EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

2 mars 2022

Avis 4/2022

sur la proposition de règlement relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»)

edps.europa.eu

Le Contrôleur européen de la protection des données (le «CEPD») est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[...] [e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur droit à la protection des données, soient respectés par les institutions et organes de l'Union», et en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Rafał Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

En vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'UE sur l'application cohérente et logique des principes de protection des données de l'UE. Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations supplémentaires, en particulier si d'autres problèmes sont détectés ou si de nouvelles informations apparaissent. En outre, le présent avis est sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont conférés par le règlement (UE) 2018/1725.

Résumé

Le 8 décembre 2021, la Commission européenne a adopté une proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil (les «décisions Prüm»). La proposition fait partie d'un paquet législatif plus vaste, dénommé «code de coopération policière de l'UE», qui comprend également une proposition de directive du Parlement européen et du Conseil relative à l'échange d'informations entre les services répressifs des États membres (sous réserve d'un avis distinct du CEPD) et une proposition de recommandation du Conseil relative à la coopération policière opérationnelle.

L'objectif de la proposition est de renforcer la coopération en matière répressive et, en particulier, l'échange d'informations entre les autorités compétentes chargées de la prévention et de la détection des infractions pénales, ainsi que des enquêtes en la matière, en définissant les conditions et les procédures applicables à la consultation automatisée de profils ADN, de données dactyloscopiques (empreintes digitales), d'images faciales, de registres de la police et de certaines données relatives à l'immatriculation des véhicules, ainsi qu'à l'échange de données à la suite d'une correspondance.

Bien que le CEPD comprenne la nécessité pour les services répressifs de bénéficier des meilleurs outils juridiques et techniques possibles pour la détection et la prévention des infractions pénales ainsi que des enquêtes en la matière, il note que le nouveau cadre Prüm proposé ne définit pas clairement les éléments essentiels de l'échange de données, tels que les types d'infractions, qui peuvent justifier une requête, et n'est pas suffisamment clair quant à l'étendue des personnes concernées affectées par l'échange automatisé de données, par exemple si les bases de données, qui font l'objet d'une requête, ne contiennent que des données de suspects et/ou de personnes reconnues coupables, ou également des données d'autres personnes concernées, telles que les victimes ou les témoins.

Le CEPD estime, en particulier, que la consultation automatisée de profils ADN et d'images faciales ne devrait être possible que dans le cadre d'enquêtes individuelles sur des infractions pénales graves, plutôt que sur toute infraction pénale, comme le prévoit la proposition. En outre, le CEPD juge nécessaire d'introduire dans la proposition des exigences et conditions communes applicables aux données figurant dans les bases de données nationales qui sont rendues accessibles aux fins de recherches automatisées, en tenant dûment compte de l'obligation, prévue à l'article 6 de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif, d'établir une distinction entre les différentes catégories de personnes concernées (c'est-à-dire les criminels reconnus coupables, les suspects, les victimes, etc.).

Le CEPD est également préoccupé par les conséquences de la consultation et de l'échange automatisés proposés de registres de la police sur les droits fondamentaux des personnes concernées. Il estime que la nécessité de la consultation et de l'échange automatisés de données des registres de la police n'est pas suffisamment démontrée. Si une telle mesure est néanmoins adoptée, même sur une base volontaire, des garanties solides supplémentaires seraient alors nécessaires pour respecter le principe de proportionnalité. En particulier, compte tenu des

problèmes de qualité des données, le futur règlement devrait, entre autres, définir explicitement les types et/ou la gravité des infractions susceptibles de justifier une requête automatisée dans les casiers judiciaires nationaux.

En ce qui concerne l'inclusion d'Europol dans le cadre Prüm, le CEPD estime que les observations et recommandations qu'il a formulées dans son avis 4/2021 sur la proposition de modification du règlement Europol restent parfaitement valables dans le cadre de la coopération Prüm, en particulier celles relatives au «défi des mégadonnées», à savoir le traitement par l'Agence d'ensembles de données vastes et complexes. Le CEPD souhaite rappeler deux des messages clés figurant dans l'avis sur Europol: des pouvoirs renforcés devraient toujours aller de pair avec un contrôle renforcé et, tout aussi important, les exceptions applicables sous la forme de dérogations ne devraient pas être autorisées à devenir la règle.

La proposition prévoit une architecture complexe de consultation et d'échange automatisés de données au titre du cadre Prüm, comportant trois solutions techniques distinctes, élaborées et gérées par trois entités différentes. Le CEPD estime que la proposition devrait être plus explicite quant à la responsabilité du traitement des données à caractère personnel, en particulier dans EUCARIS, qui n'est pas fondé sur le droit de l'UE et a un caractère intergouvernemental. De plus, le CEPD estime que, compte tenu de l'ampleur et de la sensibilité du traitement des données à caractère personnel, le modèle de gouvernance horizontal proposé du cadre Prüm n'est pas approprié et devrait être encore renforcé, par exemple en attribuant un rôle central de coordination à une entité de l'UE, comme la Commission.

En outre, dans un souci de sécurité juridique, le CEPD considère que le lien entre les règles de protection des données contenues dans la proposition et le cadre juridique existant en matière de protection des données dans l'UE, en particulier la directive en matière de protection des données dans le domaine répressif et le règlement (UE) 2018/1725 («RPDUE»), devrait être explicitement clarifié.

Par ailleurs, le présent avis analyse et formule des recommandations sur un certain nombre d'autres questions spécifiques, telles que le lien entre le cadre Prüm et le cadre d'interopérabilité, le transfert de données vers des pays tiers et à des organisations internationales ou le contrôle des opérations de traitement aux fins de la coopération Prüm.

Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif 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 et à la libre circulation de ces données[1], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1. Introduction

1. Le 8 décembre 2021, la Commission européenne a adopté une proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil (la «proposition»)[2].

2. La proposition fait partie d'un paquet législatif plus vaste, dénommé «code de coopération policière de l'UE», qui comprend également:

   - une proposition de directive du Parlement européen et du Conseil relative à l'échange d'informations entre les services répressifs des États membres, abrogeant la décision-cadre 2006/960/JAI du Conseil[3], et

   - une proposition de recommandation du Conseil relative à la coopération policière opérationnelle[4].

3. L'objectif du code de coopération policière de l'UE, comme l'indique la Commission, est de renforcer la coopération en matière répressive entre les États membres et, en particulier, l'échange d'informations entre les autorités compétentes[5]. À cet égard, la proposition établit les conditions et procédures applicables à la consultation automatisée de profils ADN, de données dactyloscopiques (empreintes digitales), d'images faciales, de registres de la police et de certaines données relatives à l'immatriculation des véhicules, ainsi qu'à l'échange de données à la suite d'une correspondance entre les autorités chargées de la prévention et de la détection des infractions pénales, ainsi que des enquêtes en la matière.

4. La proposition ainsi que, plus généralement, le code de coopération policière de l'UE sont liés aux objectifs politiques poursuivis par plusieurs documents stratégiques de l'UE dans le domaine de la justice et des affaires intérieures, en particulier la stratégie de l'UE pour l'union de la sécurité[6], la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025)[7] et la stratégie de 2021 relative à l'espace Schengen[8]. En outre, les propositions établissant le code de coopération policière devraient être examinées à la lumière de la réforme en cours d'Europol et du rôle de plus en plus important de l'Agence en tant que centre de renseignements de l'Union sur la criminalité, qui collecte et traite un volume croissant de données[9].

