EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

25 mai 2021

Avis 8/2021

sur la recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord de coopération entre l'Union européenne (UE) et INTERPOL

edps.europa.eu

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne 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 le 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, dudit règlement, «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'Union européenne sur l'application cohérente et logique des principes de protection des données de l'Union européenne lors de la négociation d'accords en matière de coopération des services répressifs. Il s'appuie sur l'obligation générale exigeant que les accords internationaux soient conformes aux dispositions du traité sur le fonctionnement de l'Union européenne (le «TFUE») et respectent les droits fondamentaux qui forment le noyau du droit de l'UE. En particulier, il convient de veiller au respect des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 16 du TFUE.

Synthèse

Le 14 avril 2021, la Commission européenne a adopté une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord de coopération entre l'Union européenne et l'Organisation internationale de police criminelle (O.I.P.C.-Interpol).

Malgré la coopération déjà en place avec Interpol, la Commission a recensé des domaines dans lesquels la coopération pourrait et devrait être intensifiée, voire mise en place dans de nouveaux domaines, aux fins de répondre à une série de besoins opérationnels indispensables et de mettre en œuvre les actes juridiques existants, dans le but de mieux aider les États membres à prévenir et à combattre le terrorisme et la criminalité organisée. Ces besoins opérationnels nécessitent la conclusion d'un accord de coopération avec Interpol.

Le CEPD tient à souligner que l'objectif consistant à soutenir la coopération (actuelle et future) entre l'Union européenne et Interpol dans le cadre d'un large éventail d'activités s'inscrivant dans un instrument juridique unique rend l'accord envisagé très hétérogène par nature. Il insiste dès lors sur la nécessité d'**une analyse d'impact approfondie** et souligne que cette approche ne devrait pas conduire à affaiblir les libertés et droits fondamentaux des personnes physiques, plus particulièrement leurs droits à la protection des données et au respect de la vie privée.

Le régime juridique de l'Union en matière de protection des données prévoit, en principe, que les transferts de données vers une organisation internationale ne peuvent avoir lieu sans exigences supplémentaires que si cette organisation internationale garantit un niveau de protection adéquat. Lorsque l'organisation internationale n'a pas été déclarée adéquate, des exceptions s'appliquent aux transferts spécifiques, jusqu'à ce que les garanties appropriées soient apportées. En conséquence, le CEPD formule également trois recommandations principales pour garantir que l'accord envisagé soit en mesure de fournir des garanties appropriées:

- Il convient de préciser dans les directives de négociation qu'il est nécessaire de veiller à ce que l'accord envisagé soit globalement conforme à la Charte, à la législation horizontale pertinente en matière de protection des données [règlement (UE) 2018/1725, règlement (UE) 2016/679 et directive (UE) 2016/680] et aux exigences et garanties spécifiques en matière de protection des données prévues dans les actes de base instituant les agences ou systèmes informatiques de l'UE.
- Le futur accord devrait préciser explicitement qu'il n'y aura pas d'accès réciproque, direct ou indirect, d'Interpol aux bases de données de l'UE.
- Dans le contexte des transferts ultérieurs, il convient de prévoir explicitement que les données à caractère personnel transférées par l'UE à Interpol ne seront pas utilisées pour demander, prononcer ni exécuter une peine de mort ou toute forme de traitement cruel et inhumain.

Enfin, le CEPD recommande que les visas cités dans le préambule de la recommandation fassent non seulement référence à la base juridique procédurale adéquate mais également à la base juridique matérielle pertinente, notamment à l'article 16 du TFUE, qui traite de l'objet du futur accord.

Le CEPD reste également disposé à fournir des conseils supplémentaires au cours des négociations et de la consultation formelle qui doit avoir lieu sur la proposition soumise au Conseil en vue de la

signature et de la conclusion de l'accord au titre de l'article 218 du TFUE, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725.

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 (la «Charte»), et notamment ses articles 7 et 8,

vu le 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)[1],

vu la 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[2],

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[3], et notamment son article 42, paragraphe 1,

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction et contexte

1. L'Organisation internationale de police criminelle (Interpol)[4], qui compte 194 pays membres, est la plus grande organisation intergouvernementale de police criminelle au monde. L'UE et Interpol entretiennent déjà une coopération étroite et de longue date dans toute une série de domaines liés à l'application de la loi. Interpol constitue un partenaire essentiel de l'UE dans le domaine de la sécurité intérieure et extérieure, notamment dans la lutte contre le terrorisme et la criminalité organisée, ainsi que dans la gestion intégrée des frontières.

