et social européen sur

la «Proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union européenne (frontières et visas) et modifiant la décision 2004/512/CE du Conseil, le règlement (CE) n° 767/2008, la décision 2008/633/JAI du Conseil, le règlement (UE) 2016/399 et le règlement (UE) 2017/2226»

[COM(2017) 793 final — 2017/0351 (COD)]

et la «Proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'Union européenne (coopération policière et judiciaire, asile et migration)»

[COM(2017) 794 final — 2017/0352 (COD)]

(2018/C 283/07)

Rapporteure: **Laure BATUT**

Consultation	Commission européenne, 18.1.2018
	Parlement européen, 28.2.2018
Base juridique	Article 304 du traité sur le fonctionnement de l'Union européenne
Compétence	Section spécialisée «Emploi, affaires sociales et citoyenneté»
Adoption en section spécialisée	25.4.2018
Adoption en session plénière	23.5.2018
Session plénière n°	535
Résultat du vote	160/3/2
(pour/contre/abstentions)	

1. **Conclusions et recommandations**

1.1. Le Comité économique et social européen (CESE) estime utile et positive la proposition de la Commission européenne visant à améliorer l'interopérabilité des systèmes d'information de l'Union européenne sur les frontières et les visas ainsi que la coopération policière, judiciaire, l'asile et la migration.

1.2. Le CESE considère que cette interopérabilité doit être un objectif stratégique de l'Union européenne pour qu'elle reste un espace ouvert, garant des droits fondamentaux et de la mobilité. L'Union européenne et les États membres ont l'obligation de protéger la vie et la sécurité de tous les êtres humains; le principe de non-refoulement devrait être pleinement respecté.

1.3. Les mesures visant l'interopérabilité seront d'autant mieux comprises qu'elles:

— garantissent, dans le cadre de la stratégie migratoire de l'Union européenne, les conditions de l'équilibre entre liberté et sécurité, dans le respect de la séparation des pouvoirs;

— garantiront aux personnes concernées leurs droits fondamentaux, en particulier la sécurisation de leurs données personnelles et de leur vie privée, le droit d'accès à leurs données, à leur rectification et à leur effacement dans un délai raisonnable, par des procédures accessibles;

— réaffirment, y compris dans tous les textes d'exécution, l'exigence de l'intégration des principes de protection des données dès la phase de conception («privacy by design»);

— ne créent pas de nouveaux obstacles aux trafics normaux de passagers et de marchandises.

1.4. Le CESE demande des procédures et des garanties en ce qui concerne l'utilisation des données à des fins répressives qui:

— prévoient d'appliquer en la matière la loi européenne la plus protectrice (RGPD);

— permettent d'accélérer la détermination de l'État membre responsable de l'examen des demandes de protection internationale;

— garantissent aux personnes concernées leur droit à deux degrés de juridiction;

— garantissent aux personnes mineures, en particulier non accompagnées, qu'elles soient en situation irrégulière, de persécution ou en situation criminelle, le droit d'obtenir un visa, d'être protégées et intégrées et de bénéficier du droit à l'oubli dans un délai plus court que pour les majeurs.

1.5. Le CESE estime que la base juridique actuelle des systèmes d'information devrait être renforcée et prendre en compte l'évolutivité des systèmes de collecte des données. Il préconise:

— le renforcement de la sécurité des bases de données existantes et celle de leurs canaux de communication;

— l'évaluation de l'impact du renforcement du contrôle a priori sur la gestion des risques;

— un contrôle et une évaluation permanente de l'architecture par les autorités de la protection des données (CEPD); il exige des responsables qu'ils fassent rapport chaque année aux autorités décisionnelles et à la Commission concernant la sécurité des éléments d'interopérabilité, ainsi que tous les deux ans sur l'impact des mesures sur les droits fondamentaux.

1.6. Le CESE estime que le projet doit s'appuyer sur un personnel compétent et préconise:

— de solides programmes de formation pour les autorités concernées et les agents d'eu-LISA;

— un contrôle strict des compétences des agents et candidats pour cette agence.

