COMMISSION
EUROPÉENNE

Strasbourg, le 12.12.2017
COM(2017) 794 final

2017/0352 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration)

{SWD(2017) 473} - {SWD(2017) 474}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Contexte de la proposition

Ces trois dernières années, l'Union a connu une hausse du nombre de franchissements irréguliers de ses frontières, ainsi qu'une menace croissante et continue pesant sur sa sécurité intérieure, comme l'a montré une série d'attaques terroristes. Les citoyens de l'Union s'attendent à ce que les contrôles exercés aux frontières extérieures sur les personnes ainsi que les vérifications au sein de l'espace Schengen soient efficaces, afin de permettre une gestion effective des migrations et de contribuer à la sécurité intérieure. Ces défis ont mis en lumière l'urgente nécessité de rassembler et de renforcer de manière globale les outils d'information de l'UE pour la gestion des frontières, les migrations et la sécurité.

L'efficacité et l'efficience de la gestion de l'information dans l'Union peuvent et doivent être améliorées, dans le plein respect des droits fondamentaux, notamment du droit à la protection des données à caractère personnel, afin de mieux protéger les frontières extérieures de l'Union, d'améliorer la gestion des migrations et de renforcer la sécurité intérieure au bénéfice de l'ensemble des citoyens. Il existe déjà un certain nombre de systèmes d'information au niveau de l'Union et d'autres systèmes sont en cours de développement afin de fournir aux garde-frontières et aux agents des services répressifs et d'immigration des informations pertinentes sur les personnes. Afin que cet appui soit efficace, les informations fournies par les systèmes d'information de l'UE doivent être complètes, précises et fiables. L'architecture de la gestion de l'information dans l'Union présente cependant des lacunes structurelles. Les autorités nationales sont confrontées à une mosaïque complexe de systèmes d'information régis de différentes façons. De plus, l'architecture de la gestion des données appliquée aux frontières et à la sécurité est fragmentée, car les informations sont stockées séparément dans des systèmes qui ne sont pas interconnectés, ce qui donne lieu à des angles morts. Par conséquent, **les différents systèmes d'information au niveau de l'Union ne sont à l'heure actuelle pas interopérables**, c'est-à-dire qu'ils ne sont pas capables d'échanger des données et de partager des informations de manière à ce que les autorités et les agents compétents disposent des informations dont ils ont besoin, au moment et à l'endroit où ils en ont besoin. L'interopérabilité des systèmes d'information au niveau de l'Union peut contribuer de manière appréciable à l'élimination des angles morts existants, en raison desquels des personnes, notamment des personnes éventuellement impliquées dans des activités terroristes, peuvent être enregistrées dans des bases de données différentes et non interconnectées, sous différents pseudonymes.

En avril 2016, la Commission a présenté une **communication intitulée «*Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*»**[1], afin de remédier à un certain nombre de lacunes structurelles affectant les systèmes d'information[2]. L'objectif de la communication d'avril 2016 était de lancer une discussion sur la manière dont les systèmes d'information dans l'Union européenne peuvent améliorer la gestion des frontières et des migrations ainsi que la sécurité intérieure. Pour sa part, le **Conseil**

[1] COM(2016) 205 du 6 avril 2016.

[2] 1) Fonctionnalités non optimales dans certains des systèmes d'information existants, 2) lacunes en matière d'information dans l'architecture de la gestion des données de l'UE, 3) mosaïque complexe de systèmes d'information régis de différentes façons, et 4) architecture fragmentée de la gestion des données appliquée aux frontières et à la sécurité, dans laquelle les informations sont stockées séparément dans des systèmes qui ne sont pas interconnectés, ce qui donne lieu à des angles morts.

a également reconnu qu'il était nécessaire d'entreprendre d'urgence des actions dans ce domaine. En juin 2016, il a approuvé une **feuille de route en vue de renforcer l'échange d'informations et la gestion de l'information**, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures[3]. L'objectif de la feuille de route était de soutenir les investigations opérationnelles et de fournir rapidement aux professionnels sur le terrain, tels que les policiers, les garde-frontières, les procureurs, les agents des services d'immigration et d'autres acteurs, des informations complètes, pertinentes et de qualité leur permettant de coopérer et d'agir efficacement. Le **Parlement européen** a également demandé que des mesures soient prises dans ce domaine. Dans sa résolution de juillet 2016[4] sur le programme de travail de la Commission pour 2017, le Parlement européen a invité à présenter des «*propositions visant à améliorer et à développer les systèmes d'information existants, à combler les lacunes en matière d'informations et à progresser vers l'interopérabilité, ainsi que [des] propositions concernant l'échange obligatoire d'informations au niveau de l'Union, assorti des garanties nécessaires en matière de protection des données*». Le président Juncker, dans son discours sur l'état de l'Union de septembre 2016[5], et le Conseil européen, dans ses conclusions de décembre 2016[6], ont insisté sur l'importance de remédier aux insuffisances dont souffre actuellement la gestion des données et d'améliorer l'interopérabilité des systèmes d'information existants.

En juin 2016, pour donner suite à la communication d'avril 2016, la Commission a créé un **groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité**[7] afin de faire face aux défis juridiques, techniques et opérationnels posés par l'amélioration de l'interopérabilité des systèmes centraux de l'Union pour les frontières et la sécurité, y compris leur nécessité, leur faisabilité technique, leur caractère proportionnel et leurs implications en ce qui concerne la protection des données. Le **rapport final** du groupe d'experts de haut niveau a été publié en mai 2017[8]. Il définit un ensemble de recommandations visant à renforcer et à développer les systèmes d'information de l'UE et leur interopérabilité. L'Agence des droits fondamentaux de l'Union européenne, le Contrôleur européen de la protection des données et le coordinateur de l'UE pour la lutte contre le terrorisme ont tous activement participé aux travaux du groupe d'experts. Chacun d'eux a présenté des déclarations de soutien, tout en reconnaissant qu'il convenait d'aborder les questions plus larges qui se posent en matière de droits fondamentaux et de protection des données à mesure que des progrès sont réalisés. Des représentants du secrétariat de la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen et du secrétariat général du Conseil étaient présents en tant qu'observateurs. Le groupe d'experts de haut niveau a conclu qu'il était **nécessaire et techniquement faisable d'œuvrer à des solutions pratiques d'interopérabilité**, qui peuvent, en principe, apporter des bénéfices opérationnels et être mises en place conformément aux exigences en matière de protection des données.

---

3 Feuille de route du 6 juin 2016 en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures – 9368/1/16 REV 1.

4 Résolution du Parlement européen du 6 juillet 2016 sur les priorités stratégiques pour le programme de travail de la Commission pour 2017 [2016/2773(RSP)].

5 État de l'Union en 2016 (14.9.2016), https://ec.europa.eu/commission/state-union-2016_fr.

6 Conclusions du Conseil européen du 15.12.2016, http://data.consilium.europa.eu/doc/document/ST-34-2016-INIT/fr/pdf.

7 Décision de la Commission du 17 juin 2016 instituant le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité – 2016/C 257/03.

8 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

En se fondant sur le rapport et les recommandations du groupe d'experts, la Commission a défini, dans le *Septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective*[9], une **nouvelle approche de la gestion des données** pour les frontières, la sécurité et la gestion des migrations, selon laquelle tous les systèmes d'information centralisés de l'UE en la matière sont interopérables, dans le plein respect des droits fondamentaux. La Commission a annoncé son intention de poursuivre ses travaux en vue de la création d'un portail de recherche européen capable d'interroger simultanément l'ensemble des systèmes de l'Union pertinents dans les domaines de la sécurité, des frontières et de la gestion des migrations, qui pourrait s'accompagner de règles simplifiées pour l'accès à des fins répressives, et de développer pour ces systèmes un service partagé d'établissement de correspondances biométriques (qui pourrait comporter une fonctionnalité d'indication de concordance[10]) ainsi qu'un répertoire commun de données d'identité. Elle a annoncé son intention de présenter, dès que possible, une proposition législative relative à l'interopérabilité.

Les conclusions du Conseil européen de juin 2017[11] ont réaffirmé la nécessité d'agir. En se fondant sur les conclusions de juin 2017[12] du Conseil «Justice et affaires intérieures», le Conseil européen a invité la Commission à préparer, dès que possible, un projet de texte législatif mettant en œuvre les recommandations formulées par le groupe d'experts de haut niveau. Cette initiative répond également à l'appel du Conseil en faveur de la création d'un cadre global pour l'accès à des fins répressives aux différentes bases de données dans le domaine de la justice et des affaires intérieures, en vue d'assurer une plus grande simplification, cohérence, efficacité et attention aux besoins opérationnels[13]. Afin de renforcer les efforts déployés pour faire de l'Union européenne une société plus sûre, dans le plein respect des droits fondamentaux, la Commission a annoncé, dans le cadre de son programme de travail pour 2018[14], qu'une proposition relative à l'interopérabilité des systèmes d'information devait être présentée avant la fin 2017.

- **Objectifs de la proposition**

Les objectifs généraux de la présente initiative résultent des objectifs fondés sur le traité consistant à améliorer la gestion des frontières extérieures de l'espace Schengen et à contribuer à la sécurité intérieure de l'Union européenne. Ils découlent également des décisions politiques de la Commission et des conclusions pertinentes du Conseil (européen). Ces objectifs ont été affinés dans l'agenda européen en matière de migration et dans les communications ultérieures, notamment la communication intitulée «Préserver et renforcer Schengen»[15], le programme européen en matière de sécurité»[16] et les travaux et rapports

---

9 COM(2017) 261 final.

10 Nouveau concept de protection de la vie privée dès la conception, qui restreint l'accès à l'ensemble des données en le limitant à une simple indication de «concordance/non-concordance» signalant la présence (ou l'absence) de données.

11 Conclusions du Conseil européen des 22 et 23 juin 2017.

12 Résultats de la 3 546e session du Conseil en matière de justice et affaires intérieures, des 8 et 9 juin 2017, 10136/17.

13 Après avoir chargé la présidence du Conseil d'ouvrir les négociations interinstitutionnelles sur le système d'entrée/de sortie de l'UE le 2 mars 2017, le comité des représentants permanents du Conseil (Coreper) a approuvé un projet de déclaration du Conseil invitant la Commission à proposer un cadre global pour l'accès à des fins répressives aux différentes bases de données dans le domaine de la justice et des affaires intérieures, en vue d'assurer une plus grande simplification, cohérence, efficacité et attention aux besoins opérationnels (compte rendu sommaire 7177/17, 21.3.2017).

14 COM(2017) 650 final.

15 COM(2017) 570 final.

d'avancement de la Commission sur la mise en place d'une union de la sécurité réelle et effective[17].

Bien qu'ils s'appuient plus particulièrement sur la communication d'avril 2016 et sur les constatations du groupe d'experts de haut niveau, les objectifs de la présente proposition sont intrinsèquement liés aux éléments mentionnés ci-dessus.

Les objectifs spécifiques de la présente proposition sont les suivants:

(1) garantir que les utilisateurs finaux, en particulier les garde-frontières, les agents des services répressifs, les agents des services d'immigration et les autorités judiciaires, disposent d'un **accès rapide, continu, systématique et contrôlé** aux informations dont ils ont besoin pour accomplir leurs tâches;

(2) fournir une solution permettant de **détecter les identités multiples** liées à un même ensemble de données biométriques, dans le double objectif de garantir l'identification correcte des personnes de bonne foi et de **lutter contre la fraude à l'identité**;

(3) faciliter les **contrôles d'identité des ressortissants de pays tiers** effectués sur le territoire d'un État membre par les autorités de police, et

(4) faciliter et **simplifier l'accès des services répressifs** aux systèmes d'information à finalité non répressive au niveau de l'Union, lorsque cela est nécessaire à des fins de prévention et de détection des infractions graves et du terrorisme, ou d'enquêtes et de poursuites en la matière.

Outre ces principaux objectifs opérationnels, la présente proposition contribuera également à:

- faciliter la **mise en œuvre** technique et opérationnelle des systèmes d'information existants et futurs **par les États membres**;
- renforcer et simplifier les **conditions de sécurité des données et de protection des données** régissant les différents systèmes, et
- améliorer et harmoniser les exigences relatives à la **qualité des données** des différents systèmes.

Enfin, la présente proposition contient des dispositions relatives à la création et à la gouvernance du format universel pour les messages (UMF), en tant que norme de l'UE pour le développement de systèmes d'information dans le domaine de la justice et des affaires intérieures, ainsi qu'à la création d'un répertoire central des rapports et statistiques.

- **Champ d'application de la proposition**

De même que la proposition complémentaire présentée le même jour, la présente proposition relative à l'interopérabilité concerne les systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations exploités au niveau central; trois de ces systèmes existent déjà, un va bientôt être développé et deux autres se trouvent au stade de propositions en cours d'examen par les colégislateurs. Chaque système a ses propres objectifs, finalités, bases juridiques, règles, groupes d'utilisateurs et contextes institutionnels.

---

[16] COM(2015) 185 final.
[17] COM(2016) 230 final.

Les trois systèmes d'information centralisés qui existent à ce jour sont:

- le **système d'information Schengen (SIS)**, qui comprend un large éventail de signalements de personnes (refus d'entrée ou de séjour, mandat d'arrêt européen, personnes disparues, concours dans le cadre d'une procédure judiciaire, contrôles discrets et spécifiques) et d'objets (notamment les documents de voyage ou d'identité égarés, volés et invalidés)[18];
- le système **Eurodac**, qui contient les empreintes digitales des demandeurs d'asile et des ressortissants de pays tiers qui ont franchi illégalement les frontières extérieures ou se trouvent en séjour irrégulier dans un État membre, et
- le **système d'information sur les visas (VIS)**, qui contient des données sur les visas de court séjour.

Outre ces systèmes existants, la Commission a proposé en 2016-2017 trois nouveaux systèmes d'information centralisés de l'UE:

- le **système d'entrée/de sortie (EES)**, dont la base juridique vient juste d'être approuvée, qui remplacera le système actuel consistant à apposer manuellement un tampon sur les passeports et qui enregistrera sous forme électronique le nom, le type de document de voyage, les données biométriques ainsi que la date et le lieu d'entrée et de sortie des ressortissants de pays tiers se rendant dans l'espace Schengen pour un court séjour;
- le **système européen d'information et d'autorisation concernant les voyages (ETIAS)**, qui, lorsque la proposition aura été adoptée, sera un système largement automatisé rassemblant et vérifiant les informations fournies par les ressortissants de pays tiers exemptés de l'obligation de visa avant leur voyage dans l'espace Schengen, et
- le **système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (système ECRIS-TCN)**, qui sera un système électronique d'échange d'informations concernant les condamnations antérieures prononcées à l'encontre de ressortissants de pays tiers par des juridictions pénales se trouvant dans l'Union.

Ces six systèmes sont complémentaires et, à l'exception du système d'information Schengen (SIS), concernent exclusivement les ressortissants de pays tiers. Ces systèmes aident les autorités nationales à gérer les frontières, les migrations, le traitement des visas et l'asile ainsi qu'à lutter contre la criminalité et le terrorisme. C'est tout particulièrement vrai dans le cas du SIS, qui est l'instrument de partage d'informations en matière répressive le plus utilisé à l'heure actuelle.

Outre ces systèmes d'information, gérés de manière centrale au niveau de l'Union, le champ d'application de la présente proposition comprend également la base de données d'**Interpol** sur les documents de voyage volés et perdus (SLTD), qui, conformément aux dispositions du code frontières Schengen, est systématiquement consultée aux frontières extérieures de l'Union, et la base de données d'Interpol sur les documents de voyage associés aux notices (TDAWN). Il couvre également les données **Europol**, dans la mesure où cela est pertinent

[18] Dans les projets de règlements relatifs au SIS présentés en décembre 2016, la Commission propose d'élargir cet éventail afin d'y inclure les décisions de retour et les contrôles d'investigation.

pour assurer le fonctionnement du système ETIAS proposé et pour aider les États membres qui recherchent des données relatives aux infractions graves et au terrorisme.

Les systèmes d'information nationaux et les systèmes d'information décentralisés de l'UE ne relèvent pas du champ d'application de la présente initiative. Les systèmes décentralisés, tels que ceux exploités en vertu du cadre Prüm[19], de la directive relative aux données des dossiers passagers (PNR)[20] et de la directive concernant l'information préalable sur les passagers[21], pourront être ultérieurement reliés à un ou plusieurs des éléments proposés dans le cadre de la présente initiative[22], à condition d'en démontrer la nécessité.

Afin de respecter la distinction entre, d'une part, les questions qui constituent un développement de l'acquis de Schengen en matière de frontières et de visas et, d'autre part, les autres systèmes qui concernent l'acquis de Schengen en matière de coopération policière ou qui ne sont pas liés à l'acquis de Schengen, la présente proposition concerne l'accès au système d'information Schengen tel qu'actuellement régi par la décision 2007/533/JAI du Conseil, ainsi qu'Eurodac et le [système ECRIS-TCN].

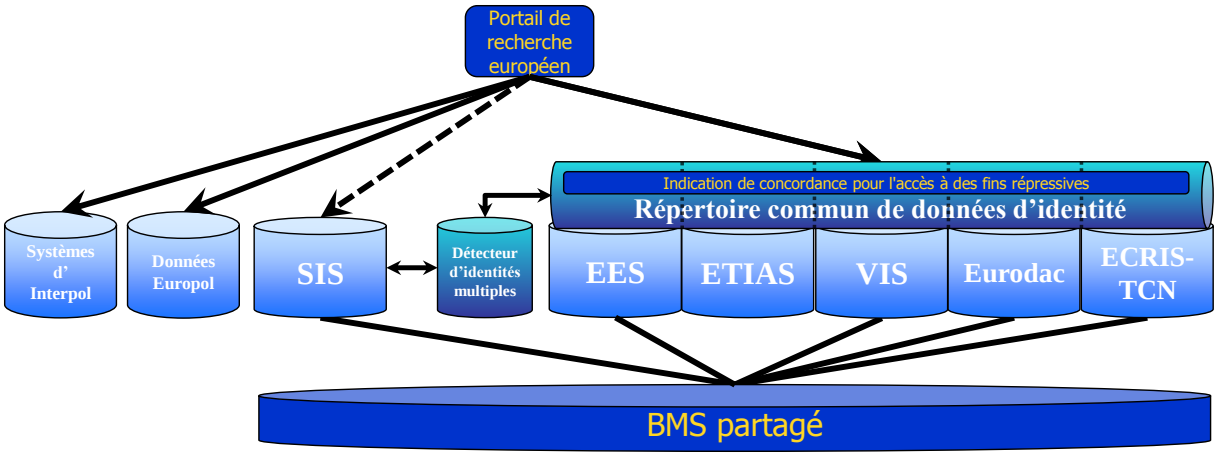
- **Les éléments techniques nécessaires pour atteindre l'interopérabilité**

Afin d'atteindre les objectifs de la présente proposition, quatre éléments d'interopérabilité doivent être établis:

- le portail de recherche européen – ESP
- le service partagé d'établissement de correspondances biométriques – BMS partagé
- le répertoire commun de données d'identité – CIR
- le détecteur d'identités multiples – MID

Chacun de ces éléments est décrit en détail dans le document de travail des services de la Commission sur l'analyse d'impact qui accompagne la présente proposition.

La combinaison des quatre éléments conduit à la solution d'interopérabilité suivante:



[19] http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1508936184412&uri=CELEX:32008D06 15.

[20] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L0681.

[21] Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

[22] De même, en ce qui concerne les systèmes douaniers, dans ses conclusions de juin 2017, le Conseil a invité la Commission à entreprendre une étude de faisabilité afin d'étudier plus avant les aspects techniques, opérationnels et juridiques de l'interopérabilité des systèmes de gestion en matière de sécurité et de frontières avec les systèmes douaniers, et à soumettre ses conclusions à l'examen du Conseil d'ici à la fin 2018.

Les objectifs et le fonctionnement de ces quatre éléments peuvent se résumer de la manière suivante:

1) Le **portail de recherche européen (ESP)** est l'élément qui permettrait d'interroger simultanément de multiples systèmes (SIS-central, Eurodac, 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). Il garantirait que les utilisateurs des systèmes d'information de l'UE disposent d'un accès rapide, continu, efficace, systématique et contrôlé à l'ensemble des informations dont ils ont besoin pour accomplir leurs tâches.

   Une recherche sur le portail de recherche européen fournirait immédiatement, en quelques secondes, des informations provenant des différents systèmes auxquels l'utilisateur a légalement accès. En fonction de l'objectif de la recherche et des droits d'accès correspondants, l'ESP serait fourni avec des configurations spécifiques.

   L'ESP ne traite pas de nouvelles données et ne stocke aucune donnée; il constituerait un guichet unique ou «courtier de messages» afin d'interroger différents systèmes centraux et de récupérer les informations nécessaires sans discontinuité, dans le plein respect des exigences en matière de contrôle de l'accès et de protection des données des systèmes sous-jacents. L'ESP faciliterait l'utilisation correcte et autorisée de chacun des systèmes d'information de l'UE existants et rendrait leur consultation et leur utilisation plus simples et moins onéreuses pour les États membres, conformément aux instruments juridiques qui régissent ces systèmes.

2) Le **service partagé d'établissement de correspondances biométriques (BMS partagé)** permettrait d'interroger et de comparer des données biométriques (empreintes digitales et images faciales) contenues dans plusieurs systèmes centraux (notamment le SIS, Eurodac, le VIS, le futur EES et le système ECRIS-TCN proposé). L'ETIAS proposé ne contiendra pas de données biométriques et ne serait donc pas relié au BMS partagé.

   Alors qu'à l'heure actuelle chaque système central existant (le SIS, Eurodac, le VIS) dispose d'un moteur de recherche spécifique et propriétaire pour les données biométriques[23], un service partagé d'établissement de correspondances biométriques fournirait une plateforme commune sur laquelle les données seraient interrogées et comparées de manière simultanée. Le BMS partagé entraînerait des avantages conséquents en matière de sécurité, de coût, de maintenance et de fonctionnement car il s'appuie sur un élément technologique unique plutôt que sur cinq éléments différents. Les données biométriques (empreintes digitales et images faciales) sont exclusivement stockées par les systèmes sous-jacents. Le BMS partagé créerait et stockerait une représentation mathématique des échantillons biométriques (un modèle) mais supprimerait les données réelles, qui resteraient donc stockées à un seul endroit et une seule fois.

   Le BMS partagé serait un instrument essentiel pour contribuer à détecter les connexions entre des ensembles de données et les différentes identités endossées par une même

[23] La dénomination technique de ces moteurs de recherche de données biométriques est «système automatisé d'identification par empreintes digitales» (AFIS) ou «système automatisé d'identification par données biométriques» (ABIS).

personne dans différents systèmes centraux. Sans BMS partagé, aucun des trois autres éléments ne pourra fonctionner.

3) Le **répertoire commun de données d'identité (CIR)** serait l'élément partagé pour le stockage des données d'identité biographiques[24] et biométriques des ressortissants de pays tiers enregistrés dans Eurodac, le VIS, le futur EES, l'ETIAS proposé et le système ECRIS-TCN proposé. Chacun de ces cinq systèmes centraux stocke ou stockera des données biographiques relatives à des personnes spécifiques pour des raisons spécifiques. Cela ne changerait pas. Les données d'identité pertinentes seraient stockées dans le CIR mais continueraient d'«appartenir» aux systèmes sous-jacents respectifs les ayant enregistrées.

Le CIR ne contiendrait pas les données du SIS. L'architecture technique complexe du SIS, qui comprend des copies nationales, des copies nationales partielles et d'éventuels systèmes nationaux d'établissement de correspondances biométriques, rendrait le CIR tellement complexe qu'il ne serait plus techniquement et financièrement réalisable.

L'objectif principal du CIR est de faciliter l'identification biographique d'un ressortissant de pays tiers. Il accélérerait les opérations, améliorerait l'efficacité et permettrait des économies d'échelle. La création du CIR est nécessaire à la réalisation de contrôles d'identité efficaces sur les ressortissants de pays tiers, y compris sur le territoire d'un État membre. De plus, l'ajout d'une «fonctionnalité d'indicateur de concordance» au CIR permettrait de vérifier la présence (ou l'absence) de données dans tous les systèmes couverts par le CIR au moyen d'une simple indication de concordance/non-concordance. Ainsi, le CIR contribuerait également à simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive, tout en conservant des garanties élevées en matière de protection des données (voir ci-dessous la section sur l'approche en deux étapes de l'accès à des fins répressives).

Parmi les cinq systèmes qui doivent être couverts par le CIR, le futur EES, l'ETIAS proposé et le système ECRIS-TCN proposé sont des nouveaux systèmes qui doivent encore être développés. L'actuel Eurodac ne contient pas de données biographiques; cette extension sera développée une fois la nouvelle base juridique d'Eurodac adoptée. Le VIS actuel contient bien des données biographiques, mais les interactions nécessaires entre le VIS et le futur EES exigeront une mise à niveau du VIS existant. La création du CIR aurait donc lieu au bon moment. Elle n'impliquerait en aucun cas de dupliquer les données existantes. D'un point de vue technique, le CIR serait développé sur la base de la plateforme EES/ETIAS.

4) Le **détecteur d'identités multiples (MID)** vérifierait si les données d'identité recherchées existent dans plus d'un des systèmes qui y seraient connectés. Le MID couvre les systèmes qui stockent des données d'identité dans le CIR (Eurodac, le VIS, le futur EES, l'ETIAS proposé et le système ECRIS-TCN proposé) ainsi que le SIS. Le MID permettrait de détecter les identités multiples liées au même ensemble de données biométriques, dans le double objectif de garantir l'identification correcte des personnes de bonne foi et de lutter contre la fraude à l'identité.

[24] Les données biographiques pouvant figurer sur les documents de voyage comprennent: le nom, le prénom, le sexe, la date de naissance, le numéro du document de voyage. Elles ne comprennent pas les adresses, les anciens noms, les données biométriques, etc.

Le MID permettrait d'établir que différents noms appartiennent à la même identité. Il constitue une innovation nécessaire afin de traiter efficacement le problème de l'utilisation frauduleuse d'identités, qui représente une grave atteinte à la sécurité. Le MID se limiterait à montrer les fiches d'identité biographique ayant un lien dans différents systèmes centraux. Ces liens seraient détectés à l'aide du service partagé d'établissement de correspondances biométriques sur la base des données biométriques et ils devraient être confirmés ou rejetés par l'autorité qui a enregistré les données dans le système d'information ayant entraîné la création du lien. Afin d'aider les utilisateurs autorisés du MID dans cette tâche, le système devrait classer les liens repérés en quatre catégories:

- lien jaune: possibilité d'identités biographiques différentes pour une même personne
- lien blanc: confirmation que les différentes identités biographiques appartiennent à une même personne de bonne foi
- lien vert: confirmation que différentes personnes de bonne foi se trouvent partager la même identité biographique
- lien rouge: soupçon qu'une même personne utilise illicitement différentes identités biographiques.

La présente proposition décrit les procédures qui seraient mises en place afin de gérer ces différentes catégories. Toute ambiguïté relative à l'identité de personnes de bonne foi concernées devrait être levée aussi rapidement que possible, en transformant le lien jaune en un lien vert ou blanc confirmé, afin de garantir qu'elles ne subiront plus de désagréments inutiles. À l'inverse, lorsque l'évaluation conduit à confirmer un lien rouge, ou à transformer un lien jaune en lien rouge, il convient d'agir en conséquence.

• **L'approche en deux étapes de l'accès à des fins répressives, prévue par le répertoire commun de données d'identité**

La répression est définie comme un objectif secondaire ou accessoire d'Eurodac, du VIS, du futur EES et de l'ETIAS proposé. Par conséquent, la possibilité d'accéder aux données stockées dans ces systèmes à des fins répressives est limitée. Les services répressifs ne peuvent consulter directement ces systèmes d'information à finalité non répressive qu'à des fins de prévention et de détection du terrorisme et d'autres infractions pénales graves, ou d'enquêtes et de poursuites en la matière. De plus, les systèmes respectifs sont régis par des conditions d'accès et des garanties différentes et certaines des règles actuelles pourraient ralentir l'utilisation légitime de ces systèmes par ces services. De manière plus générale, le principe de la recherche préalable limite la possibilité pour les services des États membres de consulter les systèmes à des fins répressives justifiées et pourrait se traduire par des occasions manquées de mettre au jour des informations nécessaires.

Dans sa communication d'avril 2016, la Commission a reconnu qu'il était nécessaire d'optimiser les outils existants à des fins répressives, tout en respectant les exigences relatives à la protection des données. Cette nécessité a été confirmée et réaffirmée par les États membres et les agences compétentes dans le cadre du groupe d'experts de haut niveau.

Eu égard à ce qui précède, en créant le CIR avec une fonctionnalité dite d'«indicateur de concordance», la présente proposition introduit la possibilité d'accéder à l'EES, au VIS, à l'ETIAS et à Eurodac selon une **approche de la consultation des données en deux étapes**.

Cette approche en deux étapes ne changerait pas le fait que la répression est un objectif strictement accessoire de ces systèmes et qu'il convient donc de respecter des règles d'accès rigoureuses.

Dans un premier temps, l'agent des services répressifs lancerait une recherche portant sur une personne spécifique à l'aide des données d'identité, des données du document de voyage ou des données biométriques de cette personne afin de vérifier si des informations relatives à celle-ci sont stockées dans le CIR. Si tel est le cas, l'agent recevra **une réponse indiquant le ou les systèmes d'information de l'UE qui contiennent des données** relatives à cette personne (l'**indicateur de concordance**). L'agent n'aurait pas effectivement accès aux données se trouvant dans les systèmes sous-jacents.

Dans un second temps, l'agent peut émettre une demande individuelle d'accès à chaque système qui lui a été signalé comme contenant des données, en vue d'obtenir le dossier complet concernant la personne en question, **dans le respect des règles et procédures existantes établies par chacun des systèmes concernés**. Un tel accès dans le cadre de la deuxième étape resterait subordonné à l'autorisation préalable d'une autorité désignée et continuerait à nécessiter un identifiant d'utilisateur spécifique et l'enregistrement des consultations.

Cette nouvelle approche apporterait également une valeur ajoutée aux services répressifs grâce à l'**existence de liens potentiels** dans le MID. Le MID aiderait le CIR à détecter les liens existants, renforçant encore ainsi la précision de la recherche. Le MID serait en mesure d'indiquer si la personne est **connue sous différentes identités** dans différents systèmes d'information.

L'approche de la consultation des données en deux étapes est particulièrement utile dans les cas où le suspect, l'auteur ou la victime présumée d'une infraction terroriste ou d'une autre infraction pénale grave **n'est pas connu**. En effet, dans de tels cas, le CIR permettrait de déterminer quel système d'information connaît la personne en une seule recherche. De ce fait, les conditions existantes concernant les recherches préalables dans les bases de données nationales et les recherches préalables dans le système automatisé d'identification par empreintes digitales d'autres États membres, prévues par la décision 2008/615/JAI («vérification Prüm»), deviennent redondantes.

La nouvelle approche de consultation en deux étapes n'**entrerait en vigueur qu'une fois les éléments** d'interopérabilité nécessaires **pleinement opérationnels**.

- **Éléments supplémentaires de la présente proposition à l'appui des éléments d'interopérabilité**

1) Outre les éléments susmentionnés, le présent projet de règlement propose également de créer un **répertoire central des rapports et statistiques (CRRS)**. Ce répertoire est nécessaire pour permettre la création et l'échange de rapports contenant des données statistiques (anonymes) à des fins stratégiques, opérationnelles et de qualité des données. La pratique actuelle consistant à collecter des données statistiques uniquement auprès des différents systèmes d'information nuit à la sécurité des données et aux performances et ne permet pas d'établir des corrélations entre les données provenant de différents systèmes.

Le CRRS constituerait un répertoire spécifique et séparé pour les statistiques anonymes extraites du SIS, du VIS, d'Eurodac, du futur EES, de l'ETIAS proposé, du système ECRIS-TCN proposé, du répertoire commun de données d'identité, du détecteur d'identités multiples et du service partagé d'établissement de correspondances biométriques. Le répertoire permettrait de partager en toute sécurité les rapports (prévus par les instruments juridiques respectifs) avec les États membres, la Commission (y compris Eurostat) et les agences de l'Union.

Le développement d'un répertoire central plutôt que de répertoires distincts pour chaque système réduirait les coûts et les efforts nécessaires à sa création, son exploitation et sa mise à jour. La sécurité des données en serait également renforcée, étant donné que les données sont stockées et que le contrôle des accès est géré dans un seul répertoire.

2) Le présent projet de règlement propose également d'établir le **format universel pour les messages (UMF)** en tant que norme utilisée au niveau de l'Union pour organiser les interactions entre les différents systèmes de manière interopérable, y compris les systèmes développés et gérés par l'eu-LISA. Europol et Interpol seraient également encouragés à utiliser la norme.

La norme UMF introduit un langage technique commun et unifié afin de décrire et de relier des éléments de données, notamment les éléments portant sur les personnes et les documents (de voyage). Le recours à l'UMF lors du développement de nouveaux systèmes d'information facilite l'intégration et l'interopérabilité avec les autres systèmes, notamment pour les États membres ayant besoin de créer des interfaces afin de communiquer avec ces nouveaux systèmes. À cet égard, il est possible de considérer que l'utilisation obligatoire de l'UMF lors du développement de nouveaux systèmes constitue une condition préalable à l'introduction des éléments d'interopérabilité proposés dans le présent règlement.

Une structure de gouvernance appropriée est proposée afin de garantir le déploiement total de la norme UMF dans l'ensemble de l'UE. La Commission serait chargée de l'établissement et du développement de la norme UMF dans le cadre d'une procédure d'examen avec les États membres. Les pays associés à l'espace Schengen, les agences de l'Union et les organismes internationaux participant aux projets UMF (comme l'eu-LISA, Europol et Interpol) seront également impliqués. La structure de gouvernance proposée est vitale pour l'UMF afin de pouvoir étendre et développer la norme tout en garantissant une fonctionnalité et une applicabilité maximales.

3) Le présent projet de règlement introduit également les concepts de **mécanismes automatisés de contrôle de la qualité des données** et d'indicateurs communs de qualité, ainsi que la nécessité pour les États membres de garantir le niveau le plus élevé de qualité des données lorsqu'ils alimentent et utilisent les systèmes. Si les données ne sont pas de la plus haute qualité, cela peut avoir pour conséquence non seulement d'empêcher l'identification des personnes recherchées, mais également de porter atteinte aux droits fondamentaux de personnes innocentes. Afin de résoudre les problèmes éventuels liés à la saisie de données par des opérateurs humains, des règles de validation automatique peuvent empêcher les opérateurs de commettre des erreurs. L'objectif serait de repérer automatiquement les communications de données manifestement incorrectes ou incohérentes afin que l'État membre qui en est à l'origine puisse vérifier les données et

mettre en œuvre les mesures correctives nécessaires. Des rapports réguliers sur la qualité des données, devant être produits par l'eu-LISA, viendraient compléter ce mécanisme.

- **Conséquences pour d'autres instruments juridiques**

De même que la proposition complémentaire, le présent projet de règlement introduit des innovations qui nécessiteront de modifier d'autres instruments juridiques:

- le règlement (UE) 2016/399 (le «code frontières Schengen»)
- le règlement (UE) 2017/2226 (le «règlement EES»)
- le règlement (CE) nº 767/2008 (le «règlement VIS»)
- la décision 2004/512/CE du Conseil (la «décision VIS»)
- la décision 2008/633/JAI du Conseil (la «décision VIS/accès à des fins répressives»)
- [le règlement ETIAS]
- [le règlement Eurodac]
- [les règlements SIS]
- [le règlement ECRIS-TCN, y compris les dispositions correspondantes du règlement (UE) 2016/1624 (règlement relatif au corps européen de garde-frontières et de garde-côtes)]
- [le règlement eu-LISA]

La présente proposition et la proposition complémentaire contiennent des dispositions détaillées concernant les modifications qu'il est nécessaire d'apporter aux instruments juridiques qui sont actuellement des textes stables adoptés par les colégislateurs: le code frontières Schengen, le règlement EES, le règlement VIS, la décision 2008/633/JAI du Conseil et la décision 2004/512/CE du Conseil.

Les autres instruments énumérés (les règlements ETIAS, Eurodac, SIS, ECRIS-TCN, eu-LISA) sont en cours de négociation au Parlement européen et au Conseil. Il n'est donc pas possible à ce stade de prévoir les modifications nécessaires de ces instruments. La Commission présentera ces modifications pour chacun des instruments en question dans les deux semaines suivant la conclusion d'un accord politique concernant les projets de règlement respectifs.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition s'inscrit dans le cadre du processus plus large lancé par la communication d'avril 2016 intitulée «*Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*», et des travaux du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité qui ont suivi. Le but est de poursuivre trois objectifs:

a) renforcer et optimiser les avantages des **systèmes d'information existants**;

b) combler les lacunes en matière d'information en créant de nouveaux systèmes d'information;

c) améliorer l'interopérabilité de ces systèmes.

En ce qui concerne le premier objectif, la Commission a adopté en décembre 2016 des propositions visant à renforcer le système d'information Schengen (SIS) existant[25]. En ce qui concerne Eurodac, à la suite de la proposition de la Commission de mai 2016[26], les négociations portant sur la base juridique révisée ont été accélérées. Une proposition de nouvelle base juridique pour le système d'information sur les visas (VIS) est également en cours de préparation et sera présentée au cours du deuxième trimestre de 2018.