5. Le 5 janvier 2022, la Commission a consulté le CEPD sur la proposition de règlement Prüm II, en application de l'article 42, paragraphe 1, du règlement (UE) 2018/1725. Les observations et recommandations contenues dans le présent avis se limitent aux dispositions les plus pertinentes de la proposition du point de vue de la protection des données.

2. Observations générales

6. Le terrorisme et les formes graves de criminalité constituent une menace grave au sein de l'Union européenne et dans le monde, et leur détection, leur prévention et leurs poursuites représentent sans aucun doute un objectif important d'intérêt général, de nature à justifier des limitations à l'exercice des libertés et droits fondamentaux de l'individu, conformément à l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne.

7. Le CEPD comprend que les autorités répressives aient besoin de disposer des meilleurs outils techniques et juridiques possibles pour s'acquitter de leurs tâches, à savoir détecter et prévenir les infractions et autres menaces à la sécurité publique et les poursuivre. À cet égard, l'article 87 TFUE reconnaît que la coopération policière, y compris l'échange d'informations pertinentes entre les services répressifs, est un instrument important pour la création d'un espace de liberté, de sécurité et de justice.

8. Le présent avis vise à présenter une appréciation juste et objective de la nécessité et de la proportionnalité des mesures proposées, ainsi qu'à formuler un certain nombre de recommandations spécifiques en vue d'assurer un juste équilibre entre les valeurs et les intérêts en jeu.

9. Le CEPD a déjà formulé des observations sur la question de l'échange automatisé de données dans son avis de 2007 sur l'initiative législative de 15 États membres en vue de l'adoption d'une décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière[10]. À l'époque déjà, le CEPD insistait sur le caractère assez inhabituel de la procédure législative suivie pour l'adoption du cadre juridique du cadre Prüm, qui avait soulevé des questions en termes de transparence et de légitimité démocratique. L'échange transfrontière d'informations, en particulier l'ADN et les empreintes digitales, a été mentionné pour la première fois dans un traité intergouvernemental, à savoir le traité de Prüm de 2005. Son intégration ultérieure dans le cadre juridique de l'UE en 2008, sous la forme des décisions 2008/615/JAI et 2008/616/JAI du Conseil, a en fait contourné les procédures législatives standard et s'est plutôt fondée sur les initiatives de certains États membres. On pourrait donc conclure qu'avec la proposition de règlement Prüm II, cette forme spécifique de coopération policière fera pour la première fois l'objet d'un examen législatif approprié.

10. Le CEPD constate avec regret que 15 ans après le premier avis, ses principales préoccupations quant à la nécessité et à la proportionnalité de l'initiative restent valables et sont encore aggravées par la proposition d'extension significative du champ d'application de l'échange automatisé de données. Ni l'augmentation des menaces pour la sécurité, ni le développement du droit européen et international, ni aucune nouvelle technologie mise en œuvre depuis 2007, n'ont modifié les principales préoccupations exprimées par le CEPD. En particulier, le cadre juridique proposé ne définit pas clairement les éléments essentiels de l'échange de données, tels que les types d'infractions pénales qui peuvent justifier une requête (recherche), en particulier de profils ADN, c'est-à-dire n'importe quelle infraction pénale ou uniquement les

infractions plus graves. En outre, la proposition n'indique pas clairement l'étendue des personnes concernées par l'échange automatisé de données, c'est-à-dire si les bases de données faisant l'objet d'une requête (recherche) ne contiennent que les données (biométriques) de suspects et/ou de personnes reconnues coupables, ou également les données d'autres personnes concernées, telles que des victimes ou des témoins.

11. Ces deux éléments jouent un rôle très important dans l'appréciation de la proportionnalité du cadre Prüm; ils font donc l'objet d'une analyse détaillée dans la suite du présent avis, tout comme d'autres aspects de la proposition jugés pertinents du point de vue de la protection des données.

3. Observations particulières

3.1. Lien avec le cadre juridique existant en matière de protection des données

12. Selon l'exposé des motifs, la base juridique de la proposition est constituée par les dispositions suivantes du traité sur le fonctionnement de l'Union européenne («TFUE»): article 16, paragraphe 2, article 87, paragraphe 2, point a), et article 88, paragraphe 2. L'article 87, paragraphe 2, point a), fait référence aux mesures relatives à la collecte, au stockage, au traitement, à l'analyse et à l'échange d'informations pertinentes afin d'assurer une coopération policière entre les autorités compétentes des États membres dans les domaines de la prévention ou de la détection des infractions pénales et des enquêtes en la matière. L'article 88, paragraphe 2, fait référence à la structure, au fonctionnement, au domaine d'action et aux tâches d'Europol.

13. En vertu de l'article 16, paragraphe 2, l'Union est habilitée à adopter des mesures relatives 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.

14. Conformément à la jurisprudence de la Cour de justice de l'Union européenne («CJUE»), l'article 16 TFUE fournit une base juridique appropriée lorsque la protection des données à caractère personnel est l'une des finalités ou des composantes essentielles des règles adoptées par le législateur de l'Union[11]. Dans le même temps, il existe déjà un cadre exhaustif de protection des données adopté sur la base de l'article 16 TFUE, constitué du règlement (UE) 2016/679 («RGPD»), du règlement (UE) 2018/1725 («RPDUE») et de la directive en matière de protection des données dans le domaine répressif[12]. Par conséquent, dans l'intérêt de la sécurité juridique, le lien entre la proposition et le cadre juridique existant en matière de protection des données dans l'UE devrait être explicitement clarifié.

15. Le CEPD note que l'exposé des motifs de la proposition indique qu'«[e] n ce qui concerne le mécanisme de Prüm, la législation applicable en matière de protection des données est la directive (UE) 2016/680»[13]. En outre, conformément à la communication de la Commission du 24 juin 2020 sur la marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données, l'un des objectifs de la révision des décisions Prüm est d'assurer «la mise en conformité parfaite du nouveau mécanisme de Prüm avec la directive, en particulier en ce qui concerne les garanties en matière de protection des données»[14].

16. Le CEPD observe que le chapitre 6 de la proposition est spécifiquement consacré à la protection des données, avec des dispositions juridiques relatives à la limitation de la finalité, à l'exactitude, à la conservation des données, à la sécurité, au contrôle, aux sanctions et autres. La plupart de ces dispositions correspondent aux règles juridiques similaires énoncées dans la directive en matière de protection des données dans le domaine répressif et, respectivement, au chapitre IX du RPDUE. Toutefois, la relation entre les règles de protection des données figurant dans la proposition de règlement Prüm II, d'une part, et les règles horizontales de la directive en matière de protection des données dans le domaine répressif (ou du RPDUE en ce qui concerne Europol et eu-LISA), d'autre part, n'est précisée ni dans les considérants ni dans le dispositif du règlement. Le CEPD souligne que le manque de clarté juridique n'est pas une question abstraite de technique juridique, mais une question de fond, qui peut avoir une incidence directe sur la mise en œuvre pratique et l'application des règles en matière de protection des données.

17. Par conséquent, dans un souci de clarté et de sécurité, **le CEPD recommande de préciser dans la proposition que les dispositions du chapitre 6 sont sans préjudice de l'application de la directive en matière de protection des données dans le domaine répressif et du RPDUE en ce qui concerne le traitement des données à caractère personnel dans le cadre de la coopération en matière répressive au titre du cadre Prüm**.