1.7. Le CESE exprime son inquiétude concernant le financement du nouveau système. Le suivi de la planification sera crucial pour éviter le dérapage des budgets et mener le projet à son terme, jusqu'en 2029.

1.8. Le CESE recommande que les citoyens soient informés de ses avancées jusqu'à l'achèvement du projet, et que les personnes reçoivent une information pédagogique sur les contrôles auxquels elles sont soumises. Il estime que doit être prévue la possibilité de tout arrêter si la liberté et les droits fondamentaux venaient à être menacés par un fonctionnement abusif du système.

2. **Introduction**

2.1. Dans le contexte international de 2017 considéré comme instable, tant sur le plan géopolitique que sur celui de la sécurité intérieure des États membres, le Conseil a demandé à plusieurs reprises à la Commission de mettre en œuvre les moyens de retrouver les traces des personnes jugées «à risque» ayant déjà fait l'objet d'un fichage dans un des États membres. Repérer leurs passages aux frontières, leurs voyages et leurs trajets en Europe pourrait être crucial pour la sécurité dans l'Union.

2.2. Dans sa résolution du 6 juillet 2016, le Parlement a invité la Commission européenne à fournir les garanties nécessaires en matière de protection des données.

2.3. Les textes à l'examen s'inscrivent dans l'objectif de «Préserver et renforcer Schengen» ([1]). L'Union s'est déjà dotée de plusieurs réglementations et services numérisés d'information dans les domaines liés au contrôle du passage aux frontières des personnes et des marchandises.

2.4. Rappel:

— **SIS: système d'information Schengen**, l'un des mécanismes les plus anciens, révisé, qui gère un large spectre d'alertes portant sur les personnes et les marchandises;

([1]) COM(2017) 570 final.

— **Eurodac: système européen de comparaison des signalements dactyloscopiques** des demandeurs d'asile et des ressortissants des pays tiers en situation irrégulière aux frontières et dans les États membres, et détermination de l'État membre responsable des demandes [CESE 2016-02981, rapporteur: M. Moreno Díaz ([2])];

— **VIS: système d'information sur les visas** (code des visas), qui gère les visas pour les séjours de courte durée [CESE 2014-02932, rapporteurs: MM. Pezzini et Pariza Castaños ([3])];

— **EES: système d'entrée/de sortie**, actuellement en attente de décision, et qui devrait gérer de manière électronique les données des passeports et dates d'entrée/de sortie des ressortissants de pays tiers visitant l'espace Schengen [CESE 2016-03098, SOC/544, rapporteur: M. Pîrvulescu ([4])];

— **ETIAS: système européen d'information et d'autorisation concernant les voyages** actuellement en attente de décision, qui devrait être un vaste système automatisé de stockage et de vérification ex ante des données des ressortissants de pays tiers exemptés de visa pour circuler dans la zone Schengen [CESE 2016-06889, SOC/556, rapporteur: M. Simons ([5])];

— **ECRIS-TCN: système européen d'échange d'informations relatives au casier judiciaire des ressortissants de pays tiers**, actuellement proposé par la Commission, un système numérique d'échange d'informations sur les décisions de justice déjà rendues par les juridictions nationales.

2.5. On peut faire l'analogie entre les moyens actuels d'une autorité habilitée et un smartphone avec différentes applications, toutes séparées et donnant chacune «ses» informations.

2.6. En dehors du SIS, ces systèmes sont centrés sur **la gestion des ressortissants de pays tiers**. Il existe six systèmes, complémentaires et décentralisés. La somme des informations recherchées est celle des différentes réponses obtenues des diverses bases par les services d'enquêtes, en fonction de leurs autorisations d'accès.

2.7. La Commission se propose de répondre à la question suivante:

— par quelle méthode, sans changer les structures déjà acquises et en conservant leur complémentarité, mettre toutes les bases de données en résonance au même moment pour que, à un point d'entrée sur le territoire européen et par une seule interrogation du système tous les renseignements déjà recueillis dans les bases existantes convergent vers l'autorité de contrôle autorisée à les questionner, le tout en respectant les réglementations sur la protection des données et les droits fondamentaux?