2. La stratégie de 2020 de l'UE pour l'union de la sécurité[5] invite les États membres à intensifier la coopération entre l'Union et Interpol, car un tel renforcement est essentiel pour améliorer la coopération et l'échange d'informations. Cette stratégie reconnaît qu'Interpol a un rôle important à jouer à cet égard. Outre la coopération déjà en place avec Interpol, des domaines dans lesquels la coopération pourrait être renforcée ou même mise en place pour répondre à une série de besoins opérationnels et pour mettre en œuvre les actes juridiques existants ont été recensés, dans le but de mieux aider les États membres à prévenir et à combattre le terrorisme et la criminalité organisée.

3. En conséquence, le 14 avril 2021, la Commission a adopté une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord de coopération entre l'Union européenne et Interpol[6] (ci-après la «recommandation»).

4. L'exposé des motifs[7] de la proposition précise que l'accord de coopération entre l'Union et Interpol envisagé poursuivrait les objectifs suivants:

- Réglementer la coopération entre l'Agence de l'Union européenne pour la coopération des services répressifs (**Europol**)[8] et Interpol, compte tenu des dernières évolutions en date dans la lutte contre le terrorisme et la grande criminalité organisée transfrontière et transnationale, des besoins opérationnels actuels, du mandat d'Europol et du régime de protection des données de l'UE le plus récent.

- Fournir les mesures de sauvegarde et les garanties nécessaires pour autoriser l'accès contrôlé **des États membres de l'UE et agences de l'UE** aux bases de données d'Interpol sur les documents de voyage volés ou perdus (SLTD) et sur les documents de voyage associés aux notices (TDAWN), par l'intermédiaire du portail de recherche européen (ESP), dans la mesure nécessaire à l'accomplissement de leurs tâches, conformément à leurs droits d'accès, à la législation de l'UE ou à la législation nationale régissant un tel accès, et dans le strict respect des exigences de l'UE en matière de protection des données et des droits fondamentaux[9].

- Fournir les mesures de sauvegarde et les garanties nécessaires pour autoriser les **États membres de l'UE** et **Frontex**[10] [plus précisément l'unité centrale du système européen d'information et d'autorisation concernant les voyages (ETIAS)] à accéder aux bases de données d'Interpol par l'intermédiaire de l'ESP, conformément aux exigences de l'UE en matière de protection des données et aux droits fondamentaux.

- Fournir les mesures de sauvegarde et les garanties nécessaires à la mise en œuvre d'un **règlement révisé concernant le système d'information sur les visas**[11], qui autorise les **États membres de l'UE** à accéder aux bases de données SLTD et TDAWN par l'intermédiaire de l'ESP lors de l'examen des demandes de visa ou de titre de séjour, dans le plein respect des exigences de l'UE en matière de protection des données et des droits fondamentaux.

- Instaurer et réglementer la coopération entre le **Parquet européen**, créé par le règlement (UE) 2017/1939 (le «règlement du Parquet européen»)[12], et Interpol, conformément à leurs mandats respectifs, et dans le strict respect des exigences de l'UE en matière de protection des données et des droits fondamentaux.

- Établir la base juridique pour autoriser **Europol, le personnel de catégorie 1 de Frontex** (personnel statutaire du contingent permanent[13]) et le **Parquet européen** à **accéder aux bases de données pertinentes d'Interpol** afin de s'acquitter de leurs tâches, dans le strict respect des exigences de l'UE en matière de protection des données et des droits fondamentaux.

- Établir la base juridique pour autoriser **Eurojust[14] et le Parquet européen** à échanger des **informations opérationnelles** avec Interpol, dans le strict respect des exigences de l'UE en matière de protection des données et des droits fondamentaux.

5. Conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, la Commission doit consulter le CEPD à la suite de l'adoption d'une recommandation au Conseil en vertu de l'article 218 du TFUE en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel. Le CEPD a également été consulté de manière informelle au cours du processus d'élaboration de la recommandation et a communiqué ses observations informelles en août 2020. Il se réjouit que son avis ait été sollicité (et mis en œuvre dans une certaine mesure) à un stade précoce de la procédure et encourage la Commission à maintenir cette bonne pratique.