En ce qui concerne le deuxième objectif, les négociations portant sur la proposition de la Commission d'avril 2016 visant à établir un système d'entrée/de sortie (EES)[27] ont été conclues dès juillet 2017, lorsque les colégislateurs sont parvenus à un accord politique qui a été confirmé par le Parlement européen en octobre 2017 et formellement adopté par le Conseil en novembre 2017. La base juridique entrera en vigueur en décembre 2017. Les négociations portant sur la proposition de novembre 2016 visant à créer un système européen d'information et d'autorisation concernant les voyages (ETIAS)[28] ont commencé et devraient s'achever dans les prochains mois. En juin 2017, la Commission a proposé une base juridique afin de combler une autre lacune en matière d'information: le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (système ECRIS-TCN)[29]. Une fois encore, les colégislateurs ont indiqué qu'ils s'efforceraient d'adopter rapidement cette base juridique.

La présente proposition répond au troisième objectif défini dans la communication d'avril 2016.

- **Cohérence avec les autres politiques de l'Union dans le domaine de la justice et des affaires intérieures**

La présente proposition et la proposition complémentaire font suite et se conforment à l'agenda européen en matière de migration et aux communications ultérieures, notamment la communication intitulée «Préserver et renforcer Schengen»[30], le programme européen en matière de sécurité[31] et les travaux et rapports d'avancement de la Commission sur la mise en place d'une union de la sécurité réelle et effective[32]. Elle est cohérente avec les autres politiques de l'Union, en particulier:

- sécurité intérieure: le programme européen en matière de sécurité déclare que des normes communes élevées pour la gestion des frontières sont essentielles à la prévention de la criminalité transfrontière et du terrorisme. La présente proposition contribue à atteindre un niveau élevé de sécurité intérieure en donnant aux autorités les moyens d'accéder de manière rapide, continue, systématique et contrôlée aux informations dont elles ont besoin;
- asile: la proposition concerne Eurodac en tant que l'un des systèmes centraux de l'Union devant être couverts par l'interopérabilité;

[25] COM(2016) 883 final.
[26] COM(2016) 272 final.
[27] COM(2016) 194 final.
[28] COM(2016) 731 final.
[29] COM(2017) 344 final.
[30] COM(2017) 570 final.
[31] COM(2015) 185 final.
[32] COM(2016) 230 final.

- gestion des frontières extérieures et sécurité: la présente proposition renforce les systèmes SIS et VIS, qui contribuent à un contrôle efficace des frontières extérieures de l'Union, de même que le futur EES, l'ETIAS proposé et le système ECRIS-TCN proposé.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La proposition se fonde principalement sur les articles suivants du traité sur le fonctionnement de l'Union européenne: l'article 16, paragraphe 2, l'article 74, l'article 78, paragraphe 2, point e), l'article 79, paragraphe 2, point c), l'article 82, paragraphe 1, point d), l'article 85, paragraphe 1, l'article 87, paragraphe 2, point a), et l'article 88, paragraphe 2.

En vertu de l'article 16, paragraphe 2, l'Union dispose du pouvoir d'adopter les mesures liées à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et les règles relatives à la libre circulation de ces données. En vertu de l'article 74, le Conseil peut adopter des mesures pour assurer une coopération administrative entre les services compétents des États membres dans le domaine de la justice, de la liberté et de la sécurité. En vertu de l'article 78, l'Union dispose du pouvoir d'adopter des mesures relatives à un système européen commun d'asile. En vertu de l'article 79, paragraphe 2, point c), l'Union dispose du pouvoir d'adopter des mesures dans le domaine de l'immigration clandestine et du séjour irrégulier. En vertu de l'article 82, paragraphe 1, point d), et de l'article 87, paragraphe 2, point a), l'Union dispose du pouvoir d'adopter des mesures visant à renforcer la coopération policière et judiciaire en ce qui concerne la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes. En vertu de l'article 85, paragraphe 1, et de l'article 88, paragraphe 2, l'Union dispose du pouvoir de déterminer les tâches d'Eurojust et d'Europol, respectivement.

• Subsidiarité

La libre circulation au sein de l'UE nécessite une gestion efficace des frontières extérieures de l'Union afin de garantir la sécurité. Les États membres sont donc convenus de répondre collectivement à ces défis, notamment en partageant des informations au moyen de systèmes d'information centralisés de l'UE dans le domaine de la justice et des affaires intérieures. Les différentes conclusions adoptées par le Conseil européen et par le Conseil, notamment depuis 2015, en témoignent.

L'absence de contrôles aux frontières intérieures nécessite une gestion solide des frontières extérieures de l'espace Schengen, dans le cadre de laquelle chaque État membre ou pays associé à l'espace Schengen doit contrôler sa frontière extérieure au nom des autres États de l'espace Schengen. Par conséquent, aucun État membre ne peut faire face à lui seul à l'immigration irrégulière et à la criminalité transfrontière. Les ressortissants de pays tiers qui entrent dans l'espace sans contrôles aux frontières intérieures peuvent s'y déplacer librement. Dans un espace sans frontières intérieures, les mesures contre l'immigration irrégulière et la criminalité et le terrorisme internationaux, y compris la détection des fraudes à l'identité, devraient être prises en commun et ces questions ne peuvent trouver une réponse efficace qu'au niveau de l'Union.

Des systèmes d'information communs essentiels sont en place au niveau de l'UE ou sont en train d'être mis en place. L'interopérabilité renforcée de ces systèmes d'information implique nécessairement une action au niveau de l'Union. Une efficacité améliorée et l'utilisation de systèmes centralisés gérés par l'eu-LISA sont au cœur de la présente proposition. En raison de l'échelle, des effets et de l'incidence des actions envisagées, les objectifs fondamentaux ne peuvent être atteints de manière efficace et systématique qu'au niveau de l'Union.

- **Proportionnalité**

Comme l'explique de manière très détaillée l'analyse d'impact accompagnant la présente proposition de règlement, les choix politiques opérés dans cette proposition sont considérés comme proportionnés. Ils n'excèdent pas ce qui est nécessaire pour atteindre les objectifs convenus.

Le **portail de recherche européen (ESP)** est un outil nécessaire afin de renforcer l'utilisation autorisée des systèmes d'information de l'UE existants et futurs. L'impact de l'ESP en matière de traitement des données est très limité. Il ne stockera aucune donnée, à l'exception des informations concernant les différents profils d'utilisateurs de l'ESP et les données et systèmes d'information auxquels ceux-ci ont accès, en conservant une trace de leur utilisation par voie d'enregistrement. Le rôle de l'ESP en tant que courtier de messages, instrument et facilitateur est proportionné, nécessaire et limité en ce qui concerne les recherches et les droits d'accès en vertu des bases juridiques relatives aux systèmes d'information et du règlement proposé en matière d'interopérabilité.

Le **service partagé d'établissement de correspondances biométriques (BMS partagé)** est nécessaire au fonctionnement de l'ESP, du répertoire commun de données d'identité et du détecteur d'identités multiples et il facilite l'utilisation et la maintenance des systèmes d'information de l'UE pertinents existants et futurs. Ses fonctionnalités permettent d'effectuer des recherches sur des données biométriques provenant de différentes sources de manière efficace, continue et systématique. Les données biométriques sont stockées et conservées par les systèmes sous-jacents. Le BMS partagé crée des modèles mais supprime les images réelles. Les données ne sont donc stockées qu'à un endroit et une seule fois.

Le **répertoire commun de données d'identité (CIR)** est nécessaire afin d'atteindre l'objectif consistant à identifier correctement tout ressortissant de pays tiers, par exemple lors d'un contrôle d'identité au sein de l'espace Schengen. Le CIR appuie également le fonctionnement du détecteur d'identités multiples et représente donc un élément nécessaire pour atteindre le double objectif de faciliter les contrôles d'identité des voyageurs de bonne foi et de lutter contre la fraude à l'identité. L'accès au CIR à ces fins est limité aux utilisateurs qui ont besoin de ces informations pour mener à bien leurs missions (ce qui implique que ces contrôles deviennent un nouvel objectif accessoire d'Eurodac, du VIS, du futur EES, de l'ETIAS proposé et du système ECRIS-TCN proposé). Les traitements de données sont strictement limités à ce qui est nécessaire pour atteindre cet objectif; de plus, des garanties appropriées seront mises en place afin de garantir que les droits d'accès sont respectés et que les données stockées dans le CIR sont réduites au minimum nécessaire. Afin de garantir la minimisation des données et d'éviter la duplication injustifiée des données, le CIR détient les données biographiques nécessaires de chacun de ses systèmes sous-jacents, qui sont stockées, ajoutées, modifiées et supprimées conformément à leur base juridique respective, sans les copier. Les conditions relatives à la conservation des données sont totalement alignées sur les dispositions prévues en la matière par les systèmes d'information sous-jacents fournissant les données d'identité.

Le **détecteur d'identités multiples (MID)** est nécessaire afin de fournir une solution pour la détection d'identités multiples, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité. Le MID contiendra les liens entre les personnes figurant dans plus d'un système d'information central, qui se limiteront strictement aux données nécessaires pour vérifier si une personne est licitement ou illicitement enregistrée sous différentes identités biographiques dans différents systèmes, mais également pour démontrer que deux personnes ayant des données biographiques similaires peuvent ne pas être une seule et même personne. Le traitement des données au moyen du MID et du BMS partagé en vue de relier des dossiers individuels de différents systèmes est limité au strict minimum. Le MID contiendra des garanties contre les possibles discriminations ou décisions défavorables pour les personnes ayant des identités licites multiples.

- **Choix de l'instrument**

Un règlement du Parlement européen et du Conseil est proposé. La législation proposée traite directement du fonctionnement des systèmes d'information centraux de l'UE pour les frontières et la sécurité, qui ont tous été créés par des règlements ou dont la création a été proposée sous cette forme. De même, l'eu-LISA, qui sera chargée de la conception et du développement des différents éléments, puis en temps utile de leur gestion technique, a été créée par un règlement. Un règlement est donc l'instrument approprié.

3. RÉSULTATS DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Consultation publique**

En vue de préparer la présente proposition, la Commission a lancé en juillet 2017 une consultation publique afin de recueillir les avis des parties intéressées concernant l'interopérabilité. La consultation a reçu 18 réponses provenant de différentes parties prenantes, y compris des gouvernements d'États membres, des organisations du secteur privé, d'autres organisations telles que des ONG et des groupes de réflexion, ainsi que de simples citoyens[33]. De manière générale, les répondants se sont largement exprimés en faveur des principes sous-jacents de la présente proposition relative à l'interopérabilité. La grande majorité des répondants a convenu que la consultation avait identifié les bons problèmes et que les objectifs poursuivis par le train de mesures relatif à l'interopérabilité étaient corrects. Plus particulièrement, les répondants ont estimé que les options décrites dans le document de consultation permettraient:

- d'aider le personnel œuvrant sur le terrain à avoir accès aux informations nécessaires;
- d'éviter la duplication des données, de réduire les chevauchements et de mettre en évidence les divergences dans les données;
- d'identifier les personnes de manière plus fiable, y compris les personnes ayant des identités multiples, et de réduire la fraude à l'identité.

Une grande majorité des répondants a soutenu chacune des options envisagées et estimé qu'elles sont nécessaires pour atteindre les objectifs de la présente initiative; dans leur réponse, ils ont souligné que des mesures fortes et claires en matière de protection des données étaient nécessaires, notamment en ce qui concerne l'accès aux informations stockées

[33] Le rapport de synthèse annexé à l'analyse d'impact contient davantage de détails.

dans les systèmes et la conservation des données, et qu'il fallait des données actualisées et de qualité élevée dans les systèmes et des mesures le garantissant.

L'ensemble des points soulevés a été pris en compte lors de l'élaboration de la présente proposition.

- **Enquête Eurobaromètre**

En juin 2017, une enquête Eurobaromètre spéciale[34] a été réalisée, qui a montré que la stratégie de l'Union consistant à partager des informations au niveau de l'Union afin de lutter contre la criminalité et le terrorisme bénéficiait d'un large soutien public: la quasi-totalité des répondants (92 %) estime que les autorités nationales devraient partager des informations avec les autorités des autres États membres afin de mieux lutter contre la criminalité et le terrorisme.

Une large majorité (69 %) des répondants a déclaré que la police et les autres services répressifs nationaux devraient partager des informations avec les autres pays de l'Union de manière systématique. Dans l'ensemble des États membres, une majorité des répondants estime que des informations devraient être échangées dans tous les cas.

- **Groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité**

Ainsi que cela a déjà été indiqué dans l'introduction, la présente proposition est fondée sur les recommandations du **groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité**[35]. Ce groupe a été créé en juin 2016 dans le but d'examiner les défis juridiques, techniques et opérationnels des options envisagées afin d'atteindre l'interopérabilité des systèmes centraux de l'UE pour les frontières et la sécurité. Le groupe a adopté une approche large et globale de l'architecture de la gestion des données appliquée à la gestion des frontières et à la répression, en tenant également compte des rôles, responsabilités et systèmes pertinents pour les autorités douanières.

Le groupe se composait d'experts des États membres et des pays associés à l'espace Schengen, ainsi que des agences de l'UE suivantes: l'eu-LISA, Europol, le Bureau européen d'appui en matière d'asile, l'Agence européenne de garde-frontières et de garde-côtes et l'Agence des droits fondamentaux de l'Union européenne. Le coordinateur de l'UE pour la lutte contre le terrorisme et le Contrôleur européen de la protection des données ont également participé aux travaux du groupe d'experts en tant que membres à part entière. En outre, des représentants du secrétariat de la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen et du secrétariat général du Conseil étaient présents en tant qu'observateurs.

Le **rapport final du groupe d'experts de haut niveau** a été publié en mai 2017[36]. Il souligne la nécessité d'agir afin de combler les lacunes structurelles recensées dans la communication

[34] Le rapport sur *L'attitude des Européens à l'égard de la sécurité* analyse les résultats de l'étude d'opinion publique spéciale de l'Eurobaromètre (464b) concernant les connaissances, les expériences et les perceptions globales des citoyens en matière de sécurité. L'étude a été réalisée par le réseau TNS Political & Social dans les 28 États membres entre le 13 et le 26 juin 2017. Quelque 28 093 citoyens de l'UE issus de différentes catégories sociales et démographiques ont été interrogés.

[35] Décision de la Commission du 17 juin 2016 instituant le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité – 2016/C 257/03.

[36] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

d'avril 2016. Il définit un ensemble de recommandations visant à renforcer et à développer les systèmes d'information de l'UE et leur interopérabilité. Il conclut qu'il est **nécessaire et techniquement faisable d'œuvrer à la réalisation du portail de recherche européen, du service partagé d'établissement de correspondances biométriques et du répertoire commun de données d'identité en tant que solutions d'interopérabilité**, qui peuvent, en principe, apporter des bénéfices opérationnels et être mises en place conformément aux exigences en matière de protection des données. Le groupe a également recommandé d'envisager l'option supplémentaire que constitue une approche en deux étapes de l'accès à des fins répressives, fondée sur une fonctionnalité d'indication de concordance.

Le présent projet de règlement répond également aux recommandations du groupe d'experts de haut niveau en ce qui concerne la qualité des données, le format universel pour les messages (UMF) et la création d'un entrepôt de données [présenté ici comme le répertoire central des rapports et statistiques (CRRS)].

Le quatrième élément d'interopérabilité proposé dans le présent projet de règlement (le détecteur d'identités multiples) n'a pas été mentionné par le groupe d'experts de haut niveau mais est apparu lors de l'analyse technique supplémentaire et de l'évaluation de la proportionnalité réalisées par la Commission.

- **Études techniques**

Trois études ont été commandées à l'appui de l'élaboration de la proposition. Dans le cadre d'un contrat conclu avec la Commission, Unisys a réalisé un rapport portant sur une étude de faisabilité du portail de recherche européen. L'eu-LISA a commandé à Gartner (en collaboration avec Unisys) un rapport technique visant à soutenir le développement du service partagé d'établissement de correspondances biométriques. PWC a fourni à la Commission un rapport technique sur le répertoire commun de données d'identité.

- **Analyse d'impact**

La présente proposition s'appuie sur une analyse d'impact, présentée dans le document de travail des services de la Commission qui l'accompagne [SWD(2017) XXX].

Le comité d'examen de la réglementation a examiné le projet d'analyse d'impact lors de sa réunion du 6 décembre 2017 et a rendu son avis (favorable avec des réserves) le 8 décembre, en indiquant que l'analyse d'impact devait être ajustée afin d'intégrer les recommandations du comité concernant certains aspects spécifiques. Ces recommandations portaient tout d'abord sur des mesures supplémentaires dans le cadre de l'option privilégiée, afin de simplifier les droits d'accès existants des utilisateurs finaux aux données contenues dans les systèmes d'information de l'UE et d'illustrer les garanties associées aux fins de la protection des données et des droits fondamentaux. Le deuxième aspect principal concernait la clarification de l'intégration du système d'information Schengen dans le cadre de l'option 2, y compris l'efficacité et les coûts, afin d'en faciliter la comparaison avec l'option privilégiée 3. La Commission a mis à jour son analyse d'impact afin de répondre à ces principales considérations et à un certain nombre d'autres commentaires formulés par le comité.

L'analyse d'impact a examiné si et de quelle manière chacun des objectifs déterminés pouvait être atteint à l'aide d'un ou plusieurs des éléments techniques recensés par le groupe d'experts de haut niveau et au moyen d'une analyse ultérieure. Le cas échéant, elle s'est également penchée sur les sous-options nécessaires pour atteindre ces objectifs, tout en respectant le cadre de la protection des données. L'analyse d'impact a conclu ce qui suit:

- Pour répondre à l'objectif consistant à fournir aux utilisateurs autorisés un accès rapide, continu, systématique et contrôlé aux systèmes d'information pertinents, il convient de créer un portail de recherche européen (ESP), fondé sur un service partagé d'établissement de correspondances biométriques (BMS partagé), afin d'interroger toutes les bases de données.
- Pour répondre à l'objectif consistant à faciliter les contrôles d'identité des ressortissants de pays tiers réalisés sur le territoire d'un État membre par des agents autorisés, il convient de créer un répertoire commun de données d'identité (CIR), contenant l'ensemble minimal de données d'identification et s'appuyant sur le même BMS partagé.
- Pour répondre à l'objectif consistant à détecter les identités multiples liées au même ensemble de données biométriques, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité, il convient de créer un détecteur d'identités multiples (MID), contenant des liens entre les identités multiples dans différents systèmes.
- Pour répondre à l'objectif consistant à faciliter et à simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive à des fins de prévention et de détection des infractions graves et du terrorisme, ou d'enquêtes et de poursuites en la matière, il convient d'ajouter une fonctionnalité d'indicateur de concordance au CIR.

Puisque tous les objectifs doivent être atteints, la **solution complète est la combinaison de l'ESP, du CIR (avec une indication de concordance) et du MID, tous s'appuyant sur le BMS partagé**.

La principale conséquence positive sera l'amélioration de la gestion des frontières et une sécurité intérieure accrue au sein de l'Union européenne. Les nouveaux éléments simplifieront et accéléreront l'accès des autorités nationales aux informations nécessaires ainsi que l'identification des ressortissants de pays tiers. Ils permettront aux autorités d'établir des liens croisés entre les informations nécessaires déjà existantes sur les personnes lors des vérifications aux frontières, des demandes de visa ou d'asile et des activités de police. Cela donnera accès à des informations permettant de prendre des décisions fiables, qu'il s'agisse d'enquêtes concernant des infractions graves ou des affaires de terrorisme ou de décisions dans le domaine de la migration et de l'asile. Bien qu'elles ne touchent pas directement les ressortissants de l'Union (les mesures proposées se concentrent principalement sur les ressortissants de pays tiers dont les données sont stockées dans un système d'information centralisé de l'UE), les propositions devraient renforcer la confiance du grand public en garantissant que leur conception et leur utilisation améliorent la sécurité des citoyens de l'Union.

Les incidences financières et économiques immédiates de la proposition se limiteront à la conception, au développement et à l'exploitation des nouvelles installations. Les coûts pèseront sur le budget de l'Union et sur les autorités des États membres exploitant les systèmes. L'incidence sur le tourisme sera positive car les mesures proposées amélioreront la sécurité au sein de l'Union européenne tout en accélérant les contrôles aux frontières. De même, l'incidence sur les aéroports, les ports et les transporteurs devrait être positive, notamment grâce à l'accélération des contrôles aux frontières.

- **Droits fondamentaux**

L'analyse d'impact s'est notamment intéressée aux incidences des mesures proposées sur les droits fondamentaux, et notamment sur le droit à la protection des données.

Conformément à la charte des droits fondamentaux de l'Union, que les institutions de l'Union et les États membres doivent respecter lorsqu'ils appliquent le droit de l'Union (article 51, paragraphe 1, de la charte), les opportunités offertes par l'interopérabilité en tant que mesure d'amélioration de la sécurité et de la protection des frontières extérieures doivent être mises en balance avec l'obligation de garantir que les atteintes aux droits fondamentaux qui peuvent découler du nouvel environnement d'interopérabilité se limitent à ce qui est strictement nécessaire afin d'atteindre effectivement les objectifs d'intérêt général poursuivis, sous réserve du principe de proportionnalité (article 52, paragraphe 1, de la charte).

Les solutions d'interopérabilité proposées sont des éléments complémentaires des systèmes existants. En tant que telles, elles ne modifieront pas l'équilibre déjà garanti par chacun des systèmes centraux existants en ce qui concerne leur incidence positive sur les droits fondamentaux.

L'interopérabilité pourrait néanmoins avoir une incidence indirecte supplémentaire sur un certain nombre de droits fondamentaux. En effet, l'identification correcte d'une personne a une incidence positive sur le droit au respect de la vie privée, et notamment sur le droit à l'identité (article 7 de la charte), car elle contribue à éviter les confusions d'identité. En revanche, procéder à des vérifications sur la base de données biométriques peut être perçu comme une atteinte au droit à la dignité (notamment lorsque cela est perçu comme humiliant) (article 1er). Toutefois, dans une enquête[37] réalisée par l'Agence des droits fondamentaux de l'Union européenne, il a précisément été demandé aux répondants s'ils estimaient que fournir leurs données biométriques dans le cadre du contrôle aux frontières pourrait être humiliant. La majorité des répondants a répondu par la négative.

Les éléments d'interopérabilité proposés donnent la possibilité d'adopter des mesures préventives ciblées afin d'améliorer la sécurité. Ils peuvent ainsi contribuer à protéger le droit des personnes à la vie (article 2 de la charte), qui implique également que les autorités ont l'obligation positive d'adopter des mesures opérationnelles préventives afin de protéger toute personne dont la vie serait en péril, si elles ont ou devraient avoir connaissance de l'existence d'un risque immédiat[38], et de faire respecter l'interdiction de l'esclavage et du travail forcé (article 5). Grâce à une identification fiable, plus accessible et plus aisée, l'interopérabilité peut contribuer à repérer les enfants disparus ou les enfants faisant l'objet de traite, ainsi qu'à une réaction rapide et ciblée.

Une identification fiable, plus accessible et plus aisée pourrait également contribuer à garantir que le droit d'asile (article 18 de la charte) et l'interdiction du refoulement (article 19 de la charte) sont bien respectés. L'interopérabilité pourrait même prévenir les situations dans lesquelles des demandeurs d'asile sont illégalement arrêtés, détenus et soumis à une expulsion injustifiée. De plus, grâce à l'interopérabilité, il sera plus facile de détecter la fraude à l'identité. Elle permettrait également de réduire le besoin de partager des données et des

[37] *Étude de la FRA dans le cadre du projet pilote eu-LISA sur les frontières intelligentes – avis et expériences des voyageurs concernant les frontières intelligentes*, rapport de l'Agence des droits fondamentaux de l'Union européenne: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_technical_report_annexes_en.pdf.

[38] Cour européenne des droits de l'homme, Osman c. Royaume-Uni, nº 87/1997/871/1083, 28 octobre 1998, point 116.

informations concernant les demandeurs d'asile avec des pays tiers (notamment le pays d'origine) en vue d'établir l'identité de la personne et d'obtenir des documents de voyage, ce qui pourrait mettre la personne concernée en danger.

- **Protection des données à caractère personnel**

Vu les données à caractère personnel impliquées, l'interopérabilité aura tout particulièrement une incidence sur le droit à la protection de ces données. L'article 8 de la charte, l'article 16 du traité sur le fonctionnement de l'Union européenne et l'article 8 de la convention européenne des droits de l'homme ont consacré ce droit. Ainsi que l'a souligné la Cour de justice de l'Union européenne[39], le droit à la protection des données à caractère personnel n'apparaît pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société[40]. La protection des données est étroitement liée au respect de la vie privée et familiale, protégé par l'article 7 de la charte.

Conformément au règlement général sur la protection des données[41], la libre circulation des données au sein de l'Union ne doit pas être limitée pour des motifs liés à la protection des données. Toutefois, une série de principes doivent être respectés. En effet, pour être légale, toute limitation de l'exercice des droits fondamentaux protégés par la charte doit être conforme aux critères suivants, prévus par l'article 52, paragraphe 1, de la charte:

- elle doit être prévue par la loi;
- elle doit respecter le contenu essentiel des droits;
- elle doit répondre effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui;
- elle doit être nécessaire, et
- elle doit être proportionnée.

La présente proposition est conforme à toutes ces règles de protection des données, comme l'explique en détail l'analyse d'impact qui l'accompagne. La proposition est fondée sur les principes de la protection des données dès la conception et par défaut. Elle inclut toutes les dispositions appropriées limitant le traitement des données à ce qui est nécessaire à son objectif spécifique et n'accordant l'accès aux données qu'aux entités qui ont «besoin d'en connaître». Les périodes de conservation des données (le cas échéant) sont appropriées et limitées. L'accès aux données est exclusivement réservé aux membres du personnel dûment autorisés des autorités des États membres ou des organes de l'Union compétents aux fins spécifiques de chaque système d'information et sa portée est limitée aux informations nécessaires pour l'exécution des missions conformément à ces fins.

---

[39] Arrêt de la Cour de justice de l'Union européenne du 9 novembre 2010 dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke et Eifert, non publié au Recueil.

[40] Conformément à l'article 52, paragraphe 1, de la charte, des limitations peuvent être imposées à l'exercice du droit à la protection des données, dans la mesure où elles sont prévues par la loi, respectent le contenu essentiel des droits et libertés et, dans le respect du principe de proportionnalité, sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui.

[41] 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).

4. INCIDENCE BUDGÉTAIRE

L'incidence budgétaire est indiquée dans la fiche financière figurant à l'annexe. Celle-ci couvre la période restante du cadre financier pluriannuel actuel (jusqu'en 2020) ainsi que les sept années de la période suivante (2021-2027). Le budget proposé pour les années 2021 et suivantes est indiqué à titre indicatif et ne préjuge pas du prochain cadre financier pluriannuel.

La mise en œuvre de la présente proposition nécessitera des dotations budgétaires pour:

(1) le **développement** et l'intégration par l'eu-LISA des quatre éléments d'interopérabilité et du répertoire central des rapports et statistiques ainsi que pour **leur maintenance et leur fonctionnement** ultérieurs;

(2) la **migration des données** vers le service partagé d'établissement de correspondances biométriques (BMS partagé) et le répertoire commun de données d'identité (CIR). Dans le cas du BMS partagé, les modèles biométriques des données correspondantes issues des trois systèmes qui utilisent actuellement des données biométriques (SIS, VIS et Eurodac) doivent être recréés dans le BMS partagé. Dans le cas du CIR, les éléments de données à caractère personnel issus du VIS doivent être transférés vers le CIR et les liens éventuellement découverts entre des identités contenues dans le SIS, le VIS et Eurodac doivent être validés. Ce dernier processus, en particulier, nécessite des ressources considérables;

(3) la mise à jour, par l'eu-LISA, de l'**interface uniforme nationale** (IUN), dont le règlement EES prévoit déjà de faire un élément générique permettant l'échange de messages entre les États membres et les systèmes centraux;

(4) l'**intégration des systèmes nationaux des États membres** avec l'IUN, qui véhiculera les messages échangés avec le CIR/le détecteur d'identités multiples au moyen du portail de recherche européen;

(5) la **formation** à l'utilisation des éléments d'interopérabilité par les utilisateurs finaux, notamment par l'intermédiaire de l'agence de l'Union européenne pour la formation des services répressifs (CEPOL).

La création et la maintenance des éléments d'interopérabilité sont effectuées en tant que programme. Tandis que le portail de recherche européen (ESP) et le détecteur d'identités multiples sont des éléments entièrement nouveaux, de même que le répertoire central des rapports et statistiques (CRRS), le BMS partagé et le CIR sont des éléments partagés qui combinent des données existantes qui sont (ou seront) détenues dans des systèmes existants ou nouveaux, pour lesquels des estimations budgétaires existent déjà.

L'**ESP** mettra en œuvre des interfaces existantes connues vers le SIS, le VIS et Eurodac et sera étendu en temps utile aux nouveaux systèmes.

L'ESP sera utilisé par les États membres et les agences au moyen d'une interface basée sur le format universel pour les messages (UMF). Cette nouvelle interface nécessitera des développements, des adaptations, des intégrations et des tests de la part des États membres, de l'eu-LISA, d'Europol et de l'Agence européenne de garde-frontières et de garde-côtes. L'ESP devrait utiliser les concepts d'interface uniforme nationale (IUN) introduits pour l'EES, ce qui réduirait les efforts d'intégration.

L'ESP entraînera des coûts supplémentaires pour Europol afin que l'interface QUEST puisse être utilisée avec les données ayant un niveau de protection minimum (BPL).

La base du **BMS partagé** sera de fait établie avec la création du nouvel EES, car celui-ci constitue de loin le volume de nouvelles données biométriques le plus important. Le budget nécessaire a été réservé en vertu de l'instrument juridique relatif à l'EES. L'ajout de nouvelles données biométriques provenant du VIS, du SIS et d'Eurodac au BMS partagé représente un coût supplémentaire, principalement lié à la migration de données existantes. Ce coût est estimé à 10 millions d'EUR pour les trois systèmes. L'ajout de nouvelles données biométriques provenant du système ECRIS-TCN proposé représente un coût supplémentaire limité, qui peut être couvert par les fonds réservés au titre de l'instrument juridique relatif au système ECRIS-TCN proposé pour créer un système automatisé d'identification par empreintes digitales.

Le répertoire commun de données d'identité sera établi avec la création du futur EES et sera élargi lors du développement de l'ETIAS proposé. Le stockage de ces données et les moteurs de recherche correspondants ont été inclus dans le budget réservé au titre des instruments juridiques relatif au futur EES et à l'ETIAS proposé. L'ajout de nouvelles données biographiques provenant d'Eurodac et du système ECRIS-TCN proposé représente un coût supplémentaire mineur, qui a déjà été réservé au titre des instruments juridiques relatifs à Eurodac et au système ECRIS-TCN proposé.

Le budget total nécessaire sur neuf ans (2019-2027) s'élève à 424,7 millions d'EUR, montant qui comprend les éléments suivants:

(1) Un budget de 225 millions d'EUR pour l'eu-LISA, couvrant le coût total du développement du programme réalisant les cinq éléments d'interopérabilité (68,3 millions d'EUR), les coûts de maintenance à partir de la livraison des éléments jusqu'en 2027 (56,1 millions d'EUR), un budget spécifique de 25 millions d'EUR pour la migration des données des systèmes existants vers le BMS partagé et les coûts supplémentaires pour la mise à jour de l'IUN, le réseau, la formation et les réunions. Un budget spécifique de 18,7 millions d'EUR couvrant le coût de la mise à niveau et du fonctionnement du système ECRIS-TCN en mode à haute disponibilité à partir de 2022.

(2) Un budget de 136,3 millions d'EUR pour permettre aux États membres de couvrir le coût des modifications de leurs systèmes nationaux qui sont nécessaires pour utiliser les éléments d'interopérabilité et l'IUN fournie par l'eu-LISA, ainsi qu'un budget pour la formation d'une communauté d'utilisateurs finaux de taille conséquente.

(3) Un budget de 48,9 millions d'EUR pour permettre à Europol de mettre à niveau ses systèmes informatiques eu égard au volume de messages à traiter et d'améliorer ses niveaux de performance[42]. L'ETIAS utilisera les éléments d'interopérabilité afin de consulter les données Europol.

(4) Un budget de 4,8 millions d'EUR destiné à l'Agence européenne de garde-frontières et de garde-côtes pour accueillir une équipe de spécialistes qui, pendant un an, validera les liens entre les identités au moment où le détecteur d'identités multiples sera mis en service.

(5) Un budget de 2,0 millions d'EUR destiné à l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) afin de préparer la formation du personnel opérationnel et de la dispenser.

[42] La capacité actuelle de traitement des informations d'Europol n'est pas compatible avec les volumes importants (100 000 interrogations par jour en moyenne) et les délais de réponse raccourcis dont l'ETIAS aura besoin.

(6) Une provision de 7,7 millions d'EUR destinée à la DG HOME afin de couvrir une augmentation limitée des effectifs et les coûts y afférents pendant la période de développement des différents éléments, étant donné que la Commission devra également exécuter des tâches supplémentaires au cours de cette période et prendre la responsabilité du comité chargé du format universel pour les messages.

Le règlement relatif au Fonds pour la sécurité intérieure (FSI) – Frontières est l'instrument financier dans lequel le budget consacré à la mise en œuvre de l'initiative relative à l'interopérabilité a été inclus. Son article 5, point b), prévoit que 791 millions d'EUR seront mis en œuvre dans le cadre d'un programme pour le développement de nouveaux systèmes informatiques, sur la base des systèmes informatiques actuels et/ou de nouveaux systèmes, permettant la gestion des flux migratoires aux frontières extérieures de l'Union, sous réserve de l'adoption des actes législatifs pertinents de l'Union et dans les conditions énoncées à l'article 15, paragraphe 5. Sur ces 791 millions d'EUR, 480,2 millions sont réservés au développement de l'EES, 210 millions à l'ETIAS et 67,9 millions à la révision du SIS. Le reste (32,9 millions d'EUR) sera réaffecté en utilisant les mécanismes du FSI-Frontières. La présente proposition nécessite 32,1 millions d'EUR pour la période du cadre financier pluriannuel actuel (2019-2020), ce qui entre donc dans le budget restant.

5. INFORMATIONS SUPPLÉMENTAIRES

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

L'eu-LISA est chargée de la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice. En tant que telle, elle est déjà responsable du fonctionnement et des améliorations techniques et opérationnelles des systèmes existants, ainsi que du développement des futurs systèmes déjà envisagés. En vertu de la présente proposition de règlement, elle définira la conception de l'architecture physique des éléments d'interopérabilité, les développera, les mettra en œuvre et, finalement, les hébergera. Les éléments respectifs seront mis en œuvre de manière progressive, conjointement avec le développement des systèmes sous-jacents.

La Commission garantira la mise en place de systèmes permettant de surveiller le développement et le fonctionnement des quatre éléments (portail de recherche européen, service partagé d'établissement de correspondances biométriques, répertoire commun de données d'identité, détecteur d'identités multiples) et du répertoire central des rapports et statistiques, et de les évaluer au regard des principaux objectifs stratégiques. Quatre ans après la création et la mise en service des fonctionnalités, puis tous les quatre ans, l'eu-LISA devrait présenter au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique des éléments d'interopérabilité. De plus, cinq ans après la création et la mise en service des fonctionnalités, puis tous les quatre ans, la Commission devrait produire une évaluation globale des éléments, notamment en ce qui concerne l'incidence directe ou indirecte des éléments et de leur application pratique en matière de droits fondamentaux. Ce rapport devrait examiner les résultats obtenus par rapport aux objectifs, déterminer si les principes de base restent valables et en tirer toutes les conséquences pour les options futures. La Commission devrait présenter les rapports d'évaluation au Parlement européen et au Conseil.

- **Explication détaillée de certaines dispositions de la proposition**

Le chapitre I comporte les dispositions générales du règlement. Il explique: les principes qui sous-tendent le règlement, les éléments qui y sont établis, les objectifs que l'interopérabilité cherche à atteindre, le champ d'application du règlement, les définitions des termes employés

dans le règlement, et le principe de non-discrimination concernant le traitement des données en vertu du règlement.

Le chapitre II comporte les dispositions relatives au portail de recherche européen (ESP). Ce chapitre prévoit la création de l'ESP et de son architecture technique, qui doit être développée par l'eu-LISA. Il précise l'objectif de l'ESP, détermine les personnes pouvant l'utiliser ainsi que la manière dont elles doivent l'utiliser, conformément aux droits d'accès existants pour chacun des systèmes centraux. Il contient une disposition prévoyant que l'eu-LISA crée des profils d'utilisateur pour chaque catégorie d'utilisateur. Ce chapitre définit la manière dont l'ESP interrogera les systèmes centraux et prévoit le contenu et le format des réponses adressées aux utilisateurs. Le chapitre II dispose également que l'eu-LISA tiendra des registres de l'ensemble des opérations de traitement, et prévoit une procédure de secours au cas où l'ESP ne serait pas en mesure d'accéder à un ou plusieurs des systèmes centraux.