2.8. La Commission européenne, dans les propositions à l'examen:

2.8.1. souhaite ajouter les possibilités supplémentaires qu'offrirait un accès aux bases de données d'Europol et d'Interpol, qui coopèrent déjà avec les autorités de contrôle européennes;

2.8.2. souhaite «synchroniser» les recherches d'information pour réduire les temps de réponse s'agissant du dossier des migrants et accélérer la réaction sécuritaire en cas de nécessité. Pour cela, elle propose de créer de nouvelles entités, qui permettraient de faire fonctionner les bases actuelles en symbiose.

2.9. **Ses objectifs sont de combler le plus possible les lacunes des systèmes distincts; améliorer** la gestion des frontières extérieures de l'espace Schengen; contribuer à la sécurité intérieure de l'Union; gérer les fraudes à l'identité, résoudre les cas d'identités multiples; retrouver les personnes suspectées ou déjà condamnées et vérifier leur identité dans l'espace Schengen.

2.10. Pour reprendre l'image du smartphone, non seulement l'autorité habilitée aurait à sa disposition de nombreuses applications, mais elle pourrait aussi recueillir simultanément et dans le cadre d'une même recherche, en utilisant ses codes d'accès, les données stockées dans tous ses supports: PC, portable, téléphone, tablette, notebook, etc.

([2]) JO C 34 du 2.2.2017, p. 144.
([3]) JO C 458 du 19.12.2014, p. 36.
([4]) JO C 487 du 28.12.2016, p. 66.
([5]) JO C 246 du 28.7.2017, p. 28.

3. **Le fonctionnement du système**

3.1. La Commission a procédé à des consultations et réuni un groupe d'experts de haut niveau ([6]) sur les systèmes d'information et l'interopérabilité, nommés par les États membres, les pays du groupe Schengen, les agences européennes comme eu-LISA2 ([7]) et FRA ([8]), sous la coordination de la direction générale de la migration et des affaires intérieures.

La méthode: interconnectivité ou interopérabilité?

3.1.1. **L'interconnectivité** des systèmes d'information est la possibilité de les relier entre eux de sorte que les données de l'un puissent être consultées automatiquement par un autre.

3.1.2. **L'interopérabilité** ([9]) est la capacité de différents systèmes à communiquer, à échanger des données et à utiliser l'information qui a été échangée, en respectant les habilitations d'accès aux systèmes.

3.2. *Le choix de l'interopérabilité*

3.2.1. La Commission estime qu'elle ne bouleverse pas les acquis des structures et compétences actuelles, et que les données resteront «en silos cloisonnés». Malgré la communicabilité renforcée, cela présenterait un avantage de sécurité pour les systèmes et les données, dont aucune ne sera évidemment accessible par l'internet. Les textes soumis à avis comportent d'importantes similitudes et portent:

— l'un, COM(2017) 793, sur l'interopérabilité des systèmes d'information relatifs aux frontières et aux visas,

— l'autre, COM(2017) 794, sur la coopération police-justice, l'asile et la migration.

3.3. *Les nouveaux outils*

3.3.1. Pour fonctionner dans l'interopérabilité, une nouvelle architecture de quatre nouveaux outils devra compléter les six bases pour travailler vite en n'interrogeant qu'une seule fois le système, en gardant les personnes habilitées à l'origine des demandes.

3.4. *Le PRE (ESP), portail de recherche européen*

3.4.1. L'autorité de contrôle habilitée (l'utilisateur final) devrait disposer d'un accès unique à l'ensemble du système. Au lieu de procéder à six recherches, elle n'en lancerait plus qu'une (polices, douanes, etc.) pour interroger simultanément plusieurs bases sur les données recherchées, sans en stocker aucune. Si elles existent, le système les trouvera. En cas de soupçon de crime ou d'activité terroriste, la première touche pourra être neutre pour la personne contrôlée («no-hit»), mais si la donnée concorde avec un deuxième renseignement («hit») existant dans les bases telles que SIS, EES, ETIAS, cela pourra conduire à des recherches approfondies et à une enquête.