6. Le CEPD a été consulté officiellement par la Commission le 14 avril 2021 et espère qu'une référence au présent avis sera intégrée dans le préambule de la décision du Conseil. Le présent avis est sans préjudice de toute observation ou recommandation supplémentaire ultérieure du CEPD, notamment si de nouvelles problématiques sont mises au jour, si de nouvelles informations sont disponibles et si une consultation formelle doit avoir lieu sur les propositions soumises au Conseil en vue de la signature et de la conclusion de l'accord au titre de l'article 218 du TFUE, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725. Sur ce point, le CEPD se félicite du considérant 19 de la recommandation, selon lequel la Commission devrait le consulter au cours de la négociation de l'accord ou, en tout état de cause, avant la conclusion de l'accord. En outre, le présent avis est sans préjudice de toute action future que pourrait entreprendre le CEPD dans l'exercice des pouvoirs que lui confère l'article 58 du règlement (UE) 2018/1725.

2. L'approche globale

7. Le CEPD souligne que l'objectif consistant à soutenir une coopération (existante et à venir) importante entre l'UE et Interpol au moyen d'un instrument juridique unique rend l'accord envisagé **très hétérogène** par nature, englobant un large éventail d'activités, notamment la coopération policière (articles 87 et 88 du TFUE), la coopération judiciaire en matière pénale (articles 82 et 85 du TFUE), la sécurité des frontières dans le cadre de la gestion des frontières (article 77 du TFUE), les visas et les titres de séjour et le Parquet européen (article 86 du TFUE), auquel tous les États membres ne participent pas[15].

8. Compte tenu d'une approche aussi hétérogène, il souligne 1) la nécessité d'une analyse d'impact approfondie, et 2) que cette approche ne doit pas entraîner un affaiblissement des libertés et droits fondamentaux des personnes physiques, et plus particulièrement de leurs droits à la protection des données et au respect de la vie privée.

2.1. Une analyse d'impact approfondie sur les droits fondamentaux fait défaut

9. L'hétérogénéité de l'accord envisagé, combinée à l'incidence potentielle d'un tel accord sur les droits fondamentaux, en particulier sur le respect de la vie privée et la protection des données, requièrent une analyse d'impact approfondie. Le CEPD regrette que la recommandation de la Commission n'ait pas été accompagnée d'une analyse d'impact sur les droits fondamentaux et encourage le Conseil à entreprendre une analyse d'impact approfondie sur les droits fondamentaux et la protection des données[16], tenant compte de a) la **nécessité et la proportionnalité de chaque mesure envisagée dans la mesure où elles limitent** les droits au respect de la vie privée et à la protection des données à caractère personnel[17] et b) la **faisabilité juridique** de réglementer toutes ces mesures dans le cadre d'un accord global **unique**[18]. Une prudence particulière s'impose[19], en raison de la sensibilité des données concernées et du nombre de pays tiers membres d'Interpol qui ne sont pas parties à un accord équivalent avec l'UE ou dont les autorités auxquelles il est prévu de transférer des données à caractère personnel ne sont pas concernées par une décision d'adéquation de la Commission[20].

10. L'analyse de la nécessité et de la proportionnalité des cas d'utilisation envisagés pour chaque objectif devrait porter en particulier sur **les finalités du traitement ainsi que sur la quantité et les catégories de données à caractère personnel concernées**. Elle devrait notamment déterminer quelles bases de données devraient être consultées - par exemple, si cela devrait également inclure les notices d'Interpol - et selon quelles modalités. L'analyse devrait également

démontrer la nécessité pour **chacune des bases de données d'Interpol** qu'elle envisage de rendre accessibles (par rapport aux bases de données déjà disponibles).

11. L'analyse d'impact devrait également **tenir compte des risques pour les personnes concernées**, en gardant à l'esprit qu'il pourrait s'agir de personnes vulnérables telles que des migrants et, éventuellement, des demandeurs d'asile.