Le chapitre III comprend les dispositions relatives au service partagé d'établissement de correspondances biométriques (BMS partagé). Ce chapitre prévoit la création du BMS partagé et de son architecture technique, qui doit être développée par l'eu-LISA. Il précise l'objectif du BMS partagé et définit les données stockées par celui-ci. Il explique les relations entre le BMS partagé et les autres éléments. Le chapitre III prévoit également que le BMS partagé ne continuera pas à stocker des données après la suppression de celles-ci des systèmes centraux respectifs, et dispose que l'eu-LISA tiendra des registres de toutes les opérations de traitement.

Le chapitre IV comporte les dispositions relatives au répertoire commun de données d'identité (CIR). Ce chapitre prévoit la création du CIR et de son architecture technique, qui doit être développée par l'eu-LISA. Il définit l'objectif du CIR et précise quelles données seront stockées et de quelle manière; il contient également des dispositions visant à garantir la qualité des données stockées. Ce chapitre prévoit que le CIR créera des dossiers individuels sur la base des données contenues dans les systèmes centraux et que les dossiers individuels seront mis à jour conformément aux modifications apportées à chaque système central. Le chapitre IV précise également la manière dont le CIR fonctionnera en lien avec le détecteur d'identités multiples. Ce chapitre définit les personnes qui pourront avoir accès au CIR ainsi que la manière dont elles pourront accéder aux données conformément aux droits d'accès; il contient des dispositions plus précises selon que l'accès a pour but l'identification ou qu'il s'agit, en tant que première étape de l'approche en deux étapes, d'accéder à l'EES, au VIS, à l'ETIAS et à Eurodac via le CIR à des fins répressives. Le chapitre IV prévoit également que l'eu-LISA tiendra des registres de l'ensemble des opérations de traitement concernant le CIR.

Le chapitre V comporte les dispositions relatives au détecteur d'identités multiples (MID). Ce chapitre prévoit la création du MID et de son architecture technique, qui doit être développée par l'eu-LISA. Il explique l'objectif du MID et réglemente l'utilisation de celui-ci conformément aux droits d'accès à chacun des systèmes centraux. Le chapitre V définit à quel moment et de quelle manière le MID lancera des recherches afin de détecter des identités multiples, ainsi que la manière dont les résultats sont fournis et font l'objet d'un suivi, y compris, si nécessaire, à l'aide d'une vérification manuelle. Le chapitre V définit une classification des types de lien pouvant résulter de la recherche, selon que le résultat montre une seule identité, des identités multiples ou des données d'identité partagées. Ce chapitre prévoit que le MID stockera les données liées contenues dans les systèmes centraux tant que ces données demeurent dans au moins deux systèmes centraux différents. Le chapitre V prévoit également que l'eu-LISA tiendra des registres de l'ensemble des opérations de traitement concernant le MID.

Le chapitre VI prévoit des mesures de soutien de l'interopérabilité. Il prévoit l'amélioration de la qualité des données, la création du format universel pour les messages en tant que norme commune pour l'échange d'informations à l'appui de l'interopérabilité et la création d'un répertoire central des rapports et statistiques.

Le chapitre VII concerne la protection des données. Ce chapitre prévoit des dispositions garantissant que les données traitées en vertu du présent règlement le sont de manière légale et appropriée, conformément aux dispositions du règlement (CE) nº 45/2001. Il explique qui sera le sous-traitant des données pour chacune des mesures d'interopérabilité proposées par le règlement, définit les mesures requises de l'eu-LISA et des autorités des États membres afin de garantir la sécurité du traitement des données, la confidentialité des données, le traitement approprié des incidents de sécurité et le suivi adéquat du respect des mesures prévues par le règlement. Ce chapitre contient également des dispositions concernant les droits des personnes concernées, y compris le droit d'être informées du fait que des données les concernant ont été stockées et traitées en vertu du règlement et le droit d'accéder aux données à caractère personnel stockées et traitées en vertu du règlement et d'en obtenir la rectification et la suppression. Ce chapitre expose en outre le principe selon lequel les données traitées en vertu du règlement ne doivent pas être transférées à un pays tiers, une organisation internationale ou une personne privée quelconque, ni être mises à leur disposition, à l'exception d'Interpol à certaines fins spécifiques ainsi que des données provenant d'Europol par l'intermédiaire du portail de recherche européen, pour lesquelles les règles du règlement (UE) 2016/794 concernant le traitement ultérieur des données s'appliquent. Enfin, ce chapitre établit des dispositions concernant le contrôle et l'audit en lien avec la protection des données.

Le chapitre VIII définit les responsabilités de l'eu-LISA avant et après la mise en œuvre des mesures contenues dans la présente proposition ainsi que celles des États membres, d'Europol et de l'unité centrale d'ETIAS.

Le chapitre IX fournit des détails concernant: les exigences en matière de statistiques et de rapports en lien avec les données traitées en vertu du règlement; les mesures transitoires qui seront nécessaires; les dispositions relatives aux coûts induits par le règlement; les exigences en matière de notifications; le processus de mise en œuvre initiale des mesures proposées par le règlement; des dispositions relatives à la gouvernance, y compris la constitution d'un comité et d'un groupe consultatif, les responsabilités de l'eu-LISA en matière de formation et un guide pratique pour soutenir la mise en œuvre et la gestion des éléments d'interopérabilité; les procédures relatives au suivi et à l'évaluation des mesures proposées dans le règlement, et les dispositions relatives à l'entrée en vigueur du règlement.

2017/0352 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération policière et judiciaire, asile et migration)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16, paragraphe 2, son article 74, son article 78, paragraphe 2, point e), son article 79, paragraphe 2, point c), son article 82, paragraphe 1, point d), son article 85, paragraphe 1, son article 87, paragraphe 2, point a), et son article 88, paragraphe 2,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

après consultation du Contrôleur européen de la protection des données,

vu l'avis du Comité économique et social européen[43],

vu l'avis du Comité des régions[44],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Dans sa communication du 6 avril 2016 intitulée «Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité»[45], la Commission a souligné la nécessité d'améliorer l'architecture de la gestion des données de l'Union appliquée à la gestion des frontières et à la sécurité. La communication a lancé un processus visant à atteindre l'interopérabilité des systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations, dans le but de remédier aux lacunes structurelles de ces systèmes qui ralentissent le travail des autorités nationales et de garantir que les garde-frontières, les autorités douanières, les policiers et les autorités judiciaires disposent des informations dont ils ont besoin.

(2) Dans sa feuille de route en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures, du 6 juin 2016[46], le Conseil a recensé plusieurs défis juridiques, techniques et opérationnels en matière d'interopérabilité des systèmes d'information de l'UE et a invité à rechercher des solutions.

[43] JO C du , p. .

[44]

[45] COM(2016) 205 du 6.4.2016.

[46] Feuille de route du 6 juin 2016 en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures – 9368/1/16 REV 1.

(3) Dans sa résolution du 6 juillet 2016 sur les priorités stratégiques pour le programme de travail de la Commission pour 2017[47], le Parlement européen a invité à présenter des propositions visant à améliorer et à développer les systèmes d'information de l'UE existants, à combler les lacunes en matière d'informations et à progresser vers l'interopérabilité, ainsi que des propositions concernant l'échange obligatoire d'informations au niveau de l'Union, assorti des garanties nécessaires en matière de protection des données.

(4) Le Conseil européen du 15 décembre 2016[48] a appelé à poursuivre les efforts en matière d'interopérabilité des systèmes d'information et des bases de données de l'Union.

(5) Dans son rapport final du 11 mai 2017[49], le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité a conclu qu'il était nécessaire et techniquement faisable d'œuvrer à des solutions pratiques d'interopérabilité, qui peuvent, en principe, apporter des bénéfices opérationnels et être mises en place conformément aux exigences en matière de protection des données.

(6) Dans sa communication du 16 mai 2017 intitulée «Septième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective»[50], la Commission a défini, conformément à sa communication du 6 avril 2016 et comme l'ont confirmé les conclusions et les recommandations du groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité, une nouvelle approche de la gestion des données pour les frontières, la sécurité et les migrations, selon laquelle tous les systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations sont interopérables, dans le plein respect des droits fondamentaux.

(7) Dans ses conclusions du 9 juin 2017[51] concernant la voie à suivre pour améliorer l'échange d'informations et assurer l'interopérabilité des systèmes d'information de l'UE, le Conseil a invité la Commission à trouver des solutions d'interopérabilité comme le proposait le groupe d'experts de haut niveau.

(8) Le Conseil européen du 23 juin 2017[52] a souligné la nécessité d'améliorer l'interopérabilité des bases de données et a invité la Commission à préparer, dès que possible, un projet de texte législatif mettant en œuvre les propositions formulées par le groupe d'experts de haut niveau sur les systèmes d'information et l'interopérabilité.

(9) Dans le but d'améliorer la gestion des frontières extérieures, de contribuer à prévenir et combattre la migration irrégulière et de favoriser un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice de l'Union, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, il convient d'établir l'interopérabilité des systèmes d'information de l'UE, à savoir le système d'entrée/de sortie (EES), le système d'information sur les visas (VIS), [le système européen d'information et d'autorisation concernant les voyages (ETIAS)], Eurodac, le système d'information Schengen (SIS) et le [système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)], afin que lesdits systèmes et leurs données se complètent

---

47 Résolution du Parlement européen du 6 juillet 2016 sur les priorités stratégiques pour le programme de travail de la Commission pour 2017 [2016/2773(RSP)].

48 http://www.consilium.europa.eu/fr/press/press-releases/2016/12/15/euco-conclusions-final/.

49 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

50 COM(2017) 261 final du 16.5.2017.

51 http://www.consilium.europa.eu/media/22185/st10136fr17-vf.pdf.

52 Conclusions du Conseil européen des 22 et 23 juin 2017.

mutuellement. À cet effet, il convient de créer un portail de recherche européen (ESP), un service partagé d'établissement de correspondances biométriques (BMS partagé), un répertoire commun de données d'identité (CIR) et un détecteur d'identités multiples (MID) en tant qu'éléments d'interopérabilité.

(10) L'interopérabilité des systèmes d'information de l'UE devrait permettre auxdits systèmes de se compléter mutuellement afin de faciliter l'identification correcte des personnes, de contribuer à la lutte contre la fraude à l'identité, d'améliorer et d'harmoniser les exigences en matière de qualité des données des différents systèmes d'information de l'UE, de faciliter la mise en œuvre technique et opérationnelle par les États membres des systèmes d'information de l'UE existants et futurs, de renforcer et de simplifier les garanties en matière de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE, de simplifier l'accès à des fins répressives à l'EES, au VIS, à l'[ETIAS] et à Eurodac et de servir les objectifs de l'EES, du VIS, de l'[ETIAS], d'Eurodac, du SIS et du [système ECRIS-TCN].

(11) Les éléments d'interopérabilité devraient concerner l'EES, le VIS, [l'ETIAS], Eurodac, le SIS et le [système ECRIS-TCN]. Ils devraient également concerner les données Europol dans la mesure nécessaire pour que celles-ci puissent être interrogées en même temps que ces systèmes d'information de l'UE.

(12) Les éléments d'interopérabilité devraient concerner les personnes dont les données à caractère personnel sont susceptibles d'être traitées dans les systèmes d'information de l'UE et par Europol, c'est-à-dire les ressortissants de pays tiers dont les données à caractère personnel sont traitées dans les systèmes d'information de l'UE et par Europol et les citoyens de l'Union dont les données à caractère personnel sont traitées dans le SIS et par Europol.

(13) Le portail de recherche européen (ESP) devrait être créé afin de faciliter d'un point de vue technique la capacité des autorités des États membres et des organes de l'UE à disposer d'un accès rapide, continu, efficace, systématique et contrôlé aux systèmes d'information de l'UE, aux données Europol et aux bases de données d'Interpol dont ils ont besoin pour accomplir leurs tâches, conformément à leurs droits d'accès, et pour servir les objectifs de l'EES, du VIS, [de l'ETIAS], d'Eurodac, du SIS, [du système ECRIS-TCN] et des données Europol. En permettant d'interroger simultanément l'ensemble des systèmes d'information de l'UE en parallèle, ainsi que les données Europol et les bases de données d'Interpol, l'ESP devrait constituer un guichet unique ou «courtier de messages» afin d'effectuer des recherches dans plusieurs systèmes centraux et de récupérer les informations nécessaires sans discontinuité et dans le plein respect des exigences en matière de contrôle de l'accès et de protection des données des systèmes sous-jacents.

(14) Les utilisateurs finaux du portail de recherche européen (ESP) qui ont le droit d'accéder aux données Europol en vertu du règlement (UE) 2016/794 du Parlement européen et du Conseil[53] devraient pouvoir interroger les données Europol en même temps que les systèmes d'information de l'UE auxquels ils ont accès. Tout traitement ultérieur de données faisant suite à une telle interrogation devrait avoir lieu

[53] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

conformément au règlement (UE) 2016/794, y compris les limitations d'accès ou d'utilisation imposées par le fournisseur de données.

(15) Le portail de recherche européen (ESP) devrait être développé et configuré de telle sorte qu'il ne permette pas d'utiliser aux fins d'une recherche des champs de données qui ne sont pas liés aux personnes ou aux documents de voyage ou qui ne figurent pas dans un système d'information de l'UE, dans les données Europol ou dans les bases de données d'Interpol.

(16) Afin d'assurer une utilisation rapide et systématique de l'ensemble des systèmes d'information de l'UE, le portail de recherche européen (ESP) devrait être utilisé pour interroger le répertoire commun de données d'identité, l'EES, le VIS, [l'ETIAS], Eurodac et [le système ECRIS-TCN]. Toutefois, la connexion nationale aux différents systèmes d'information de l'UE devrait être conservée en tant que solution de secours technique. Les organes de l'Union devraient également utiliser l'ESP afin d'interroger le SIS central, conformément à leurs droits d'accès et afin d'exécuter leurs missions. L'ESP devrait constituer un moyen supplémentaire d'interroger le SIS central, les données Europol et les systèmes d'Interpol, en complément des interfaces spécifiques existantes.

(17) Les données biométriques, telles que les empreintes digitales et les images faciales, sont uniques et donc bien plus fiables que les données alphanumériques pour identifier une personne. Le service partagé d'établissement de correspondances biométriques (BMS partagé) devrait être un outil technique permettant de renforcer et de faciliter le fonctionnement des systèmes d'information de l'UE pertinents et des autres éléments d'interopérabilité. L'objectif principal du BMS partagé devrait être de faciliter l'identification d'une personne pouvant être enregistrée dans différentes bases de données, en faisant correspondre ses données biométriques contenues dans différents systèmes et en s'appuyant sur un élément technologique unique plutôt que sur cinq éléments différents contenus dans les systèmes sous-jacents. Le BMS partagé devrait contribuer à la sécurité et procurer des avantages sur les plans financier, opérationnel et de la maintenance en s'appuyant sur un élément technologique unique plutôt que sur cinq éléments contenus dans les systèmes sous-jacents. Tous les systèmes automatisés d'identification par empreintes digitales, y compris ceux actuellement utilisés pour Eurodac, le VIS et le SIS, utilisent des modèles biométriques se composant de données résultant d'une extraction des caractéristiques d'échantillons biométriques réels. Le BMS partagé devrait regrouper et stocker tous ces modèles biométriques à un seul endroit, facilitant ainsi les comparaisons de données biométriques entre les systèmes et permettant des économies d'échelle dans le développement et la maintenance des systèmes centraux de l'UE.

(18) Les données biométriques sont des données à caractère personnel sensibles. Le présent règlement devrait établir les conditions et les garanties du traitement de ces données dans le but d'identifier de manière unique les personnes concernées.

(19) Pour être efficaces, les systèmes créés par le règlement (UE) 2017/2226 du Parlement européen et du Conseil[54], le règlement (CE) nº 767/2008 du Parlement européen et du

[54] Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) nº 767/2008 et (UE) nº 1077/2011 (règlement EES) (JO L 327 du 9.12.2017, p. 20).

Conseil[55] et [le règlement ETIAS] pour la gestion des frontières de l'Union, le système créé par [le règlement Eurodac] pour identifier les demandeurs de protection internationale et lutter contre la migration irrégulière et le système créé par [le règlement sur le système ECRIS-TCN] doivent s'appuyer sur l'identification précise des ressortissants de pays tiers dont les données à caractère personnel y sont stockées.

(20) Le répertoire commun de données d'identité (CIR) devrait donc faciliter et favoriser l'identification correcte des personnes enregistrées dans l'EES, le VIS, [l'ETIAS], Eurodac et [le système ECRIS-TCN].

(21) Les données à caractère personnel stockées dans ces systèmes d'information de l'UE peuvent correspondre à la même personne, mais sous des identités différentes ou incomplètes. Les États membres disposent de moyens efficaces d'identifier leurs citoyens ou les résidents permanents enregistrés sur leur territoire, mais il en va autrement des ressortissants de pays tiers. L'interopérabilité des systèmes d'information de l'UE devrait contribuer à l'identification correcte des ressortissants de pays tiers. Le répertoire commun de données d'identité (CIR) devrait stocker les données à caractère personnel des ressortissants de pays tiers qui figurent dans les systèmes et qui sont nécessaires à l'identification plus précise de ces personnes, à savoir notamment leurs données d'identité, les données de leur document de voyage et leurs données biométriques, quel que soit le système dans lequel ces informations ont été collectées à l'origine. Seules les données à caractère personnel strictement nécessaires pour procéder à un contrôle d'identité précis devraient être stockées dans le CIR. Les données à caractère personnel enregistrées dans le CIR ne devraient pas être conservées pendant une période plus longue que ce qui est strictement nécessaire aux fins des systèmes sous-jacents et elles devraient être automatiquement supprimées lorsque les données sont supprimées des systèmes sous-jacents conformément à leur séparation logique.

(22) La nouvelle opération de traitement consistant à stocker ces données dans le répertoire commun de données d'identité (CIR) plutôt que dans chacun des systèmes distincts est nécessaire afin d'augmenter la précision de l'identification, rendue possible par la comparaison et la mise en correspondance automatisées de ces données. Le fait que les données d'identité et les données biométriques des ressortissants de pays tiers soient stockées dans le CIR ne devrait en aucun cas ralentir le traitement des données aux fins des règlements relatifs à l'EES, au VIS, à l'ETIAS, à Eurodac ou au système ECRIS-TCN, étant donné que le CIR devrait être un nouvel élément partagé de ces systèmes sous-jacents.

(23) À cet égard, il est nécessaire de créer un dossier individuel dans le répertoire commun de données d'identité (CIR) pour chaque personne enregistrée dans l'EES, le VIS, l'ETIAS, Eurodac ou le système ECRIS-TCN, afin d'atteindre l'objectif consistant à identifier correctement les ressortissants de pays tiers au sein de l'espace Schengen et d'appuyer le détecteur d'identités multiples, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité. Le dossier individuel devrait enregistrer toutes les identités possibles liées à une personne en un seul endroit et les mettre à la disposition des utilisateurs finaux dûment autorisés.

[55] Règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (JO L 218 du 13.8.2008, p. 60).

(24) Le répertoire commun de données d'identité (CIR) devrait donc appuyer le fonctionnement du détecteur d'identités multiples afin de faciliter et de simplifier l'accès des services répressifs aux systèmes d'information de l'UE qui n'ont pas été exclusivement créés à des fins de prévention et de détection des infractions graves, ou d'enquêtes et de poursuites en la matière.

(25) Le répertoire commun de données d'identité (CIR) devrait prévoir un réservoir partagé pour les données d'identité et les données biométriques des ressortissants de pays tiers enregistrés dans l'EES, le VIS, [l'ETIAS], Eurodac et le [système ECRIS-TCN], qui constituerait l'élément partagé entre ces systèmes aux fins du stockage de ces données et permettrait de les interroger.

(26) Toutes les données enregistrées dans le répertoire commun de données d'identité (CIR) devraient être logiquement séparées au moyen d'un étiquetage automatique de chaque donnée indiquant le système sous-jacent dont elle provient. Le contrôle de l'accès au CIR devrait utiliser ces étiquettes afin de permettre d'accéder ou non à la donnée.

(27) Afin de garantir l'identification correcte d'une personne, les autorités des États membres compétentes pour prévenir et combattre la migration irrégulière et les autorités compétentes au sens de l'article 3, point 7, de la directive (UE) 2016/680 devraient être autorisées à interroger le répertoire commun de données d'identité (CIR) à l'aide des données biométriques de cette personne relevées lors d'un contrôle d'identité.

(28) Lorsque les données biométriques de la personne ne peuvent pas être utilisées ou si la recherche effectuée avec ces données échoue, la recherche devrait être effectuée à l'aide des données d'identité de cette personne, combinées aux données du document de voyage. Lorsque la recherche indique que des données concernant cette personne sont stockées dans le répertoire commun de données d'identité (CIR), les autorités des États membres devraient pouvoir consulter les données d'identité de la personne qui sont stockées dans le CIR, sans qu'aucune indication ne soit fournie en ce qui concerne le système d'information de l'UE dont les données proviennent.

(29) Les États membres devraient adopter des mesures législatives nationales désignant les autorités compétentes pour réaliser des contrôles d'identité à l'aide du répertoire commun de données d'identité (CIR) et définissant les procédures, les conditions et les critères de ces contrôles, conformément au principe de proportionnalité. En particulier, les mesures législatives nationales devraient prévoir le pouvoir de collecter des données biométriques lors d'un contrôle de l'identité d'une personne présente devant un agent de ces autorités.

(30) Le présent règlement devrait également introduire, pour les autorités répressives désignées par les États membres et pour Europol, une nouvelle possibilité d'accès simplifié aux données autres que les données d'identité se trouvant dans l'EES, le VIS, [l'ETIAS] ou Eurodac. Les données, y compris les données autres que les données d'identité contenues dans ces systèmes, peuvent être nécessaires, dans des cas particuliers, à la prévention et à la détection des infractions terroristes ou d'infractions pénales graves, ou aux poursuites et enquêtes en la matière.

(31) L'accès complet aux données contenues dans les systèmes d'information de l'UE qui sont nécessaires à des fins de prévention et de détection des infractions terroristes ou d'autres infractions pénales graves, ainsi que d'enquêtes en la matière, en plus des données d'identité pertinentes couvertes par le répertoire commun de données

d'identité (CIR) et obtenues à l'aide des données biométriques d'une personne relevées lors d'un contrôle d'identité, devrait continuer à être régi par les dispositions figurant dans les instruments juridiques respectifs. Les autorités répressives désignées et Europol ne savent pas à l'avance quels systèmes d'information de l'UE contiennent des données concernant les personnes sur lesquelles ils enquêtent. Cela conduit à des retards et à des manques d'efficacité dans l'exercice de leurs fonctions. L'utilisateur final autorisé par l'autorité désignée devrait par conséquent pouvoir voir dans quels systèmes d'information de l'UE les données correspondant à la recherche effectuée sont enregistrées. Le système concerné serait donc signalé après la vérification automatisée de la présence d'un résultat positif dans le système (fonctionnalité dite d'indicateur de concordance).

(32) Le registre des recherches dans le répertoire commun de données d'identité devrait indiquer l'objectif de la recherche. Lorsque la recherche a été effectuée selon l'approche de la consultation des données en deux étapes, les registres devraient comporter une référence au dossier national de l'enquête ou de l'affaire et donc indiquer que cette recherche a été lancée à des fins de prévention et de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière.

(33) L'interrogation du répertoire commun de données d'identité (CIR) par les autorités désignées des États membres et Europol en vue d'obtenir une réponse indiquant une concordance, c'est-à-dire signalant que les données sont enregistrées dans l'EES, le VIS, [l'ETIAS] ou Eurodac, nécessite un traitement automatisé de données à caractère personnel. Un indicateur de concordance ne révélerait pas les données à caractère personnel de la personne concernée mais signalerait seulement que certaines de ses données sont stockées dans l'un des systèmes. L'utilisateur final autorisé ne devrait prendre aucune décision faisant grief à la personne concernée en se fondant uniquement sur l'existence d'une concordance. L'accès de l'utilisateur final à un indicateur de concordance ne constituerait par conséquent qu'une atteinte très limitée au droit à la protection des données à caractère personnel de la personne concernée, tandis qu'il serait nécessaire de permettre à l'autorité désignée et à Europol d'adresser plus pratiquement leur demande d'accès aux données à caractère personnel directement au système signalé comme contenant ces données.

(34) L'approche de la consultation des données en deux étapes est particulièrement utile dans les cas où le suspect, l'auteur ou la victime présumée d'une infraction terroriste ou d'une autre infraction pénale grave n'est pas connu. Dans de tels cas, le répertoire commun de données d'identité (CIR) devrait permettre de déterminer quel système d'information connaît la personne en une seule recherche. En créant l'obligation d'utiliser cette nouvelle approche de l'accès à des fins répressives dans de tels cas, l'accès aux données à caractère personnel stockées dans l'EES, le VIS, [l'ETIAS] et Eurodac ne devrait pas s'accompagner des exigences consistant à réaliser une recherche préalable dans les bases de données nationales et à lancer une recherche préalable dans les systèmes automatisés d'identification par empreintes digitales d'autres États membres en vertu de la décision 2008/615/JAI. Le principe de la recherche préalable limite en effet la possibilité pour les autorités des États membres de consulter les systèmes à des fins répressives justifiées et pourrait se traduire par des occasions manquées de mettre au jour des informations nécessaires. Les exigences consistant à réaliser une recherche préalable dans les bases de données nationales et à lancer une recherche préalable dans les systèmes automatisés d'identification par empreintes digitales d'autres États membres en vertu de la décision 2008/615/JAI ne

devraient cesser d'être applicables qu'après que la nouvelle garantie de l'approche en deux étapes de l'accès à des fins répressives au moyen du CIR sera devenue opérationnelle.

(35) Le détecteur d'identités multiples (MID) devrait être créé afin de soutenir le fonctionnement du répertoire commun de données d'identité et de servir les objectifs de l'EES, du VIS, [de l'ETIAS], d'Eurodac, du SIS et du [système ECRIS-TCN]. Afin d'être efficaces dans la poursuite de leurs objectifs respectifs, tous ces systèmes d'information de l'UE nécessitent l'identification précise des personnes dont les données à caractère personnel y sont stockées.

(36) La possibilité d'atteindre les objectifs des systèmes d'information de l'UE est mise à mal par l'incapacité actuelle des autorités utilisant ces systèmes à réaliser des contrôles d'identité suffisamment fiables sur les ressortissants de pays tiers dont les données sont stockées dans différents systèmes. Cette incapacité provient du fait que l'ensemble de données d'identité stocké dans un système donné peut être frauduleux, incorrect ou incomplet et qu'il n'existe à l'heure actuelle aucune possibilité de détecter de telles données d'identité frauduleuses, incorrectes ou incomplètes en les comparant aux données stockées dans un autre système. Pour remédier à cette situation, il est nécessaire de disposer d'un instrument technique au niveau de l'Union qui permette l'identification précise des ressortissants de pays tiers à ces fins.

(37) Le détecteur d'identités multiples (MID) devrait créer et stocker des liens entre les données contenues dans les différents systèmes d'information de l'UE afin de détecter les identités multiples, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité. Le MID ne devrait contenir que les liens entre des personnes figurant dans plus d'un système d'information de l'UE, qui se limiteront strictement aux données nécessaires pour vérifier si une personne est licitement ou illicitement enregistrée sous différentes identités biographiques dans différents systèmes ou pour démontrer que deux personnes ayant des données biographiques similaires peuvent ne pas être une seule et même personne. Le traitement des données au moyen du portail de recherche européen (ESP) et du service partagé d'établissement de correspondances biométriques (BMS partagé) en vue de relier des dossiers individuels entre différents systèmes devrait être limité au strict minimum et se borner par conséquent à la détection d'identités multiples lorsque de nouvelles données sont ajoutées à l'un des systèmes d'information inclus dans le répertoire commun de données d'identité et dans le SIS. Le MID devrait prévoir des garanties contre les possibles discriminations ou décisions défavorables pour les personnes ayant des identités licites multiples.

(38) Le présent règlement prévoit de nouvelles opérations de traitement des données ayant pour but d'identifier correctement les personnes concernées. Cela constitue une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la charte des droits fondamentaux. Étant donné que la mise en œuvre effective des systèmes d'information de l'UE dépend de l'identification correcte des personnes concernées, une telle atteinte est justifiée par les mêmes objectifs que ceux pour lesquels chacun de ces systèmes a été créé, à savoir la gestion efficace des frontières de l'Union, la sécurité intérieure de l'Union, l'application efficace des politiques de l'Union en matière d'asile et de visas et la lutte contre la migration irrégulière.

(39) Le portail de recherche européen (ESP) et le service partagé d'établissement de correspondances biométriques (BMS partagé) devraient comparer les données concernant les personnes figurant dans le répertoire commun de données d'identité

(CIR) et dans le SIS lorsqu'une autorité nationale ou un organe de l'Union crée de nouvelles entrées. Cette comparaison devrait être automatisée. Le CIR et le SIS devraient utiliser le BMS partagé afin de détecter les liens possibles sur la base des données biométriques. Le CIR et le SIS devraient utiliser l'ESP afin de détecter les liens possibles sur la base des données alphanumériques. Le CIR et le SIS devraient être en mesure de détecter les données identiques ou similaires relatives à un ressortissant de pays tiers stockées dans plusieurs systèmes. Dans un tel cas, un lien indiquant qu'il s'agit de la même personne devrait être établi. Le CIR et le SIS devraient être configurés de manière à ce que les erreurs de translittération ou d'orthographe mineures soient détectées afin d'éviter que le ressortissant de pays tiers concerné n'en pâtisse de manière injustifiée.

(40) L'autorité nationale ou l'organe de l'Union ayant enregistré les données dans le système d'information de l'UE concerné devrait confirmer ou modifier ces liens. Cette autorité devrait avoir accès aux données stockées dans le répertoire commun de données d'identité (CIR) ou dans le SIS ainsi que dans le détecteur d'identités multiples (MID) afin de procéder à une vérification d'identité manuelle.

(41) L'accès au détecteur d'identités multiples (MID) des autorités des États membres et des organes de l'Union ayant accès à au moins un système d'information de l'UE inclus dans le répertoire commun de données d'identité (CIR) ou dans le SIS devrait être limité aux liens dits rouges, qui indiquent que les données liées comportent les mêmes données biométriques mais des données d'identité différentes et que l'autorité chargée de la vérification des différentes identités a conclu que ces données désignaient de manière illicite la même personne, ou qui indiquent que les données liées comportent des données d'identité similaires et que l'autorité chargée de la vérification des différentes identités a conclu que ces données désignaient de manière illicite la même personne. Lorsque les données d'identité liées ne sont pas similaires, un lien jaune devrait être créé et une vérification manuelle devrait intervenir afin de confirmer le lien ou d'en changer la couleur en conséquence.

(42) La vérification manuelle des identités multiples devrait être effectuée par l'autorité qui crée ou met à jour les données qui ont donné lieu à un résultat positif entraînant l'établissement d'un lien avec des données déjà stockées dans un autre système d'information de l'UE. L'autorité chargée de la vérification des identités multiples devrait déterminer l'existence d'identités licites ou illicites multiples. Lorsque cela est possible, cette détermination devrait avoir lieu en présence du ressortissant de pays tiers et, lorsque cela est nécessaire, des explications ou des informations complémentaires devraient être demandées. Il convient de procéder à cette détermination sans délai, conformément aux exigences légales prévues par le droit national et de l'Union en matière de précision des informations.

(43) En ce qui concerne les liens obtenus avec le système d'information Schengen (SIS) portant sur les signalements de personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, de personnes disparues ou vulnérables, de personnes recherchées aux fins de concours dans le cadre d'une procédure judiciaire, de personnes aux fins de contrôle discret ou de contrôle spécifique ou de personnes recherchées inconnues, l'autorité chargée de la vérification des identités multiples devrait être le bureau SIRENE de l'État membre qui a créé le signalement. En effet, ces catégories de signalements figurant dans le SIS sont sensibles et ne devraient pas nécessairement être partagées avec les autorités qui créent ou mettent à jour les données dans l'un des autres systèmes d'information de l'UE. La création d'un lien

avec les données du SIS devrait se faire sans préjudice des conduites à tenir conformément aux [règlements SIS].

(44) L'eu-LISA devrait mettre en place des mécanismes automatisés de contrôle de la qualité des données et des indicateurs communs de qualité des données. Elle devrait être chargée de développer une capacité centrale de suivi de la qualité des données et de produire des rapports réguliers d'analyse des données afin d'améliorer le contrôle de la mise en œuvre et de l'application des systèmes d'information de l'UE par les États membres. Les indicateurs communs de qualité devraient inclure les normes de qualité minimales pour le stockage de données dans les systèmes d'information de l'UE ou les éléments d'interopérabilité. Ces normes de qualité des données devraient avoir pour objectif de permettre aux systèmes d'information de l'UE et aux éléments d'interopérabilité de repérer automatiquement les communications de données manifestement incorrectes ou incohérentes afin que l'État membre qui en est à l'origine puisse vérifier les données et adopter les mesures correctives nécessaires.

(45) La Commission devrait évaluer les rapports de l'eu-LISA sur la qualité et, le cas échéant, adresser des recommandations aux États membres. Les États membres devraient être chargés de préparer un plan d'action décrivant les mesures visant à remédier à toute lacune dans la qualité des données et ils devraient établir des rapports réguliers à cet égard.

(46) Le format universel pour les messages (UMF) devrait établir une norme pour l'échange structuré d'informations transfrontières entre les systèmes d'information, les autorités et/ou les organisations dans le domaine de la justice et des affaires intérieures. L'UMF devrait définir un vocabulaire commun et des structures logiques pour les informations habituellement échangées, dans le but de faciliter l'interopérabilité en permettant la création et la lecture des contenus de l'échange d'une manière cohérente et sémantiquement équivalente.

(47) Un répertoire central des rapports et statistiques (CRRS) devrait être créé afin de générer des données statistiques intersystèmes et des rapports analytiques à des fins stratégiques, opérationnelles et de qualité des données. L'eu-LISA devrait établir, mettre en œuvre et héberger le CRRS sur ses sites techniques contenant des données statistiques anonymes issues des systèmes susmentionnés, du répertoire commun de données d'identité, du détecteur d'identités multiples et du service partagé d'établissement de correspondances biométriques. Les données contenues dans le CRRS ne devraient pas permettre d'identifier les personnes. L'eu-LISA devrait rendre les données anonymes et enregistrer ces données anonymes dans le CRRS. Le processus d'anonymisation des données devrait être automatisé et le personnel de l'eu-LISA ne devrait pouvoir accéder directement à aucune donnée à caractère personnel stockée dans les systèmes d'information de l'UE ou dans les éléments d'interopérabilité.

(48) Le règlement (UE) 2016/679 devrait s'appliquer au traitement des données à caractère personnel réalisé en vertu du présent règlement par les autorités nationales, à moins que ce traitement ne soit effectué par les autorités désignées ou par les points d'accès centraux des États membres à des fins de prévention et de détection des infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, auquel cas la directive (UE) 2016/680 du Parlement européen et du Conseil devrait s'appliquer.

(49) Les dispositions spécifiques concernant la protection des données contenues dans le [règlement Eurodac], [le règlement SIS dans le domaine répressif] [le règlement SIS

dans le domaine du retour illégal] et le [règlement sur le système ECRIS-TCN] devraient s'appliquer au traitement des données à caractère personnel dans les systèmes respectivement concernés.

(50) Le règlement (CE) nº 45/2001 du Parlement européen et du Conseil[56] devrait s'appliquer au traitement des données à caractère personnel par l'eu-LISA et par d'autres institutions et organes de l'Union dans l'exercice de leurs missions en vertu du présent règlement, sans préjudice du règlement (UE) 2016/794, qui devrait s'appliquer au traitement des données à caractère personnel par Europol.

(51) Les autorités de contrôle instituées conformément au [règlement (UE) 2016/679] devraient contrôler la licéité du traitement des données à caractère personnel par les États membres, tandis que le Contrôleur européen de la protection des données, créé par le règlement (CE) nº 45/2001, devrait contrôler les activités des institutions et organes de l'Union concernant le traitement des données à caractère personnel. Le Contrôleur européen de la protection des données et les autorités de contrôle devraient coopérer en ce qui concerne le contrôle du traitement des données à caractère personnel par les éléments d'interopérabilité.

(52) «[…] Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001, et a rendu son avis le […].»

(53) Dans la mesure où la confidentialité est concernée, les dispositions pertinentes du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne devraient s'appliquer aux fonctionnaires ou autres agents employés et travaillant en lien avec le SIS.

(54) Les États membres et l'eu-LISA devraient disposer de plans de sécurité afin de faciliter la mise en œuvre des obligations en matière de sécurité, et ils devraient coopérer pour remédier aux problèmes de sécurité. L'eu-LISA devrait également s'assurer de l'utilisation continue des dernières évolutions technologiques afin de garantir l'intégrité des données en ce qui concerne le développement, la conception et la gestion des éléments d'interopérabilité.

(55) Aux fins de l'établissement de statistiques et de rapports, il est nécessaire de permettre aux membres autorisés du personnel des autorités compétentes, institutions et organes indiqués dans le présent règlement de consulter certaines données liées à certains éléments d'interopérabilité, sans permettre l'identification des personnes.