3.2. Champ d'application de la proposition

18. Conformément à l'article premier, la proposition établirait un cadre pour l'échange d'informations entre les autorités chargées de la prévention et de la détection des infractions pénales ainsi que des enquêtes en la matière. Conformément à l'article 3 de la proposition, le règlement s'appliquerait aux bases de données nationales utilisées pour le transfert automatisé des catégories de profils ADN, de données dactyloscopiques, d'images faciales, de registres de la police et de certaines données relatives à l'immatriculation des véhicules.

19. Afin d'apprécier la nécessité et la proportionnalité de l'ingérence dans le droit fondamental à la protection des données à caractère personnel, à la lumière de l'article 52, paragraphe 1, de la Charte, il est essentiel d'identifier le champ d'application personnel et matériel des mesures, c'est-à-dire les catégories de personnes concernées qui seront directement affectées, ainsi que les conditions objectives susceptibles de justifier une consultation automatisée dans les bases de données d'autres États membres ou d'Europol.

20. Les articles 25, 33 et 39 de la proposition font référence à des catégories de personnes concernées dont les données à caractère personnel peuvent faire l'objet d'opérations de traitement spécifiques au titre du cadre Prüm, à savoir les «suspects», les «criminels» ou les «auteurs». Le CEPD relève que le règlement ne donne pas de définitions des catégories «suspects», «criminels» et «auteurs». En outre, ces termes s'écartent des catégories de personnes concernées définies dans le règlement Europol («personnes qui sont soupçonnées d'avoir commis une infraction pénale ou d'avoir participé à une infraction pénale [...], ou qui ont été condamnées pour une telle infraction» et «personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire qu'elles commettront des infractions pénales»[15]), ou dans la directive en matière de protection des données dans le domaine répressif («personnes reconnues coupables d'une infraction pénale»[16]).

21. Le CEPD souligne qu'il importe de définir clairement les catégories de personnes concernées, en particulier lorsque l'on entend limiter le traitement à certaines catégories de personnes

concernées en raison de la nature particulièrement intrusive de la mesure, par exemple le partage de profils ADN ou de dossiers de police. Par conséquent, **le CEPD estime que les catégories de personnes concernées devraient être alignées sur la directive en matière de protection des données dans le domaine répressif et sur le règlement Europol afin d'éviter les incohérences au niveau de l'application**. **Dans ce contexte, les références aux «criminels» ou aux «auteurs» devraient donc être remplacées par l'expression «personnes reconnues coupables d'une infraction pénale».**

22. L'article 33 de la proposition imposerait aux autorités compétentes des États membres et à Europol de conserver une justification des requêtes effectuées au titre du cadre Prüm. La justification devrait inclure l'objet de la requête, une référence à l'affaire ou à l'enquête spécifique et une indication permettant de déterminer si la requête concerne un suspect ou un «auteur» d'une infraction pénale (ce dernier étant entendu comme une «personne reconnue coupable d'une infraction pénale»).

23. Toutefois, il n'y a pas d'obligation de fournir, dans le cadre de la justification, une référence à l'infraction pénale spécifique que la personne est soupçonnée d'avoir commise ou pour laquelle elle a été reconnue coupable. Comme expliqué plus loin dans l'avis, conformément à la jurisprudence de la CJUE, une ingérence grave dans les droits fondamentaux ne pourrait être justifiée que si elle était liée à une infraction pénale grave[17]. Par conséquent, afin de garantir la nécessité et la proportionnalité du traitement et de réduire les risques d'abus éventuels, **le CEPD recommande d'ajouter à la justification requise au titre de l'article 33, paragraphe 2, des informations relatives à l'infraction pénale spécifique**.

3.3. Consultation automatisée des profils ADN

24. L'une des principales nouveautés dans le domaine de la coopération policière, introduite par le cadre Prüm (à savoir le traité de Prüm et les décisions Prüm), a été la consultation automatisée des profils ADN. Le CEPD a déjà observé dans son avis de 2007 qu'en fait, le traité de Prüm avait été conçu comme un «laboratoire» pour l'échange transfrontière d'informations, notamment de fichiers d'analyses ADN, ce qui avait permis aux États membres d'expérimenter ces échanges[18].

25. Conformément à l'article 4 de la proposition, on entend par «profil ADN» un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci), et par «partie non codante de l'ADN» les régions chromosomiques non génétiquement exprimées, c'est-à-dire non connues pour fournir des propriétés fonctionnelles d'un organisme. Les profils ADN échangés au titre du cadre Prüm constituent des données biométriques. À cet égard, le CEPD rappelle avoir toujours considéré que la collecte et la conservation de données biométriques à caractère personnel, en raison de leur nature même et de leur caractère sensible, entraînent des risques accrus pour les personnes concernées et devraient toujours s'accompagner de garanties strictes[19].

26. Le CEPD est particulièrement préoccupé par le fait que la proposition ne précise pas clairement les conditions et exigences communes concernant la justification d'une consultation automatisée de profils ADN. L'article 6 de la proposition définit le champ d'application général des «enquêtes en matière d'infractions pénales» et fait référence au respect du droit national. Toutefois, les évaluations effectuées tant par le Conseil[20] que par le Parlement européen[21] ont révélé d'importantes divergences entre les États membres en ce qui concerne le champ d'application matériel et personnel de leurs bases de données ADN nationales. Par exemple, si

la majorité des États membres autorisent l'accès aux données ADN des criminels reconnus coupables et des suspects, certains pays élargissent le champ d'application aux données relatives aux victimes de la criminalité et aux proches des personnes disparues[22].

27. En outre, la jurisprudence de la Cour européenne des droits de l'homme («CEDH») révèle des différences considérables dans les pratiques nationales en ce qui concerne les durées de conservation des profils ADN[23]. En fait, la législation de deux États membres actuels de l'UE prévoit même la conservation à durée indéterminée des profils ADN à la suite d'une condamnation pour une infraction pénale mineure[24].

28. L'exposé des motifs de la proposition rappelle la jurisprudence de la CJUE, selon laquelle 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[25]. Il renvoie également aux critères énoncés à l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne concernant d'éventuelles limitations de l'exercice des droits et libertés fondamentaux, en particulier les exigences de nécessité et de proportionnalité[26].

29. Le CEPD convient que les enquêtes sur les infractions pénales représentent un objectif important d'intérêt général, de nature à justifier de telles limitations. Dans le même temps, il rappelle que le principe de proportionnalité exige qu'une ingérence grave dans les droits fondamentaux – en l'occurrence, l'accès à des catégories de données biométriques extrêmement sensibles telles que l'ADN — ne puisse être justifiée que lorsque l'infraction pénale est également considérée comme «grave»[27].

30. Par conséquent, le CEPD estime que le règlement envisagé devrait introduire des conditions et des exigences communes pour la consultation automatisée de profils ADN, qui correspondent au caractère sensible des données traitées et au niveau d'intrusion de cette forme de coopération policière. **Le CEPD estime, en particulier, que la consultation automatisée de profils ADN et d'images faciales ne devrait être possible que dans le cadre d'enquêtes individuelles sur des infractions pénales graves, plutôt que sur toute infraction pénale, comme le prévoit la proposition. En outre, en tenant dûment compte de l'obligation prévue à l'article 6 de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif d'établir une distinction entre les différentes catégories de personnes concernées (c'est-à-dire les criminels reconnus coupables, les suspects, les victimes, etc.),** la proposition devrait préciser les catégories de personnes concernées dont les profils ADN, stockés dans les bases de données ADN nationales, seraient rendus accessibles pour des consultations automatisées. Le CEPD est d'avis que l'accès aux données d'autres catégories que les criminels reconnus coupables ou les suspects requiert une justification détaillée, étant donné que les données de ces autres catégories sont généralement collectées à des fins limitées.