2.2. L'accord envisagé ne devrait pas abaisser le niveau de protection

12. Le CEPD estime que la **recommandation devrait être clarifiée afin d'éviter le risque d'abaisser le niveau de protection des personnes, actuellement garanti en vertu du droit primaire et du droit dérivé de l'UE**.

13. Il note que **les échanges de données à caractère personnel prévus par la recommandation pourraient ne pas toujours être compatibles avec le droit dérivé de l'Union établissant ou réglementant les activités des institutions, agences, bureaux et organes de l'UE** qui coopéreraient avec Interpol.

14. Le manque de clarté quant aux finalités spécifiques, aux types de données à échanger ainsi qu'à la répartition exacte des rôles et des responsabilités, nuit à l'exigence de qualité de la législation, qui revêt une importance capitale pour **toutes les mesures limitant les droits** consacrés aux articles 7 et 8 de la Charte et à l'article 16 du TFUE.

15. Cette préoccupation est notamment soulevée par des formulations telles que «l'*accord devrait constituer la base juridique pour autoriser Europol, le personnel statutaire du contingent permanent de Frontex (personnel de catégorie 1) et le Parquet européen à* ***accéder aux bases de données pertinentes d'Interpol*** pour s'acquitter de leurs tâches ou missions»[21]. Compte tenu de la nature sensible des données concernées, le CEPD rappelle qu'**il est primordial que toutes les spécifications nécessaires figurent dans les directives de négociation**.

16. Plus précisément, le CEPD estime que **chaque type de coopération** avec Interpol régie par l'accord global envisagé devrait:

- **préciser** clairement **la ou les finalités et les objectifs de la coopération entre Interpol et chaque institution, organe, office et agence de l'UE concerné(e)**. Il importe que la finalité spécifiée n'aille pas au-delà de ce qui est prescrit dans les instruments juridiques existants et qu'elle soit notamment conforme au mandat respectif de l'institution, de l'organe, de l'office ou de l'agence de l'UE concerné(e). L'accord envisagé ne devrait pas introduire de nouvelles opérations de traitement de données qui ne sont pas couvertes par les bases juridiques existantes. Sur ce point, nous recommandons de préciser que l'accord envisagé ne prévoira pas **un accès réciproque, direct ou indirect, d'Interpol aux bases de données de l'UE**;

- tenir dûment compte de **la différence** entre *la coopération judiciaire en matière pénale et la coopération policière*, d'une part, et *la gestion des frontières*, d'autre part;

- être **conforme aux règles prévues par les actes juridiques de l'UE** portant création des agences, offices et organes de l'Union, réglementant leurs activités ou encore prévues par le cadre de la protection des données de l'UE.

17. À cet égard, le **point (2) de l'annexe** des directives de négociation précise que l'accord doit prévoir les mesures de sauvegarde et garanties nécessaires pour autoriser l'accès contrôlé aux bases de données SLTD et TDAWN par l'intermédiaire de l'[ESP] pour les États membres et les

agences de l'UE, dans la mesure nécessaire à l'accomplissement de leurs tâches, dans le respect de leurs droits d'accès, au droit de l'Union ou au droit national régissant cet accès et dans le strict respect des exigences de l'Union en matière de protection des données et des droits fondamentaux» (caractères gras ajoutés). Le CEPD estime que ce passage manque de clarté, étant donné que d'autres directives de négociation abordent déjà l'accès à ces bases de données par Frontex (ETIAS et le personnel de catégorie 1 de Frontex), Europol et le Parquet européen[22]. Le **CEPD est d'avis que la nécessité pour les autres agences de l'UE d'avoir un tel accès n'a pas été démontrée**. Si elle devait être démontrée[23], **les directives de négociation devraient indiquer clairement les agences de l'UE qui devraient disposer de droits d'accès aux fins de la conduite de leurs tâches ou missions spécifiques**.