(56) Afin de permettre aux autorités compétentes et aux organes de l'Union de s'adapter aux nouvelles exigences concernant l'utilisation du portail de recherche européen (ESP), il est nécessaire de prévoir une période transitoire. De même, afin de permettre le fonctionnement cohérent et optimal du détecteur d'identités multiples (MID), il convient de définir des mesures transitoires pour le début de ses activités.

(57) Les coûts du développement des éléments d'interopérabilité prévus en vertu du cadre financier pluriannuel actuel sont inférieurs au montant restant du budget alloué aux frontières intelligentes dans le règlement (UE) nº 515/2014 du Parlement européen et

[56] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

du Conseil[57]. En conséquence, conformément à l'article 5, paragraphe 5, point b), du règlement (UE) nº 515/2014, le présent règlement devrait réattribuer le montant actuellement alloué au développement de systèmes informatiques permettant la gestion des flux migratoires aux frontières extérieures.

(58) Afin de compléter certains aspects techniques détaillés du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne les profils des utilisateurs du portail de recherche européen (ESP) et le contenu et le format des réponses de l'ESP. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes établis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016[58]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts devraient systématiquement avoir accès aux réunions des groupes d'experts de la Commission chargés de la préparation des actes délégués.

(59) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer à la Commission des compétences d'exécution lui permettant d'adopter des règles détaillées concernant les mécanismes, procédures et indicateurs automatisés de contrôle de la qualité des données, le développement de la norme UMF, les procédures permettant de déterminer les cas d'identités similaires, le fonctionnement du répertoire central des rapports et statistiques, et la procédure de coopération en cas d'incidents de sécurité. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil[59].

(60) Le règlement (UE) 2016/794 s'applique à tout traitement de données Europol aux fins du présent règlement.

(61) Le présent règlement est sans préjudice de l'application de la directive 2004/38/CE.

(62) Conformément à l'article 3 de l'accord entre la Communauté européenne et le Royaume de Danemark concernant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée au Danemark ou dans tout autre État membre de l'Union européenne et le système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin[60], le Danemark doit notifier à la Commission sa décision d'appliquer ou non le contenu du présent règlement, dans la mesure où celui-ci concerne Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)].

---

57 Règlement (UE) nº 515/2014 du Parlement européen et du Conseil du 16 avril 2014 portant création, dans le cadre du Fonds pour la sécurité intérieure, de l'instrument de soutien financier dans le domaine des frontières extérieures et des visas et abrogeant la décision nº 574/2007/CE (JO L 150 du 20.5.2014, p. 143).

58 http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016Q0512(01).

59 Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

60

(63) Dans la mesure où ses dispositions concernent le SIS tel que régi par la décision 2007/533/JAI, le Royaume-Uni participe au présent règlement, conformément à l'article 5, paragraphe 1, du protocole nº 19 sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (le «protocole sur l'acquis de Schengen»), et à l'article 8, paragraphe 2, de la décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen[61]. En outre, dans la mesure où ses dispositions concernent Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)], le Royaume-Uni peut notifier au président du Conseil son souhait de participer à l'adoption et à l'application du présent règlement, conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE (le «protocole sur la position du Royaume-Uni et de l'Irlande»). Dans la mesure où ses dispositions concernent [le système ECRIS-TCN], conformément aux articles 1er et 2 et à l'article 4 *bis*, paragraphe 1, du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, le Royaume-Uni ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application. Conformément à l'article 3 et à l'article 4 *bis*, paragraphe 1, du protocole nº 21, le Royaume-Uni peut notifier son souhait de participer à l'adoption du présent règlement.

(64) Dans la mesure où ses dispositions concernent le SIS tel que régi par la décision 2007/533/JAI, l'Irlande participe au présent règlement, conformément à l'article 5, paragraphe 1, du protocole nº 19 sur l'acquis de Schengen intégré dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (le «protocole sur l'acquis de Schengen»), et à l'article 6, paragraphe 2, de la décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen[62]. En outre, dans la mesure où ses dispositions concernent Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)], l'Irlande peut notifier au président du Conseil son souhait de participer à l'adoption et à l'application du présent règlement, conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (le «protocole sur la position du Royaume-Uni et de l'Irlande»). Dans la mesure où ses dispositions concernent [le système ECRIS-TCN], conformément aux articles 1er et 2 et à l'article 4 *bis*, paragraphe 1, du

61

62

protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ni soumis à son application. Conformément à l'article 3 et à l'article 4 *bis*, paragraphe 1, du protocole nº 21, l'Irlande peut notifier son souhait de participer à l'adoption du présent règlement.

(65) Pour ce qui est de l'Islande et de la Norvège, en ce qui concerne Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)], le présent règlement constitue une mesure nouvelle au sens de l'accord entre la Communauté européenne, la République d'Islande et le Royaume de Norvège relatif aux critères et aux mécanismes permettant de déterminer l'État responsable de l'examen d'une demande d'asile présentée dans un État membre, en Islande ou en Norvège.

(66) Pour ce qui est de la Suisse, en ce qui concerne Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)], le présent règlement constitue une mesure nouvelle liée à Eurodac au sens de l'accord entre la Communauté européenne et la Confédération suisse relatif aux critères et mécanismes de détermination de l'État responsable de l'examen d'une demande d'asile présentée dans un État membre ou en Suisse.

(67) Pour ce qui est du Liechtenstein, en ce qui concerne Eurodac [et le système automatisé pour l'enregistrement et le suivi des demandes, et pour le mécanisme d'attribution des demandes de protection internationale visé à l'article 44 du règlement (UE) XX/XX établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride (refonte)], le présent règlement constitue une mesure nouvelle au sens du protocole entre la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein relatif à l'adhésion de la Principauté de Liechtenstein à l'accord entre la Communauté européenne et la Confédération suisse relatif aux critères et mécanismes de détermination de l'État responsable de l'examen d'une demande d'asile présentée dans un État membre ou en Suisse.

(68) Le présent règlement respecte les droits fondamentaux et observe les principes consacrés notamment par la charte des droits fondamentaux de l'Union européenne et est appliqué conformément à ces droits et principes,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I
Dispositions générales

Article premier
Objet

1. Le présent règlement, conjointement avec le [règlement 2018/xx relatif à l'interopérabilité (frontières et visas)], crée un cadre visant à garantir l'interopérabilité entre le système d'entrée/de sortie (EES), le système d'information sur les visas (VIS), [le système européen d'information et d'autorisation concernant les voyages (ETIAS)], Eurodac, le système d'information Schengen (SIS) et [le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)] afin que ces systèmes et leurs données se complètent mutuellement.

2. Le cadre se compose des éléments d'interopérabilité suivants:

   (a) un portail de recherche européen (ESP);

   (b) un service partagé d'établissement de correspondances biométriques (BMS partagé);

   (c) un répertoire commun de données d'identité (CIR);

   (d) un détecteur d'identités multiples (MID).

3. Le présent règlement établit également des dispositions concernant les exigences en matière de qualité des données, le format universel pour les messages (UMF), le répertoire central des rapports et statistiques (CRRS), et définit les responsabilités des États membres et de l'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 (eu-LISA) à l'égard de la conception et du fonctionnement des éléments d'interopérabilité.

4. Le présent règlement adapte également les procédures et les conditions d'accès des autorités répressives des États membres et de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) au système d'entrée/de sortie (EES), au système d'information sur les visas (VIS), [au système européen d'information et d'autorisation concernant les voyages (ETIAS)] et à Eurodac aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves relevant de leur compétence, et aux fins des enquêtes en la matière.

Article 2
Objectifs de l'interopérabilité

1. En garantissant l'interopérabilité, le présent règlement poursuit les objectifs suivants:

   (a) améliorer la gestion des frontières extérieures;

   (b) contribuer à prévenir et lutter contre la migration irrégulière;

   (c) contribuer à l'établissement d'un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union, y compris au maintien de la sécurité publique et de l'ordre public et à la préservation de la sécurité sur le territoire des États membres;

(d) améliorer la mise en œuvre de la politique commune en matière de visas; et

(e) aider à l'examen des demandes de protection internationale.

2. Les objectifs consistant à garantir l'interopérabilité sont atteints:

(a) en assurant l'identification correcte des personnes;

(b) en contribuant à la lutte contre la fraude à l'identité;

(c) en améliorant et en harmonisant les exigences relatives à la qualité des données des différents systèmes d'information de l'UE;

(d) en facilitant la mise en œuvre technique et opérationnelle, par les États membres, des systèmes d'information de l'UE, existants et à venir;

(e) en renforçant, en simplifiant et en rendant plus uniformes les conditions de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE;

(f) en rationalisant les conditions d'accès à des fins répressives à l'EES, au VIS, [à l'ETIAS] et à Eurodac;

(g) en soutenant les objectifs de l'EES, du VIS, [de l'ETIAS], d'Eurodac, du SIS et [du système ECRIS-TCN].

Article 3
Champ d'application

1. Le présent règlement s'applique à Eurodac, au système d'information Schengen (SIS) et [au système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN)].

2. Il s'applique également aux données Europol dans la mesure nécessaire pour permettre à celles-ci d'être interrogées simultanément avec les systèmes d'information de l'UE mentionnés au paragraphe 1 conformément au droit de l'Union.

3. Le présent règlement s'applique aux personnes à l'égard desquelles des données à caractère personnel peuvent être traitées dans les systèmes d'information de l'UE mentionnés au paragraphe 1 et dans les données Europol mentionnées au paragraphe 2.

Article 4
Définitions

Aux fins du présent règlement, on entend par:

(1) «frontières extérieures», les frontières extérieures telles que définies à l'article 2, point 2), du règlement (UE) 2016/399;

(2) «vérifications aux frontières», les vérifications aux frontières telles que définies à l'article 2, point 11), du règlement (UE) 2016/399;

(3) «autorité frontalière», le garde-frontière chargé, conformément au droit national, d'effectuer les vérifications aux frontières;

(4) «autorités de contrôle», l'autorité de contrôle instituée conformément à l'article 51, paragraphe 1, du règlement (UE) 2016/679 et l'autorité de contrôle

instituée conformément à l'article 41, paragraphe 1, de la directive (UE) 2016/680;

(5) «vérification», le processus consistant à comparer des séries de données en vue d'établir la validité d'une identité déclarée (contrôle par comparaison de deux échantillons);

(6) «identification», le processus consistant à déterminer l'identité d'une personne par interrogation d'une base de données et comparaison avec plusieurs séries de données (contrôle par comparaison de plusieurs échantillons);

(7) «ressortissant de pays tiers», toute personne qui n'est pas citoyen de l'Union au sens de l'article 20, paragraphe 1, du traité, ou toute personne apatride ou toute personne dont la nationalité n'est pas connue;

(8) «données alphanumériques», les données représentées par des lettres, des chiffres, des caractères spéciaux, des espaces et des signes de ponctuation;

(9) «données d'identité», les données visées à l'article 27, paragraphe 3, points a) à h);

(10) «données dactyloscopiques», les données relatives aux empreintes digitales d'une personne;

(11) «image faciale», les images numériques du visage;

(12) «données biométriques», les données dactyloscopiques et/ou l'image faciale;

(13) «modèle biométrique», une représentation mathématique obtenue par l'extraction de caractéristiques des données biométriques, se limitant aux caractéristiques nécessaires pour procéder à des identifications et à des vérifications;

(14) «document de voyage», un passeport ou un document équivalent, autorisant son titulaire à franchir les frontières extérieures et pouvant revêtir un visa;

(15) «données du document de voyage», le type, le numéro et le pays de délivrance du document de voyage, la date d'expiration de sa validité et le code à trois lettres du pays de délivrance du document de voyage;

(16) «autorisation de voyage», l'autorisation de voyage telle que définie à l'article 3 du [règlement ETIAS];

(17) «visa de court séjour», le visa tel que défini à l'article 2, point 2) a), du règlement (CE) nº 810/2009;

(18) «systèmes d'information de l'UE», les systèmes informatiques à grande échelle gérés par l'eu-LISA;

(19) «données Europol», les données à caractère personnel fournies à Europol pour les finalités visées à l'article 18, paragraphe 2, point a), du règlement (UE) 2016/794;

(20) «bases de données d'Interpol», la base de données d'Interpol sur les documents de voyage volés et perdus (SLTD) et la base de données d'Interpol sur les documents de voyage associés aux notices (TDAWN Interpol);

(21) «correspondance», l'existence d'une correspondance établie en comparant deux ou plusieurs occurrences de données à caractère personnel enregistrées ou

en cours d'enregistrement dans un système d'information ou dans une base de données;

(22) «résultat positif», la confirmation d'une ou plusieurs correspondances;

(23) «autorité de police», une «autorité compétente» au sens de l'article 3, point 7), de la directive (UE) 2016/680;

(24) «autorités désignées», les autorités désignées par les États membres visées à l'article 29, paragraphe 1, du règlement (UE) 2017/2226, à l'article 3, paragraphe 1, de la décision 2008/633/JAI du Conseil, [à l'article 43 du règlement ETIAS] et [à l'article 6 du règlement Eurodac];

(25) «infraction terroriste», une infraction prévue par le droit national qui correspond ou est équivalente à l'une des infractions visées dans la directive (UE) 2017/541;

(26) «infraction pénale grave», une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, au titre du droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans;

(27) «EES», le système d'entrée/de sortie tel que visé dans le règlement (UE) 2017/2226;

(28) «VIS», le système d'information sur les visas tel que visé dans le règlement (CE) nº 767/2008;

(29) [«ETIAS», le système européen d'information et d'autorisation concernant les voyages tel que visé dans le règlement ETIAS];

(30) «Eurodac», Eurodac tel que visé dans le [règlement Eurodac];

(31) «SIS», le système d'information Schengen tel que visé dans [le règlement SIS dans le domaine des vérifications aux frontières, le règlement SIS dans le domaine répressif et le règlement SIS dans le domaine du retour des personnes en séjour irrégulier];

(32) [«système ECRIS-TCN», le système européen d'information sur les casiers judiciaires contenant des informations relatives aux condamnations des ressortissants de pays tiers et des personnes apatrides tel que visé dans le règlement ECRIS-TCN];

(33) «ESP», le portail de recherche européen tel que visé à l'article 6;

(34) «BMS partagé», le service partagé d'établissement de correspondances biométriques tel que visé à l'article 15;

(35) «CIR», le répertoire commun de données d'identité tel que visé à l'article 17;

(36) «MID», le détecteur d'identités multiples tel que visé à l'article 25;

(37) «CRRS», le répertoire central des rapports et statistiques tel que visé à l'article 39.

Article 5
Non-discrimination

Le traitement de données à caractère personnel aux fins du présent règlement ne donne lieu à aucune discrimination à l'encontre des personnes, fondée notamment sur le sexe, l'origine raciale ou ethnique, la religion ou les croyances, le handicap, l'âge ou l'orientation sexuelle. Il respecte pleinement la dignité humaine et l'intégrité des personnes. Une attention particulière est accordée aux enfants, aux personnes âgées et aux personnes handicapées.

CHAPITRE II
Portail de recherche européen

Article 6
Portail de recherche européen

1. Un portail de recherche européen (ESP) est créé afin de garantir que les autorités des États membres et les organes de l'UE bénéficient d'un accès rapide, continu, efficace, systématique et contrôlé aux systèmes d'information de l'UE, aux données Europol et aux bases de données d'Interpol dont ils ont besoin pour accomplir leurs tâches conformément à leurs droits d'accès, et afin de soutenir les objectifs de l'EES, du VIS, [de l'ETIAS], d'Eurodac, du SIS, [du système ECRIS-TCN] et des données Europol.

2. L'ESP se compose des éléments suivants:

   (a) une infrastructure centrale comportant un portail de recherche permettant d'interroger simultanément l'EES, le VIS, [l'ETIAS], Eurodac, le SIS, [le système ECRIS-TCN] ainsi que les données Europol et les bases de données d'Interpol;

   (b) un canal de communication sécurisé entre l'ESP, les États membres et les organes de l'UE qui sont autorisés à utiliser l'ESP conformément au droit de l'Union;

   (c) une infrastructure de communication sécurisée entre l'ESP et l'EES, le VIS, [l'ETIAS], Eurodac, le SIS central, [le système ECRIS-TCN], les données Europol et les bases de données d'Interpol ainsi qu'entre l'ESP et les infrastructures centrales du répertoire commun de données d'identité (CIR) et du détecteur d'identités multiples (MID).

3. L'eu-LISA développe l'ESP et en assure la gestion technique.

Article 7
Utilisation du portail de recherche européen

1. L'utilisation de l'ESP est réservée aux autorités des États membres et aux organes de l'UE ayant accès à l'EES, [à l'ETIAS], au VIS, au SIS, à Eurodac et [au système ECRIS-TCN], au CIR et au détecteur d'identités multiples, ainsi qu'aux données Europol et aux bases de données d'Interpol conformément au droit de l'Union ou au droit national régissant cet accès.

2. Les autorités visées au paragraphe 1 utilisent l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans les systèmes centraux d'Eurodac et du [système ECRIS-TCN] conformément aux droits

d'accès que leur confèrent le droit de l'Union et le droit national. Elles utilisent aussi l'ESP pour interroger le CIR conformément aux droits d'accès dont elles bénéficient en vertu du présent règlement aux fins visées aux articles 20, 21 et 22.

3. Les autorités des États membres visées au paragraphe 1 peuvent utiliser l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans le SIS central visé dans [le règlement SIS dans le domaine des vérifications aux frontières et le règlement SIS dans le domaine répressif]. L'accès au SIS central par l'intermédiaire de l'ESP est établi par le système national (N.SIS) de chaque État membre conformément à [l'article 4, paragraphe 2, du règlement SIS dans le domaine des vérifications aux frontières et du règlement SIS dans le domaine répressif].

4. Les organes de l'UE utilisent l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans le SIS central.

5. Les autorités des États membres visées au paragraphe 1 peuvent utiliser l'ESP pour effectuer des recherches dans les données relatives à des personnes ou à leurs documents de voyage dans les données Europol conformément aux droits d'accès que leur confèrent le droit de l'Union et le droit national.

Article 8
Profils des utilisateurs du portail de recherche européen

1. Afin de permettre l'utilisation de l'ESP, l'eu-LISA crée un profil pour chaque catégorie d'utilisateurs de l'ESP conformément aux détails techniques et aux droits d'accès visés au paragraphe 2, indiquant, conformément au droit de l'Union et au droit national:

   (a) les champs de données à utiliser pour la recherche;

   (b) les systèmes d'information de l'UE, les données Europol et les bases de données d'Interpol qui sont et peuvent être consultés et qui fournissent une réponse à l'utilisateur; et

   (c) les données fournies dans chaque réponse.

2. La Commission adopte des actes délégués conformément à l'article 63, afin de préciser les détails techniques des profils visés au paragraphe 1 pour les utilisateurs de l'ESP visés à l'article 7, paragraphe 1, conformément à leurs droits d'accès.

Article 9
Recherches

1. Les utilisateurs de l'ESP lancent une recherche en introduisant des données dans l'ESP conformément à leur profil d'utilisateur et à leurs droits d'accès. Lorsqu'une recherche a été lancée, l'ESP interroge simultanément, à l'aide des données introduites par l'utilisateur de l'ESP, l'EES, [l'ETIAS], le VIS, le SIS, Eurodac, [le système ECRIS-TCN] et le CIR ainsi que les données Europol et les bases de données d'Interpol.

2. Les champs de données utilisés pour lancer une recherche par l'intermédiaire de l'ESP correspondent aux champs de données relatifs à des personnes ou à des documents de voyage qui peuvent être utilisés pour interroger les différents systèmes

d'information de l'UE, les données Europol et les bases de données d'Interpol conformément aux instruments juridiques qui les régissent.

3. L'eu-LISA met en œuvre pour l'ESP un document de contrôle des interfaces (DCI) basé sur l'UMF visé à l'article 38.

4. L'EES, [l'ETIAS], le VIS, le SIS, Eurodac, [le système ECRIS-TCN], le CIR et le détecteur d'identités multiples, ainsi que les données Europol et les bases de données d'Interpol, fournissent les données qu'ils contiennent par suite de l'interrogation de l'ESP.

5. Lors de l'interrogation des bases de données d'Interpol, la conception de l'ESP garantit que les données employées par l'utilisateur de l'ESP pour lancer sa recherche ne sont pas partagées avec les propriétaires des données Interpol.

6. La réponse fournie à l'utilisateur de l'ESP est unique et comporte toutes les données auxquelles l'utilisateur a accès en vertu du droit de l'Union. Si nécessaire, la réponse fournie par l'ESP indique à quel système d'information ou à quelle base de données appartiennent les données.

7. La Commission adopte un acte délégué conformément à l'article 63 afin de préciser le contenu et le format des réponses de l'ESP.

Article 10
Tenue de registres

1. Sans préjudice de [l'article 39 du règlement Eurodac], [des articles 12 et 18 du règlement SIS dans le domaine répressif, [de l'article 29 du règlement ECRIS-TCN] et de l'article 40 du règlement (UE) 2016/794, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans l'ESP. Ces registres comprennent notamment les éléments suivants:

   (a) l'autorité de l'État membre et l'utilisateur individuel de l'ESP, notamment le profil ESP utilisé tel que visé à l'article 8;

   (b) la date et l'heure de la recherche;

   (c) les systèmes d'information de l'UE et les données Europol qui ont été interrogés;

   (d) conformément aux règles nationales ou au règlement (UE) 2016/794 ou, le cas échéant, au règlement (UE) nº 45/2001, les données d'identification de la personne qui a effectué la recherche.

2. Ces registres ne peuvent être utilisés que pour contrôler la protection des données, y compris la vérification de l'admissibilité d'une recherche et de la licéité du traitement des données, et pour garantir la sécurité des données en vertu de l'article 42. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création, sauf s'ils sont nécessaires à des procédures de contrôle déjà engagées.

Article 11

Procédures de secours en cas d'impossibilité technique d'utiliser le portail de recherche européen

1. Lorsqu'il est techniquement impossible d'utiliser l'ESP pour interroger un ou plusieurs des systèmes d'information de l'UE visés à l'article 9, paragraphe 1, ou le CIR, en raison d'une défaillance de l'ESP, l'eu-LISA en avertit les utilisateurs de l'ESP.

2. Lorsqu'il est techniquement impossible d'utiliser l'ESP pour interroger un ou plusieurs des systèmes d'information de l'UE visés à l'article 9, paragraphe 1, ou le CIR, en raison d'une défaillance de l'infrastructure nationale d'un État membre, l'autorité compétente de cet État membre en avertit l'eu-LISA et la Commission.

3. Dans les deux cas, et jusqu'à ce qu'il soit remédié à la défaillance technique, l'obligation visée à l'article 7, paragraphes 2 et 4, ne s'applique pas et les États membres peuvent accéder aux systèmes d'information visés à l'article 9, paragraphe 1, ou au CIR directement au moyen de leurs interfaces uniformes nationales ou de leurs infrastructures de communication nationales respectives.

CHAPITRE III
Service partagé de mise en correspondance de données biométriques

Article 12

Service partagé d'établissement de correspondances biométriques

1. Un service partagé d'établissement de correspondances biométriques (BMS partagé) stockant des modèles biométriques et permettant d'effectuer des recherches à l'aide de données biométriques dans plusieurs systèmes d'information de l'UE est mis en place afin de soutenir le CIR et le détecteur d'identités multiples ainsi que les objectifs de l'EES, du VIS, d'Eurodac, du SIS et [du système ECRIS-TCN].

2. Le BMS partagé se compose des éléments suivants:

   (a) une infrastructure centrale comportant un moteur de recherche et le stockage des données visées à l'article 13;

   (b) une infrastructure de communication sécurisée entre le BMS partagé, le SIS central et le CIR.

3. L'eu-LISA développe le BMS partagé et en assure la gestion technique.

Article 13

Données stockées dans le service partagé d'établissement de correspondances biométriques

1. Le BMS partagé stocke les modèles biométriques qu'il obtient à partir des données biométriques suivantes:

   (a) les données visées à l'article 16, paragraphe 1, point d), et à l'article 17, paragraphe 1, points b) et c), du règlement (UE) 2017/2226;

   (b) les données visées à l'article 9, point 6), du règlement (CE) nº 767/2008;

   (c) [les données visées à l'article 20, paragraphe 2, points w) et x), du règlement SIS dans le domaine des vérifications aux frontières;

(d) les données visées à l'article 20, paragraphe 3, points w) et x), du règlement SIS dans le domaine répressif;

(e) les données visées à l'article 4, paragraphe 3, points t) et u), du règlement SIS dans le domaine du retour des personnes en séjour irrégulier];

(f) [les données visées à l'article 13, point a), du règlement Eurodac;]

(g) [les données visées à l'article 5, paragraphe 1, point b), et à l'article 5, paragraphe 2, du règlement ECRIS-TCN.]

2. Le BMS partagé inclut, dans chaque modèle biométrique, une référence aux systèmes d'information dans lesquels les données biométriques correspondantes sont stockées.

3. Les modèles biométriques sont introduits dans le BMS partagé uniquement après que ce dernier a effectué un contrôle automatisé de la qualité des données biométriques ajoutées à l'un des systèmes d'information, afin de s'assurer du respect d'une norme de qualité des données minimale.

4. Le stockage des données visées au paragraphe 1 respecte les normes de qualité visées à l'article 37, paragraphe 2.

Article 14
Recherche dans des données biométriques à l'aide du service partagé d'établissement de correspondances biométriques

Afin que des recherches puissent être effectuées dans les données biométriques stockées dans le CIR et le SIS, le CIR et le SIS utilisent les modèles biométriques stockés dans le BMS partagé. Les recherches effectuées à l'aide de données biométriques sont effectuées conformément aux finalités prévues dans le présent règlement et dans le règlement EES, le règlement VIS, le règlement Eurodac, les [règlements SIS] et [le règlement ECRIS-TCN].

Article 15
Conservation des données dans le service partagé d'établissement de correspondances biométriques

Les données visées à l'article 13 sont stockées dans le BMS partagé tant que les données biométriques correspondantes sont stockées dans le CIR ou le SIS.

Article 16
Tenue de registres

1. Sans préjudice de [l'article 39 du règlement Eurodac], [des articles 12 et 18 du règlement SIS dans le domaine répressif, et [de l'article 29 du règlement ECRIS-TCN], l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le BMS partagé. Ces registres comprennent notamment les éléments suivants:

(a) l'historique lié à la création et au stockage des modèles biométriques;

(b) une référence aux systèmes d'information de l'UE interrogés à l'aide des modèles biométriques stockés dans le BMS partagé;

(c) la date et l'heure de la recherche;

(d) le type de données biométriques utilisées pour lancer la recherche;

(e) la durée de la recherche;

(f) les résultats de la recherche ainsi que la date et l'heure des résultats;

(g) conformément aux règles nationales ou au règlement (UE) 2016/794 ou, le cas échéant, au règlement (UE) nº 45/2001, les données d'identification de la personne qui a effectué la recherche.

2. Ces registres ne peuvent être utilisés que pour contrôler la protection des données, y compris la vérification de l'admissibilité d'une recherche et de la licéité du traitement des données, et pour garantir la sécurité des données en vertu de l'article 42. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création, sauf s'ils sont nécessaires à des procédures de contrôle déjà engagées. Les registres visés au paragraphe 1, point a), sont effacés une fois les données supprimées.

CHAPITRE IV
Répertoire commun de données d'identité

Article 17
Répertoire commun de données d'identité

1. Un répertoire commun de données d'identité (CIR), créant un dossier individuel pour chaque personne enregistrée dans l'EES, le VIS, [l'ETIAS], Eurodac ou [le système ECRIS-TCN] contenant les données visées à l'article 18, est établi afin de simplifier et de faciliter l'identification correcte des personnes enregistrées dans l'EES, le VIS, [l'ETIAS], Eurodac et [le système ECRIS-TCN], d'appuyer le fonctionnement du détecteur d'identités multiples et de faciliter et de rationaliser l'accès des services répressifs aux systèmes d'information à finalité non répressive au niveau de l'UE, lorsque cela est nécessaire à des fins de prévention et de détection des infractions graves, d'enquêtes et de poursuites en la matière.

2. Le CIR se compose des éléments suivants:

(a) une infrastructure centrale qui remplace les systèmes centraux de l'EES, du VIS, [de l'ETIAS], d'Eurodac et [du système ECRIS-TCN] respectivement, dans la mesure où elle stocke les données visées à l'article 18;

(b) un canal de communication sécurisé entre le CIR, les États membres et les organes de l'UE qui sont autorisés à utiliser le portail de recherche européen (ESP) conformément au droit de l'Union;

(c) une infrastructure de communication sécurisée entre le CIR et l'EES, [l'ETIAS], le VIS, Eurodac et [le système ECRIS-TCN], ainsi que les infrastructures centrales de l'ESP, du BMS partagé et du détecteur d'identités multiples.

3. L'eu-LISA développe le CIR et en assure la gestion technique.

Article 18

Données du répertoire commun de données d'identité

1. Le CIR stocke les données suivantes – logiquement séparées – en fonction du système d'information dont elles proviennent:

   (a) – (sans objet);

   (b) – (sans objet);

   (c) – (sans objet);

   (d) les données visées à l'article 13, point a) à e), g) et h) du [règlement Eurodac];

   (e) [Les données visées à l'article 5, paragraphe 1, point b), et à l'article 5, paragraphe 2, ainsi que les données suivantes visées à l'article 5, paragraphe 1, point a), du règlement ECRIS-TCN: nom de famille; prénom(s); sexe; date de naissance; lieu et pays de naissance; nationalité(s); genre et, s'il y a lieu, nom et prénoms précédents, pseudonyme(s) et/ou nom(s) d'emprunt.]

2. Pour chaque ensemble de données visé au paragraphe 1, le CIR comporte une référence aux systèmes d'information auxquels appartiennent les données.

3. Le stockage des données visées au paragraphe 1 respecte les normes de qualité visées à l'article 37, paragraphe 2.

Article 19

Ajout, modification et suppression de données dans le répertoire commun de données d'identité

1. Lorsque des données sont ajoutées, modifiées ou supprimées dans Eurodac ou dans [le système ECRIS-TCN], les données visées à l'article 18 qui sont stockées dans le dossier individuel du CIR font l'objet, de manière automatisée, d'un ajout, d'une modification ou d'une suppression en conséquence.

2. Lorsque le détecteur d'identités multiples crée un lien blanc ou rouge conformément aux articles 32 et 33 entre les données de deux ou plusieurs des systèmes d'information de l'UE alimentant le CIR, au lieu de créer un nouveau dossier individuel, le CIR ajoute les nouvelles données au dossier individuel des données liées.

Article 20

Accès au répertoire commun de données d'identité pour identification

1. Lorsqu'une autorité de police d'un État membre y a été habilitée par les mesures législatives nationales visées au paragraphe 2, elle peut, uniquement aux fins de l'identification d'une personne, interroger le CIR à l'aide des données biométriques de cette personne relevées lors d'un contrôle d'identité.

   Lorsque la recherche indique que des données concernant cette personne sont stockées dans le CIR, l'autorité de l'État membre a accès aux données visées à l'article 18, paragraphe 1, pour les consulter.

   Lorsque les données biométriques de la personne ne peuvent pas être utilisées ou lorsque la recherche effectuée avec ces données échoue, la recherche est effectuée à

l'aide des données d'identité de cette personne, combinées aux données du document de voyage, ou à l'aide des données d'identité fournies par cette personne.

2. Les États membres qui souhaitent faire usage de la possibilité prévue au présent article adoptent des mesures législatives nationales. Ces mesures législatives indiquent les finalités précises des contrôles d'identité, parmi les finalités visées à l'article 2, paragraphe 1, points b) et c). Elles désignent les autorités de police compétentes et fixent les procédures, les conditions et les critères relatifs à ces contrôles.

Article 21

Accès au répertoire commun de données d'identité pour la détection d'identités multiples

1. Lorsque le résultat d'une interrogation du CIR donne lieu à un lien jaune conformément à l'article 28, paragraphe 4, l'autorité chargée de la vérification des différentes identités déterminée conformément à l'article 29 a accès, aux seules fins de cette vérification, aux données d'identité stockées dans le CIR qui appartiennent aux différents systèmes d'information connectés au lien jaune.

2. Lorsque le résultat d'une interrogation du CIR donne lieu à un lien rouge conformément à l'article 32, les autorités visées à l'article 26, paragraphe 2, ont accès, aux seules fins de lutter contre la fraude à l'identité, aux données d'identité stockées dans le CIR qui appartiennent aux différents systèmes d'information connectés au lien rouge.

Article 22

Interrogation du répertoire commun de données d'identité à des fins répressives

1. Aux fins de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, et des enquêtes en la matière, dans un cas particulier et pour savoir si des données sur une personne en particulier sont présentes dans Eurodac, les autorités désignées des États membres et Europol peuvent consulter le CIR.

2. Les autorités désignées des États membres et Europol ne sont pas autorisés à consulter les données appartenant à [l'ECRIS-TCN] lors de la consultation du CIR aux fins indiquées au paragraphe 1.

3. Lorsque, en réponse à une recherche, le CIR indique que des données sur cette personne sont présentes dans Eurodac, le CIR fournit aux autorités désignées des États membres et à Europol une réponse, sous la forme d'une référence, indiquant le ou les systèmes d'information qui contiennent les données correspondantes visées à l'article 18, paragraphe 2. Le CIR fournit une réponse selon des modalités qui ne compromettent pas la sécurité des données.

4. L'accès complet aux données figurant dans les systèmes d'information de l'UE aux fins de prévenir et détecter les infractions terroristes et les infractions pénales graves, et d'enquêter sur celles-ci, reste soumis aux conditions et procédures prévues dans les instruments législatifs respectifs régissant cet accès.

Article 23

Conservation des données dans le répertoire commun de données d'identité

1. Les données visées à l'article 18, paragraphes 1 et 2, sont supprimées du CIR conformément aux dispositions relatives à la conservation des données du [règlement Eurodac] et [du règlement ECRIS-TCN] respectivement.

2. Le dossier individuel est stocké dans le CIR tant que les données correspondantes sont stockées dans au moins un des systèmes d'information dont les données figurent dans le CIR. La création d'un lien n'a aucune incidence sur la période de conservation de chaque élément des données liées.

Article 24

Tenue de registres

1. Sans préjudice de [l'article 39 du règlement Eurodac] et [de l'article 29 de la proposition ECRIS-TCN], l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR conformément aux paragraphes 2, 3 et 4.

2. En ce qui concerne tout accès au CIR en vertu de l'article 20, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR. Ces registres comprennent notamment les éléments suivants:

   (a) la finalité de l'accès par l'utilisateur qui effectue la recherche par l'intermédiaire du CIR;

   (b) la date et l'heure de la recherche;

   (c) le type de données utilisées pour lancer la recherche;

   (d) les résultats de la recherche;

   (e) conformément aux règles nationales ou au règlement (UE) 2016/794 ou, le cas échéant, au règlement (UE) nº 45/2001, les données d'identification de la personne qui a effectué la recherche.

3. En ce qui concerne tout accès au CIR en vertu de l'article 21, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR. Ces registres comprennent notamment les éléments suivants:

   (a) la finalité de l'accès par l'utilisateur qui effectue la recherche par l'intermédiaire du CIR;

   (b) la date et l'heure de la recherche;

   (c) s'il y a lieu, les données utilisées pour lancer la recherche;

   (d) s'il y a lieu, les résultats de la recherche;

   (e) conformément aux règles nationales ou au règlement (UE) 2016/794 ou, le cas échéant, au règlement (UE) nº 45/2001, les données d'identification de la personne qui a effectué la recherche.

4. En ce qui concerne tout accès au CIR en vertu de l'article 22, l'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le CIR. Ces registres comprennent notamment les éléments suivants:

   (a) la référence du dossier national;

(b) la date et l'heure de la recherche;

(c) le type de données utilisées pour lancer la recherche;

(d) les résultats de la recherche;

(e) le nom de l'autorité consultant le CIR;

(f) conformément aux règles nationales ou au règlement (UE) 2016/794 ou, le cas échéant, au règlement (UE) nº 45/2001, les données d'identification de l'agent qui a effectué la recherche et celles de l'agent qui l'a ordonnée.

L'autorité de contrôle compétente instituée conformément à l'article 51 du règlement (UE) 2016/679 ou conformément à l'article 41 de la directive (UE) 2016/680 vérifie régulièrement les registres de ces accès, à des intervalles ne dépassant pas six mois, afin de vérifier si les procédures et conditions prévues à l'article 22, paragraphes 1 à 3, sont remplies.

5. Chaque État membre tient des registres des recherches effectuées par le personnel dûment autorisé à utiliser le CIR en vertu des articles 20, 21 et 22.

6. Les registres visés aux paragraphes 1 et 5 ne peuvent être utilisés que pour contrôler la protection des données, y compris la vérification de l'admissibilité d'une demande et de la licéité du traitement des données, et pour garantir la sécurité des données en vertu de l'article 42. Ils sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création, sauf s'ils sont nécessaires à des procédures de contrôle déjà engagées.

7. L'eu-LISA tient des registres relatifs à l'historique des données stockées dans le dossier individuel, aux fins définies au paragraphe 6. Les registres relatifs à l'historique des données stockées sont effacés une fois les données supprimées.