3.4. Consultation automatisée d'images faciales

31. La proposition vise à étendre le champ d'application des consultations automatisées en introduisant l'échange d'images faciales dans le cadre Prüm[28]. Les définitions figurant à l'article 4, paragraphes 10 et 11, précisent que l'expression «image faciale» désigne une image numérique du visage et donc des données biométriques. Par conséquent, les observations déjà formulées concernant le caractère sensible des données biométriques, les risques plus élevés

pour les personnes concernées et la nécessité de garanties strictes s'appliquent pleinement en cas de consultation automatisée d'images faciales dans le contexte du mécanisme de Prüm.

32. L'échange d'images faciales au titre du cadre Prüm de coopération policière soulève des difficultés supplémentaires, qui sont spécifiques à ce type de données biométriques. Le CEPD rappelle les préoccupations du comité européen de la protection des données («EDPB»), exprimées en 2020 dans une lettre adressée à des députés du Parlement européen[29], au sujet du «*grand risque que les États membres puissent collecter et traiter de manière disproportionnée une grande quantité de données de reconnaissance faciale, étant donné que la différence entre les données ADN et les données dactyloscopiques, d'une part, et les données relatives à la reconnaissance faciale, d'autre part, réside notamment dans le fait que ces dernières peuvent être collectées beaucoup plus facilement et sans que les personnes concernées en aient connaissance*». À cet égard, l'EDPB a réclamé une analyse d'impact approfondie afin de s'assurer que la nécessité et la proportionnalité de cette mesure et l'essence du droit fondamental à la protection des données soient respectées.

33. L'étude susmentionnée de la commission LIBE du Parlement européen[30] a abouti à des conclusions similaires sur les «*graves implications pour les droits fondamentaux des recherches par images faciales*», recommandant, *entre autres*, de préciser les sources des images faciales et les garanties en matière de protection des données assurant que «la qualité des images faciales est suffisamment élevée pour éviter le risque d'augmentation des fausses correspondances, qui peuvent conduire à des pratiques discriminatoires». En outre, l'étude a insisté sur le fait que «les finalités spécifiques de la recherche d'images faciales devraient également être limitées afin d'éviter des pratiques de surveillance à grande échelle au niveau national».

34. Le CEPD prend note des assurances données par la Commission dans le rapport d'analyse d'impact accompagnant la proposition[31], telles que «l'échange d'images faciales au titre du cadre Prüm ne prévoit pas l'utilisation d'un système d'identification biométrique à distance dans des espaces accessibles au public»[32] et qu'«il n'y aurait pas de profilage». Toutefois, aucune de ces garanties n'apparaît dans la proposition proprement dite, laquelle fait uniquement référence au «respect du droit national de l'État membre requérant».

35. Le CEPD note également que la consultation automatisée d'images faciales ne se limite pas uniquement aux infractions pénales graves, mais qu'elle pourrait également être effectuée aux fins de la prévention et de la détection d'infractions pénales, même mineures, et des enquêtes en la matière. Compte tenu des risques pour les droits et libertés fondamentaux des personnes concernées, déjà expliqués ci-dessus, le CEPD doute sérieusement que ce type d'échange de données biométriques sous sa forme actuelle puisse répondre aux exigences de nécessité et de proportionnalité.

36. Par conséquent, **le CEPD considère que la proposition devrait être développée davantage en ce qui concerne les garanties relatives aux droits fondamentaux des personnes concernées en cas d'échange d'images faciales, en établissant des exigences et des conditions communes pour la consultation automatisée d'images faciales stockées dans les bases de données nationales. En particulier, conformément à l'obligation énoncée à l'article 6 de la directive en matière de protection des données dans le domaine répressif d'établir une distinction entre les différentes catégories de personnes concernées, seules les images faciales des criminels reconnus coupables et des suspects devraient être accessibles pour consultation.** En outre, **la consultation automatisée d'images faciales doit être limitée aux seules enquêtes individuelles portant sur des infractions pénales graves, et non sur toute infraction pénale, comme le prévoit la proposition**.

3.5. Consultation et échange automatisés de registres de la police

37. La proposition entraînerait une autre modification substantielle du cadre Prüm, à savoir la possibilité de consulter et d'échanger des registres de la police de manière automatisée[33]. Bien que cet élément ne concerne pas les données biométriques, telles que l'ADN ou les images faciales, il suscite néanmoins de vives inquiétudes quant à son incidence sur les droits et libertés fondamentaux des personnes concernées.

38. Dans ce contexte, les questions qui revêtent une importance particulière pour l'appréciation de la nécessité et de la proportionnalité de l'initiative sont la définition de ce qui constitue un registre de la police, la quantité d'informations figurant dans l'index, la durée de conservation d'un registre de la police, les finalités pour lesquelles il peut être utilisé, et les autorités qui pourraient y avoir accès[34].

39. La définition figurant à l'article 4, paragraphe 16, de la proposition définit les registres de la police comme «toutes les informations disponibles dans le ou les registres nationaux qui contiennent les données des autorités compétentes à des fins de prévention et de détection des infractions pénales ainsi que d'enquêtes en la matière». Les critères d'introduction et de conservation des données relatives à un individu dans un registre de la police sont entièrement laissés à la discrétion des États membres et de leurs règles nationales. Le fait qu'en vertu de l'article 25, paragraphe 1, de la proposition, l'échange automatisé de registres de la police au titre du mécanisme de Prüm se limite aux «données biographiques des suspects et des criminels dans leurs index nationaux de registres de la police créés aux fins d'enquêtes en matière d'infractions pénales» ne permet pas de préciser le champ d'application matériel et personnel du traitement de données à caractère personnel proposé.

40. Le CEPD note une fois de plus que l'échange automatisé proposé n'est ni lié ni subordonné à la gravité de l'infraction pénale, c'est-à-dire qu'il pourrait être justifié à la fois par une enquête sur un acte terroriste et par une infraction routière (mineure), si ceux-ci sont pénalisés dans le droit pénal national. En outre, l'analyse d'impact accompagnant la proposition ne mentionne aucune étude sur la qualité des données figurant dans les registres nationaux de la police, en particulier sur la mesure dans laquelle les données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

41. Le CEPD rappelle que, conformément à l'article 7 de la directive en matière de protection des données dans le domaine répressif, les autorités répressives compétentes doivent établir une distinction entre les données à caractère personnel fondées sur des faits, dans la mesure du possible, et les données à caractère personnel fondées sur des évaluations personnelles. Dans le même ordre d'idées, dans tous les cas de transmission de données à caractère personnel, il convient d'ajouter les informations nécessaires permettant à l'autorité compétente destinataire d'évaluer le degré d'exactitude, d'exhaustivité et de fiabilité des données à caractère personnel, ainsi que la mesure dans laquelle elles sont à jour.

42. En outre, il convient de garder à l'esprit que les registres nationaux de la police peuvent contenir des données qui n'ont pas été examinées par une autorité judiciaire, par exemple des renseignements criminels sur un «suspect» potentiel d'une infraction pénale, qui peut ne pas avoir fait l'objet de poursuites et d'une enquête formelle pour diverses raisons. Par conséquent, l'échange proposé de données provenant des registres de la police diffère sensiblement du système existant d'échange d'informations sur les condamnations à partir des casiers judiciaires nationaux, à savoir le système européen d'information sur les casiers judiciaires (ECRIS)[35].