18. Qui plus est, en ce qui concerne Frontex, le **considérant 13** de la recommandation renvoie à l'article 68, paragraphe 1, du règlement Frontex comme base juridique appropriée pour la coopération de Frontex avec Interpol et indique que, conformément à son article 82, paragraphe 1, l'accès aux bases de données d'Interpol (notamment la base de données SLTD) devrait être accordé aux membres des équipes de catégorie 1 pour s'acquitter des tâches et exercer les compétences en matière de contrôle aux frontières prévues à l'article 8, paragraphe 3, point a) i), à l'article 8, paragraphe 3, point a) ii), et à l'article 6, paragraphe 1, point e), du règlement (UE) 2016/399 du Parlement européen et du Conseil[24] (le «code frontières Schengen»). Conformément à ces dispositions, ces membres du personnel de Frontex peuvent effectuer des vérifications concernant des ressortissants de pays tiers dans les bases de données d'Interpol, en particulier la SLTD, aux frontières extérieures des États membres et des pays tiers associés à la mise en œuvre, à l'application et au développement de l'acquis de Schengen en matière de contrôle des personnes aux frontières extérieures. Cette dernière disposition comprend, entre autres conditions d'entrée pour les ressortissants de pays tiers, la condition selon laquelle les ressortissants de pays tiers ne sont pas considérés comme constituant une menace pour l'ordre public, la sécurité intérieure, la santé publique ou les relations internationales de l'un des États membres. La recommandation semble cependant aller au-delà du champ d'application de cette disposition lorsqu'elle indique, dans son exposé des motifs[25], que cet accès servira non seulement aux contrôles aux frontières, mais également à prévenir les infractions terroristes et à mener les enquêtes en la matière. Par conséquent, le **CEPD recommande de préciser dans la recommandation les finalités pour lesquelles cet accès devrait être accordé, en veillant à la cohérence avec l'article 10, point q), et l'article 90 du règlement Frontex, dans le cas où lesdites finalités incluent la prévention des infractions terroristes et les enquêtes en la matière. Le mandat devrait également préciser les bases de données qui devraient être consultées par les membres des équipes de catégorie 1 et à quelles fins.** En tout état de cause, conformément à la base juridique mentionnée au considérant 13, le CEPD note que l'accord envisagé ne couvrirait que l'accès aux bases de données d'Interpol pour les contrôles des ressortissants de pays tiers.

19. Plus généralement, le CEPD estime que l'accord envisagé ne devrait pas contraindre les agences de l'UE à coopérer avec Interpol au-delà de ce qui est déjà prévu dans le droit de l'Union applicable.

20. Enfin, il convient de préciser si la notion d'«**informations opérationnelles**» figurant au **point 7) de l'annexe** à la recommandation fait référence à toute information recueillie et analysée au cours des opérations, y compris à des fins administratives (telles que les entretiens ou le traitement administratif des personnes entrantes, etc.) ou s'entend comme des «données opérationnelles à caractère personnel» au sens du règlement (UE) 2018/1725, c'est-à-dire des données à caractère personnel traitées par les organes, offices ou agences de l'Union lorsqu'ils mènent des activités relevant de la coopération judiciaire en matière pénale et de la coopération policière au sens du TFUE, afin d'atteindre les objectifs et de remplir les tâches ou missions qui

leur sont confiés dans les actes juridiques en portant création. **À cet égard, la formulation utilisée au point 7) de l'annexe reste très large, de sorte qu'elle pourrait être interprétée comme donnant mandat pour établir une coopération plus étendue que ce qui est déjà prévu par le droit dérivé de l'Union**.

3. Sur la nécessité de prévoir des mesures de sauvegarde appropriées en matière de protection des données

21. L'acquis de l'Union européenne en matière de protection des données, qui doit être interprété à la lumière de l'article 8 de la Charte et de l'article 16 du TFUE, dispose, en règle générale, que les transferts internationaux de données peuvent être réalisés à destination d'une organisation internationale sans exigences supplémentaires uniquement dans le cas où ladite organisation internationale garantit un niveau de protection adéquat. Lorsque l'organisation internationale n'a pas été déclarée adéquate, des exceptions s'appliquent aux transferts spécifiques, jusqu'à ce que les garanties appropriées soient apportées.