CHAPITRE V
Détecteur d'identités multiples

Article 25
Détecteur d'identités multiples

1. Un détecteur d'identités multiples (MID) qui crée et stocke des liens entre les données des systèmes d'information de l'UE figurant dans le répertoire commun de données d'identité (CIR) et dans le SIS et qui, par conséquent, détecte les identités multiples, dans le double objectif de faciliter les contrôles d'identité et de lutter contre la fraude à l'identité, est établi afin de soutenir le fonctionnement du CIR et les objectifs de l'EES, du VIS, [de l'ETIAS], d'Eurodac, du SIS et [du système ECRIS-TCN].

2. Le MID se compose des éléments suivants:

(a) une infrastructure centrale qui stocke des liens et des références aux systèmes d'information;

(b) une infrastructure de communication sécurisée pour connecter le MID au SIS et aux infrastructures centrales du portail de recherche européen et du CIR.

3. L'eu-LISA développe le MID et en assure la gestion technique.

Article 26
Accès au détecteur d'identités multiples

1. Aux fins de la vérification manuelle des identités visée à l'article 29, l'accès aux données visées à l'article 34 stockées dans le MID est accordé:

   (a) – (sans objet);

   (b) – (sans objet);

   (c) – (sans objet);

   (d) aux autorités compétentes pour évaluer une demande de protection internationale prévues dans le règlement Eurodac, lorsqu'elles examinent une nouvelle demande de protection internationale;

   (e) aux bureaux SIRENE de l'État membre qui créent [un signalement conformément au règlement SIS dans le domaine du retour des personnes en séjour irrégulier];

   (f) [aux autorités centrales de l'État membre de condamnation lorsqu'elles enregistrent ou actualisent des données dans le système ECRIS-TCN conformément à l'article 5 du règlement ECRIS-TCN.]

2. Les autorités des États membres et les organes de l'UE ayant accès à au moins un système d'information de l'UE alimentant le répertoire commun de données d'identité ou au SIS ont accès aux données visées à l'article 34, points a) et b), en ce qui concerne les liens rouges visés à l'article 32.

Article 27
Détection d'identités multiples

1. Une détection d'identités multiples dans le répertoire commun de données d'identité et le SIS est lancée lorsque:

   (a) – (sans objet);

   (b) – (sans objet);

   (c) – (sans objet);

   (d) [une demande de protection internationale est créée ou actualisée dans Eurodac conformément à l'article 10 du règlement Eurodac];

   (e) [un signalement de personne est créé ou actualisé dans le SIS conformément aux chapitres VI, VII, VIII et IX du règlement sur le SIS dans le domaine répressif et à l'article 3 du règlement sur le SIS dans le domaine du retour illégal];

   (f) [un enregistrement de données est créé ou actualisé dans le système ECRIS-TCN conformément à l'article 5 du règlement sur l'ECRIS-TCN.]

2. Lorsque les données figurant dans un système d'information mentionné au paragraphe 1 comportent des données biométriques, le répertoire commun de données d'identité (CIR) et le SIS central utilisent le service partagé d'établissement de correspondances biométriques (BMS partagé) pour détecter les identités multiples. Le BMS partagé compare les modèles biométriques obtenus à partir de toute nouvelle donnée biométrique avec les modèles biométriques figurant déjà dans

le BMS partagé afin de vérifier si des données relatives au même ressortissant de pays tiers sont déjà stockées dans le CIR ou dans le SIS central.

3. Outre le processus exposé au paragraphe 2, le CIR et le SIS central utilisent le portail de recherche européen pour effectuer des recherches dans les données stockées dans le CIR et le SIS central, à l'aide des données suivantes:

(a) – (sans objet);

(b) – (sans objet);

(c) – (sans objet);

(d) [nom(s); prénom(s); nom(s) à la naissance, noms utilisés antérieurement et pseudonymes; date de naissance, lieu de naissance, nationalité(s) et sexe tels que visés à l'article 12 du règlement Eurodac];

(e) – (sans objet);

(f) [nom(s); prénom(s); nom(s) à la naissance, noms utilisés antérieurement et pseudonymes; date de naissance, lieu de naissance, nationalité(s) et sexe tels que visés à l'article 20, paragraphe 3, du règlement SIS dans le domaine répressif];

(g) [nom(s); prénom(s); nom(s) à la naissance, noms utilisés antérieurement et pseudonymes; date de naissance, lieu de naissance, nationalité(s) et sexe tels que visés à l'article 4 du règlement SIS dans du retour des personnes en séjour irrégulier];

(h) [nom (nom de famille); prénom(s); date de naissance, lieu de naissance, nationalité(s) et sexe tels que visés à l'article 5, paragraphe 1, point a), du règlement ECRIS-TCN];

4. La détection d'identités multiples n'est lancée que pour comparer les données disponibles dans un système d'information à celles qui sont disponibles dans d'autres systèmes d'information.

Article 28
Résultats de la détection d'identités multiples

1. Lorsque la recherche visée à l'article 27, paragraphe 2 ou 3, ne génère aucun résultat positif, les procédures visées à l'article 27, paragraphe 1, se poursuivent conformément aux règlements respectifs qui les régissent.

2. Lorsque la recherche visée à l'article 27, paragraphe 2 ou 3, génère un ou plusieurs résultats positifs, le répertoire commun de données d'identité et, s'il y a lieu, le SIS créent un lien entre les données utilisées pour lancer la recherche et les données ayant produit le résultat positif.

Lorsque plusieurs résultats positifs sont signalés, un lien est créé entre toutes les données ayant donné lieu au résultat positif. Lorsque les données étaient déjà liées, le lien existant est étendu aux données utilisées pour lancer la recherche.

3. Lorsque la recherche visée à l'article 27, paragraphe 2 ou 3, génère un ou plusieurs résultats positifs et que les données d'identité des dossiers liés sont identiques ou similaires, un lien blanc est créé conformément à l'article 33.

4. Lorsque la recherche visée à l'article 27, paragraphe 2 ou 3, génère un ou plusieurs résultats positifs et que les données d'identité des dossiers liés ne peuvent pas être

considérées comme similaires, un lien jaune est créé conformément à l'article 30 et la procédure visée à l'article 29 s'applique.

5. La Commission définit, dans des actes d'exécution, les procédures permettant de déterminer les cas dans lesquels les données d'identité peuvent être considérées comme identiques ou similaires. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 64, paragraphe 2.

6. Les liens sont stockés dans le dossier de confirmation d'identité visé à l'article 34.

La Commission définit, dans des actes d'exécution, les règles techniques permettant de lier les données de différents systèmes d'information. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 64, paragraphe 2.

Article 29
Vérification manuelle des différentes identités

1. Sans préjudice du paragraphe 2, l'autorité chargée de la vérification des différentes identités est:

(a) – (sans objet);

(b) – (sans objet);

(c) – (sans objet);

(d) l'autorité compétente pour évaluer une demande de protection internationale prévue dans le règlement Eurodac, en ce qui concerne les résultats positifs générés lors de l'examen de cette demande;

(e) les bureaux SIRENE de l'État membre en ce qui concerne les résultats positifs générés lors de la création d'un signalement SIS conformément aux [règlements sur le SIS dans le domaine répressif et sur le SIS dans le domaine du retour illégal];

(f) les autorités centrales de l'État membre de condamnation en ce qui concerne les résultats positifs générés lors de l'enregistrement ou de l'actualisation de données dans le système ECRIS-TCN conformément à l'article 5 du [règlement ECRIS-TCN.]

Le détecteur d'identités multiples indique l'autorité chargée de vérifier les différentes identités dans le dossier de vérification des identités.

2. L'autorité chargée de la vérification des différentes identités dans le dossier de confirmation d'identité est le bureau SIRENE de l'État membre qui a créé le signalement lorsqu'un lien est créé vers les données figurant:

(a) dans un signalement de personnes recherchées en vue d'une arrestation aux fins de remise ou d'extradition, visé à l'article 26 [du règlement SIS dans le domaine répressif];

(b) dans un signalement de personnes disparues ou vulnérables, visé à l'article 32 du [règlement SIS dans le domaine répressif];

(c) dans un signalement de personnes recherchées dans le but de rendre possible leur concours dans le cadre d'une procédure judiciaire, visé à l'article 34 du [règlement SIS dans le domaine répressif];

(d) [dans un signalement de retour conformément au règlement SIS dans le

domaine du retour des personnes en séjour irrégulier];

(e) dans un signalement de personnes aux fins de contrôle discret, de contrôle d'investigation ou de contrôle spécifique, visé à l'article 36 du [règlement SIS dans le domaine répressif];

(f) dans un signalement de personnes recherchées inconnues à des fins d'identification conformément au droit national et consultation à l'aide de données biométriques, visé à l'article 40 du [règlement SIS dans le domaine répressif].

3. Sans préjudice du paragraphe 4, l'autorité chargée de la vérification des différentes identités a accès aux données connexes figurant dans le dossier de confirmation d'identité pertinent et aux données d'identité liées figurant dans le répertoire commun de données d'identité et, s'il y a lieu, dans le SIS, et elle évalue les différentes identités, met à jour le lien conformément aux articles 31, 32 et 33, puis l'ajoute sans délai au dossier de confirmation d'identité.

4. – (sans objet).

5. En cas d'obtention de plusieurs liens, l'autorité chargée de la vérification des différentes identités évalue chaque lien séparément.

6. Lorsque des données faisant l'objet d'un résultat positif sont déjà liées, l'autorité chargée de la vérification des différentes identités tient compte des liens existants lorsqu'elle envisage d'en créer de nouveaux.

Article 30
Lien jaune

1. Un lien entre des données provenant d'au moins deux systèmes d'information est classé comme jaune dans les cas suivants:

(a) les données liées comportent les mêmes données biométriques mais des données d'identité différentes et aucune vérification manuelle des différentes identités n'a été effectuée;

(b) les données liées comportent des données d'identité différentes et aucune vérification manuelle des différentes identités n'a été effectuée.

2. Lorsqu'un lien est classé comme jaune conformément au paragraphe 1, la procédure prévue à l'article 29 s'applique.

Article 31
Lien vert

1. Un lien entre des données provenant d'au moins deux systèmes d'information est classé comme vert lorsque les données liées ne comportent pas les mêmes données biométriques mais contiennent des données d'identité similaires et que l'autorité chargée de la vérification des différentes identités a conclu que ces données désignaient deux personnes différentes.

2. Lorsque le répertoire commun de données d'identité (CIR) ou le SIS sont interrogés et qu'il existe un lien vert entre au moins deux systèmes d'information alimentant le CIR, ou avec le SIS, le détecteur d'identités multiples indique que les données d'identité des données liées ne correspondent pas à la même personne. Le système

d'information interrogé fournit une réponse indiquant uniquement les données de la personne dont les données ont été utilisées pour la recherche, sans donner lieu à un résultat positif au regard des données qui font l'objet du lien vert.

Article 32
Lien rouge

1. Un lien entre des données provenant d'au moins deux systèmes d'information est classé comme rouge dans les cas suivants:

   (a) les données liées comportent les mêmes données biométriques mais des données d'identité différentes et l'autorité chargée de la vérification des différentes identités a conclu que ces données désignaient de manière illicite la même personne;

   (b) les données liées comportent des données d'identité similaires et l'autorité chargée de la vérification des différentes identités a conclu que ces données désignaient de manière illicite la même personne.

2. Lorsque le CIR ou le SIS sont interrogés et qu'il existe un lien rouge entre au moins deux systèmes d'information alimentant le CIR, ou avec le SIS, le détecteur d'identités multiples fournit une réponse indiquant les données visées à l'article 34. Les mesures à prendre pour donner suite à un lien rouge sont exécutées conformément au droit l'Union et au droit national.

3. Lorsqu'un lien rouge est créé entre des données provenant de l'EES, du VIS, [de l'ETIAS], d'Eurodac ou [du système ECRIS-TCN], le dossier individuel stocké dans le CIR est mis à jour conformément à l'article 19, paragraphe 1.

4. Sans préjudice des dispositions relatives au traitement des signalements dans le SIS visé dans le [règlement SIS dans le domaine des vérifications aux frontières, le règlement SIS dans le domaine répressif et le règlement SIS dans le domaine du retour des personnes en séjour irrégulier], et sans préjudice des restrictions nécessaires pour protéger la sécurité et l'ordre public, prévenir la criminalité et garantir qu'aucune enquête nationale ne sera compromise, lorsqu'un lien rouge est créé, l'autorité chargée de la vérification des différentes identités informe la personne de la présence d'identités multiples illicites.

5. Lorsqu'un lien rouge est créé, l'autorité chargée de la vérification des différentes identités indique la référence des autorités responsables des données liées.

Article 33
Lien blanc

1. Un lien entre des données provenant d'au moins deux systèmes d'information est classé comme blanc dans les cas suivants:

   (a) les données liées comportent les mêmes données biométriques et des données d'identité identiques ou similaires;

   (b) les données liées comportent des données d'identité identiques ou similaires et au moins l'un des systèmes d'information ne contient pas de données biométriques sur la personne;

   (c) les données liées comportent les mêmes données biométriques mais des données d'identité différentes et l'autorité chargée de la vérification des

différentes identités a conclu que ces données désignaient la même personne qui possède, légalement, des données d'identité différentes.

2. Lorsque le CIR ou le SIS sont interrogés et qu'il existe un lien blanc entre au moins deux systèmes d'information alimentant le CIR, ou avec le SIS, le détecteur d'identités multiples indique que les données d'identité des données liées correspondent à la même personne. Les systèmes d'information interrogés fournissent une réponse indiquant, le cas échéant, toutes les données liées sur la personne, donnant ainsi lieu à un résultat positif au regard des données qui font l'objet du lien blanc, si l'autorité qui a lancé la recherche a accès aux données liées en vertu du droit de l'Union ou du droit national.

3. Lorsqu'un lien blanc est créé entre des données provenant de l'EES, du VIS, [de l'ETIAS], d'Eurodac ou [du système ECRIS-TCN], le dossier individuel stocké dans le CIR est mis à jour conformément à l'article 19, paragraphe 1.

4. Sans préjudice des dispositions relatives au traitement des signalements dans le SIS visé dans le [règlement SIS dans le domaine des vérifications aux frontières, le règlement SIS dans le domaine répressif et le règlement SIS dans le domaine du retour des personnes en séjour irrégulier], lorsqu'un lien blanc est créé à la suite d'une vérification manuelle des identités multiples, l'autorité chargée de la vérification des différentes identités informe la personne de l'existence de divergences entre les données à caractère personnel la concernant figurant dans les systèmes et lui indique la référence des autorités responsables des données liées.

Article 34
Dossier de confirmation d'identité

Le dossier de confirmation d'identité contient les données suivantes:

(a) les liens, notamment leur description sous forme de couleurs, visés aux articles 30 à 33;

(b) une référence aux systèmes d'information dont les données sont liées;

(c) un numéro d'identification unique permettant d'extraire, des systèmes d'information, les données des dossiers liés correspondants;

(d) s'il y a lieu, l'autorité responsable de la vérification des différentes identités.

Article 35
Conservation des données dans le détecteur d'identités multiples

Les dossiers de confirmation d'identité et leurs données, y compris les liens, ne sont stockés dans le détecteur d'identités multiples (MID) que tant que les données liées sont stockées dans au moins deux systèmes d'information de l'UE.

Article 36
Tenue de registres

1. L'eu-LISA tient des registres de toutes les opérations de traitement de données effectuées dans le MID. Ces registres comprennent notamment les éléments suivants:

(a) la finalité de l'accès par l'utilisateur et les droits d'accès de celui-ci;

(b) la date et l'heure de la recherche;

(c) le type de données utilisées pour lancer la ou les recherches;

(d) la référence aux données liées;

(e) l'historique du dossier de confirmation d'identité;

(f) les données d'identification de la personne qui a effectué la recherche.

2. Chaque État membre tient un registre du personnel dûment autorisé à utiliser le MID.

3. Ces registres ne peuvent être utilisés que pour contrôler la protection des données, y compris la vérification de l'admissibilité d'une demande et de la licéité du traitement des données, et pour garantir la sécurité des données en vertu de l'article 42. Ces registres sont protégés par des mesures appropriées empêchant tout accès non autorisé et sont effacés un an après leur création, sauf s'ils sont nécessaires à des procédures de contrôle déjà engagées. Les registres relatifs à l'historique du dossier de confirmation d'identité sont effacés une fois que les données de ce dossier ont été supprimées.

CHAPTER VI
Mesures soutenant l'interopérabilité

Article 37
Qualité des données

1. L'eu-LISA met en place des mécanismes et procédures automatisés de contrôle de la qualité des données pour les données stockées dans le SIS, Eurodac, [le système ECRIS-TCN], le service partagé d'établissement de correspondances biométriques (BMS partagé), le répertoire commun de données d'identité (CIR) et le détecteur d'identités multiples (MID).

2. L'eu-LISA établit des indicateurs communs de qualité des données et les normes de qualité minimales pour le stockage de données dans le SIS, Eurodac, [le système ECRIS-TCN], le BMS partagé, le CIR et le MID.

3. L'eu-LISA présente aux États membres des rapports réguliers sur les mécanismes et procédures automatisés de contrôle de la qualité des données et les indicateurs communs de qualité des données. L'eu-LISA fournit également à la Commission un rapport régulier sur les problèmes rencontrés et les États membres concernés.

4. Les détails des mécanismes et procédures automatisés de contrôle de la qualité des données, des indicateurs communs de qualité des données et des normes de qualité minimales pour le stockage de données dans le SIS, Eurodac, [le système ECRIS-TCN], le BMS partagé, le CIR et le MID, notamment en ce qui concerne les données biométriques, sont définis dans des actes d'exécution. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 64, paragraphe 2.

5. Un an après la mise en place des mécanismes et procédures automatisés de contrôle de la qualité des données et des indicateurs communs de qualité des données, puis tous les ans, la Commission évalue chaque année la mise en œuvre de la qualité des données par les États membres et formule les recommandations nécessaires en la matière. Les États membres fournissent à la Commission un plan d'action visant à

remédier aux manquements constatés dans le rapport d'évaluation et font rapport sur les progrès réalisés au regard de ce plan d'action jusqu'à ce que celui-ci soit entièrement mis en œuvre. La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne instituée par le règlement (CE) nº 168/2007 du Conseil[63].

Article 38
Format universel pour les messages

1. La norme de format universel pour les messages (UMF) est établie. L'UMF définit les normes applicables à certains contenus des échanges d'informations transfrontières entre les systèmes d'information, les autorités et/ou les organismes dans le domaine de la justice et des affaires intérieures.

2. La norme UMF est utilisée pour le développement d'[Eurodac], du [système ECRIS-TCN], du portail de recherche européen, du CIR, du MID et, au besoin, pour l'élaboration, par l'eu-LISA ou tout autre organe de l'UE, de nouveaux modèles d'échange d'informations et systèmes d'information dans le domaine de la justice et des affaires intérieures.

3. La mise en œuvre de la norme UMF peut être envisagée dans le SIS et dans tout modèle ou système d'information transfrontière, existant ou nouveau, dans le domaine de la justice et des affaires intérieures, mis au point par les États membres ou les pays associés.

4. La Commission adopte un acte d'exécution pour définir et élaborer la norme UMF visée au paragraphe 1. Cet acte d'exécution est adopté conformément à la procédure d'examen visée à l'article 64, paragraphe 2.

Article 39
Répertoire central des rapports et statistiques

1. Un répertoire central des rapports et statistiques (CRRS) est créé pour soutenir les objectifs d'[Eurodac], du SIS et du [système ECRIS-TCN] et pour produire des statistiques intersystèmes et des rapports analytiques aux fins des politiques menées, des exigences opérationnelles et de la qualité des données.

2. L'eu-LISA établit, met en œuvre et héberge le CRRS sur ses sites techniques, contenant les données visées à [l'article 42, paragraphe 8, du règlement Eurodac], [à l'article 71 du règlement SIS dans le domaine répressif] et [à l'article 30 du règlement ECRIS-TCN], logiquement séparées. Les données figurant dans le CRRS ne permettent pas l'identification des personnes. L'accès au répertoire est accordé de manière sécurisée par l'intermédiaire du réseau de services télématiques transeuropéens sécurisés entre administrations (TESTA), moyennant un contrôle de l'accès et des profils d'utilisateur spécifiques, aux seules fins de l'élaboration de rapports et de statistiques, aux autorités visées à [l'article 42, paragraphe 8, du règlement Eurodac], [à l'article 71 du règlement SIS dans le domaine répressif] et [à l'article 30 du règlement ECRIS-TCN].

[63] Règlement (CE) nº 168/2007 du Conseil du 15 février 2007 portant création d'une Agence des droits fondamentaux de l'Union européenne (JO L 53 du 22.2.2007, p. 1).

3. L’eu-LISA anonymise les données et enregistre ces données anonymisées dans le CRRS. Le processus d’anonymisation des données est automatisé.

4. Le CRRS se compose des éléments suivants:

   (a) une infrastructure centrale, comprenant un répertoire de données permettant de rendre les données anonymes;

   (b) une infrastructure de communication sécurisée pour connecter le CRRS au SIS, à Eurodac et au [système ECRIS-TCN], ainsi qu'aux infrastructures centrales du BMS partagé, du CIR et du MID.

5. La Commission établit des règles détaillées concernant le fonctionnement du CRRS, notamment des garanties spécifiques pour le traitement des données à caractère personnel visées aux paragraphes 2 et 3, ainsi que des règles de sécurité applicables au répertoire, au moyen d’actes d’exécution. Ces actes d’exécution sont adoptés conformément à la procédure d’examen visée à l’article 64, paragraphe 2.

CHAPITRE VII
Protection des données

Article 40
Responsable du traitement des données

1. En ce qui concerne le traitement des données dans le service partagé d’établissement de correspondances biométriques (BMS partagé), les autorités des États membres qui sont responsables du traitement pour le SIS, Eurodac et le [système ECRIS-TCN], respectivement, sont également considérées comme responsables du traitement au sens de l’article 4, point 7), du règlement (UE) 2016/679 en ce qui concerne les modèles biométriques obtenus à partir des données visées à l’article 13 qu’elles saisissent dans les systèmes respectifs et sont chargées du traitement des modèles biométriques dans le BMS partagé.

2. En ce qui concerne le traitement des données dans le répertoire commun de données d’identité (CIR), les autorités des États membres qui sont responsables du traitement pour Eurodac et le [système ECRIS-TCN], respectivement, sont également considérées comme responsables du traitement au sens de l’article 4, point 7), du règlement (UE) 2016/679 en ce qui concerne les données visées à l’article 18 qu’elles saisissent dans les systèmes respectifs et sont chargées du traitement de ces données à caractère personnel dans le CIR.

3. En ce qui concerne le traitement des données dans le détecteur d’identités multiples:

   (a) l’Agence européenne de garde-frontières et de garde-côtes est considérée comme responsable du traitement au sens de l’article 2, point b), du règlement (CE) nº 45/2001 en ce qui concerne le traitement des données à caractère personnel par l’unité centrale de l’ETIAS;

   (b) les autorités des États membres qui ajoutent des données dans le dossier de confirmation d’identité ou en modifient les données doivent également être considérées comme responsables du traitement au sens de l’article 4, point 7), du règlement (UE) 2016/679 et sont chargées du traitement des données à caractère personnel dans le détecteur d’identités multiples.

Article 41
Sous-traitant

En ce qui concerne le traitement des données à caractère personnel dans le CIR, l'eu-LISA doit être considérée comme le sous-traitant au sens de l'article 2, point e), du règlement (CE) nº 45/2001.

Article 42
Sécurité du traitement

1. L'eu-LISA et les autorités des États membres veillent à la sécurité des opérations de traitement de données à caractère personnel effectuées en application du présent règlement. L'eu-LISA, [l'unité centrale de l'ETIAS] et les autorités des États membres coopèrent pour l'exécution des tâches liées à la sécurité.

2. Sans préjudice de l'article 22 du règlement (CE) nº 45/2001, l'eu-LISA prend les mesures nécessaires pour assurer la sécurité des éléments d'interopérabilité et des infrastructures de communication qui y sont liées.

3. En particulier, l'eu-LISA adopte les mesures nécessaires, y compris un plan de sécurité, un plan de continuité des activités et un plan de rétablissement après sinistre, afin:

   (a) d'assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques;

   (b) d'empêcher toute lecture, copie ou modification ou tout retrait non autorisés de supports de données;

   (c) d'empêcher l'introduction non autorisée de données et le contrôle, la modification ou l'effacement non autorisés de données à caractère personnel enregistrées;

   (d) d'empêcher le traitement non autorisé de données ainsi que toute copie, toute modification ou tout effacement non autorisés de données;

   (e) de garantir que les personnes autorisées à avoir accès aux éléments d'interopérabilité n'ont accès qu'aux données couvertes par leur autorisation d'accès, uniquement grâce à l'attribution d'identifiants individuels et à des modes d'accès confidentiels;

   (f) de garantir la possibilité de vérifier et d'établir à quels organismes les données à caractère personnel peuvent être transmises au moyen de matériel de transmission de données;

   (g) de garantir la possibilité de vérifier et d'établir quelles données ont été traitées dans les éléments d'interopérabilité, à quel moment, par qui et dans quel but;

   (h) d'empêcher toute lecture, copie, modification ou tout effacement non autorisés de données à caractère personnel pendant leur transmission à partir des éléments d'interopérabilité ou vers ceux-ci, ou durant le transport de supports de données, en particulier au moyen de techniques de cryptage adaptées;

   (i) de contrôler l'efficacité des mesures de sécurité visées au présent paragraphe et de prendre les mesures organisationnelles nécessaires en matière de contrôle interne pour assurer le respect du présent règlement.

4. Les États membres prennent des mesures équivalentes à celles visées au paragraphe 3 en ce qui concerne la sécurité du traitement des données à caractère personnel par les autorités ayant un droit d'accès à l'un des éléments d'interopérabilité.

Article 43
Confidentialité des données du SIS

1. Chaque État membre applique à l'égard de toutes les personnes et de tous les organismes appelés à travailler avec des données du SIS, auxquelles ils accèdent par l'intermédiaire des éléments d'interopérabilité, ses règles relatives au secret professionnel ou leur impose des obligations de confidentialité équivalentes, conformément à sa législation nationale. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après que ces organismes ont cessé leur activité.

2. Sans préjudice de l'article 17 du statut des fonctionnaires et du régime applicable aux autres agents de l'Union européenne, l'eu-LISA applique à tous les membres de son personnel appelés à travailler avec des données du SIS des règles appropriées en matière de secret professionnel, ou leur impose des obligations de confidentialité équivalentes, qui répondent à des normes comparables à celles visées au paragraphe 1. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la fin de leurs activités.

Article 44
Incidents de sécurité

1. Tout événement ayant ou pouvant avoir un impact sur la sécurité des éléments d'interopérabilité et susceptible de causer aux données qui y sont stockées des dommages ou des pertes est considéré comme un incident de sécurité, en particulier lorsque des données peuvent avoir été consultées sans autorisation ou que la disponibilité, l'intégrité et la confidentialité de données ont été ou peuvent avoir été compromises.

2. Les incidents de sécurité sont gérés de telle sorte qu'une réponse rapide, efficace et idoine y soit apportée.

3. Sans préjudice de la notification et de la communication de toute violation de données à caractère personnel en application de l'article 33 du règlement (UE) 2016/679, de l'article 30 de la directive (UE) 2016/680 ou de ces deux dispositions, les États membres signalent les incidents de sécurité à la Commission, à l'eu-LISA et au Contrôleur européen de la protection des données. En cas d'incident de sécurité concernant l'infrastructure centrale des éléments d'interopérabilité, l'eu-LISA en informe la Commission et le Contrôleur européen de la protection des données.

4. Les informations relatives à un incident de sécurité ayant ou pouvant avoir un impact sur le fonctionnement des éléments d'interopérabilité, ou sur la disponibilité, l'intégrité et la confidentialité des données, sont communiquées aux États membres et consignées conformément au plan de gestion des incidents qui doit être élaboré par l'eu-LISA.

5. Les États membres concernés et l'eu-LISA coopèrent en cas d'incident de sécurité. La Commission établit les modalités de cette procédure de coopération au moyen

d'actes d'exécution. Ces actes d'exécution sont adoptés conformément à la procédure d'examen visée à l'article 64, paragraphe 2.

Article 45
Autocontrôle

Les États membres et les organes de l'UE concernés veillent à ce que chaque autorité habilitée à avoir accès aux éléments d'interopérabilité prenne les mesures nécessaires pour vérifier qu'elle respecte le présent règlement et coopère, au besoin, avec l'autorité de contrôle.

Les responsables du traitement visés à l'article 40 prennent les mesures nécessaires afin de contrôler la conformité des opérations de traitement au regard du présent règlement, notamment en vérifiant fréquemment les registres, et coopèrent, au besoin, avec les autorités de contrôle visées aux articles 49 et 50.

Article 46
Droit à l'information

1. Sans préjudice du droit à l'information visé aux articles 11 et 12 du règlement (CE) nº 45/2001 et aux articles 13 et 14 du règlement (UE) 2016/679, les personnes dont les données sont stockées dans le service partagé d'établissement de correspondances biométriques, le répertoire commun de données d'identité ou le détecteur d'identités multiples sont informées par l'autorité qui collecte leurs données, au moment de la collecte de ces données, du traitement de données à caractère personnel aux fins du présent règlement, y compris de l'identité et des coordonnées des responsables du traitement respectifs, des procédures pour exercer leurs droits d'accès, de rectification et d'effacement, ainsi que des coordonnées du Contrôleur européen de la protection des données et de l'autorité de contrôle nationale de l'État membre responsable de la collecte des données.

2. Les personnes dont les données sont enregistrées dans Eurodac ou dans [le système ECRIS-TCN] sont informées du traitement de données aux fins du présent règlement conformément au paragraphe 1 lorsque:

   (a) – (sans objet);

   (b) – (sans objet);

   (c) – (sans objet);

   (d) [une demande de protection internationale est créée ou actualisée dans Eurodac conformément à l'article 10 du règlement Eurodac];

   (e) [un enregistrement de données est créé ou actualisé dans le système ECRIS-TCN conformément à l'article 5 du règlement ECRIS-TCN.]

Article 47
Droit d'accès, de rectification et d'effacement

1. Pour exercer ses droits au titre des articles 13, 14, 15 et 16 du règlement (CE) nº 45/2001 et des articles 15, 16, 17 et 18 du règlement (UE) 2016/679, toute personne a le droit de s'adresser à l'État membre responsable de la vérification manuelle des différentes identités ou à tout État membre qui examine la demande et y répond.

2. L'État membre responsable de la vérification manuelle des différentes identités visée à l'article 29 ou l'État membre auquel la demande a été présentée répond à cette demande dans un délai de quarante-cinq jours à compter de la réception de celle-ci.

3. Si une demande de rectification ou d'effacement de données à caractère personnel est présentée à un État membre autre que l'État membre responsable, l'État membre auquel la demande a été présentée prend contact avec les autorités de l'État membre responsable dans un délai de sept jours et l'État membre responsable vérifie l'exactitude des données et la licéité du traitement des données dans un délai de trente jours à compter de cette prise de contact.

4. Lorsque, à la suite d'un examen, il apparaît que les données stockées dans le détecteur d'identités multiples (MID) sont matériellement erronées ou y ont été enregistrées de façon illicite, l'État membre responsable ou, le cas échéant, l'État membre auquel la demande a été présentée rectifie ou efface ces données.

5. Lorsque des données figurant dans le MID sont modifiées par l'État membre responsable au cours de leur période de validité, l'État membre responsable procède au traitement prévu à l'article 27 et, selon le cas, à l'article 29 afin de déterminer si les données modifiées doivent être liées. Lorsque le traitement ne génère aucun résultat positif, l'État membre responsable ou, le cas échéant, l'État membre auquel la demande a été présentée supprime les données du dossier de confirmation d'identité. Lorsque le traitement automatisé génère un ou plusieurs résultats positifs, l'État membre responsable crée ou met à jour le lien correspondant conformément aux dispositions pertinentes du présent règlement.

6. Lorsque l'État membre responsable ou, le cas échéant, l'État membre auquel la demande a été présentée n'estime pas que les données stockées dans le MID sont matériellement erronées ou y ont été enregistrées de façon illicite, il adopte une décision administrative indiquant par écrit et sans délai à la personne concernée les raisons pour lesquelles il n'est pas disposé à rectifier ou à effacer les données la concernant.

7. Cette décision fournit également à la personne concernée des précisions sur la possibilité de contester la décision prise au sujet de la demande visée au paragraphe 3 et, s'il y a lieu, des informations sur les modalités de recours ou de plainte devant les autorités ou les juridictions compétentes, ainsi que sur toute aide disponible, y compris de la part des autorités de contrôle nationales compétentes.

8. Toute demande présentée en vertu du paragraphe 3 comporte les informations nécessaires à l'identification de la personne concernée. Ces informations ne sont utilisées que pour permettre l'exercice des droits visés au paragraphe 3 et sont ensuite immédiatement effacées.

9. L'État membre responsable ou, le cas échéant, l'État membre auquel la demande a été présentée consigne, dans un document écrit, la présentation d'une demande visée au paragraphe 3 et son traitement, et met sans tarder ce document à la disposition des autorités de contrôle nationales compétentes en matière de protection des données.

Article 48

Communication de données à caractère personnel à des pays tiers, à des organisations internationales et à des entités privées

Les données à caractère personnel stockées dans, ou accessibles par, les éléments d'interopérabilité ne peuvent être transférées à un pays tiers, à une organisation internationale ou à une entité privée, ni être mises à leur disposition.

Article 49

Contrôle par l'autorité de contrôle nationale

1. L'autorité de contrôle ou les autorités désignées en vertu de l'article 49 du règlement (UE) 2016/679 veillent à ce que les autorités nationales responsables réalisent, tous les quatre ans au minimum, un audit des opérations de traitement des données, conformément aux normes internationales d'audit applicables.

2. Les États membres veillent à ce que leur autorité de contrôle dispose de ressources suffisantes pour s'acquitter des tâches qui lui sont confiées en vertu du présent règlement.

Article 50

Contrôle par le Contrôleur européen de la protection des données

Le Contrôleur européen de la protection des données veille à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement des données à caractère personnel menées par l'eu-LISA, répondant aux normes internationales applicables en matière d'audit. Le rapport d'audit est communiqué au Parlement européen, au Conseil, à l'eu-LISA, à la Commission et aux États membres. L'eu-LISA a la possibilité de formuler des observations avant l'adoption des rapports.

Article 51

Coopération entre les autorités de contrôle nationales et le Contrôleur européen de la protection des données

1. Le Contrôleur européen de la protection des données agit en étroite coopération avec les autorités de contrôle nationales sur les questions particulières exigeant une participation nationale, notamment si le Contrôleur européen de la protection des données ou une autorité de contrôle nationale découvre des différences importantes entre les pratiques des États membres ou l'existence de transferts potentiellement illicites transitant par les canaux de communication des éléments d'interopérabilité, ou dans le contexte de questions soulevées par une ou plusieurs autorités de contrôle nationales concernant la mise en œuvre et l'interprétation du présent règlement.

2. Dans les cas visés au paragraphe 1, un contrôle coordonné est assuré conformément à l'article 62 du règlement (UE) nº XXXX/2018 [règlement nº 45/2001 révisé].

CHAPITRE VIII
Responsabilités

Article 52

Responsabilités de l'eu-LISA durant la phase de conception et de développement

1. L'eu-LISA veille à ce que les infrastructures centrales des éléments d'interopérabilité soient exploitées conformément au présent règlement.

2. Les éléments d'interopérabilité sont hébergés par l'eu-LISA sur ses sites techniques et fournissent les fonctionnalités prévues dans le présent règlement conformément aux conditions de sécurité, de disponibilité, de qualité et de rapidité visées à l'article 53, paragraphe 1.

3. L'eu-LISA est responsable du développement des éléments d'interopérabilité, de toutes les adaptations nécessaires pour établir l'interopérabilité entre les systèmes centraux de l'EES, du VIS, de l'[ETIAS], du SIS, d'Eurodac, et [du système ECRIS-TCN] et le portail de recherche européen, le service partagé d'établissement de correspondances biométriques, le répertoire commun de données d'identité et le détecteur d'identités multiples.

   L'eu-LISA définit la conception de l'architecture matérielle des éléments d'interopérabilité, y compris leur infrastructure de communication, ainsi que les spécifications techniques et leur évolution en ce qui concerne l'infrastructure centrale et l'infrastructure de communication sécurisée, qui sont adoptées par le conseil d'administration après avis favorable de la Commission. L'eu-LISA met également en œuvre tout aménagement éventuellement nécessaire du SIS, d'Eurodac ou [du système ECRIS-TCN], résultant de l'établissement de l'interopérabilité et prévu par le présent règlement.

   L'eu-LISA développe et met en œuvre les éléments d'interopérabilité dès que possible après l'entrée en vigueur du présent règlement et l'adoption par la Commission des mesures prévues à l'article 8, paragraphe 2, à l'article 9, paragraphe 7, à l'article 28, paragraphes 5 et 6, à l'article 37, paragraphe 4, à l'article 38, paragraphe 4, à l'article 39, paragraphe 5 et à l'article 44, paragraphe 5.

   Le développement consiste en l'élaboration et la mise en œuvre des spécifications techniques, en la réalisation d'essais et en la coordination générale du projet.