3.5. *Le BMS partagé (shared biometric matching service)*

3.5.1. Cette plateforme partagée de mise en concordance permettra la recherche et la comparaison simultanées de données mathématisées, biométriques, empreintes digitales et photographies d'identité, depuis les différentes bases, comme SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, mais pas *ETIAS*; leurs données devront être compatibles.

3.5.2. Les données mathématisées ne seront pas conservées sous leur forme originale.

3.6. *Le CIR (common identity repository)*

3.6.1. Un «répertoire commun de données d'identité» rassemblera les données relatives à l'identité biographique et biométrique des personnes contrôlées des pays tiers, qu'elles soient à la frontière ou dans les États membres (de Schengen). Un indicateur de concordance des renseignements dans les différentes bases accélérera les recherches. Sous la responsabilité et avec les moyens de sécurité de l'agence eu-LISA, ces données seront sauvegardées de sorte qu'aucune personne ne puisse accéder à plus d'une ligne alphanumérique à la fois. Développé à partir d'EES et ETIAS, le CIR ne devrait pas aboutir à dupliquer les données. Le répertoire pourra aussi servir à des recherches civiles.

([6]) Direction générale de la migration et des affaires intérieures, unité B/3; décision C(2016) 3780 de la Commission du 17 juin 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=FR

([7]) Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.

([8]) Agence des droits fondamentaux de l'Union européenne.

([9]) Commission, COM(2016) 205 final, communication, «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité».

([10]) Les italiques rappellent que les textes concernant ces organes ne sont pas encore adoptés.

3.7. *Le MID (multiple-identity detector)*

3.7.1. Il aura pour rôle de vérifier l'identité correcte des personnes de bonne foi, et de combattre les fraudes à l'identité, par une recherche dans toutes les bases en même temps. Aucune administration n'a encore utilisé pareil outil, qui devrait permettre d'éviter les usurpations d'identité.

3.8. *Le rôle de l'agence eu-LISA* ([11])

3.8.1. L'agence, créée en 2011, a pour mission de faciliter les politiques de l'Union européenne dans les domaines de la justice, de la sécurité et de la liberté. Établie à Tallin, en Estonie, elle assure déjà l'échange d'informations entre les différentes autorités répressives des États membres et le fonctionnement sans discontinuité des systèmes informatiques de grande échelle ainsi que la liberté de mouvement des personnes dans l'espace Schengen.

3.8.2. Elle travaille au projet «Smart Borders» et aura dans la nouvelle architecture d'échanges de données un rôle de conservation des éléments liés aux personnes comme ceux relatifs aux autorités, aux enquêtes et enquêteurs. Elle contrôlera les habilitations des demandeurs, et assurera la sécurité des données, y compris en cas «d'incident» [article 44, propositions COM(2017) 793 et 794].

3.8.3. **L'utilisation de l'UMF** (*Universal Message Format*), qui reste à créer, devrait faciliter le travail avec les nouveaux systèmes, qui seront obligatoires, imposant la création d'interfaces dans les États membres qui n'en ont pas encore et un système de traduction temporaire d'un langage vers l'autre.

3.9. *La protection des données personnelles (articles 8 et 7 de la charte)*

3.9.1. La proposition de règlement reconnaît la possibilité d'accidents de sécurité. Les États membres et leurs systèmes de données doivent, les premiers, respecter les principes de protection des données prévus par les textes, le traité, la charte des droits fondamentaux et le RGPD ([12]) qui entrera en vigueur le 25 mai 2018.

4. **Discussion**

4.1. *Valeur ajoutée de l'interopérabilité en démocratie*

4.1.1. L'Union a besoin de régulation et de moyens d'investigation qui la protègent contre la criminalité. L'interopérabilité des systèmes d'information est une opportunité de faire valoir la primauté du droit et la défense des droits de l'homme.

4.1.2. *EES et ETIAS*, couplés au BMS et au CIR, vont permettre de contrôler les passages aux frontières des personnes suspectes, et de conserver leurs données. Cependant, la possibilité pour les «services répressifs [d'accéder par le BMS] aux systèmes d'information à finalité non répressive au niveau de l'Union européenne» [article 17, CIR, propositions COM (2017) 794 et 793], ne peut être compatible avec les fins énoncées comme bases des propositions à l'examen. Le Comité (article 300, paragraphe 4, du traité sur le fonctionnement de l'Union européenne) se doit d'évoquer ici le principe de proportionnalité et demande à la Commission d'éviter tout schéma de type «Big Brother» ([13]) et la création d'obstacles à la liberté de circuler des européens (article 3 du traité sur l'Union européenne).