43. Les risques pour les droits fondamentaux des personnes concernées par le traitement de données figurant dans les registres nationaux de la police ont été examinés par la CEDH, qui a constaté, dans un certain nombre d'affaires, une violation de l'article 8 de la convention européenne des droits de l'homme[36]. Par conséquent, le CEPD estime que la proposition visant à étendre le cadre Prüm à la consultation et à l'échange automatisés des registres de la police devrait faire l'objet d'une analyse d'impact plus détaillée et plus approfondie. Le caractère volontaire de la participation à l'échange de registres de la police, sous réserve de la décision de chaque État membre[37], n'est pas suffisant pour atténuer les risques pour les personnes concernées et pourrait même être interprété comme une indication des doutes que la Commission elle-même nourrit sur cet aspect de la proposition.

44. Le CEPD prend note avec satisfaction de l'utilisation proposée de la pseudonymisation aux fins de l'échange automatisé des registres de la police. Conformément à l'article 25, paragraphe 2, de la proposition, toutes les données de recherche, à l'exception de la date de naissance et du sexe, seraient pseudonymisées. Si le CEPD se félicite de l'application pratique envisagée des principes de protection des données dès la conception, il rappelle néanmoins que les données pseudonymisées restent des données à caractère personnel et doivent respecter les règles en matière de protection des données.

45. Le CEPD attire l'attention sur un autre aspect important, qui peut avoir une incidence sur le droit à la protection des données à caractère personnel, à savoir la qualité des correspondances résultant de la consultation automatisée des registres de la police. Étant donné que la plupart des données seraient pseudonymisées et qu'il y aurait des champs de recherche obligatoires et facultatifs[38], le CEPD souligne la nécessité de disposer d'outils et de mesures efficaces pour évaluer et garantir la qualité des correspondances afin d'éviter, notamment, les faux positifs. En outre, le CEPD invite la Commission à fournir davantage d'informations sur la ou les méthodes de pseudonymisation (par exemple, dans l'acte d'exécution visé à l'article 44, paragraphe 7, de la proposition)[39].

46. Compte tenu de l'ensemble des considérations qui précèdent, **le CEPD estime que la nécessité de la consultation et de l'échange automatisés de données des registres de la police proposés n'est pas suffisamment démontrée. À cet égard, l'analyse d'impact accompagnant la proposition ne fournit pas de preuve convaincante que cette mesure sera réellement efficace et la moins intrusive pour les droits fondamentaux concernés, notamment les risques en matière de protection des données introduits par la nouvelle activité de traitement proposée[40].**

47. Si les colégislateurs décident néanmoins que cela doit faire partie du droit de l'Union, même sur une base volontaire, **il est probable que des garanties supplémentaires solides seront nécessaires pour respecter le principe de proportionnalité[41]. Si des mesures techniques telles que la pseudonymisation sont les bienvenues, elles ne sont toutefois pas suffisantes. Le futur règlement devrait à tout le moins définir les types et/ou la gravité des infractions pénales susceptibles de justifier une consultation automatisée des registres nationaux de la police, sans préjudice de la nécessité de prévoir des garanties supplémentaires pour faire face aux problèmes de qualité des données qui se poseraient inévitablement.**

3.6. Le rôle d'Europol

48. Le chapitre 5 de la proposition prévoit l'inclusion d'Europol dans le cadre Prüm, ce qui permettrait aux États membres d'accéder aux données biométriques obtenues auprès de pays

tiers et stockées par Europol (article 49) et à Europol de vérifier les données obtenues auprès de pays tiers dans les bases de données nationales des États membres (article 50). En outre, Europol serait responsable du développement et de la gestion technique du système d'index européen des registres de la police (EPRIS), l'outil de consultation automatisée des registres de la police (article 64).

49. Selon le considérant 13 de la proposition, «[c]es dernières années, Europol a reçu de plusieurs pays tiers un grand nombre de données biométriques de terroristes et de criminels présumés ou reconnus coupables. L'intégration dans le cadre Prüm des données obtenues auprès de pays tiers et stockées au sein d'Europol, et, partant, la mise à disposition des services répressifs de ces données sont nécessaires pour améliorer la prévention des infractions pénales et les enquêtes en la matière».

50. Le CEPD rappelle le processus législatif en cours visant à renforcer et à élargir le mandat d'Europol, qui est entré dans sa phase finale[42]. Le CEPD a formulé ses observations et recommandations dans l'avis 4/2021 sur la proposition de modification du règlement Europol[43], ainsi que dans les observations ultérieures à l'intention du colégislateur[44]. **Ces recommandations restent pleinement valables dans le contexte de la participation envisagée d'Europol au cadre Prüm, en particulier celles relatives au «défi des mégadonnées», à savoir le traitement par l'Agence d'ensembles de données vastes et complexes. Le CEPD souhaite rappeler deux des messages clés figurant dans l'avis sur Europol. D'une part, des pouvoirs renforcés doivent toujours aller de pair avec un contrôle renforcé** exercé par les colégislateurs. **D'autre part, et c'est tout aussi important, les exceptions et dérogations accordées à Europol ne devraient pas être autorisées à devenir la règle.**

51. En outre, conformément à l'article 49, paragraphe 1, de la proposition, les États membres auront accès aux données biométriques qui ont été fournies à Europol par des pays tiers aux fins de l'article 18, paragraphe 2, points a), b) et c), du règlement Europol et pourront les consulter. Le CEPD observe que presque toutes les données à caractère personnel fournies par des pays tiers à Europol relèveraient de l'une des finalités énumérées à l'article 18, paragraphe 2, points a), b) et c), et que, par conséquent, cette condition ne sert pas à limiter les consultations effectuées par les États membres. L'accès devrait toutefois être conforme aux conditions dans lesquelles les pays tiers ont partagé des données à caractère personnel avec Europol (par exemple, une autorisation préalable pour une transmission ultérieure, le cas échéant); l'article 49 devrait donc inclure une référence à cette exigence.

52. En outre, étant donné que les pays tiers peuvent partager avec Europol des données biométriques relative à un ensemble plus large de catégories de personnes concernées (contacts, associés, victimes), **le CEPD recommande de préciser le champ d'application personnel, c'est-à-dire les catégories de personnes concernées qui font l'objet de requêtes au titre des articles 49 et 50**.

53. La proposition établirait des dispositions relatives à la tenue par les États membres et Europol de registres des opérations de traitement de données relevant du cadre Prüm (articles 20, 40 et 45), ainsi qu'un relevé des justifications des requêtes effectuées par les autorités compétentes et Europol (article 33). Les registres prévoient le contrôle de la protection des données, la vérification de la recevabilité d'une requête et de la licéité du traitement des données, y compris par les autorités de contrôle et le CEPD, conformément aux articles 56, 60 et 61 de la proposition. La proposition prévoit que les registres et justifications susvisés doivent être effacés un an après leur création. Lorsque ces articles concernent Europol, le CEPD note que cette durée de conservation s'écarte de la période de conservation de trois ans accordée à

la journalisation et à la documentation prévue à l'article 40 du règlement Europol. **Le CEPD recommande d'aligner les délais de conservation des registres afin d'assurer la cohérence avec le règlement Europol et de permettre un contrôle et une enquête efficaces sur les réclamations des personnes concernées.**

3.7. Transfert de données à caractère personnel vers des pays tiers et à des organisations internationales

54. Conformément à l'article 62 de la proposition, «[l]es données traitées conformément au présent règlement ne sont pas transférées à des pays tiers ou à des organisations internationales ni mises à leur disposition de manière automatisée». Compte tenu des observations formulées au point 3.1 ci-dessus sur la relation entre les garanties en matière de protection des données prévues dans la proposition et le cadre juridique général de l'Union en matière de protection des données, **le CEPD souligne que tout transfert vers un pays tiers ou à une organisation internationale doit être pleinement conforme au chapitre V de la directive en matière de protection des données dans le domaine répressif et aux dispositions pertinentes du règlement (UE) 2016/794**.