4. Pendant la phase de conception et de développement, un conseil de gestion du programme, composé d'un maximum de 10 membres, est créé. Il est constitué de sept membres nommés par le conseil d'administration de l'eu-LISA parmi ses membres ou ses suppléants, du président du groupe consultatif sur l'interopérabilité visé à l'article 65, d'un membre représentant l'eu-LISA désigné par son directeur exécutif et d'un membre désigné par la Commission. Les membres nommés par le conseil d'administration de l'eu-LISA sont choisis uniquement parmi les États membres qui sont pleinement liés, en vertu du droit de l'Union, par les instruments législatifs régissant le développement, la création, le fonctionnement et l'utilisation de tous les systèmes d'information à grande échelle gérés par l'eu-LISA et qui participeront aux éléments d'interopérabilité.

5. Le conseil de gestion du programme se réunit régulièrement et au moins trois fois par trimestre. Il veille à la bonne gestion de la phase de conception et de développement des éléments d'interopérabilité.

Le conseil de gestion du programme soumet chaque mois au conseil d'administration des rapports écrits sur l'état d'avancement du projet. Le conseil de gestion du programme n'a aucun pouvoir décisionnel ni aucun mandat lui permettant de représenter les membres du conseil d'administration de l'eu-LISA.

6. Le conseil d'administration de l'eu-LISA définit le règlement intérieur du conseil de gestion du programme, qui comprend notamment des règles sur:

(a) la présidence;

(b) les lieux de réunion;

(c) la préparation des réunions;

(d) l'admission d'experts aux réunions;

(e) les plans de communication assurant l'information exhaustive des membres du conseil d'administration non participants.

La présidence est exercée par un État membre qui est pleinement lié, en vertu du droit de l'Union, par les instruments législatifs régissant le développement, la création, le fonctionnement et l'utilisation de tous les systèmes d'information à grande échelle gérés par l'eu-LISA.

Tous les frais de voyage et de séjour exposés par les membres du conseil de gestion du programme sont pris en charge par l'agence et l'article 10 du règlement intérieur de l'eu-LISA s'applique mutatis mutandis. Le secrétariat du conseil de gestion du programme est assuré par l'eu-LISA.

Le groupe consultatif sur l'interopérabilité visé à l'article 65 se réunit régulièrement jusqu'à la mise en service des éléments d'interopérabilité. Après chaque réunion, il rend compte au comité de gestion du programme. Il fournit l'expertise technique nécessaire à l'appui des tâches du conseil de gestion du programme et suit l'état de préparation des États membres.

Article 53
Responsabilités de l'eu-LISA après la mise en service

1. Après la mise en service de chaque élément d'interopérabilité, l'eu-LISA est responsable de la gestion technique de l'infrastructure centrale et des interfaces uniformes nationales. Elle veille, en coopération avec les États membres, à ce que la meilleure technologie disponible soit utilisée en permanence, sous réserve d'une analyse coûts-avantages. l'eu-LISA est également responsable de la gestion technique de l'infrastructure de communication visée aux articles 6, 12, 17, 25 et 39.

La gestion technique des éléments d'interopérabilité comprend toutes les tâches nécessaires au fonctionnement de ceux-ci 24 heures sur 24, 7 jours sur 7, conformément au présent règlement, en particulier les travaux de maintenance et les perfectionnements techniques indispensables pour que les éléments d'interopérabilité fonctionnent à un niveau satisfaisant de qualité technique, notamment quant au temps de réponse pour l'interrogation des infrastructures centrales, conformément aux spécifications techniques.

2. Sans préjudice de l'article 17 du statut des fonctionnaires de l'Union européenne, l'eu-LISA applique des règles appropriées en matière de secret professionnel ou impose des obligations de confidentialité équivalentes à tous les membres de son personnel appelés à travailler avec les données stockées dans les éléments

d'interopérabilité. Cette obligation continue de s'appliquer après que ces personnes ont cessé leurs fonctions ou quitté leur emploi ou après la cessation de leur activité.

3. L'eu-LISA élabore et gère un mécanisme et des procédures de contrôle de la qualité des données stockées dans le service partagé d'établissement de correspondances biométriques et dans le répertoire commun de données d'identité, conformément à l'article 37.

4. L'eu-LISA s'acquitte aussi des tâches liées à la fourniture d'une formation relative à l'utilisation technique des éléments d'interopérabilité.

Article 54
Responsabilités des États membres

1. Chaque État membre est responsable:

(a) de la connexion à l'infrastructure de communication du portail de recherche européen (ESP) et du répertoire commun de données d'identité (CIR);

(b) de l'intégration des systèmes et infrastructures nationaux existants avec l'ESP, le service partagé de mise en correspondance de données biométriques, le CIR et le détecteur d'identités multiples;

(c) de l'organisation, de la gestion, du fonctionnement et de la maintenance de son infrastructure nationale existante et de sa connexion aux éléments d'interopérabilité;

(d) de la gestion et des modalités de l'accès à l'ESP, au CIR et au détecteur d'identités multiples du personnel dûment autorisé et du personnel dûment habilité des autorités nationales compétentes, conformément au présent règlement, ainsi que de l'établissement d'une liste de ce personnel et de ses qualifications et de la mise à jour régulière de cette liste;

(e) de l'adoption des mesures législatives visées à l'article 20, paragraphe 3, aux fins de l'accès au CIR pour identification;

(f) de la vérification manuelle des différentes identités visée à l'article 29;

(g) de la mise en œuvre des exigences en matière de qualité des données dans les systèmes d'information de l'UE et dans les éléments d'interopérabilité;

(h) de la correction des manquements constatés dans le rapport d'évaluation de la Commission concernant la qualité des données visé à l'article 37, paragraphe 5.

2. Chaque État membre connecte au CIR ses autorités désignées visées à l'article 4, point 24).

Article 54 bis
Responsabilités d'Europol

1. Europol assure le traitement des recherches lancées par l'ESP concernant des données Europol et adapte en conséquence son interface d'interrogation des systèmes d'Europol (Querying Europol Systems – QUEST) pour les données nécessitant un niveau de protection de base (basic protection level – BPL).

2. Europol est responsable de la gestion et des modalités de l'accès à l'ESP et au CIR et de leur utilisation par son personnel dûment autorisé, conformément au présent

règlement, ainsi que de l'établissement d'une liste de ce personnel et de ses qualifications et de la mise à jour régulière de cette liste.

Article 55
Responsabilités de l'unité centrale de l'ETIAS

L'unité centrale de l'ETIAS est responsable:

(a) de la vérification manuelle des différentes identités, visée à l'article 29;

(b) de la détection d'identités multiples parmi les données stockées dans le VIS, Eurodac et le SIS, visée à l'article 59.

CHAPITRE IX
Dispositions finales

Article 56
Établissement de rapports et de statistiques

1. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et de l'eu-LISA est autorisé à consulter les données énumérées ci-après concernant le portail de recherche européen (ESP), uniquement aux fins de l'établissement de rapports et de statistiques, sans que l'identification individuelle ne soit permise:

   (a) le nombre de recherches par utilisateur du profil ESP;

   (b) – (sans objet).

2. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et de l'eu-LISA est autorisé à consulter les données énumérées ci-après concernant le répertoire commun de données d'identité, uniquement aux fins de l'établissement de rapports et de statistiques, sans que l'identification individuelle ne soit permise:

   (a) le nombre de recherches aux fins des articles 20, 21 et 22;

   (b) la nationalité, le sexe et l'année de naissance de la personne;

   (c) le type de document de voyage et le code à trois lettres du pays de délivrance;

   (d) le nombre de recherches effectuées avec et sans données biométriques.

3. Le personnel dûment autorisé des autorités compétentes des États membres, de la Commission et de l'eu-LISA est autorisé à consulter les données énumérées ci-après concernant le détecteur d'identités multiples, uniquement aux fins de l'établissement de rapports et de statistiques, sans que l'identification individuelle ne soit permise:

   (a) la nationalité, le sexe et l'année de naissance de la personne;

   (b) le type de document de voyage et le code à trois lettres du pays de délivrance;

   (c) le nombre de recherches effectuées avec et sans données biométriques;

   (d) le nombre de chaque type de lien.

4. Le personnel dûment autorisé de l'Agence européenne de garde-frontières et de garde-côtes créée par le règlement (UE) 2016/1624 du Parlement européen et du

Conseil[64] est autorisé à consulter les données mentionnées aux paragraphes 1, 2 et 3 aux fins de l'analyse des risques et de l'évaluation de la vulnérabilité visées aux articles 11 et 13 dudit règlement.

5. Aux fins du paragraphe 1 du présent article, l'eu-LISA stocke les données mentionnées au paragraphe 1 du présent article dans le répertoire central des rapports et statistiques visé au chapitre VII du présent règlement. Les données figurant dans le répertoire ne permettent pas l'identification des individus mais permettent aux autorités énumérées au paragraphe 1 du présent article d'obtenir des rapports et des statistiques personnalisables afin d'améliorer l'efficacité des vérifications aux frontières, d'aider les autorités à traiter les demandes de visa et de favoriser l'élaboration, au niveau de l'Union, de politiques en matière de migration et de sécurité fondées sur des données concrètes.

Article 57
Période transitoire pour l'utilisation du portail de recherche européen

Pendant une période de deux ans à compter de la date de la mise en service de l'ESP, les obligations visées à l'article 7, paragraphes 2 et 4, ne s'appliquent pas et l'utilisation de l'ESP est facultative.

Article 58
Période transitoire applicable aux dispositions relatives à l'accès au répertoire commun de données d'identité à des fins répressives

L'article 22 s'applique à partir de la date de mise en service visée à l'article 62, paragraphe 1.

Article 59
Période transitoire pour la détection d'identités multiples

1. Pendant une période d'un an à compter de la notification par l'eu-LISA de l'achèvement de l'essai visé à l'article 62, paragraphe 1, point b), concernant le détecteur d'identités multiples (MID) et avant la mise en service du MID, l'unité centrale de l'ETIAS visée à [l'article 33 *bis* du règlement (UE) 2016/1624] est responsable de la détection d'identités multiples parmi les données stockées dans le VIS, Eurodac et le SIS. Les détections d'identités multiples ne sont effectuées qu'à l'aide de données biométriques conformément à l'article 27, paragraphe 2, du présent règlement.

2. Lorsque la recherche génère un ou plusieurs résultats positifs et que les données d'identité des dossiers liés sont identiques ou similaires, un lien blanc est créé conformément à l'article 33.

   Lorsque la recherche génère un ou plusieurs résultats positifs et que les données d'identité des dossiers liés ne peuvent pas être considérées comme similaires, un lien jaune est créé conformément à l'article 30 et la procédure visée à l'article 29 s'applique.

[64] Règlement (UE) 2016/1624 du Parlement européen et du Conseil du 14 septembre 2016 relatif au corps européen de garde-frontières et de garde-côtes, modifiant le règlement (UE) 2016/399 du Parlement européen et du Conseil et abrogeant le règlement (CE) nº 863/2007 du Parlement européen et du Conseil, le règlement (CE) nº 2007/2004 du Conseil et la décision 2005/267/CE du Conseil (JO L 251 du 16.9.2016, p. 1).

Lorsque plusieurs résultats positifs sont générés, un lien est créé vers chaque élément de donnée ayant donné lieu au résultat positif.

3. Lorsqu'un lien jaune est créé conformément au paragraphe 3, le MID accorde à l'unité centrale de l'ETIAS l'accès aux données d'identité figurant dans les différents systèmes d'information.

4. Lorsqu'un lien est créé avec un signalement figurant dans le SIS, autre qu'un signalement aux fins de refus d'entrée ou un signalement de document de voyage signalé comme perdu, volé ou invalidé conformément à l'article 24 du règlement SIS dans le domaine des vérifications aux frontières et à l'article 38 du règlement SIS dans le domaine répressif, respectivement, le MID accorde au bureau SIRENE de l'État membre qui a créé le signalement l'accès aux données d'identité présentes dans les différents systèmes d'information.

5. L'unité centrale de l'ETIAS ou le bureau SIRENE de l'État membre qui a créé le signalement a accès aux données figurant dans le dossier de confirmation d'identité, évalue les différentes identités et met à jour le lien conformément aux articles 31, 32 et 33, puis l'ajoute au dossier de confirmation d'identité.

6. L'eu-LISA aide, au besoin, l'unité centrale de l'ETIAS à effectuer la détection d'identités multiples visée au présent article.

Article 60
Coûts

1. Les coûts afférents à la création et au fonctionnement de l'ESP, du service partagé de mise en correspondance de données biométriques, du répertoire commun de données d'identité (CIR) et du MID sont à la charge du budget général de l'Union.

2. Les coûts afférents à l'intégration des infrastructures nationales existantes et à leur connexion avec les interfaces uniformes nationales, ainsi qu'à l'hébergement des interfaces uniformes nationales, sont à la charge du budget général de l'Union.

Les coûts suivants ne sont pas admissibles:

(a) coûts afférents au bureau de gestion de projet des États membres (réunions, missions, locaux);

(b) hébergement des systèmes d'information nationaux (espace, mise en œuvre, électricité, refroidissement);

(c) fonctionnement des systèmes d'information nationaux (contrats conclus avec les opérateurs et contrats d'appui);

(d) conception, développement, mise en œuvre, fonctionnement et maintenance des réseaux de communication nationaux.

3. Les coûts afférents aux autorités désignées visées à l'article 4, point 24), sont à la charge de chaque État membre et d'Europol, respectivement. Les coûts afférents à la connexion des autorités désignées avec le CIR sont à la charge de chaque État membre et d'Europol, respectivement.

Article 61
Notifications

1. Les États membres notifient à l'eu-LISA le nom des autorités visées aux articles 7, 20, 21 et 26 qui peuvent, respectivement, utiliser l'ESP, le CIR et le MID ou y avoir accès.

   Une liste consolidée de ces autorités est publiée au *Journal officiel de l'Union européenne* dans un délai de trois mois à compter de la date à laquelle chaque élément d'interopérabilité a été mis en service conformément à l'article 62. En cas de modifications apportées à cette liste, l'eu-LISA publie une fois par an une version consolidée actualisée.

2. L'eu-LISA informe la Commission des résultats concluants des essais visés à l'article 62, paragraphe 1, point b).

3. L'unité centrale de l'ETIAS informe la Commission l'exécution concluante de la mesure transitoire prévue à l'article 59.

4. La Commission met les informations communiquées en application du paragraphe 1 à la disposition des États membres et du public, par l'intermédiaire d'un site web public actualisé en permanence.

Article 62
Mise en service

1. La Commission décide de la date à laquelle chaque élément d'interopérabilité doit être mis en service, une fois les conditions suivantes remplies:

   (a) les mesures visées à l'article 8, paragraphe 2, à l'article 9, paragraphe 7, à l'article 28, paragraphes 5 et 6, à l'article 37, paragraphe 4, à l'article 38, paragraphe 4, à l'article 39, paragraphe 5, et à l'article 44, paragraphe 5, ont été adoptées;

   (b) l'eu-LISA a déclaré que les essais complets de l'élément d'interopérabilité considéré, qu'elle devait mener en coopération avec les États membres, étaient concluants;

   (c) l'eu-LISA a validé les aménagements techniques et juridiques nécessaires pour recueillir et transmettre les données visées à l'article 8, paragraphe 1, ainsi qu'aux articles 13, 19, 34 et 39 et les a notifiés à la Commission;

   (d) les États membres ont adressé à la Commission les notifications visées à l'article 61, paragraphe 1;

   (e) pour le détecteur d'identités multiples, l'unité centrale de l'ETIAS a adressé à la Commission la notification visée à l'article 61, paragraphe 3.

2. La Commission informe le Parlement européen et le Conseil des résultats des essais effectués conformément au paragraphe 1, point b).

3. La décision de la Commission visée au paragraphe 1 est publiée au *Journal officiel de l'Union européenne*.

4. Les États membres et Europol commencent à utiliser les éléments d'interopérabilité à partir de la date fixée par la Commission conformément au paragraphe 1.

Article 63
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter les actes délégués visés à l'article 8, paragraphe 2, et à l'article 9, paragraphe 7, est conféré à la Commission pour une durée indéterminée à partir [*de la date d'entrée en vigueur du présent règlement*].

3. La délégation de pouvoir visée à l'article 8, paragraphe 2, et à l'article 9, paragraphe 7, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016.

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 8, paragraphe 2, et de l'article 9, paragraphe 7, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de [deux mois] à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de [deux mois] à l'initiative du Parlement européen ou du Conseil.

Article 64
Procédure de comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Article 65
Groupe consultatif

L'eu-LISA crée un groupe consultatif chargé de lui apporter son expertise en rapport avec l'interopérabilité, notamment dans le contexte de l'élaboration de son programme de travail et de son rapport d'activité annuels. Durant la phase de conception et de développement des instruments d'interopérabilité, l'article 52, paragraphes 4 à 6, s'applique.

Article 66
Formation

L'eu-LISA s'acquitte des tâches liées à la fourniture d'une formation relative à l'utilisation technique des éléments d'interopérabilité conformément au règlement (UE) nº 1077/2011.

Article 67
Manuel pratique

La Commission, en étroite coopération avec les États membres, l'eu-LISA et les autres agences concernées, met à disposition un manuel pratique sur la mise en œuvre et la gestion des éléments d'interopérabilité. Le manuel pratique contient des orientations techniques et opérationnelles, des recommandations et des bonnes pratiques. La Commission adopte le manuel pratique sous la forme d'une recommandation.

Article 68
Suivi et évaluation

1. L'eu-LISA veille à ce que des procédures soient mises en place pour suivre le développement des éléments d'interopérabilité par rapport aux objectifs fixés en matière de planification et de coûts et suivre le fonctionnement des éléments d'interopérabilité par rapport aux objectifs fixés en matière de résultats techniques, de coût-efficacité, de sécurité et de qualité du service.

2. Au plus tard [*six mois après l'entrée en vigueur du présent règlement* – OPOCE: remplacer par la date effective], puis tous les six mois pendant la phase de développement des éléments d'interopérabilité, l'eu-LISA présente un rapport au Parlement européen et au Conseil sur l'état d'avancement du développement des éléments d'interopérabilité. Une fois le développement achevé, un rapport est présenté au Parlement européen et au Conseil, qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été atteints, et justifie les éventuels écarts.

3. Aux fins de la maintenance technique, l'eu-LISA a accès aux informations nécessaires concernant les opérations de traitement de données effectuées dans les éléments d'interopérabilité.

4. Quatre ans après la mise en service de chaque élément d'interopérabilité, puis tous les quatre ans, l'eu-LISA présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique des éléments d'interopérabilité, y compris sur leur sécurité.

5. En outre, un an après chaque rapport de l'eu-LISA, la Commission réalise une évaluation globale des éléments d'interopérabilité, y compris:

   (a) une évaluation de l'application du présent règlement;

   (b) un examen des résultats obtenus par rapport aux objectifs fixés et de l'impact sur les droits fondamentaux;

   (c) une évaluation permettant de déterminer si les principes de base des éléments d'interopérabilité restent valables;

   (d) une évaluation de la sécurité des éléments d'interopérabilité;

   (e) une évaluation de toute conséquence ayant une incidence disproportionnée sur la fluidité du trafic aux points de passage frontaliers ou un impact sur le budget de l'Union.

   Les évaluations comprennent les éventuelles recommandations nécessaires. La Commission transmet le rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits

fondamentaux de l'Union européenne instituée par le règlement (CE) nº 168/2007 du Conseil[65].

6. Les États membres et Europol communiquent à l'eu-LISA et à la Commission les informations nécessaires à l'établissement des rapports visés aux paragraphes 4 et 5. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre des indications sur les sources, les membres du personnel ou les enquêtes des autorités désignées.

7. L'eu-LISA fournit à la Commission les informations nécessaires pour élaborer les évaluations visées au paragraphe 5.

8. Tout en respectant les dispositions du droit national relatives à la publication d'informations sensibles, chaque État membre et Europol établissent des rapports annuels sur l'efficacité de l'accès aux données stockées dans le répertoire commun de données d'identité à des fins répressives, comportant des informations et des statistiques sur:

   (a) l'objet précis de la consultation, notamment la nature de l'infraction terroriste ou de l'infraction pénale grave;

   (b) les motifs raisonnables invoqués pour soupçonner que le suspect, l'auteur ou la victime relève du règlement Eurodac;

   (c) le nombre de demandes d'accès au répertoire commun de données d'identité à des fins répressives;

   (d) le nombre et le type de cas qui ont permis une identification;

   (e) la nécessité de traiter les cas exceptionnels d'urgence, les cas d'urgence effectivement traités, y compris ceux qui n'ont pas été approuvés par le point d'accès central lors de la vérification a posteriori.

   Les rapports annuels des États membres et d'Europol sont transmis à la Commission au plus tard le 30 juin de l'année suivante.

Article 69
Entrée en vigueur et applicabilité

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Strasbourg, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*

[65] Règlement (CE) nº 168/2007 du Conseil du 15 février 2007 portant création d'une Agence des droits fondamentaux de l'Union européenne (JO L 53 du 22.2.2007, p. 1).

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. Nature de la proposition/de l'initiative

1.4. Objectif(s)

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

3.2.1. Synthèse de l'incidence estimée sur les dépenses

3.2.2. Incidence estimée sur les crédits opérationnels

3.2.3. Incidence estimée sur les crédits de nature administrative

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations.

1.2. Domaine(s) politique(s) concerné(s)

Affaires intérieures (titre 18)

1.3. Nature de la proposition/de l'initiative

X La proposition/l'initiative porte sur une **action nouvelle**

☐ La proposition/l'initiative porte sur **une action nouvelle suite à un projet pilote/une action préparatoire**[66]

☐ La proposition/l'initiative est relative à **la prolongation d'une action existante**

☐ La proposition/l'initiative porte sur **une action réorientée vers une nouvelle action**

1.4. Objectif(s)

1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative

Gestion des frontières – sauver des vies et assurer la sécurité des frontières extérieures

Les éléments d'interopérabilité permettent une meilleure utilisation des informations contenues dans les systèmes existants de l'UE pour la sécurité, les frontières et la gestion des migrations. Ces mesures évitent principalement que la même personne soit enregistrée dans des systèmes différents avec des identités différentes. Actuellement, l'identification unique d'une personne est possible dans un système donné, mais pas dans l'ensemble des systèmes. Cette situation peut conduire les autorités à prendre des décisions erronées ou, à l'inverse, être exploitée par des voyageurs de mauvaise foi pour dissimuler leur identité réelle.

Meilleur échange d'informations

Les mesures proposées prévoient également un accès simplifié mais toujours limité des services répressifs à ces données. Toutefois, contrairement à ce qui se passe aujourd'hui, il existe une seule série de conditions et non une série différente pour chaque ensemble de données.

1.4.2. Objectif(s) spécifique(s) et objectif spécifique nº [...]

La mise en place des éléments d'interopérabilité poursuit les objectifs généraux suivants:

(a) améliorer la gestion des frontières extérieures;

(b) contribuer à prévenir et combattre la migration irrégulière, et

[66] Tel(le) que visé(e) à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

(c) contribuer à assurer un niveau élevé de sécurité au sein de l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres.

Les objectifs visant à garantir l'interopérabilité seront atteints:

a) en assurant l'identification correcte des personnes;

b) en contribuant à la lutte contre la fraude à l'identité;

c) en améliorant et en harmonisant les exigences relatives à la qualité des données des différents systèmes d'information de l'UE;

d) en facilitant la mise en œuvre technique et opérationnelle des systèmes d'information de l'UE existants et futurs par les États membres;

e) en renforçant, en simplifiant et en rendant plus uniformes les conditions de sécurité des données et de protection des données régissant les différents systèmes d'information de l'UE;

f) en simplifiant et en rendant plus uniformes les conditions d'accès à des fins répressives à l'EES, au VIS, à l'ETIAS et à Eurodac;

g) en soutenant les objectifs de l'EES, du VIS, de l'ETIAS, d'Eurodac, du SIS et du système ECRIS-TCN.

Activité(s) ABM/ABB concernée(s)

Chapitre Sécurité et protection des libertés: sécurité intérieure

1.4.3. Résultat(s) et incidence(s) attendu(s)

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Les objectifs généraux de la présente initiative découlent des deux objectifs fondés sur le traité:

1. améliorer la gestion des frontières extérieures de l'espace Schengen, en s'appuyant sur l'agenda européen en matière de migration et les communications ultérieures, y compris la communication sur la préservation et le renforcement de l'espace Schengen;

2. contribuer à la sécurité intérieure de l'Union européenne, en s'appuyant sur le programme européen en matière de sécurité et les travaux de la Commission en vue d'une union de la sécurité réelle et effective.

Les objectifs politiques spécifiques de la présente initiative relative à l'interopérabilité sont les suivants:

Les objectifs spécifiques de la présente proposition sont les suivants:

1. garantir que les utilisateurs finaux, en particulier les garde-frontières, les agents des services répressifs, les agents des services d'immigration et les autorités judiciaires, disposent d'un accès rapide, continu, systématique et contrôlé aux informations dont ils ont besoin pour accomplir leurs tâches;

2. fournir une solution permettant de détecter les identités multiples liées au même ensemble de données biométriques, dans le double objectif de garantir l'identification correcte des personnes de bonne foi et de lutter contre la fraude à l'identité;

3. faciliter les contrôles d'identité des ressortissants de pays tiers effectués sur le territoire d'un État membre par les autorités de police, et

4. faciliter et simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive au niveau de l'Union, lorsque cela est nécessaire à des fins de prévention et de détection des infractions graves et du terrorisme, ou d'enquêtes et de poursuites en la matière.

Pour atteindre l'objectif spécifique 1, le portail de recherche européen (ESP) sera développé.

Pour atteindre l'objectif spécifique 2, le détecteur d'identités multiples (MID) sera mis en place, appuyé par le répertoire commun de données d'identité (CIR) et le service partagé d'établissement de correspondances biométriques (BMS partagé).

Pour atteindre l'objectif spécifique 3, les fonctionnaires autorisés auront accès au CIR aux fins d'identification.

Pour atteindre l'objectif 4, le CIR comprendra une fonctionnalité d'indicateur de concordance qui permettra une approche en deux étapes de l'accès à des fins répressives aux systèmes de gestion des frontières.

Outre ces quatre éléments d'interopérabilité, les objectifs décrits à la section 1.4.2 seront soutenus par la création et la gouvernance du format universel pour les messages (UMF), en tant que norme de l'UE pour le développement de systèmes d'information dans le domaine de la justice et des affaires intérieures, ainsi que par la création d'un répertoire commun des rapports et statistiques.

1.4.4. Indicateurs de résultats et d'incidences

Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.

Chacune des mesures proposées nécessite le développement, puis la maintenance et l'exploitation, de l'élément concerné.

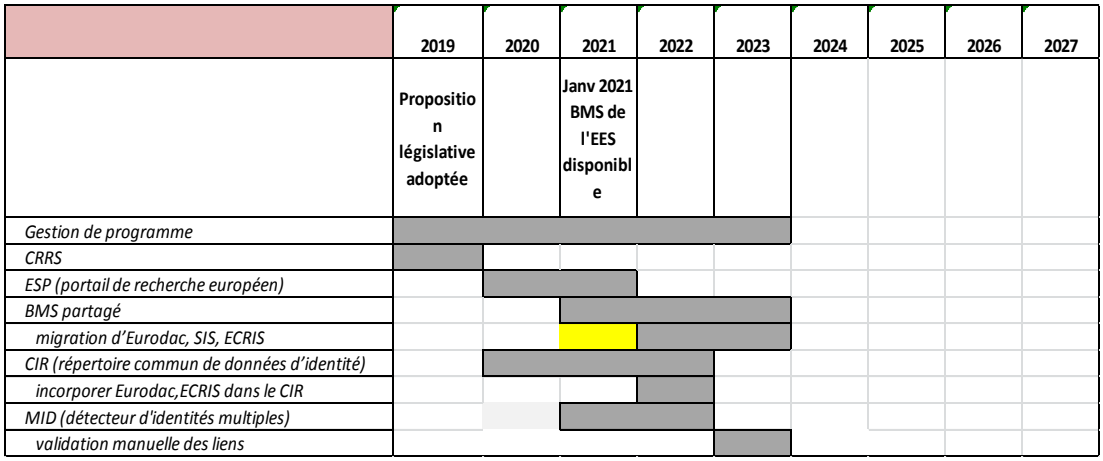
Pendant le développement

Le développement de chaque élément se fera une fois que les conditions préalables seront remplies, c'est-à-dire que la proposition législative sera adoptée par les colégislateurs et que les conditions techniques préalables seront remplies, étant donné que certains éléments ne pourront être mis en place qu'une fois que d'autres seront disponibles.

Objectif spécifique: le système doit être prêt à être mis en service à la date d'échéance cible

D'ici à la fin 2017, la proposition sera envoyée aux colégislateurs pour adoption. Il est supposé que le processus d'adoption sera achevé en 2018, par analogie avec le temps nécessaire pour d'autres propositions.

Dans cette hypothèse, le lancement de la période de développement est fixé au début de 2019 (= T0) afin d'avoir un point de référence à partir duquel les durées sont comptées et non des dates absolues. Si l'adoption par les colégislateurs intervient à une date ultérieure, l'ensemble du calendrier sera décalé en conséquence. Par ailleurs, le BMS partagé doit être disponible avant que le CIR et le MID puissent être achevés. Les durées de développement sont indiquées dans le graphique ci-dessous:



(La période indiquée en jaune concerne une tâche spécifique liée à Eurodac.)

- répertoire commun des rapports et statistiques (CRRS): date d'échéance: T0 + 12 mois (2019-2020)

- portail de recherche européen (ESP): date d'échéance: T0 + 36 mois (2019-2021)

- le service partagé d'établissement de correspondances biométriques (BMS partagé) est d'abord créé pour réaliser le système d'entrée/de sortie (EES). Lorsque cette importante étape sera franchie, les applications qui utiliseront le BMS partagé devront être mises à jour et les données contenues dans le système automatisé d'identification par empreintes digitales (AFIS) du SIS et dans l'AFIS d'Eurodac ainsi que les données du système ECRIS-TCN seront transférées dans le BMS partagé. La date d'échéance pour l'achèvement des travaux est fixée à la fin de 2023.

- le répertoire commun de données d'identité (CIR) est d'abord créé dans le cadre de la mise en œuvre de l'EES. Lorsque l'EES sera achevé, les données d'Eurodac et de l'ECRIS seront intégrées dans le CIR. La date d'échéance pour l'achèvement des travaux est fixée à la fin de 2022 (disponibilité du BMS partagé + 12 mois).

- le détecteur d'identités multiples (MID) est créé après la mise en service du CIR. La date d'échéance pour l'achèvement des travaux est fixée à la fin de 2022 (disponibilité du BMS partagé + 24 mois), mais la période de validation des liens entre identités proposés par le MID nécessitera beaucoup de ressources. Chacun des liens estimés doit être validé manuellement. Cette tâche durera jusqu'à la fin de 2023.

La période de fonctionnement commence dès que la période de développement indiquée ci-dessus est terminée.

Fonctionnement

Les indicateurs relatifs à chaque objectif spécifique mentionné au point 1.4.3 sont les suivants:

1. Objectif spécifique: accès rapide, continu et systématique aux sources de données autorisées

- Nombre de cas d'utilisation (= nombre de recherches pouvant être traitées par l'ESP) par période de temps.

- Nombre de recherches traitées par l'ESP par rapport au nombre total de recherches (via l'ESP et directement dans les systèmes) par période de temps.

2. Objectif spécifique: détecter les identités multiples

- Nombre d'identités liées au même ensemble de données biométriques par rapport au nombre d'identités comprenant des informations biographiques, par période de temps.

- Nombre de cas de fraude à l'identité détectés par rapport au nombre d'identités liées et au nombre total d'identités, par période de temps.

3. Objectif spécifique: faciliter l'identification des ressortissants de pays tiers

- Nombre de vérifications effectuées à des fins d'identification par rapport au nombre total de transactions par période de temps.

4. Objectif spécifique: simplifier l'accès aux sources de données autorisées à des fins répressives

- Nombre d'accès à des fins répressives dans le cadre de l'«étape 1» (= vérification de la présence de données) par période de temps.

- Nombre d'accès à des fins répressives dans le cadre de l'«étape 2» (= consultation effective des données des systèmes de l'UE relevant du champ d'application) par période de temps.

5. Objectif transversal supplémentaire: améliorer la qualité des données et leur utilisation pour améliorer l'élaboration des politiques

- Publication régulière de rapports de suivi de la qualité des données.

- Nombre de demandes ponctuelles d'informations statistiques par période de temps.

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme

Comme le montre l'analyse d'impact qui accompagne la présente proposition législative, les différents éléments proposés sont nécessaires pour parvenir à l'interopérabilité:

- Pour répondre à l'objectif consistant à fournir aux utilisateurs autorisés un accès rapide, continu, systématique et contrôlé aux systèmes d'information pertinents, il convient de créer un portail de recherche européen (ESP), fondé sur un BMS partagé, afin d'interroger toutes les bases de données.

- Pour répondre à l'objectif consistant à faciliter les contrôles d'identité des ressortissants de pays tiers réalisés sur le territoire d'un État membre par des agents autorisés, il convient de créer un répertoire commun de données d'identité (CIR), contenant l'ensemble minimal de données d'identification et s'appuyant sur le même BMS partagé.

- Pour répondre à l'objectif consistant à détecter les identités multiples liées au même ensemble de données biométriques, dans le double objectif de faciliter les contrôles d'identité pour les voyageurs de bonne foi et de lutter contre la fraude à l'identité, il convient de créer un détecteur d'identités multiples (MID), contenant des liens entre les identités multiples dans différents systèmes.

- Pour répondre à l'objectif consistant à faciliter et à simplifier l'accès des services répressifs aux systèmes d'information à finalité non répressive à des fins de prévention et de détection des infractions graves et du terrorisme, ou d'enquêtes et de poursuites en la matière, il convient d'ajouter une fonctionnalité d'indication de concordance au répertoire commun de données d'identité (CIR).

Puisque tous les objectifs doivent être atteints, la solution complète est la combinaison de l'ESP, du CIR (avec un indicateur de concordance) et du MID, tous s'appuyant sur le BMS partagé.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été produite par la seule action des États membres.

Des mesures doivent être prises au niveau européen car les systèmes qu'il est proposé de rendre interopérables sont des systèmes utilisés par plusieurs États membres: soit tous les États membres (dans le cas d'Eurodac), soit tous les États membres faisant partie de l'espace Schengen (pour l'EES, le VIS, l'ETIAS et le SIS). Par définition, on ne peut tout simplement pas agir à un autre niveau.

La principale valeur ajoutée attendue est d'éliminer les cas de fraude à l'identité, de recenser les cas dans lesquels une personne a utilisé différentes identités pour entrer dans l'UE et d'éviter que les personnes de bonne foi ne soient confondues avec des personnes de mauvaise foi portant le même nom. Une valeur ajoutée supplémentaire réside dans le fait que l'interopérabilité proposée ici facilite la mise en œuvre et la maintenance des systèmes d'information à grande échelle de l'UE. En ce qui concerne les services répressifs, les mesures proposées devraient permettre un accès plus fréquent et plus efficace à des données spécifiques au sein des systèmes

d'information à grande échelle de l'UE. Au niveau opérationnel, la qualité des données ne peut être maintenue et améliorée que si elle est contrôlée. En outre, pour ce qui est de l'élaboration des politiques et de la prise de décisions, il est nécessaire de permettre d'effectuer des recherches ponctuelles sur des données anonymisées.

L'analyse d'impact comprend une analyse coûts-avantages et, compte tenu des seuls avantages qui peuvent être quantifiés, les avantages escomptés peuvent raisonnablement être estimés à environ 77,5 millions d'EUR par an et reviennent principalement aux États membres. Ces avantages découlent essentiellement des éléments suivants:

- la réduction du coût des modifications apportées aux applications nationales lorsque le système central sera opérationnel (estimée à 6 millions d'EUR par an pour les services informatiques des États membres);

- une économie de coûts grâce à la mise en place d'un BMS central partagé au lieu d'un BMS par système central contenant des données biométriques (estimée à 1,5 million d'EUR par an, l'eu-LISA réalisant une économie ponctuelle de 8 millions d'EUR);

- une économie de coûts liée à l'identification des identités multiples par rapport à la situation dans laquelle le même résultat serait obtenu sans les moyens proposés. Cela représenterait une économie d'au moins 50 millions d'EUR par an pour les administrations des États membres chargées de la gestion des frontières, des migrations et de la répression;

- une économie de coûts liée à la formation d'un grand groupe d'utilisateurs finaux par rapport à une situation où la formation est exigée de manière récurrente, estimée à 20 millions d'EUR par an pour les administrations des États membres chargées de la gestion des frontières, des migrations et de la répression.

1.5.3. Leçons tirées d'expériences similaires

L'expérience acquise dans le cadre du développement du système d'information Schengen de deuxième génération (SIS II) et du système d'information sur les visas (VIS) a permis de tirer les enseignements ci-après:

1. Afin d'éviter autant que possible les dépassements de budget et les retards dus à une modification des exigences, tout nouveau système d'information dans le domaine de la liberté, de la sécurité et de la justice, en particulier s'il s'agit d'un système d'information à grande échelle, ne devrait pas être développé avant que les instruments juridiques de base définissant son objet, sa portée, ses fonctions et ses caractéristiques techniques aient été définitivement adoptés.