4.1.3. Le modèle proposé pour la collecte et l'utilisation des données personnelles obtenues à la frontière et dans le territoire de l'Union lors de contrôles des mouvements et des documents détenus est présenté comme étanche, ouvert seulement à des personnes habilitées et à des fins de sécurité et de gestion, et il apportera une plus grande fluidité des procédures.

4.1.4. Le Comité s'interroge sur l'étanchéité: des lacunes demeureront, la construction étagée sur neuf ans s'appuie sur des «fondations» qui n'existent pas encore, comme les bases EES ou ETIAS, ou les interfaces nationales. Le contexte technologique est en constante évolution, le projet repose par nécessité sur l'état de la technique et ne prévoit pas, budgétairement, de gérer l'obsolescence qui apparaîtrait dans certains secteurs numériques.

([11]) Règlement (UE) n° 1077/2011 du Parlement européen et du Conseil du 25 octobre 2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice.

([12]) 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). Avis du CESE: JO C 229 du 31.7.2012, p. 90 et JO C 345 du 13.10.2017, p. 138.

([13]) In *1984*, George Orwell.

4.1.5. Par ailleurs, le développement rapide de l'utilisation des algorithmes dits de l'intelligence artificielle (IA) aurait pu être considéré dans le projet, à la fois comme outil de contrôle des systèmes et comme clé de sécurité à confier aux autorités décisionnelles pour garantir l'utilisation démocratique de l'architecture.

4.1.6. La proposition développe un système pour des protagonistes de bonne foi, respectueux des lois. Le fait que des hommes soient aux commandes est rassurant, mais ils peuvent aussi être les maillons faibles. Le Comité suggère l'ajout d'un article prévoyant des «disjoncteurs différentiels», pour les cas de crise politique et/ou de «management», tout problème dans une base pourrait représenter un risque pour l'ensemble de l'architecture ([14]). La généralisation de l'UMF pourrait déboucher sur un usage international, très positif mais très risqué pour la protection des données. Les autorités habilitées porteront une lourde responsabilité. Ces aspects ne sont pas envisagés dans les textes à l'examen.

4.2. *La protection des droits fondamentaux*

4.2.1. Les droits fondamentaux sont absolus; ils ne peuvent subir des atteintes limitées que si celles-ci sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union et que si leur contenu essentiel est respecté (article 8 et article 52, paragraphe 1, de la charte des droits fondamentaux). Le Comité se demande comment peut être évaluée la proportionnalité des mesures de contrôle, dans le cas de migrants fuyant les persécutions et cherchant asile sur les côtes de l'Union? [COM(2017) 794 final — Exposé des motifs — Droits fondamentaux]. La recherche de suspects en vue de prévenir les actes criminels, notamment terroristes, **ne doit pas rapprocher nos démocraties du concept de délit par anticipation**; la différence doit subsister entre «activités» troublant l'ordre public et «opinions».

4.2.2. Le respect pour toute personne des droits énoncés dans la charte doit assurer l'équilibre entre sécurité et liberté, sans lequel meurt la démocratie. Le Comité estime que cet équilibre est fondamental et doit être un objectif permanent pour toutes les autorités, y compris de contrôle, au niveau national comme au niveau européen.

4.2.3. La chaîne des autorités associées à une recherche ainsi que les métadonnées qui s'y rattachent seront conservées dans le système. Ces autorités habilitées elles-mêmes doivent voir leurs droits fondamentaux respectés à propos des données générées, notamment à l'égard de leur sécurité, de leur vie privée, en cas d'intrusion malveillante dans la structure et d'utilisation détournée des données entre le moment de la saisie et celui de leur effacement.