3.8. Solutions techniques pour l'échange de données et modèle de gouvernance

55. La proposition envisage une architecture complexe pour la consultation et l'échange automatisés de données au titre du cadre Prüm, comportant trois solutions techniques distinctes:

- un routeur central pour l'échange de profils ADN, de données dactyloscopiques et d'images faciales;

- un système d'index européen des registres de la police (EPRIS) pour l'échange de registres de la police; et

- un système d'information européen concernant les véhicules et les permis de conduire (EUCARIS) pour l'échange de données relatives à l'immatriculation des véhicules.

56. Chacun des outils susvisés serait mis au point et géré par une entité différente: le routeur par l'Agence de l'UE 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) et l'EPRIS par Europol. EUCARIS existe déjà et, contrairement aux deux systèmes précédents, il n'est pas fondé sur un acte juridique de l'UE, mais a un caractère intergouvernemental, à savoir le traité EUCARIS[45].

57. Le CEPD note que la proposition tente de remédier à la complexité du modèle de gouvernance au chapitre 7, qui est spécifiquement consacré aux responsabilités des différents acteurs. En outre, conformément à l'article 53, eu-LISA et Europol sont considérés comme des sous-traitants, respectivement pour le routeur et pour l'EPRIS. Le CEPD estime que les dispositions actuelles ne sont pas suffisantes et devraient être développées plus avant.

58. Le CEPD souligne la nécessité d'établir une distinction claire entre les rôles en matière de protection des données. Alors que les États membres et Europol conserveront la «propriété»[46] des données à caractère personnel échangées (en tant que responsables du traitement), il pourrait arriver que l'Agence et un ou plusieurs États membres agissent en tant que responsables conjoints du traitement. En outre, la désignation proposée d'eu-LISA et d'Europol

comme sous-traitants crée une incertitude quant aux responsabilités en cas de violation de données à caractère personnel, par exemple l'autorité de contrôle qui devrait être informée, mais aussi celle qui devrait informer les personnes concernées, si nécessaire. Le CEPD rappelle que les données biométriques ont un caractère sensible et qu'une violation de données à caractère personnel entraînerait très probablement un risque élevé pour les personnes concernées. Nonobstant toute base juridique permettant de retarder, de limiter ou d'omettre la notification aux personnes concernées, par exemple pour éviter d'entraver les enquêtes, les notifications de violation de données aux personnes concernées devraient faire l'objet d'une évaluation approfondie, être documentées et faire l'objet d'un suivi.

59. Le CEPD note également la disposition du considérant 9, dernière phrase, selon laquelle il n'y aura pas d'élément central nécessaire pour établir la communication via EUCARIS, chaque État membre communiquant directement avec les autres États membres connectés, ainsi que l'article 19, paragraphe 2, selon lequel les informations échangées via EUCARIS devraient être transmises sous une forme cryptée. Toutefois, **le CEPD estime que la proposition devrait déterminer explicitement la responsabilité du traitement des données à caractère personnel dans EUCARIS**.

60. De plus, **le CEPD est convaincu que, compte tenu de l'ampleur et de la sensibilité du traitement des données à caractère personnel, le modèle de gouvernance horizontal proposé du cadre Prüm n'est pas approprié et devrait être encore renforcé, par exemple en attribuant un rôle central de coordination à une entité de l'UE, comme la Commission**.

3.9. Interopérabilité

61. Un autre élément important de la proposition, qui requiert une analyse approfondie de ses implications en matière de droits fondamentaux, est l'alignement du cadre Prüm sur le cadre d'interopérabilité des systèmes d'information de l'UE dans le domaine de la justice et des affaires intérieures[47].

62. L'interopérabilité est la capacité des systèmes d'information à échanger des données et à partager des informations. À cette fin, les règlements relatifs à l'interopérabilité ont introduit plusieurs nouveaux éléments, dont le répertoire commun de données d'identité (CIR) et le portail de recherche européen (ESP). Le CIR stockerait les données à caractère personnel nécessaires à l'identification des personnes dont les données sont stockées dans les systèmes interopérables, notamment leurs données d'identité, les données figurant dans leurs documents de voyage et leurs données biométriques, quel que soit le système dans lequel ces informations ont été collectées à l'origine. L'ESP ferait office de guichet unique ou de «courtier de messages» pour consulter les différents systèmes centraux et récupérer les informations nécessaires.

63. Le CEPD est convaincu que l'interopérabilité devrait avant tout être considérée comme un choix politique, et non comme une solution technologique, en raison de ses lourdes conséquences juridiques et sociétales. Alors que nous vivons dans un monde basé sur les données, il n'est pas surprenant que la politique de l'Union au sein de l'espace de liberté, de sécurité et de justice repose de plus en plus sur un partage d'informations efficace et efficient. Toutefois, le cadre juridique de l'Union doit garantir que les droits fondamentaux de tous les individus concernés ne sont limités que dans la mesure strictement nécessaire.

64. Conformément à l'article 39 de la proposition, les utilisateurs du routeur visés à l'article 36 de la proposition peuvent interroger les bases de données des États membres et les données d'Europol simultanément à une requête effectuée dans le répertoire commun de données d'identité lorsque les conditions applicables prévues par le droit de l'Union sont remplies et dans le respect de leurs droits d'accès. À cette fin, le routeur interroge le répertoire commun de données d'identité via le portail de recherche européen. Les requêtes simultanées ne peuvent être lancées que lorsqu'il est probable que des données sur un suspect, un auteur ou une victime d'une infraction terroriste ou d'autres infractions pénales graves sont stockées dans le répertoire commun de données d'identité.

65. Le CEPD rappelle que le répertoire commun de données d'identité contient les données d'identité (informations alphanumériques) des personnes concernées, séparées logiquement par système informatique d'origine, tandis que les données biométriques sont stockées dans le service partagé d'établissement de correspondances biométriques (SBMS). Ce dernier ne stocke que les empreintes digitales et les images faciales, et non les profils ADN. L'eu-LISA devrait tenir compte de ce fait lors du développement de l'infrastructure de communication entre le cadre Prüm et l'architecture d'interopérabilité.

66. En outre, le CEPD attire l'attention sur le fait que les images faciales provenant des bases de données nationales, qui font l'objet de recherches automatisées au titre du cadre Prüm, peuvent différer de celles stockées dans les systèmes informatiques à grande échelle de l'UE (par exemple, le VIS, l'EES) en termes de format et de qualité. À cet égard, des questions se posent quant à la performance de l'algorithme d'établissement de correspondances biométriques du SBMS en cas de mise en correspondance d'images faciales de données de suspects enregistrées dans des conditions différentes, par exemple par une caméra de sécurité, avec des images faciales prises dans un environnement contrôlé, par exemple dans une cabine durant la procédure de délivrance des visas. Des mesures appropriées devraient être **élaborées et mises en œuvre pour faire face aux risques découlant des mauvaises performances des algorithmes d'établissement de correspondances**.