2. Pour le SIS II et le VIS, les développements nationaux dans les États membres pouvaient être cofinancés au titre du Fonds pour les frontières extérieures, mais cela n'était pas obligatoire. Il était donc impossible de disposer d'un aperçu de l'état d'avancement dans les États membres qui n'avaient pas prévu les activités correspondantes dans leur programmation pluriannuelle ou qui avaient manqué de précision dans leur programmation. C'est pourquoi il est désormais proposé que la Commission rembourse l'intégralité des coûts d'intégration exposés par les États membres, de manière à pouvoir surveiller l'état d'avancement de ces développements.

3. En vue de faciliter la coordination générale de la mise en œuvre, tous les échanges de messages proposés entre les systèmes nationaux et centraux réutiliseront les réseaux existants et l'interface uniforme nationale.

1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés

Compatibilité avec le CFP actuel

Le règlement relatif au Fonds pour la sécurité intérieure (FSI) – Frontières est l'instrument financier dans lequel le budget consacré à la mise en œuvre de l'initiative relative à l'interopérabilité a été inclus.

Son article 5, point b), prévoit que 791 millions d'EUR seront mis en œuvre dans le cadre d'un programme pour le développement de nouveaux systèmes informatiques, sur la base des systèmes informatiques actuels et/ou de nouveaux systèmes, permettant la gestion des flux migratoires aux frontières extérieures de l'Union, sous réserve de l'adoption des actes législatifs pertinents de l'Union et dans les conditions prévues par l'article 15. Sur ces 791 millions d'EUR, 480,2 millions sont réservés au développement de l'EES, 210 millions à l'ETIAS et 67,9 millions à la révision du SIS II. Le reste (32,9 millions d'EUR) sera réaffecté en utilisant les mécanismes du FSI-Frontières. La présente proposition nécessite 32,1 millions d'EUR pour la période du cadre financier pluriannuel actuel, ce qui entre dans le budget restant.

La présente proposition requiert un budget total de 424,7 millions d'EUR (rubrique 5 comprise) pour la période 2019-2027. Le CFP actuel ne couvre que la période de deux ans 2019-2020. Les coûts ont toutefois été estimés jusqu'en 2027 inclus afin de pouvoir donner un avis éclairé sur les conséquences financières de la présente proposition, sans préjuger du prochain cadre financier pluriannuel.

Le budget demandé sur neuf ans s'élève à 424,7 millions d'EUR, les éléments suivants étant également couverts:

1) 136,3 millions d'EUR pour permettre aux États membres de couvrir les coûts des modifications à apporter à leurs systèmes nationaux pour utiliser les éléments d'interopérabilité et l'IUN fournie par l'eu-LISA, ainsi qu'un budget pour la formation d'une communauté d'utilisateurs finaux de taille conséquente. Il n'y a pas d'incidence sur le CFP actuel, car le financement est assuré à partir de 2021.

2) 4,8 millions d'EUR destinés à l'Agence européenne de garde-frontières et de garde-côtes (Frontex) pour accueillir une équipe de spécialistes qui, pendant un an (2023), validera les liens entre les identités au moment où le MID sera mis en service. Les activités de l'équipe peuvent être associées à la mission consistant à lever les ambiguïtés en matière d'identité, attribuée à l'Agence européenne de garde-frontières et de garde-côtes en vertu de la proposition relative à l'ETIAS. Il n'y a pas d'incidence sur le CFP actuel, car le financement est assuré à partir de 2021.

3) 48,9 millions d'EUR pour permettre à Europol de mettre à niveau ses systèmes informatiques eu égard au volume de messages à traiter et d'améliorer ses niveaux de performance. L'ETIAS utilisera les éléments d'interopérabilité afin de consulter les données Europol. Cependant, la capacité actuelle de traitement des informations d'Europol n'est pas compatible avec les volumes importants (100 000 interrogations par jour en moyenne) et les délais de réponse raccourcis. Un montant de 9,1 millions d'EUR est alloué au titre du CFP actuel.

4) 2,0 millions d'EUR pour le CEPOL afin de préparer la formation du personnel opérationnel et de la dispenser. Un montant de 0,1 million d'EUR est prévu en 2020.

5) 225 millions d'EUR destinés à l'eu-LISA pour couvrir le coût total du développement du programme réalisant les cinq éléments d'interopérabilité (68,3 millions d'EUR), les coûts de maintenance à partir de la livraison des éléments jusqu'en 2027 (56,1 millions d'EUR), un budget spécifique de 25,0 millions d'EUR pour la migration des données des systèmes existants vers le BMS partagé et les coûts supplémentaires pour la mise à jour de l'IUN, le réseau, la formation et les réunions. Un budget spécifique de 18,7 millions d'EUR couvre le coût de la mise à niveau et de l'exploitation du système ECRIS-TCN en mode à haute disponibilité à partir de 2022. Sur le montant total, 23 millions d'EUR sont alloués dans le cadre du CFP actuel.

6) 7,7 millions d'EUR destinés à la DG HOME afin de couvrir une augmentation limitée des effectifs et les coûts y afférents pendant la période de développement des différents éléments, étant donné que la Commission prendra également la responsabilité du comité chargé du format universel pour les messages (UMF). Ce budget, qui relève de la rubrique 5, ne sera pas couvert par le budget FSI. Pour information, un montant de 2,0 millions d'EUR est dû pour la période 2019-2020.

Compatibilité avec les initiatives antérieures

La présente initiative est compatible avec ce qui suit:

En avril 2016, la Commission a présenté une **communication intitulée «*Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*»**, afin de remédier à un certain nombre de lacunes structurelles affectant les systèmes d'information. Trois séries de mesures en ont découlé:

Premièrement, la Commission a pris **des mesures pour renforcer et optimiser les avantages des systèmes d'information existants**. En décembre 2016, la Commission a adopté des propositions visant à renforcer le système d'information Schengen (SIS) existant. Dans l'intervalle, à la suite de la proposition de la Commission de mai 2016, les négociations portant sur la base juridique révisée d'Eurodac – la base de données de l'UE contenant les empreintes digitales des demandeurs d'asile – ont été accélérées. Une proposition de nouvelle base juridique pour le système d'information sur les visas (VIS) est également en cours de préparation et sera présentée au cours du deuxième trimestre de 2018.

Deuxièmement, la Commission a proposé **des systèmes d'information supplémentaires pour combler les lacunes recensées** dans l'architecture de la gestion des données de l'UE. Les négociations portant sur la proposition de la Commission d'avril 2016 visant à établir un système d'entrée/de sortie (EES)[67] – afin d'améliorer les procédures de vérification aux frontières pour les ressortissants de pays tiers se rendant dans l'UE – ont été conclues dès juillet 2017, lorsque les colégislateurs sont parvenus à un accord politique qui a été confirmé par le Parlement européen en octobre 2017 et formellement adopté par le Conseil en novembre 2017. En novembre 2016, la Commission a également présenté une proposition visant à créer un système européen d'information et d'autorisation concernant les voyages (ETIAS)[68]. Cette proposition vise à renforcer les contrôles de sécurité des voyageurs exemptés de l'obligation de visa, en permettant de procéder à des vérifications préalables en matière d'immigration irrégulière et de sécurité. Cette proposition fait actuellement l'objet de négociations entre les colégislateurs. En juin 2017, le système

[67] COM(2016) 194 du 6 avril 2016.

[68] COM(2016) 731 du 16 novembre 2016.

européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (système ECRIS-TCN)[69] a également été proposé pour combler la lacune constatée en ce qui concerne l'échange d'informations entre États membres sur les ressortissants de pays tiers condamnés.

Troisièmement, la Commission a travaillé **à l'interopérabilité des systèmes d'information**, en se concentrant sur les quatre options présentées dans la communication[70] d'avril 2016 pour parvenir à l'interopérabilité. Trois des quatre options sont précisément l'ESP, le CIR et le BMS partagé. Par la suite, il est devenu évident qu'il fallait opérer une distinction entre le CIR en tant que base de données d'identité et un nouvel élément qui détecte les identités multiples liées à un même identifiant biométrique (MID). Les quatre éléments sont donc désormais: l'ESP, le CIR, le MID et le BMS partagé.

Synergie

La synergie est ici comprise comme l'avantage obtenu en réutilisant les solutions existantes et en évitant de nouveaux investissements.

Il existe une importante synergie entre ces initiatives et le développement de l'EES et de l'ETIAS.

Pour le fonctionnement de l'EES, un dossier individuel est créé pour tous les ressortissants de pays tiers entrant dans l'espace Schengen pour un court séjour. À cette fin, le système actuel d'établissement de correspondances biométriques utilisé pour le VIS, qui contient les modèles d'empreintes digitales pour tous les voyageurs soumis à l'obligation de visa, sera étendu aux données biométriques des voyageurs exemptés de l'obligation de visa. Le BMS partagé est donc conceptuellement une généralisation plus poussée du dispositif de correspondances biométriques qui sera développé dans le cadre de l'EES. Les modèles biométriques contenus dans le dispositif de correspondances biométriques du SIS et d'Eurodac seront ensuite migrés (tel est le terme technique utilisé lorsque des données sont transférées d'un système à un autre) vers ce BMS partagé. Selon les données des fournisseurs, le stockage dans des bases de données distinctes coûte en moyenne 1 EUR par ensemble biométrique (il y a potentiellement 200 millions d'ensembles de données au total), alors que le coût moyen tombera à 0,35 EUR par ensemble biométrique lorsqu'une solution BMS partagée sera créée. Les coûts plus élevés du matériel nécessaire pour un volume élevé de données compensent en partie ces avantages, mais en fin de compte, le coût estimé d'un BMS partagé serait inférieur de 30 % à celui du stockage des mêmes données dans plusieurs systèmes BMS plus petits.

Pour le fonctionnement de l'ETIAS, il faut disposer d'un élément d'interopérabilité pour interroger un ensemble de systèmes de l'UE. Soit l'ESP est utilisé, soit un élément spécifique est créé dans le cadre de la proposition relative à l'ESP. La proposition relative à l'interopérabilité permet de créer un seul élément plutôt que deux.

Une autre synergie est également obtenue en réutilisant la même interface uniforme nationale (IUN) que celle utilisée pour l'EES et l'ETIAS. L'IUN devra être mise à jour, mais elle continuera d'être utilisée.

[69] COM(2017) 344 du 29 juin 2017.
[70] COM(2016) 205 du 6 avril 2016.

1.6. Durée et incidence financière

☐ Proposition/initiative à **durée limitée**

– ☐ Proposition/initiative en vigueur à partir de [JJ/MM]AAAA jusqu'en [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

☒ Proposition/initiative à **durée illimitée**

– Période de développement de 2019 à 2023 inclus, puis un fonctionnement en rythme de croisière au-delà.

– La durée de l'incidence financière est donc prévue pour 2019-2027.

1.7. Mode(s) de gestion prévu(s)[71]

☒ **Gestion directe** par la Commission

– X dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☒ **Gestion partagée** avec les États membres

☒ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☒ aux organismes visés aux articles 208 et 209 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

Périodes	Phase de développement	Phase de fonctionnement	Mode de gestion	Acteur
Développement et maintenance (d'éléments	X	X	Indirecte	eu-LISA Europol

[71] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx.

Périodes	Phase de développement	Phase de fonctionnement	Mode de gestion	Acteur
d'interopérabilité pour les systèmes centraux, formation au système)				CEPOL
Migration des données (migration de modèles biométriques vers un BMS partagé), coûts de réseau, mise à jour de l'IUN, réunions et formation	X	X	Indirecte	eu-LISA
Validation des liens lors de la création du MID	X	-	Indirecte	Frontex
Personnalisation de l'IUN, intégration des systèmes nationaux et formation des utilisateurs finaux	X	X	Partagée (ou directe) (1)	COM + États membres

(1) Le présent instrument ne prévoit aucun montant pour la phase de fonctionnement.

La période de développement commence en 2019 et dure jusqu'à la livraison de chaque élément, de 2019 à 2023 (voir section 1.4.4).

1. Gestion directe par la DG HOME: pendant la période de développement, si nécessaire, des mesures peuvent également être mises en œuvre directement par la Commission. Il pourrait s'agir, en particulier, d'un soutien financier de l'Union à certaines activités sous forme de subventions (y compris aux autorités nationales des États membres), de marchés publics et/ou du remboursement des coûts supportés par des experts externes.

2. Gestion partagée: pendant la phase de développement, les États membres seront tenus d'adapter leurs systèmes nationaux afin d'accéder à l'ESP plutôt qu'à des systèmes individuels (pour les messages sortants des États membres) et pour modifier les réponses aux demandes de recherche (messages entrants à l'intention des États membres). Une mise à jour de l'IUN existante mise en œuvre pour l'EES et l'ETIAS sera également effectuée.

3. Gestion indirecte: l'eu-LISA couvrira la partie «développement» de tous les volets informatiques du projet, à savoir les éléments d'interopérabilité, la mise à jour de l'interface uniforme nationale (IUN) dans chaque État membre, la mise à jour de l'infrastructure de communication entre les systèmes centraux et les interfaces uniformes nationales, la migration des modèles biométriques des systèmes d'établissement de correspondances biométriques existants du SIS et d'Eurodac vers le BMS partagé, ainsi que l'activité de nettoyage des données qui s'y rattache.

Pendant la période de fonctionnement, l'eu-LISA se chargera de l'ensemble des activités techniques liées à la maintenance des éléments.

L'Agence européenne de garde-frontières et de garde-côtes intégrera une équipe supplémentaire dédiée à la validation des liens dès la mise en service du MID. Il s'agit d'une tâche limitée dans le temps.

Europol couvrira le développement et la maintenance de ses systèmes pour assurer l'interopérabilité avec l'ESP et l'ETIAS. Le CEPOL prépare la formation des services opérationnels et la dispense selon une approche de formation des formateurs.

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Règles en matière de suivi et de compte rendu pour le développement et la maintenance d'autres systèmes:

1. L'eu-LISA veille à ce que des procédures soient mises en place pour suivre le développement des éléments d'interopérabilité au regard des objectifs fixés en matière de planification et de coûts et pour suivre le fonctionnement des éléments au regard des objectifs fixés en matière de résultats techniques, de coût-efficacité, de sécurité et de qualité du service.

2. Dans les six mois suivant l'entrée en vigueur du présent règlement, puis tous les six mois pendant la phase de développement des éléments, l'eu-LISA présente un rapport au Parlement européen et au Conseil sur l'état d'avancement du développement de chaque élément. Une fois le développement achevé, un rapport est soumis au Parlement européen et au Conseil, qui explique en détail la manière dont les objectifs, en particulier ceux ayant trait à la planification et aux coûts, ont été atteints, et justifie les éventuels écarts.

3. Aux fins de la maintenance technique, l'eu-LISA a accès aux informations nécessaires concernant les opérations de traitement de données effectuées dans les éléments.

4. Quatre ans après la mise en service du dernier élément mis en œuvre, puis tous les quatre ans, l'eu-LISA présente au Parlement européen, au Conseil et à la Commission un rapport sur le fonctionnement technique des éléments.

5. Cinq ans après la mise en service du dernier élément mis en œuvre, puis tous les quatre ans, la Commission réalise une évaluation globale et formule les recommandations nécessaires. Cette évaluation globale comprend: les résultats obtenus par les éléments au regard de leurs objectifs d'interopérabilité, de maintenabilité, de performance et d'implications financières, ainsi que l'incidence sur les droits fondamentaux.

La Commission transmet le rapport d'évaluation au Parlement européen et au Conseil.

6. Les États membres et Europol fournissent à l'eu-LISA et à la Commission les informations nécessaires à l'établissement des rapports prévus aux points 4 et 5, dans le respect des indicateurs quantitatifs prédéfinis par la Commission et/ou l'eu-LISA. Ces informations ne peuvent porter préjudice aux méthodes de travail ni comprendre d'indications sur les sources, l'identité des membres du personnel ou les enquêtes des autorités désignées.

7. L'eu-LISA fournit à la Commission les informations nécessaires pour élaborer les évaluations globales visées au point 5.

8. Tout en respectant les dispositions du droit national relatives à la publication d'informations sensibles, chaque État membre et Europol établissent des rapports annuels sur l'efficacité de l'accès aux systèmes de l'UE à des fins répressives, qui comprennent des informations et des statistiques sur:

- l'objet précis de la consultation, notamment la nature de l'infraction terroriste ou de l'infraction pénale grave;

- les motifs raisonnables invoqués pour soupçonner que le suspect, l'auteur ou la victime relève du présent règlement;

- le nombre de demandes d'accès aux éléments à des fins répressives;

- le nombre et le type de cas qui ont permis une identification;

- la nécessité de traiter les cas exceptionnels d'urgence et les cas de ce type effectivement traités, y compris ceux dont le caractère urgent n'a pas été approuvé par le point d'accès central lors de la vérification a posteriori.

Les rapports annuels des États membres et d'Europol sont transmis à la Commission au plus tard le 30 juin de l'année suivante.

2.2. Système de gestion et de contrôle

2.2.1. Risque(s) identifié(s)

Les risques sont ceux liés au développement informatique de cinq éléments par un prestataire externe géré par l'eu-LISA. Il s'agit de risques typiques associés à des projets:

1. le risque de ne pas terminer le projet à temps;

2. le risque de ne pas terminer le projet dans les limites du budget;

3. le risque de ne pas réaliser la totalité du projet.

Le premier risque est le plus important, car un dépassement de délai entraîne des coûts plus élevés, la plupart des coûts étant liés à la durée: frais de personnel, frais de licence payés par an, etc.

Ces risques peuvent être atténués par l'application de techniques de gestion de projet, notamment en prévoyant des mesures d'urgence dans les projets de développement et une dotation en personnel suffisante pour pouvoir absorber les pics de travail. En effet, l'effort est généralement estimé en supposant que la charge de travail est uniformément répartie dans le temps, alors que la réalité des projets consiste en une charge de travail inégale qui est absorbée par des allocations de ressources plus élevées.

Le recours à un prestataire externe pour ces travaux de développement comporte plusieurs risques:

1. en particulier, le risque que le prestataire n'alloue pas des ressources suffisantes au projet ou qu'il conçoive et développe un système qui ne soit pas du dernier cri;

2. le risque que les techniques et modalités administratives de gestion des systèmes d'information à grande échelle ne soient pas intégralement respectées, le prestataire y voyant un moyen de réduire les coûts;

3. enfin, on ne saurait totalement exclure le risque que le prestataire se heurte à des difficultés financières pour des raisons étrangères au projet.

Ces risques sont atténués par l'attribution de contrats sur la base de critères de qualité rigoureux, la vérification des références des prestataires et le maintien d'une relation étroite avec eux. Enfin, en dernier recours, des clauses de pénalité et de résiliation sévères peuvent être incluses et appliquées au besoin.

2.2.2. Informations concernant le système de contrôle interne mis en place

L'eu-LISA est appelée à être un centre d'excellence dans le domaine du développement et de la gestion des systèmes d'information à grande échelle. Elle exécute les activités liées au développement et au fonctionnement des différents éléments d'interopérabilité, y compris la maintenance de l'interface uniforme nationale dans les États membres.

Pendant la phase de développement, toutes les activités de développement seront menées à bien par l'eu-LISA. Cela concernera la partie «développement» de tous les volets du projet. Les coûts liés à l'intégration des systèmes dans les États membres au cours du développement seront gérés par la Commission au moyen d'une gestion partagée ou de subventions.

Pendant la phase opérationnelle, l'eu-LISA sera chargée de la gestion technique et financière des éléments utilisés au niveau central, notamment l'attribution et la gestion des contrats. La Commission gérera les fonds destinés aux États membres pour les dépenses des unités nationales au moyen du FSI – Frontières (programmes nationaux).

Pour éviter les retards au niveau national, une gouvernance efficace entre toutes les parties intéressées doit être prévue avant le début du développement. La Commission part du principe qu'une architecture interopérable doit être définie au début du projet afin d'être appliquée dans les projets EES et ETIAS, étant donné que ces projets mettent en œuvre et utilisent le BMS partagé, le répertoire commun de données d'identité et le portail de recherche européen. Un membre de l'équipe de gestion du projet d'interopérabilité devrait faire partie de la structure de gouvernance des projets EES et ETIAS.

2.2.3. Estimation du coût-bénéfice des contrôles et évaluation du niveau attendu de risque d'erreur

Aucune estimation n'est fournie, car le contrôle et l'atténuation des risques constituent une tâche inhérente à la structure de gouvernance du projet.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées.

Les mesures prévues pour lutter contre la fraude sont exposées à l'article 35 du règlement (UE) nº 1077/2011, qui dispose ce qui suit:

1. Afin de lutter contre la fraude, la corruption et d'autres activités illégales, le règlement (CE) nº 1073/1999 s'applique.

2. L'agence adhère à l'accord interinstitutionnel relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF) et arrête immédiatement les dispositions appropriées applicables à l'ensemble de son personnel.

3. Les décisions de financement et les accords et instruments d'application qui en découlent prévoient expressément que la Cour des comptes et l'OLAF peuvent, au besoin, effectuer des contrôles sur place auprès des bénéficiaires des crédits de l'agence ainsi qu'auprès des agents responsables de l'attribution de ces crédits.

Conformément à cette disposition, le conseil d'administration de l'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 a adopté le 28 juin 2012 sa décision relative aux conditions et modalités des enquêtes internes en

matière de lutte contre la fraude, la corruption et toute activité illégale préjudiciable aux intérêts de l'Union.

La stratégie de prévention et de détection des fraudes de la DG HOME s'appliquera.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

L'INCIDENCE ESTIMÉE SUR LES DÉPENSES ET LE PERSONNEL POUR LES ANNÉES 2021 ET AU-DELÀ DANS LA PRÉSENTE FICHE FINANCIÈRE LÉGISLATIVE EST AJOUTÉE À TITRE INDICATIF ET NE PRÉJUGE PAS DU PROCHAIN CADRE FINANCIER PLURIANNUEL

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro [Libellé……...……]	CD/CND[72].	de pays AELE[73]	de pays candidats[74]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
3	18.02.01.03 – Frontières intelligentes	CD	Non	Non	Oui	Non
3	18.02.03 – Agence européenne de garde-frontières et de garde-côtes (Frontex)	CD	Non	Non	Oui	Non
3	18.02.04 – EUROPOL	CD	Non	Non	Non	Non
3	18.02.05 - CEPOL	CND	Non	Non	Non	Non
3	18.02.07 – 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 (eu-LISA)	CD	Non	Non	Oui	Non

72 CD = crédits dissociés / CND = crédits non dissociés.

73 AELE: Association européenne de libre-échange.

74 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence estimée sur les dépenses

[Cette partie est à compléter en utilisant la **feuille de calcul sur les données budgétaires de nature administrative** (second document en annexe à cette fiche financière) à charger dans DECIDE pour les besoins de la consultation interservices.]

3.2.1. Synthèse de l'incidence estimée sur les dépenses

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	3	Sécurité et citoyenneté

DG Home			Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**Année 2028**	**TOTAL**
• Crédits opérationnels													
18.02.01.03 – Frontières intelligentes	Engagements	(1)	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Paiements	(2)	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[75]													
Numéro de ligne budgétaire		(3)											
TOTAL des crédits pour la DG HOME	Engagements	=1+1a +3	0	0	43,150	48,150	45,000	0	**0**	**0**	**0**	**0**	**136,300**
	Paiements	=2+2a +3	0	0	34,520	47,150	45,630	9,000	**0**	**0**	**0**	**0**	136,300

Les dépenses couvriront les coûts suivants:

[75] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

– le coût d'adaptation de l'IUN (interface uniforme nationale), dont le développement est financé au titre de la proposition EES, un montant budgétisé pour les modifications des systèmes dans les États membres afin de tenir compte des modifications des systèmes centraux et un montant budgétisé pour la formation des utilisateurs finaux.

18.0203 – Frontex			Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Titre 1: dépenses de personnel	Engagements	(1)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
	Paiements	(2)	0	0	0	0,488	2,154	0,337	0	0	0	2,979
Titre 2: dépenses d'infrastructure et de fonctionnement	Engagements	(1a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
	Paiements	(2a)	0	0	0	0,105	0,390	0,065	0	0	0	0,560
Titre 3: dépenses opérationnelles	Engagements	(3a)	0	0	0	0,183	2,200	0	0	0	0	2,383
	Paiements	(3b)	0	0	0	0,183	2,200	0	0	0	0	2,383
TOTAL des crédits pour Europol	(Total engagements = Total paiements)	=1+1a +3a	**0**	**0**	**0**	**0,776**	**4,744**	**0,402**	**0**	**0**	**0**	**5,923**

– Le budget de l'Agence européenne de garde-frontières et de garde-côtes couvre les dépenses d'une équipe dédiée à la validation des liens générés par le MID (détecteur d'identités multiples) sur les données anciennes (quelque 14 millions d'enregistrements). Le volume de liens à valider manuellement est estimé à environ 550 000.
L'équipe dédiée mise en place à cet effet vient s'ajouter à l'équipe de l'agence mise en place pour l'ETIAS car elle est fonctionnellement proche et cela évite les coûts de mise en place d'une nouvelle équipe. Les travaux devraient avoir lieu en 2023. Les agents contractuels seront donc recrutés jusqu'à 3 mois à l'avance et leur contrat prendra fin jusqu'à 2 mois après la fin de l'activité de migration. Par hypothèse, une autre partie des ressources nécessaires ne sera pas recrutée avec le statut d'agent contractuel et sera engagée avec celui de consultant. Ceci explique les coûts du titre 3 pour 2023. Il est supposé que les recrutements auront lieu un mois à l'avance. D'autres détails sur les niveaux de personnel sont fournis plus loin.

– Le titre 1 comprend donc le coût de 20 agents internes et les dispositions relatives au renforcement du personnel d'encadrement et de soutien.

– Le titre 2 comprend le coût supplémentaire lié à l'hébergement des 10 agents supplémentaires du prestatie.

– Le titre 3 comprend les honoraires des 10 agents supplémentaires du prestataire. Il n'y a pas d'autres types de frais inclus.

18.0204 - Europol			Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Titre 1: dépenses de personnel	Engagements	(1)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
	Paiements	(2)	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
Titre 2: dépenses d'infrastructure et de fonctionnement	Engagements	(1a)	0	0	0	0	0	0	0	0	0	0
	Paiements	(2a)	0	0	0	0	0	0	0	0	0	0
Titre 3: dépenses opérationnelles	Engagements	(3a)	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
	Paiements	(3b)	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
TOTAL des crédits pour Europol	(Total engagements = Total paiements)	=1+1a +3a	0,690	8,382	8,382	3,589	3,589	3,382	8,732	8,732	3,382	48,860

Les dépenses d'Europol couvriront la mise à niveau des capacités de ses systèmes TIC pour faire face au volume de messages à traiter et l'amélioration nécessaire de ses niveaux de performance (temps de réponse).

Le titre 1 (dépenses de personnel) couvre les coûts liés au personnel TIC supplémentaire à recruter pour renforcer les systèmes d'information d'Europol pour les raisons décrites ci-dessus. De plus amples informations sont fournies ci-après sur la répartition des postes entre agents temporaires et agents contractuels, ainsi que sur leurs compétences.

Le titre 3 inclut les coûts du matériel et des logiciels nécessaires au renforcement des systèmes d'information d'Europol. À l'heure actuelle, les systèmes informatiques d'Europol sont au service d'une communauté restreinte déterminée d'agents d'Europol, d'officiers de liaison Europol et d'enquêteurs dans les États membres qui utilisent ces systèmes à des fins d'analyse et d'enquête. Avec la mise en œuvre de QUEST (l'interface système qui permettra à l'ESP d'interroger les données Europol) au niveau de protection minimum (actuellement, les systèmes d'information d'Europol sont accrédités jusqu'au niveau «restreint UE» et «confidentiel UE»), les systèmes d'information d'Europol seront mis à la disposition d'une bien plus grande communauté répressive autorisée. En plus de ces extensions, l'ETIAS utilisera l'ESP pour interroger automatiquement les données Europol afin de traiter les autorisations de voyage. Cela augmentera le volume des recherches dans les données Europol, qui passera d'environ 107 000 interrogations par mois à l'heure actuelle à plus de 100 000 interrogations par jour, et exigera également une disponibilité des systèmes d'information d'Europol 24 heures sur 24 et 7 jours sur 7 et des délais de réponse très courts pour satisfaire aux exigences imposées par

le règlement ETIAS. La majorité des coûts sont limités à la période précédant la mise en service des éléments d'interopérabilité, mais certains engagements permanents sont nécessaires pour garantir en permanence la haute disponibilité des systèmes d'information d'Europol. En outre, certains travaux de développement sont nécessaires pour qu'Europol puisse mettre en œuvre les éléments d'interopérabilité en tant qu'utilisateur.

18.0205 - CEPOL			Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Titre 1: dépenses de personnel	Engagements	(1)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
	Paiements	(2)	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
Titre 2: dépenses d'infrastructure et de fonctionnement	Engagements	(1a)	0	0	0	0	0	0	0	0	0	0
	Paiements	(2a)	0	0	0	0	0	0	0	0	0	0
Titre 3: dépenses opérationnelles	Engagements	(3a)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
	Paiements	(3b)	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
TOTAL des crédits pour le CEPOL	(Total engagements = Total paiements)	=1+1a +3a	0	0,144	0,384	0,482	0,208	0,208	0,208	0,208	0,208	2,050

Une formation au niveau de l'UE, coordonnée au niveau central, améliore la cohérence de la mise en œuvre des cours de formation au niveau national et, par conséquent, assure une mise en œuvre et une utilisation correctes et efficaces des éléments d'interopérabilité. Le CEPOL – en tant qu'Agence européenne de formation des services répressifs – est bien placé pour dispenser une formation au niveau central de l'UE. Ces dépenses couvrent la préparation de la «formation des formateurs des États membres», nécessaire à l'utilisation des systèmes centraux une fois que ceux-ci auront été rendus interopérables. Les coûts comprennent les coûts liés à une petite augmentation des effectifs pour permettre au CEPOL de coordonner, gérer, organiser et mettre à jour les cours, ainsi que les coûts liés à la fourniture d'un certain nombre de sessions de formation par an et à la préparation du cours en ligne. Le détail de ces coûts est expliqué ci-dessous. L'effort de formation est concentré sur les périodes précédant immédiatement la mise en service. Un effort continu reste nécessaire au-delà de la mise en service, étant donné que les éléments interopérables font l'objet d'une maintenance et que les formateurs ne sont pas en permanence les mêmes personnes, compte tenu de l'expérience acquise en matière de formation sur le système d'information Schengen.

18.0207 - eu-LISA			Année	Année	Année	Année	Année	Année	Année	Année	Année	**TOTAL**

			2019	2020	2021	2022	2023	2024	2025	2026	2027	
Titre 1: dépenses de personnel	Engagements	(1)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
	Paiements	(2)	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
Titre 2: dépenses d'infrastructure et de fonctionnement	Engagements	(1a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
	Paiements	(2a)	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
Titre 3: dépenses opérationnelles	Engagements	(3a)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
	Paiements	(3b)	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
TOTAL des crédits pour l'eu-LISA	(Total engagements = Total paiements)	=1+1a +3a	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**

Ces dépenses couvriront:

– Le développement et la maintenance des quatre éléments d'interopérabilité [portail de recherche européen (ESP), service partagé d'établissement de correspondances biométriques (BMS partagé), répertoire commun de données d'identité (CIR) et détecteur d'identités multiples (MID)] inclus dans la proposition législative, ainsi que le répertoire central des rapports et statistiques (CRRS). L'eu-LISA agira en tant que représentant du maître d'ouvrage et utilisera son propre personnel pour rédiger les cahiers des charges, sélectionner les prestataires, diriger les travaux, soumettre les résultats à une série d'essais et accepter le travail effectué.

– Les coûts liés à la migration des données des systèmes existants vers les nouveaux éléments. L'eu-LISA n'a toutefois aucun rôle direct dans le chargement initial des données pour le MID (validation des liens) car il s'agit d'une action sur le contenu des données lui-même. La migration des données biométriques des systèmes existants concerne le format et l'étiquetage des données et non leur contenu.

– Les coûts de mise à niveau et d'exploitation du système ECRIS-TCN en tant que système à haute disponibilité à partir de 2022. Le système ECRIS-TCN est le système central contenant le casier judiciaire des ressortissants de pays tiers. Le système devrait être disponible d'ici à 2020. Les éléments d'interopérabilité devraient également avoir accès à ce système, qui devrait donc également devenir un système à haute disponibilité. Les dépenses opérationnelles comprennent le coût supplémentaire permettant d'obtenir cette haute disponibilité. Le coût de développement est important pour 2021, suivi d'un coût de maintenance et d'exploitation constant. Ces

coûts ne sont pas inclus dans la fiche financière législative de la révision du règlement instituant l'eu-LISA[76], qui ne comprend que les budgets de 2018 à 2020, et il n'y a donc pas de chevauchement avec la présente demande de budget.

– La structure des dépenses est le résultat du séquençage des projets. Comme les différents éléments ne sont pas indépendants les uns des autres, la période de développement s'étend de 2019 à 2023. Cependant, la maintenance et l'exploitation des premiers éléments disponibles commenceront dès 2020. Cela explique pourquoi les dépenses démarrent lentement, augmentent puis diminuent pour atteindre une valeur constante.

– Les dépenses relevant du titre 1 (dépenses de personnel) suivent le séquençage des projets: davantage de personnel est nécessaire pour exécuter le projet avec le prestataire (dont les dépenses sont indiquées au titre 3). Lorsque le projet est réalisé, une partie de l'équipe y ayant participé est affectée aux travaux d'évolution et de maintenance. Parallèlement, le personnel affecté à l'exploitation des nouveaux systèmes augmente.

– Les dépenses relevant du titre 2 (dépenses d'infrastructure et de fonctionnement) couvrent les locaux à usage de bureaux supplémentaires pour l'accueil temporaire des équipes du prestataire en charge des tâches de développement, de maintenance et d'exploitation. L'évolution dans le temps des dépenses suit donc également l'évolution des effectifs. Les coûts d'hébergement de matériel supplémentaire ont déjà été inclus dans le budget de l'eu-LISA. Il n'y a pas non plus de frais supplémentaires pour l'hébergement du personnel de l'eu-LISA, car ceux-ci sont inclus dans les coûts ordinaires de personnel.

– Les dépenses relevant du titre 3 (dépenses opérationnelles) comprennent le coût supporté par le prestataire pour le développement et la maintenance du système, l'acquisition du matériel et des logiciels spécifiques.
Les coûts liés au prestataire commencent initialement avec les études de spécification des éléments, et le développement ne commence que pour un seul élément (le CRRS). Au cours de la période 2020-2022, les coûts augmentent ensuite à mesure que d'autres éléments sont développés en parallèle. Les coûts ne diminuent pas après le pic car les tâches de migration des données sont particulièrement lourdes dans ce portefeuille de projets. Les coûts liés au prestataire diminuent ensuite à mesure que les éléments sont livrés et commencer à fonctionner, ce qui exige une répartition stable des ressources.
En même temps que les dépenses relevant du titre 3, les dépenses augmentent fortement en 2020 par rapport à l'année précédente en raison de l'investissement initial en matériel et logiciels nécessaires au développement. Les dépenses relevant du titre 3 (charges opérationnelles) connaissent une forte hausse en 2021 et 2022 car les coûts d'investissement en matériel et logiciels pour les environnements informatiques opérationnels (production et pré-production tant pour l'unité centrale que pour l'unité centrale de secours) sont encourus dans l'année précédant la mise en service, respectivement pour les éléments d'interopérabilité (le CIR et le MID)

[76] COM 2017/0145 (COD) Proposition de règlement du Parlement européen et du Conseil relatif à l'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, et modifiant le règlement (CE) nº 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) nº 1077/2011.

ayant des exigences élevées en matière de logiciels et de matériel. Une fois en service, les coûts du matériel et des logiciels sont essentiellement des coûts de maintenance.

– De plus amples détails sont donnés plus loin.

Rubrique du cadre financier pluriannuel	**5**	«Dépenses administratives»

En Mio EUR (à la 3e décimale)

		Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
DG HOME											
• Ressources humaines Numéro de ligne budgétaire 18.01		0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Autres frais administratifs (réunions, etc.)		0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
TOTAL DG HOME	Crédits	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

TOTAL des crédits pour la RUBRIQUE 5 du cadre financier pluriannuel	(Total engagements = Total paiements)	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

En Mio EUR (à la 3e décimale)

		Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	Année 2028	**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 5 du cadre financier pluriannuel	Engagements	**7,533**	**26,569**	**104,672**	**98,591**	**83,363**	**25,256**	**28,088**	**28,008**	**22,658**	**0**	**424,738**
	Paiements	**7,533**	**26,569**	**96,042**	**97,591**	**83,993**	**34,256**	**28,088**	**28,008**	**22,658**	**0**	**424 738**

3.2.2. Incidence estimée sur les crédits opérationnels

3.2.2.1. Incidence estimée sur les crédits de l'Agence européenne de garde-frontières et de garde-côtes

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
Agence Frontex ⇩	Type [77]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1 [78] Validation des liens																						
Nbre de collaborateurs recrutés comme experts pour valider les liens	Coûts de prestataire		0	0	0	0	0	0	0,8	0,183	10	2,200	0	0	0	0	0	0	0	0		2,383
Sous-total objectif spécifique nº 1			**0**	**0**	**0**	**0**	**0**	**0**	**0,8**	**0,183**	**10**	**2,200**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**2,383**

Ces dépenses couvriront:

- Le recrutement d'un personnel supplémentaire suffisant (estimé à une dizaine d'experts), s'ajoutant au personnel interne existant (estimé à une vingtaine de personnes), qui sera accueilli au sein de l'agence afin de valider les liens. Le recrutement commencera seulement un mois avant la date de début prévue pour atteindre les effectifs requis.