4.3. *Protection des données*

4.3.1. Les propositions reconnaissent le principe de la protection des données personnelles dès la conception et par défaut, bien que leur exposé des motifs rappelle que, selon la Cour (CJUE), il ne s'agit pas d'une prérogative absolue. Le Comité reconnaît les avantages de mesures préventives garantissant la sécurité, de la lutte contre les fausses identités et de la garantie du droit d'asile. Mais il tient à souligner les limites de la mathématisation et de l'anonymisation des données: les personnes concernées peuvent avoir besoin ultérieurement de leurs données.

4.3.2. Il souligne également que le type de données conservées, biométriques et biologiques, revêt un intérêt particulier pour certaines entreprises et pour la criminalité. La cybersécurité est ici aussi importante que la sécurité physique, et elle est trop peu évoquée dans les propositions. Les données conservées seront stockées à un seul emplacement physique; même sanctuarisé, il peut être exposé.

4.3.3. Le CESE rappelle que s'agissant de la protection des données et du droit à l'effacement (droit à l'oubli), les institutions et organes de l'Union sont soumis au respect du règlement (CE) n° 45/2001, moins protecteur que le RGPD ([15]) de 2016 (qui entre en vigueur en mai 2018) que doivent respecter les États membres. Le Comité souligne la complexité de la mise en œuvre de ce droit et redoute que les voyageurs, migrants et demandeurs d'asile ne soient pas en capacité de le faire respecter:

1) la protection des données personnelles doit être validée pour toutes les bases existantes, nationales et européennes, pour que l'ensemble soit protégé;

2) elle est fondamentale pour que les citoyens acceptent cet immense maillage de surveillance au-dessus de leur tête.

4.3.4. La durée de conservation des données recueillies par les autorités habilitées n'est pas précisée clairement dans les propositions. Les textes évoquent la procédure du droit à rectification et/ou effacement qui fait des allers-retours entre État de la demande et État responsable, mais ne fixe pas de délais de conservation des données (article 47 des propositions). Le Comité préconise que ce délai soit fixé, et soit plus court pour les mineurs (charte, article 24), sauf en cas de terrorisme, de sorte que ceux-ci puissent avoir leurs chances de s'intégrer.

([14]) CEPD, annexe, rapport final du groupe d'experts de haut niveau, mai 2017.
([15]) RGPD, règlement général sur la protection des données [règlement (UE) 2016/679].

4.4. *Gouvernance et obligation de rendre compte*

4.4.1. Les bases internationales ne sont pas soumises aux mêmes règles que les systèmes informatisés européens. La mise en place d'un format universel d'accès, qui pourrait tendre à devenir international, ne sera qu'un élément technique qui n'unifiera pas les réglementations, même si Interpol doit certainement respecter l'article 17 du pacte onusien ([16]). Par ailleurs, les habilitations resteront du domaine des États membres. Le CESE estime que ce point devrait être abordé dans les propositions.

4.4.2. Une seule interrogation, et la symbiose des bases européennes donnera son verdict. Le CESE souligne que la bureaucratie générée sera plus que proportionnelle à la vitesse acquise. La gouvernance sera assurée par la Commission dans le cadre d'une procédure de contrôle avec les États membres. Le pivot sera l'agence eu-LISA, chargée notamment de mettre en place les procédures de collecte des informations sur le fonctionnement de l'interopérabilité; elle recevra les informations des États membres et d'Europol, et présentera au Conseil, au Parlement européen et à la Commission, tous les quatre ans, un rapport d'évaluation technique, la Commission préparant elle-même un rapport global un an plus tard (article 68 des propositions). Pour le Comité, ces séquences sont beaucoup trop longues. L'évaluation de la sécurité des éléments d'interopérabilité [article 68, paragraphe 5, point d)] devrait au moins avoir lieu chaque année, et celle de l'impact sur les droits fondamentaux au moins tous les deux ans [article 68, paragraphe 5, point b)].

4.4.3. Le Comité regrette que des questions aussi fondamentales que celles abordées par ces propositions soient gérées par des agences européennes, dont le recrutement et le fonctionnement sont obscurs pour beaucoup de citoyens. Il estime nécessaire de croiser les bonnes pratiques et d'associer pour avis toutes les autorités indépendantes de contrôle de l'utilisation des données (CEPD), et d'autres agences comme FRA et ENISA.