67. Enfin, le CEPD note que l'article 30 de la proposition, qui délègue à la Commission le pouvoir d'adopter des actes d'exécution afin de préciser les modalités techniques, ne comprend pas l'élément d'interopérabilité visé à l'article 39. **Par conséquent, le CEPD invite le colégislateur à envisager la nécessité d'un acte d'exécution ou d'un acte délégué spécifique sur l'interopérabilité.**

3.10. Contrôle

68. L'échange de données, y compris de données biométriques, au titre du cadre Prüm constitue une ingérence grave dans le droit à la protection des données à caractère personnel et impose un contrôle strict et efficace au niveau national et au niveau de l'Union. **Le CEPD se félicite donc de l'approche adoptée à l'article 61 de la proposition, qui fait référence au modèle de contrôle coordonné entre les autorités de contrôle nationales et le CEPD, établi par l'article 62 du règlement (UE) 2018/1725.** Ce dernier prévoit une coopération régulière et structurée dans le cadre du comité européen de la protection des données.

69. Le CEPD note également avec satisfaction l'obligation, prévue à l'article 60, paragraphe 1, de la proposition, d'effectuer des audits réguliers des opérations de traitement des données à caractère personnel effectuées aux fins du règlement Prüm II par l'eu-LISA et Europol. Dans le même temps, il estime que **l'exigence d'audits réguliers devrait être étendue et couvrir également les opérations de traitement de données à caractère personnel au niveau**

national. À cet égard, afin de garantir l'efficacité du contrôle, **le CEPD rappelle la nécessité de doter les autorités de contrôle de ressources humaines et techniques suffisantes**[48].

70. Le CEPD note que l'article 60, paragraphe 2, de la proposition fait référence à certains des pouvoirs de contrôle du CEPD vis-à-vis d'eu-LISA et d'Europol, à savoir l'accès illimité aux documents et aux locaux. Toutefois, en l'absence de dispositions claires sur la relation entre le présent règlement et le cadre juridique existant en matière de protection des données, en particulier le RPDUE et la directive en matière de protection des données dans le domaine répressif, comme expliqué au point 3.1 ci-dessus, il existe un risque d'interprétation restrictive des compétences du CEPD. Par conséquent, **l'article 60, paragraphe 2, de la proposition devrait être modifié pour faire référence aux compétences du CEPD en vertu de l'article 58 du RPDUE en général, et pas seulement à certains d'entre eux**.

71. Le chapitre 9 de la proposition prévoirait des dispositions permettant aux autorités concernées d'obtenir des rapports et des statistiques afin d'évaluer l'efficacité de la coopération au titre du mécanisme. Les statistiques doivent notamment inclure le nombre de requêtes et le nombre de correspondances. **Le CEPD estime que le signalement de l'exactitude des réponses positives par l'État membre demandeur/Europol serait très utile pour mesurer l'efficacité du mécanisme de Prüm, en particulier lorsqu'il s'agit de correspondances de données biométriques, telles que des images faciales. Par conséquent, il recommande d'inclure explicitement cet élément dans les statistiques**.

72. Conformément à l'article 55 de la proposition, l'eu-LISA et Europol doivent notifier à la CERT-UE tout incident de sécurité impliquant des menaces informatiques, des vulnérabilités ou des incidents de cybersécurité importants. À cet égard, **le CEPD rappelle que cette obligation est sans préjudice de l'obligation faite aux institutions, organes et agences de l'UE de notifier les violations de données à caractère personnel au CEPD, conformément aux articles 92 et 34 du RPDUE**.

4. Conclusions

73. Le nouveau cadre Prüm proposé n'établit pas clairement les composantes essentielles de l'échange de données, telles que les types d'infractions pénales qui peuvent justifier une requête (recherche), en particulier de profils ADN, c'est-à-dire toute infraction pénale ou uniquement les infractions plus graves. En outre, la proposition n'indique pas clairement l'étendue des personnes concernées par l'échange automatisé de données, c'est-à-dire si les bases de données faisant l'objet d'une requête ne contiennent que les données de suspects et/ou de personnes reconnues coupables, ou également les données d'autres personnes concernées, telles que des victimes ou des témoins.

74. Afin de garantir la nécessité et la proportionnalité de l'ingérence dans le droit fondamental à la protection des données à caractère personnel, à la lumière de l'article 52, paragraphe 1, de la Charte, il est essentiel de préciser le champ d'application personnel et matériel des mesures, c'est-à-dire les catégories de personnes concernées qui seront directement affectées, ainsi que les conditions objectives susceptibles de justifier une recherche automatisée dans les bases de données d'autres États membres ou d'Europol.

75. Le CEPD estime, en particulier, que la consultation automatisée de profils ADN et d'images faciales ne devrait être possible que dans le cadre d'enquêtes individuelles sur des infractions

pénales graves, plutôt que sur toute infraction pénale, comme le prévoit la proposition. En outre, conformément à l'obligation prévue à l'article 6 de la directive en matière de protection des données dans le domaine répressif d'établir une distinction entre les différentes catégories de personnes concernées, la proposition devrait prévoir une limitation des catégories de personnes concernées dont les profils ADN et les images faciales, stockés dans les bases de données nationales, devraient être rendus accessibles pour des consultations automatisées, compte tenu notamment de la limitation de la finalité inhérente aux données provenant d'autres catégories que les criminels reconnus coupables ou les suspects.

76. Le CEPD estime que la nécessité de la consultation et de l'échange automatisés proposés des données des registres de la police n'est pas suffisamment démontrée. Si une telle mesure était néanmoins adoptée, même sur une base volontaire, des garanties supplémentaires solides seraient nécessaires pour respecter le principe de proportionnalité. En particulier, compte tenu des problèmes de qualité des données, qui ne peuvent être résolus par des mesures techniques telles que la seule pseudonymisation, le futur règlement devrait à tout le moins déterminer les types et/ou la gravité des infractions pénales susceptibles de justifier une consultation automatisée des registres nationaux de la police.

77. En ce qui concerne l'inclusion d'Europol dans le cadre Prüm, le CEPD est d'avis que les observations et recommandations qu'il a formulées dans son avis 4/2021 sur la proposition de modification du règlement Europol restent parfaitement valables dans le cadre de la coopération Prüm, en particulier celles relatives au traitement par l'Agence d'ensembles de données vastes et complexes. En outre, le CEPD recommande de clarifier le champ d'application personnel, c'est-à-dire de préciser les catégories de personnes concernées qui font l'objet de requêtes au titre des articles 49 et 50, ainsi que d'aligner les durées de conservation des registres, afin de garantir la cohérence avec le règlement Europol.

78. La proposition prévoit une architecture complexe de consultation et d'échange automatisés de données au titre du cadre Prüm, comportant trois solutions techniques distinctes, élaborées et gérées par trois entités différentes. En outre, l'un d'entre eux – EUCARIS – n'est pas fondé sur un acte juridique de l'UE, mais a un caractère intergouvernemental. Toutefois, le CEPD estime que la proposition devrait aborder explicitement la responsabilité du traitement des données à caractère personnel dans EUCARIS. De plus, le CEPD considère que, compte tenu de l'ampleur et de la sensibilité du traitement des données à caractère personnel, le modèle de gouvernance horizontal proposé du cadre Prüm n'est pas approprié et devrait être encore renforcé, par exemple en attribuant un rôle central de coordination à une entité de l'UE, comme la Commission.