[77] Les sorties sont les produits et services à fournir (par ex.: nombre d'échanges étudiants financés, nombre de km de routes construites, etc.).

[78] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

- Il n'y a pas d'autres coûts estimés pour le prestataire. Le logiciel nécessaire fait partie des coûts de licence du BMS partagé. Il n'y a pas de capacité matérielle de traitement spécifique. Il est supposé que le personnel du prestataire sera accueilli par l'agence. C'est pourquoi, dans le cadre des dépenses relevant du titre 2, le coût annuel de 12 mètres carrés est ajouté en moyenne par personne.

3.2.2.2. Incidence estimée sur les crédits d'Europol

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations **Europol** ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [79]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1 [80] Développement et maintenance des systèmes (Europol)																						
Environnement informatique	Infrastructure					1,840		1,840		0,736		0,736		0,736		0,736		0,736		0,736		8,096
Environnement informatique	Matériel					3,510		3,510		1,404		1,404		1,404		5,754		5,754		1,404		26,144

[79] Les sorties sont les produits et services à fournir (par ex.: nombre d'échanges étudiants financés, nombre de km de routes construites, etc.).

[80] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

Environnement informatique	Logiciels				0,670		0,670		0,268		0,268		0,268		0,268		0,268		2,948
Travaux de développement	Prestataire				0,360		0,360												0,720
Sous-total			**0**		**6,380**		**6,380**		**2,408**		**2,408**		**2,408**		**7,758**		**7,758**		**2,408**		**37,908**

Ces dépenses couvriront les besoins liés au renforcement des systèmes d'information et de l'infrastructure d'Europol pour faire face à l'augmentation du nombre de requêtes. Ces coûts comprennent:

– la mise à niveau de l'infrastructure de sécurité et de réseau, du matériel (serveurs, stockage) et des logiciels (licences). Ces mises à niveau doivent être finalisées avant que le portail de recherche européen et l'ETIAS ne deviennent opérationnels en 2021, les coûts ayant été répartis également entre 2020 et 2021. À partir de 2022, le taux de maintenance annuel de 20 % a été pris comme base pour calculer les coûts de maintenance. En outre, le cycle quinquennal standard de remplacement du matériel et de l'infrastructure obsolètes a été pris en considération.

– les coûts de prestataire pour les travaux de développement pour la mise en œuvre de QUEST au niveau de protection de base.

3.2.2.3. Incidence estimée sur les crédits du CEPOL

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations			Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**

CEPOL ⇩	Type [81]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1 [82] Mise au point des séances de formation et organisation de ces dernières																						
Nombre de cours résidentiels	0,34 par cours		0		1	0,040	4	0,136	8	0,272	2	0,068	2	0,068	2	0,068	2	0,068	2	0,068		0,788
Formation en ligne	0,02			0				0,040		0,002		0,002		0,002		0,002		0,002		0,002		0,052
Sous-total				**0**		**0,040**		**0,176**		**0,274**		**0,070**		**0,070**		**0,070**		**0,070**		**0,070**		**0,840**

Afin d'assurer une mise en œuvre et une utilisation uniformes des solutions d'interopérabilité, la formation sera organisée tant au niveau central de l'UE par le CEPOL que par les États membres. Les dépenses de formation au niveau de l'UE incluent:

– l'élaboration de programmes d'études communs devant être utilisés par les États membres lors de la mise en œuvre d'une formation nationale;

– des activités résidentielles pour former les formateurs. Dans les deux ans, immédiatement après la mise en service des solutions d'interopérabilité, la formation devrait être mise en œuvre à plus grande échelle, puis poursuivie par deux cours résidentiels par an.

– un cours en ligne pour compléter les activités résidentielles au niveau de l'UE et dans les États membres.

[81] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[82] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

3.2.2.4. Incidence estimée sur les crédits de l'eu-LISA

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations **eu-LISA** ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type[83]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[84] Développement des éléments d'interopérabilité																						
Systèmes construits	Prestataire			1,800		4,930		8,324		4,340		1,073		1,000		0,100		0,020		0,020		21,607
Produits logiciels	Logiciels			0,320		3,868		15,029		8,857		3,068		0,265		0,265		0,265		0,265		32,202
Produits matériels	Matériel			0,250		2,324		5,496		2,904		2,660		0,500		0		0		0		14,133
Formation informatique	Formation et autre			0,020		0,030		0,030		0,030		0,030		0,050		0,050		0,050		0,050		0,340
Sous-total objectif spécifique nº 1				**2,390**		**11,151**		**28,879**		**16,131**		**6,830**		**1,815**		**0,415**		**0,335**		**0,335**		**68,281**

[83] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[84] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

– Cet objectif ne comprend que les coûts de livraison des quatre éléments d'interopérabilité et du CRRS.

– Les coûts du BMS partagé ont été estimés en tenant compte de l'hypothèse selon laquelle l'EES qui est sur le point d'être développé servira de système de base pour le développement. Il est donc prévu de réutiliser les licences de logiciels biométriques (36 millions d'EUR) incluses pour l'EES.

– Dans le cadre de ce budget, le BMS partagé est considéré comme une extension du BMS destiné à l'EES. C'est pourquoi la fiche financière actuelle inclut le coût marginal des licences de logiciels (6,8 millions d'EUR) pour l'ajout des quelque 20 millions d'ensembles de données biométriques contenus dans l'AFIS du SIS (l'AFIS est le système automatisé d'identification par empreintes digitales = le «BMS» du SIS), l'AFIS d'Eurodac et le futur ECRIS-TCN (système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers) au BMS livré pour l'EES. Les coûts d'intégration des différents systèmes (SIS, Eurodac, ECRIS-TCN) dans le BMS partagé sont inclus dans cette fiche financière.

– Dans le cadre des travaux pour 2019 et 2020, il sera demandé à l'eu-LISA d'élaborer la solution technique précise qui ne peut être définie au moment de la soumission de la proposition législative et d'estimer les conséquences financières de la mise en œuvre de la solution technique privilégiée. Cela pourrait nécessiter une modification de l'estimation des coûts fournie ici.

– Tous les éléments seront livrés avant la fin de l'année 2023, ce qui explique pourquoi les dépenses du prestataire ont été réduites à près de zéro à cette date. Il ne reste plus qu'un montant résiduel pour la mise à jour récurrente du CRSS.

– Au cours de la période 2019-2021, les dépenses relatives aux logiciels augmentent de manière substantielle car les coûts des licences logicielles sont supportés pour les différents environnements nécessaires à la production, à la pré-production et aux essais, et ce tant sur le site central que sur le site de sauvegarde. De plus, certains éléments logiciels spécifiques et indispensables sont facturés en fonction du nombre «d'objets référencés» (c'est-à-dire le volume de données). Comme la base de données contiendra à terme environ 220 millions d'identités, le prix du logiciel est proportionnel à cette valeur.

Indiquer les objectifs et les réalisations eu-LISA ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [85]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 2 Maintenance et exploitation des éléments d'interopérabilité																						
Systèmes maintenus opérationnels	Prestataire			0		0		0		1,430		2,919		2,788		2,788		2,788		2,788		15,501
Produits logiciels	Logiciels			0		0,265		0,265		1,541		5,344		5,904		5,904		5,904		5,904		31,032
Produits matériels	Matériel			0		0,060		0,060		0,596		1,741		1,741		1,741		1,741		1,741		9,423
Formation	Formation			0		0		0		0		0,030		0,030		0,030		0,030		0,030		0,150
Sous-total objectif spécifique nº 2				**0**		**0,325**		**0,325**		**3,567**		**10,034**		**10,464**		**10,464**		**10,464**		**10,464**		**56,105**

– La maintenance commence dès la livraison de certains éléments. Par conséquent, le budget relatif à un prestataire chargé de la maintenance est inclus à partir du moment où l'ESP est livré (en 2021). Le budget consacré à la maintenance augmente au fur et à mesure qu'un plus grand nombre d'éléments sont livrés et atteint ensuite une valeur plus ou moins constante représentant un pourcentage (entre 15 et 22 %) de l'investissement initial.

[85] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

– La maintenance du matériel et des logiciels commence à partir de l'année de mise en service: l'évolution des coûts est similaire à celle des coûts liés au prestataire.

Indiquer les objectifs et les réalisations **eu-LISA** ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [86]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 3[87] Migration des données																						
Migration des anciennes	Vers le BMS partagé			0		0		0		7,000		3,000		0		0		0		0		10,000
Anciennes données d'EDAC	Reconception et reconstruction d'EDAC			0		0		7,500		7,500				0		0		0		0		15,000
Sous-total objectif spécifique nº 3				**0**		**0**		**7,500**		**14,500**		**3,000**										**25,000**

– Dans le cas du projet de BMS partagé, les données doivent être transférées des autres moteurs biométriques vers le BMS partagé, car ce système commun est plus efficace sur le plan opérationnel et présente également un avantage financier par rapport à une situation où plusieurs systèmes de BMS plus petits continueraient à être maintenus.

– La logique opérationnelle actuelle d'Eurodac n'est pas clairement séparée du mécanisme d'établissement de correspondances biométriques, comme c'est le cas du système BMS fonctionnant avec le VIS. Le fonctionnement interne d'Eurodac et le mécanisme par lequel les services opérationnels utilisent les services d'établissement de correspondances biométriques sous-jacents constituent une boîte noire pour le public extérieur et reposent sur une technologie propriétaire. Il ne sera pas possible de simplement migrer les données

[86] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[87] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

vers un BMS partagé et de conserver la strate opérationnelle existante. Par conséquent, la migration des données s'accompagne de coûts importants liés à la modification des mécanismes d'échange avec l'application centrale d'Eurodac.

Indiquer les objectifs et les réalisations **eu-LISA** ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [88]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 4 [89] Réseau																						
Connexions du réseau	Mise en place du réseau			0		0		0		0,505										0		0,505
Trafic de réseau géré	Opérations de réseau			0		0						0,246		0,246		0,246		0,246		0,246		1,230
Sous-total objectif spécifique nº 4				**0**		**0**		**0**		**0,505**		**0,246**		**0,246**		**0,246**		**0,246**		**0,246**		**1,735**

– Les éléments d'interopérabilité n'ont qu'un effet marginal sur le trafic réseau. En termes de données, seuls des liens entre les données existantes sont créés, ce qui constitue un élément à faible volume. Le coût inclus ici n'est que l'augmentation marginale du budget requis en plus des budgets EES et ETIAS pour la mise en place du réseau et le trafic.

[88] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[89] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

Indiquer les objectifs et les réalisations eu-LISA ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [90]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 5 [91] Mise à jour IUN																						
IUN mise à jour	Prestataire			0		0		0		0,505		0,505								0		1,010
Sous-total objectif spécifique nº 5				**0**		**0**		**0**		**0,505**		**0,505**										**1,010**

– La proposition EES a introduit le concept de l'interface uniforme nationale (IUN), dont le développement et la maintenance doivent être assurés par l'eu-LISA. Le tableau ci-dessus présente le budget pour la mise à jour de l'IUN pour un type supplémentaire d'échange d'informations. Il n'y a pas de coût supplémentaire pour l'exploitation de l'IUN, qui étaient déjà budgétisée dans le cadre de la proposition EES.

[90] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[91] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

Indiquer les objectifs et les réalisations eu-LISA ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type[92]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 6: Réunions et formation																						
Réunions de suivi mensuelles (Développement)		0,021 par réunion x 10 par an	10	*0,210*	10	*0,210*	10	*0,210*	10	*0,210*											40	0,840
Réunions trimestrielles (exploitation)		0,021 x 4 par an	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Groupes consultatifs		0,021 x 4 par an	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	4	0,084	36	0,756
Formation États membres		0,025 par formation	2	0,050	4	0,100	4	0,100	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	6	0,150	24	1,150
Sous-total objectif spécifique nº 6			20	**0,428**	22	**0,478**	22	**0,478**	24	**0,528**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**	14	**0,318**		**3,502**

[92] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

– Le sous-total 6 comprend les coûts liés à l'organisation de réunions par l'instance gestionnaire (dans le cas présent, l'eu-LISA) pour la gouvernance du projet. Il s'agit des frais de réunions supplémentaires pour la livraison des éléments d'interopérabilité.

– Le sous-total 6 comprend les coûts afférents aux réunions entre l'eu-LISA et le personnel des États membres chargé du développement, de la maintenance et de l'exploitation des éléments d'interopérabilité, ainsi qu'à l'organisation et à la formation du personnel des services informatiques des États membres.

– Pendant la phase de développement, le budget comprend 10 réunions de projet par année. Une fois la phase d'exploitation préparée (et c'est le cas à partir de 2019), quatre réunions sont organisées par an. À un niveau hiérarchique plus élevé, un groupe consultatif est créé dès le début pour mettre en œuvre les décisions d'exécution de la Commission. Quatre réunions par an sont prévues, comme pour les groupes consultatifs existants. En outre, l'eu-LISA prépare et dispense une formation à l'attention du personnel des services informatiques des États membres. Il s'agit d'une formation sur les aspects techniques des éléments d'interopérabilité.

Indiquer les objectifs et les réalisations **eu-LISA** ⇩			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [93]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE n° 7 [94] Haute disponibilité du système ECRIS-TCN																						
Système à haute disponibilité	Mise en place du système			0		0		8,067												0		8,067

[93] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[94] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

Exploitation à haute disponibilité	Maintenance et exploitation du système		0		0		0		1,768		1,768		1,768		1,768		1,768		1,768		10,608
Sous-total objectif spécifique nº 4			**0**		**0**		**8,067**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**1,768**		**18,675**

– L’objectif 7 consiste à faire convertir l’ECRIS-TCN, qui est un système à disponibilité «standard», en un système à haute disponibilité. En 2021, le système ECRIS-TCN subira cette mise à niveau, qui nécessite essentiellement l’acquisition de matériel supplémentaire. Étant donné que le système ECRIS-TCN devrait être achevé en 2020, il est tentant de construire dès le départ ce système en tant que système hautement disponible et intégré aux éléments d’interopérabilité. Toutefois, étant donné que de nombreux projets deviennent dépendants les uns des autres, il est prudent de ne pas faire cette hypothèse et d’établir un budget pour des actions distinctes. Ce budget est un budget supplémentaire aux coûts de développement, de maintenance ou d’exploitation du système ECRIS-TCN en 2019 et 2020.

3.2.2.5. Impact estimé sur les crédits de la DG HOME

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☒ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations			Année **2019**		Année **2020**		Année **2021**		Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
DG Home ⇩	Type [95]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1: Intégration des systèmes nationaux (des États membres)																						
IUN prête à l'emploi	Personnalisation IUN - développements						30	3,150	30	3,150											30	6,300
Systèmes des États membres adaptés à l'interopérabilité	Coûts d'intégration						30	40,000	30	40,000	30	40,000									30	120,000
Utilisateurs finaux formés	10 000 sessions utilisateur final au total, à 1 000 EUR par session								5000	5,000	5000	5,000									10 000	10,000
Sous-total objectif spécifique nº 1								**43,150**		**48,150**		**45,000**										**136,300**

[95] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

– L’objectif spécifique 1 concerne les fonds mis à la disposition des États membres pour tirer parti des systèmes centraux interopérables. L’IUN est personnalisée à la fois lors de la mise en œuvre de l’ESP et lorsque le MID devient opérationnel. Chaque État membre doit alors opérer un changement relativement modéré (estimé à 150 jours-hommes) pour s’adapter à ces échanges de messages actualisés avec les systèmes centraux. Le changement du contenu des données que l’interopérabilité introduira et qui est couvert par le «coût d’intégration» est plus substantiel. Ces fonds concernent les changements apportés au type de messages envoyés au système central et au traitement de la réponse renvoyée. Pour estimer les coûts de ces changements, un budget de 4 millions d’EUR est alloué par État membre. Ce montant est le même que pour l’EES, car il faut un volume de travail comparable pour adapter l’intégration des systèmes nationaux aux IUN.

– Les utilisateurs finaux doivent être formés aux systèmes. Cette formation destinée à une très large population d’utilisateurs finaux sera financée sur la base de 1 000 EUR par session de 10 à 20 utilisateurs finaux pour les 10 000 sessions qui seront organisées par tous les États membres dans leurs propres locaux.

3.2.3. Incidence estimée sur les ressources humaines

3.2.3.1. Synthèse pour l'Agence européenne de garde-frontières et de garde-côtes

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Fonctionnaires (grades AD)										
Fonctionnaires (grades AST)	0									
Agents contractuels	0	0	0	0,350	1,400	0,233	0	0	0	1,983
Agents temporaires	0	0	0	0	0	0	0	0	0	0
Experts nationaux détachés										
TOTAL	**0,0**	**0,0**	**0,0**	**0,350**	**1,400**	**0,233**	**0,0**	**0,0**	**0,0**	**1,983**

Le travail qui devrait être effectué par ces effectifs supplémentaires à l'Agence européenne de garde-frontières et de garde-côtes est limité dans le temps (2023), plus précisément à partir de 24 mois après la date de disponibilité du moteur biométrique pour l'EES. Cependant, le personnel doit être recruté à l'avance (une moyenne de trois mois est calculée) ce qui explique la valeur en 2022. Le travail effectué est suivi de tâches de dernière vérification/finalisation pendant deux mois, ce qui explique le niveau des effectifs en 2024.

Le niveau des effectifs lui-même est calculé sur 20 personnes requises pour les travaux à effectuer (plus 10 personnes fournies par un prestataire, ce dont rend compte le titre 3). Les tâches sont également supposées se dérouler pendant des heures de travail prolongées et ne pas se limiter aux heures normales de travail. Le personnel d'appui et les gestionnaires sont censés être fournis en fonction des ressources de l'Agence.

Le nombre de collaborateurs est fondé sur l'hypothèse qu'environ 550 000 empreintes digitales devront être évaluées en 5 à 10 minutes en moyenne par cas (17 000 empreintes par an vérifiées)[96].

Nombre d'agents	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total
Personnel pour le traitement manuel des liens et des décisions	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Titre 1 - AC	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3
Total Titre 1 - AT	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Total Titre 1	0,0	0,0	0,0	5,0	20,0	3,3	0,0	0,0	0,0	28,3

3.2.3.2. Synthèse pour Europol

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Fonctionnaires (grades AD)										
Fonctionnaires (grades AST)	0									
Agents contractuels	0,000	0,070	0,070	0,560	0,560	0,560	0,560	0,560	0,560	3,500
Agents temporaires	0,690	1,932	1,932	0,621	0,621	0,414	0,414	0,414	0,414	7,452
Experts nationaux détachés										
TOTAL	**0,690**	**2,002**	**2,002**	**1,181**	**1,181**	**0,974**	**0,974**	**0,974**	**0,974**	**10,952**

Ces coûts sont estimés sur la base des effectifs suivants:

Nombre d'ETP	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**total**

[96] Les effectifs pour 2020 et les années ultérieures sont indicatifs et devront être évalués, qu'ils s'ajoutent ou non aux prévisions des effectifs de l'Agence européenne de garde-frontières et de garde-côtes figurant dans le document COM(2015) 671.

pour les TIC										
Agents contractuels	0,0	1,0	1,0	8,0	8,0	8,0	8,0	8,0	8,0	50,0
Agents temporaires	5,0	14,0	14,0	4,5	4,5	3,0	3,0	3,0	3,0	54,0
Total des effectifs (ETP)	**5,0**	**15,0**	**15,0**	**12,5**	**12,5**	**11,0**	**11,0**	**11,0**	**11,0**	**104,0**

Il est envisagé d'affecter du personnel informatique supplémentaire à Europol pour renforcer les systèmes d'information d'Europol afin de pouvoir répondre au nombre croissant de recherches effectuées à partir de l'ESP et de l'ETIAS et, ultérieurement, de maintenir les systèmes opérationnels 24 heures sur 24 et 7 jours sur 7.

– Pour la phase de mise en œuvre de l'ESP (en 2020 et 2021), il y a un besoin supplémentaire d'experts techniques (architectes, ingénieurs, développeurs, testeurs). Un nombre réduit d'experts techniques sera nécessaire à partir de 2022 pour mettre en œuvre le reste des éléments d'interopérabilité et assurer la maintenance des systèmes.

– À partir du second semestre de 2021, il conviendra de mettre en place une surveillance des systèmes d'information et de communication, 24 heures sur 24 et 7 jours sur 7, pour garantir les niveaux de service de l'ESP et de l'ETIAS. Cette tâche sera assurée par 4 équipes de 2 agents contractuels se relayant 24 heures sur 24 et 7 jours sur 7.

– Dans la mesure du possible, les profils ont été répartis entre agents temporaires et agents contractuels. Il convient toutefois de noter qu'en raison des exigences élevées en matière de sécurité, il est possible que, pour plusieurs postes, on n'ait recours qu'à des agents temporaires. La demande d'agents temporaires tiendra compte des résultats de la conciliation sur la procédure budgétaire 2018.

3.2.3.3. Synthèse pour le CEPOL

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Fonctionnaires (grades AD)										
Fonctionnaires (grades AST)										

Agents contractuels			0,070	0,070						**0,140**
Agents temporaires		0,104	0,138	0,138	0,138	0,138	0,138	0,138	0,138	1,070
Experts nationaux détachés										

TOTAL		**0,104**	**0,208**	**0,208**	**0,138**	**0,138**	**0,138**	**0,138**	**0,138**	**1,210**

Des effectifs supplémentaires sont nécessaires, car la formation des formateurs des États membres doit être élaborée spécifiquement en vue de l'utilisation des éléments d'interopérabilité dans des conditions opérationnelles.

- L'élaboration du programme d'études et des modules de formation devrait commencer au moins 8 mois avant que le système ne soit opérationnel. Au cours des deux premières années qui suivront sa mise en service, la formation sera la plus intense. Toutefois, elle devra être maintenue pendant une période plus longue pour garantir une mise en œuvre cohérente, sur la base de l'expérience acquise avec le système d'information Schengen.

- Le personnel supplémentaire est nécessaire pour préparer, coordonner et mettre en œuvre le programme d'études, les cours résidentiels et les cours en ligne. Ces cours ne peuvent être mis en œuvre qu'en complément du catalogue de formation existant du CEPOL, d'où la nécessité de personnel supplémentaire.

- Il est prévu que le responsable des cours soit un agent temporaire tout au long de la période de développement et de maintenance, lequel sera assisté par un agent contractuel pendant la période de formation la plus intense.

3.2.3.4. Synthèse pour l'eu-LISA

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
Fonctionnaires (grades AD)										
Fonctionnaires (grades AST)										
Agents contractuels	0,875	1,400	1,855	2,555	2,415	2,170	2,100	2,100	2,100	17,570

Agents temporaires	2,001	3,450	4,347	4,347	4,209	3,312	3,036	3,036	3,036	30,774
Experts nationaux détachés										

TOTAL	**2,876**	**4,850**	**6,202**	**6,902**	**6,624**	**5,482**	**5,136**	**5,136**	**5,136**	**48,344**

– Les besoins en personnel tiennent compte du fait que les quatre éléments d'interopérabilité et le CRRS constituent un portefeuille de projets présentant des dépendances (c'est-à-dire un programme). Pour gérer les dépendances entre les projets, une équipe de gestion du programme est créée, composée des responsables du programme et des projets et comprenant des profils (souvent appelés architectes) qui doivent définir les éléments communs entre eux. La réalisation du programme/des projets nécessite également des profils d'appui au programme et aux projets.

– Les besoins en personnel par projet ont été estimés par analogie avec les projets précédents (système d'information sur les visas) et en distinguant la phase d'achèvement du projet et la phase opérationnelle.

– Les profils qui doivent rester actifs pendant la phase d'exploitation sont recrutés comme agents temporaires. Les profils requis durant l'exécution du programme/des projets sont recrutés en tant qu'agents contractuels. Afin d'assurer la continuité attendue des tâches et de conserver les connaissances au sein de l'Agence, le nombre de postes est réparti presque à parts égales entre les agents temporaires et les agents contractuels.

– On part du principe qu'il n'y aurait pas besoin de personnel supplémentaire pour entreprendre le projet ECRIS-TCN à haute disponibilité et que les effectifs du projet eu-LISA proviendraient de personnels de projets qui seraient réemployés après l'achèvement de ces projets à cette période.

Ces estimations sont fondées sur les niveaux d'effectifs suivants:

Pour les agents contractuels:

3.2.1. Réalisations EU-LISA (égal à T1) en nombre de personnes	2019	2020	2021	2022	2023	2024	2025	2026	2027	Total (formule)
Agents contractuels										-
Gestion de programme/projets	4,0	5,0	5,5	5,5	4,5	3,0	3,0	3,0	3,0	36,5
GP CRRS	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*1,5*
MID	*0,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*2,0*
Bureau de programme/projets	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*14,0*
Assurance qualité	*1,0*	*2,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*19,0*
Finances et marchés publics	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Gestion financière										*0,0*
Planification et contrôle budgétaires										*0,0*
Gestion marchés publics/contrats	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Experts techniques	7,0	7,0	7,0	7,0	6,0	5,0	5,0	5,0	5,0	54,0
CRRS	*3,0*	*3,0*	*3,0*	*3,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*22,0*
ESP	*4,0*	*4,0*	*4,0*	*4,0*	*4,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
BMS partagé	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Essais	1,5	3,0	4,0	4,0	4,0	3,0	2,0	2,0	2,0	25,5
CRRS	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*0,5*	*6,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partagé	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,5*	*1,0*	*2,0*	*2,5*	*2,5*	*1,5*	*1,0*	*1,0*	*1,0*	*13,0*
MID	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*6,5*
Suivi du système	0,0	5,0	10,0	20,0	20,0	20,0	20,0	20,0	20,0	135,0
Commun (24:7)	0,0	*5,0*	*10,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*20,0*	*135,0*
Coordination générale	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Ressources humaines	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RH	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Sous-total du personnel contractuel	**12,5**	**20,0**	**26,5**	**36,5**	**34,5**	**31,0**	**30,0**	**30,0**	**30,0**	**251,0**

Pour les agents temporaires:

Agents temporaires										
Gestion de programme/projets	3,0	4,0	5,5	5,5	5,5	4,5	4,0	4,0	4,0	40,0
Gestion de programme	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestion de projets	*0,0*	*0,0*	*1,0*	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*12,0*
Bureau de programme/projets	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
ESP	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
BMS partagé	*0,5*	*0,5*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*4,0*
CIR	*0,0*	*0,5*	*1,0*	*1,0*	*0,5*	*0,0*	*0,0*	*0,0*	*0,0*	*3,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Finances et marchés publics	3,0	3,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	34,0
Gestion financière	*0,0*	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*7,0*
Planification et contrôle budgétaires	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*9,0*
Gestion marchés publics/contrats	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*18,0*
Experts techniques	6,0	14,0	17,0	17,0	15,0	11,0	10,0	10,0	10,0	110,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partagé	*2,0*	*3,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
CIR	*2,0*	*5,0*	*5,0*	*5,0*	*3,0*	*3,0*	*3,0*	*3,0*	*3,0*	*32,0*
Sécurité	*1,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*2,0*	*17,0*
MID	*0,0*	*2,0*	*2,0*	*2,0*	*2,0*	*1,0*	*1,0*	*1,0*	*1,0*	*12,0*
Architectes	*1,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,0*	*1,0*	*1,0*	*17,0*
Essais	2,5	3,0	4,0	4,0	4,0	2,5	2,0	2,0	2,0	26,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,5*	*1,0*	*1,0*	*1,0*	*1,0*	*0,5*	*0,5*	*0,5*	*0,5*	*6,5*
BMS partagé	*2,0*	*2,0*	*3,0*	*3,0*	*3,0*	*2,0*	*1,5*	*1,5*	*1,5*	*19,5*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Suivi du système	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
CRRS	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
ESP	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
BMS partagé	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
CIR	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
MID	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*	*0,0*
Formation	0,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	8,0
Formation	*0,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*1,0*	*8,0*
Ressources humaines	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
RH	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	*0,0*
Autre	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	5,0
Spécialiste de la protection des données	0,0	0,0	0,0	0,0	1,0	1,0	1,0	1,0	1,0	*5,0*
Sous-total Agents temporaires	**14,5**	**25,0**	**31,5**	**31,5**	**30,5**	**24,0**	**22,0**	**22,0**	**22,0**	**223,0**
Total	**27,0**	**45,0**	**58,0**	**68,0**	**65,0**	**55,0**	**52,0**	**52,0**	**52,0**	**474,0**

3.2.4. Incidence estimée sur les crédits de nature administrative

3.2.4.1. DG Home: synthèse

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☒ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
RUBRIQUE 5 du cadre financier pluriannuel										
Ressources humaines DG HOME	0,690	0,690	0,690	0,690	0,690	0,690	0,276	0,276	0,276	4,968
Autres dépenses administratives	0,323	0,323	0,323	0,323	0,323	0,323	0,263	0,263	0,263	2,727
Sous-total RUBRIQUE 5 du cadre financier pluriannuel	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695

Hors RUBRIQUE 5[97] du cadre financier pluriannuel	(non utilisé)									
Ressources humaines										
Autres dépenses de nature administrative										
Sous-total hors RUBRIQUE 5 du cadre financier pluriannuel										

TOTAL	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**1,013**	**0,539**	**0,539**	**0,539**	**7,695**

.

[97] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.4.2. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☒ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

	Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
•Emplois du tableau des effectifs (fonctionnaires et agents temporaires)										
18 01 01 01 (au siège et dans les représentations de la Commission) - DG HOME	5,0	5,0	5,0	5,0	5,0	5,0	2,0	2,0	2,0	36,0
XX 01 01 02 (en délégation)										
XX 01 05 01 (recherche indirecte)										
10 01 05 01 (recherche directe)										
•Personnel externe (en équivalents temps plein: ETP)[98]										
XX 01 02 02 (AC, AL, END, INT et JED dans les délégations)										
XX 01 04 **yy** 99 - au siège										
XX 01 04 **yy** 99 - en délégation										
XX 01 05 02 (AC, END, INT sur recherche indirecte)										
10 01 05 02 (AC, END, INT sur recherche directe)										
Autres lignes budgétaires (à préciser)										
TOTAL	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**5,0**	**2,0**	**2,0**	**2,0**	**36,0**

18 est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Surveillance et suivi du projet. Trois fonctionnaires pour le suivi. Le personnel assume les obligations de la Commission pour l'exécution du programme: vérifier le respect des instruments législatifs, résoudre les problèmes de conformité, élaborer des rapports pour le Parlement européen et le Conseil, évaluer les progrès réalisés par les États membres. Étant donné que le programme est une activité venant s'ajouter aux charges de travail existantes, des effectifs supplémentaires sont nécessaires. Cette augmentation des effectifs est limitée en termes de durée et ne couvre que la période de développement.

Gestion de l'UMF

La Commission gérera la norme UMF au quotidien. Deux fonctionnaires sont nécessaires à cette fin: une personne en tant qu'expert du domaine répressif et une autre personne ayant une bonne connaissance de la modélisation des processus ainsi que des TIC.

Le format universel pour les messages (UMF) établit une norme pour l'échange d'informations transfrontière structuré entre les systèmes d'information, les autorités et/ou les organismes dans le domaine de la justice et des

98 AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JED = jeune expert en délégation.

99 Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

affaires intérieures. L'UMF définit un vocabulaire commun et des structures logiques pour les informations échangées communément, dans le but de faciliter l'interopérabilité en permettant la création et la lecture des contenus de l'échange d'une manière cohérente et sémantiquement équivalente.

Afin d'assurer des conditions uniformes pour la mise en œuvre du format universel pour les messages, il est proposé de conférer des compétences d'exécution à la Commission. Il est proposé que ces compétences soient exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission.

3.2.5. Compatibilité avec le cadre financier pluriannuel actuel

– ☐ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

– ☒ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants. Le règlement relatif au Fonds pour la sécurité intérieure (FSI) - Frontières est l'instrument financier dans lequel le budget consacré à la mise en œuvre de l'initiative «interopérabilité» a été inclus. Son article 5, point b), prévoit que 791 millions d'EUR seront alloués au moyen d'un programme pour le développement de nouveaux systèmes informatiques, sur la base des systèmes informatiques actuels et/ou de nouveaux systèmes, permettant la gestion des flux migratoires aux frontières extérieures de l'Union, sous réserve de l'adoption des actes législatifs pertinents de l'Union et dans les conditions prévues à l'article 15. Sur ces 791 millions d'EUR, 480,2 millions sont réservés au développement de l'EES, 210 millions à l'ETIAS et 67,9 millions à la révision du SIS II. Le reste (32,9 millions d'EUR) seront réaffectés à l'aide des mécanismes de FSI-Frontières. **La présente proposition nécessite 32,1 millions d'EUR pour la période du cadre financier pluriannuel actuel, un montant qui cadre avec le budget restant.**

La conclusion dans l'encadré ci-dessus quant au montant requis de 32,1 millions d'EUR est le résultat de la feuille de calcul suivante:

ENGAGEMENTS										
3.2. Incidence estimée sur les dépenses DG HOME										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (horiz.)**
18 02 01 03 - Frontières intelligentes (couvre le soutien aux États membres)	0	0	43,150	48,150	45,000	0	0	0	0	136,300
Total (1)	**0**	**0**	**43,150**	**48,150**	**45,000**	**0**	**0**	**0**	**0**	**136,300**
18.0207 -3.2. eu-LISA										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formule)**
T1: Dépenses de personnel	2,876	4,850	6,202	6,902	6,624	5,482	5,136	5,136	5,136	48,344
T2: Dépenses d'infrastructure et de fonctionnement	0,136	0,227	0,292	0,343	0,328	0,277	0,262	0,262	0,262	2,389
T3: Dépenses opérationnelles	2,818	11,954	45,249	37,504	22,701	14,611	13,211	13,131	13,131	174,309
Total (2)	**5,830**	**17,031**	**51,743**	**44,749**	**29,653**	**20,370**	**18,609**	**18,529**	**18,529**	**225,041**
		22,861							**202,181**	**225,041**
18.02.04 -3.2. Europol										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formule)**
T1: Dépenses de personnel	0,690	2,002	2,002	1,181	1,181	0,974	0,974	0,974	0,974	10,952
T2: Dépenses d'infrastructure et de fonctionnement	0	0	0	0	0	0	0	0	0	0
T3: Dépenses opérationnelles	0	6,380	6,380	2,408	2,408	2,408	7,758	7,758	2,408	37,908
Total (3)	**0,690**	**8,382**	**8,382**	**3,589**	**3,589**	**3,382**	**8,732**	**8,732**	**3,382**	**48,860**
		9,072							39,788	48,860
18.02.05 -3.2. CEPOL										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formule)**
T1: Dépenses de personnel	0	0,104	0,208	0,208	0,138	0,138	0,138	0,138	0,138	1,210
T2: Dépenses d'infrastructure et de fonctionnement	0	0	0	0	0	0	0	0	0	0
T3: Dépenses opérationnelles	0	0,040	0,176	0,274	0,070	0,070	0,070	0,070	0,070	0,840
Total (4)	**0**	**0,144**	**0,384**	**0,482**	**0,208**	**0,208**	**0,208**	**0,208**	**0,208**	**2,050**
		0,144							**1,906**	**2,050**
18.02.0 -3.2. Frontex										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total (formule)**
T1: Dépenses de personnel	0	0	0	0,350	1,400	0,233	0	0	0	1,983
T2: Dépenses d'infrastructure et de fonctionnement	0	0	0	0,075	0,300	0,050	0	0	0	0,425
T3: Dépenses opérationnelles	0	0	0	0,183	2,200	0	0	0	0	2,383
Total (5)	**0**	**0**	**0**	**0,608**	**3,900**	**0,283**	**0**	**0**	**0**	**4,792**
		0							**4,792**	**4,792**
TOTAL (1)+(2)+(3) +(4) +(5)	6,520	25,556	103,659	97,578	82,350	24,243	27,549	27,469	22,119	417,043
		32,076							384,966	
3.2. DG HOME Rubrique 5 «Dépenses administratives»										
	2019	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Total (6)	1,013	1,013	1,013	1,013	1,013	1,013	0,539	0,539	0,539	7,695
TOTAL (1)+(2)+(3)+(4)+(5)+(6)	7,533	26,569	104,672	98,591	83,363	25,256	28,088	28,008	22,658	424,738

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel.

3.2.6. Participation de tiers au financement

– La proposition/l'initiative **ne prévoit pas** de cofinancement par des tierces parties.

3.3. Incidence estimée sur les recettes

– ☐ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☒ La proposition/l'initiative a une incidence financière décrite ci-après:

– – ☐ sur les ressources propres

– – ☒ sur les recettes diverses

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[100]								
		Année **2019**	Année **2020**	Année **2021**	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**
Article 6313 - Contribution pays associés Schengen (CH, NO, LI, IS)		pm	pm	pm	pm	pm	pm	pm	pm	pm

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

18 0207

Préciser la méthode de calcul de l'incidence sur les recettes.

Le budget comprendra une contribution financière des pays associés à la mise en œuvre, à l'application et au développement de l'acquis de Schengen et aux mesures relatives à Eurodac, comme prévu dans les accords respectifs.

[100] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 25 % de frais de perception.