4.4.4. La mise en place de toutes ces nouvelles structures et procédures se fera au moyen d'actes délégués et d'actes d'exécution de la Commission. Le Comité souhaiterait que l'objectif de respect des droits fondamentaux et de la protection des données personnelles reste inscrit dans tous ces actes au fil du temps, dans une approche d'accueil amélioré des personnes aux frontières. Le CESE recommande que les citoyens européens soient informés des étapes jusqu'à l'achèvement du projet, et que les personnes reçoivent une information pédagogique sur les contrôles auxquels elles sont soumises.

5. **Les formations nécessaires des autorités de contrôle dans toute l'Union**

5.1. Le Comité estime que de nombreuses formations seront nécessaires dans la première période (après 2021), contrairement à ce qu'avance la Commission dans son résumé de l'analyse d'impact (C). Elle évoque 76 millions d'EUR par an. Le passage à de nouvelles procédures demande toujours une mise à niveau. Il s'agit ici de toutes les frontières de l'Union et des systèmes nationaux. Certains États membres ne sont pas encore dotés de systèmes compatibles et devront fournir un effort important et mettre en place des interfaces les rendant capables de participer. Pour que fonctionne l'interopérabilité, les disparités entre États membres devront être aplanies.

5.2. La formation à l'utilisation des données de qualité et de l'UMF sera essentielle. Le Comité suggère qu'un pôle de formations communes pour les autorités habilitées, incluant l'eu-LISA dont les membres devraient voir leurs compétences strictement vérifiées, soit organisé avec CEPOL ([17]), Frontex, Europol, etc.

5.3. Un outil tel que le MID n'existe nulle part ailleurs. En cas de succès, l'outil sera puissant. La nouvelle architecture exigera la plus grande qualité des données. Pour que l'ensemble soit à la hauteur des espérances du projet, tous les États membres doivent participer au même niveau, sans quoi les lacunes seront plus graves qu'auparavant. Et dans ce cas, le droit d'asile et le droit d'accès à une protection internationale seraient fragilisés (article 18 et 19 de la charte).

6. **Le financement**

6.1. L'ensemble de l'architecture proposée repose sur certaines hypothèses: l'adoption par les autorités décisionnelles des systèmes *EES, ETIAS,* l'*UMF*, le bon fonctionnement du *MID* et la sécurisation du *CIR*. Deux organes, le CEPD, l'agence eu-LISA, et peut-être aussi l'agence ENISA, disposeront-ils d'effectifs et de moyens financiers suffisants? La Commission propose un cofinancement de l'Union européenne et des États membres. Le Comité note que la gestion du «Semestre» se fait encore avec des budgets d'austérité, et que, par ailleurs, l'utilisation actuelle des bases existantes (SIS, VIS, Prüm, *EES*) doit encore être optimisée dans le respect des exigences légales (rapport du groupe d'experts).

([16]) Pacte international relatif aux droits civils et politiques, ONU: «Article 17: 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.»

([17]) CEPOL, Agence de l'Union européenne pour la formation des services répressifs (Budapest, Hongrie).

6.2. Le CESE s'interroge sur l'incidence budgétaire du «Brexit», bien que le Royaume-Uni ne soit pas dans le système Schengen, et plus globalement, sur la future complexité de la gestion de l'interopérabilité dans les pays européens non-SIS, mais participant à d'autres bases, telle Eurodac.

6.3. Le fonds prévu est le FSI, Fonds pour la sécurité intérieure et les frontières. Le début de la mise en fonctionnement est prévu pour 2023. Le Comité se demande si cinq ans suffiront pour réduire les disparités européennes et réunir les conditions du succès. Le budget prévu est de 424,7 millions d'EUR sur neuf ans (2019-2027). L'Union (FSI) et les États membres devront payer. Les États doivent se mettre en situation de faire fonctionner correctement les systèmes actuels avec la nouvelle architecture informatique. Le Comité estime que le retour de la croissance devra servir la réalisation de ces investissements.

Bruxelles, le 23 mai 2018.

Le président
du Comité économique et social européen
Luca JAHIER