79. Un autre élément important de la proposition, qui requiert une analyse approfondie de ses implications en matière de droits fondamentaux, est l'alignement du cadre Prüm sur le cadre d'interopérabilité des systèmes d'information de l'UE dans le domaine de la justice et des affaires intérieures. Le CEPD invite le colégislateur à examiner la nécessité de prévoir des règles supplémentaires à cet égard, par exemple dans un acte d'exécution ou un acte délégué, qui devraient répondre à des défis spécifiques tels que la qualité et la performance des algorithmes de mise en correspondance pour les images faciales.

80. Compte tenu du fait que la base juridique de la proposition comprend, entre autres, l'article 16 du TFUE, par souci de clarté et de sécurité, le CEPD recommande de préciser dans la proposition que les dispositions relatives à la protection des données figurant au chapitre 6 sont sans préjudice de l'application de la directive en matière de protection des données dans le domaine répressif et du RPDUE en ce qui concerne le traitement des données à caractère personnel dans le cadre de la coopération en matière répressive relevant du cadre Prüm.

81. En outre, le CEPD estime que l'obligation d'effectuer des audits réguliers des opérations de traitement de données à caractère personnel aux fins du règlement Prüm II devrait être étendue et couvrir également les opérations de traitement de données à caractère personnel au niveau national. Dans ce contexte, le CEPD recommande que l'article 60, paragraphe 2, de la proposition fasse référence, de manière générale, aux compétences du CEPD, conformément à l'article 58 du RPDUE, et pas seulement à certains d'entre eux.

Bruxelles, le 2 mars 2022

[signature électronique]
Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 295 du 21.11.2018, p. 39.
[2] COM(2021) 784 final.
[3] COM(2021) 782 final.
[4] COM(2021) 780 final.
[5] https://ec.europa.eu/home-affairs/news/boosting-police-cooperation-across-borders-enhanced-security-2021-12-08_en
[6] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité, COM(2020)605 final.
[7] Communication de la Commission relative à la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025), COM(2021)170 final.
[8] Communication de la Commission «Une stratégie pour un espace Schengen pleinement opérationnel et résilient», COM(2021)277 final.
[9] Pour de plus amples informations, voir avis 4/2021 du CEPD, https://edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf.
[10] Avis du CEPD sur l'initiative de 15 États membres en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, disponible à l'adresse suivante: https://edps.europa.eu/sites/default/files/publication/07-04-04_crossborder_cooperation_en.pdf.
[11] Avis du 26 juillet 2017, PNR Canada, procédure d'avis 1/15, ECLI:EU:C:2017:592, point 96. Voir aussi l'avis conjoint 5/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), 18 juin 2021, paragraphe 11.
[12] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).
[13] Exposé des motifs, p. 8.
[14] COM(2020)262 final, p. 8.
[15] Voir article 18, paragraphe 1, point a), du règlement (UE) 2016/794.
[16] Voir article 6, point b), du règlement (UE) 2016/680.
[17] Voir CJUE, arrêt du 2 octobre 2018 (grande chambre), Ministerio Fiscal, C-207/16, EU:C:2018:788, point 58.
[18] Avis du CEPD sur l'initiative législative de 15 État membres en vue de l'adoption de la décision du Conseil relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, paragraphe 10.
[19] Voir aussi avis 07/2016 du CEPD sur le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin); avis 06/2016 sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne — Recommandations sur la proposition révisée visant à créer un système d'entrée/sortie; avis 3/2016 sur les échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS).
[20] Document du Conseil 5197/1/20 REV 1, disponible à l'adresse suivante: https://data.consilium.europa.eu/doc/document/ST-5197-2020-REV-1/en/pdf.
[21] Étude du Parlement européen intitulée «Échange d'informations policières – Évolutions futures du traité de Prüm et de la directive API», commandée par la commission LIBE, disponible à l'adresse suivante: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/658542/IPOL_STU(2020)658542_EN.pdf.
[22] Étude du Parlement européen intitulée «Échange d'informations policières – Évolutions futures du traité de Prüm et de la directive API», page 20, point 2.3.2.
[23] Voir, par exemple, CEDH, affaire Gaughran c. Royaume-Uni, arrêt du 13 février 2020; affaire Aycaguer c. France, arrêt du 22 juin 2017; affaire S. et Marper c. Royaume-Uni, arrêt du 4 décembre 2008.
[24] Voir arrêt de la CEDH dans l'affaire Gaughran c. Royaume-Uni, point 53.
[25] Arrêt de la CJUE du 9 novembre 2010, affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke et Eifert, Rec. 2010, p. I-0000.
[26] Pour un complément d'information, voir les lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, disponibles à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf.
[27] CJUE, arrêt du 2 octobre 2018 (grande chambre), Ministerio Fiscal, C-207/16, EU:C:2018:788, point 58.
[28] Voir chapitre II, section 4, de la proposition.

[29] Lettre de l'EDPB du 28 juillet 2020, disponible à l'adresse suivante: https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0090-prumframework.pdf.
[30] Étude du Parlement européen intitulée «Échange d'informations policières – Évolutions futures du traité de Prüm et de la directive API», pages 51 et 52.
[31] SWD(2021)378 final, p. 25.
[32] Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), 18 juin 2021, disponible à l'adresse suivante: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.
[33] Voir chapitre 2, section 5, et chapitre 3, section 2, de la proposition.
[34] Étude du Parlement européen intitulée «Échange d'informations policières – Évolutions futures du traité de Prüm et de la directive API», page 52.
[35] Pour en savoir plus, voir: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en#background.
[36] Voir CEDH, affaire Khelili c. Suisse, arrêt du 18 octobre 2011, affaire Segerstedt-Wiberg et autres c. Suède, arrêt du 6 juin 2006, affaire Cemalettin Canli c. Turquie, arrêt du 18 novembre 2008.
[37] Voir considérant 12 de la proposition.
[38] Article 43, paragraphes 1 et 2, de la proposition.
[39] Par exemple, les fonctions de hachage pourraient permettre le chiffrement irréversible des données à caractère personnel et, dans le même temps, permettre de comparer deux ensembles de données, étant donné que les deux parties (demandeur et destinataire) utiliseront le même algorithme et la même clé pour créer les valeurs de hachage.
[40] Pour de plus amples informations sur l'appréciation de la nécessité de mesures législatives, voir le guide pour l'évaluation de la nécessité du CEPD, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[41] Voir également les lignes directrices du CEPD sur la proportionnalité, disponibles à l'adresse suivante: https://edps.europa.eu/data-protection/our-work/publications/guidelines/assessing-proportionality-measures-limit_en.
[42] Pour en savoir plus, voir: https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-strengthening-of-europol-s-mandate/01-2022.
[43] https://edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf
[44] https://edps.europa.eu/system/files/2022-02/2022-02-01-remarks_at_the_libe_committee_on_europol_en.pdf
[45] Pour en savoir plus, voir: https://www.eucaris.net/general-information/legal-basis/.
[46] Exposé des motifs, p. 6.
[47] Établi par le règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil et par le règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816.
[48] Voir contribution de l'EDPB à l'évaluation, par la Commission européenne, de la directive en matière de protection des données dans le domaine répressif,
conformément à l'article 62, paragraphe 14, disponible à l'adresse suivante: https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.