22. En conséquence, en l'absence de décision d'adéquation concernant Interpol, l'accord envisagé pourrait prévoir une base juridique permettant le transfert de données à caractère personnel à Interpol **à la condition** qu'il soit **juridiquement contraignant et opposable à toutes les parties à l'accord et qu'il s'accompagne de mesures de sauvegarde appropriées en matière de protection des données.** Conformément à l'article 46 du règlement (UE) 2018/1725, tout transfert de données à caractère personnel par les institutions, agences et offices de l'UE vers des organisations internationales doit également remplir les conditions des autres dispositions du règlement. Par conséquent, chaque transfert doit respecter les principes de protection des données énoncés à l'article 4 et se prévaloir d'une base juridique parmi celles prévues aux articles 5 et 10 (en ce qui concerne les catégories particulières de données). Il convient donc d'adopter une approche en deux étapes: premièrement, le traitement des données devrait être légal conformément à toutes les dispositions pertinentes du règlement et, dans un second temps, les dispositions du chapitre V doivent être respectées. L'article 46 dispose qu'un transfert de données vers une organisation internationale ne porte pas atteinte au niveau de protection garanti par le présent règlement et, plus particulièrement, que **les personnes concernées doivent se voir garantir des droits opposables et effectifs**[26].

23. Le CEPD se félicite que plusieurs directives de négociation figurant en annexe fassent référence à la garantie d'une coopération dans le strict respect des exigences de l'UE en matière de protection des données et de droits fondamentaux. Il convient toutefois de préciser dans le mandat que cette expression «*dans le strict respect des exigences de l'UE en matière de protection des données et des droits fondamentaux*», comprend les trois niveaux de conformité suivants:

    – de manière générale avec la Charte, ce qui inclut notamment ses articles 7, 8 et 52;

    – avec la législation horizontale pertinente en matière de protection des données: avec le règlement (UE) 2018/1725, la directive (UE) 2016/680 et le règlement (UE) 2016/679;

    – avec les exigences et garanties spécifiques en matière de protection des données prévues dans les actes de base instituant les agences ou systèmes informatiques de l'UE.

24. Sur ce point, le CEPD souligne que l'article 94 du règlement (UE) 2018/1725 s'applique au transfert de données opérationnelles à des fins répressives, à l'exception du Parquet européen

et d'Europol, auxquels s'appliquent leurs règlements respectifs. Par conséquent, le **considérant 16** consacré aux transferts de données opérationnelles est bienvenu, mais semble **incomplet,** dans la mesure où il ne fait pas référence aux dispositions spécifiques relatives aux transferts de données opérationnelles par Europol et le Parquet européen, lesquels ne sont pas concernés par le règlement (UE) 2018/1725, mais par les règlements Europol et du Parquet européen. Il convient par ailleurs d'ajouter une **référence au règlement Eurojust** étant donné que les règles générales du chapitre distinct du règlement (UE) 2018/1725 relatif au traitement des données opérationnelles s'appliquent sans préjudice des règles spécifiques en matière de protection des données contenues dans le règlement Eurojust[27].

25. Dans le même temps, le CEPD se félicite de ce que le point c) de l'annexe dispose que l'accord doit «*définir clairement et précisément les mesures de sauvegarde et les contrôles nécessaires à la protection des données à caractère personnel, des libertés et droits fondamentaux des personnes, indépendamment de la nationalité et du lieu de résidence, dans l'échange de données à caractère personnel avec Interpol*» et mentionne, aux points i) à xi), certains principes et mesures de sauvegarde. Il insiste cependant sur l'importance de prévoir des **mesures de sauvegarde concrètes, spécifiques et efficaces pour chaque type de coopération prévus dans l'accord**. Compte tenu du contexte répressif et des risques potentiels que ces transferts de données pourraient présenter pour les personnes concernées, les garanties prévues dans ce futur accord avec Interpol devraient prévoir et atténuer ces risques de manière satisfaisante.

26. L'approche globale comporte des risques particuliers pour les droits fondamentaux: premièrement, le risque d'abaisser le niveau de protection conféré par le cadre juridique actuel de l'UE et, deuxièmement, de créer une insécurité juridique. **Les directives de négociation, notamment au point c) consacré aux garanties et contrôles nécessaires, n'établissent pas de distinction claire entre les différents types d'activités et le traitement des données,** même s'ils sont régis par différents instruments juridiques[28], et requièrent donc des ensembles appropriés de garanties et d'exigences adaptées à chaque «scénario», le cas échéant. Sur ce point, le CEPD souhaite attirer l'attention sur le fait que la Commission européenne a suivi une approche différente en ce qui concerne le droit dérivé de l'UE s'agissant de l'accès aux bases de données SLTD et TDAWN d'Interpol par l'intermédiaire de l'ESP pour les frontières et les visas, d'une part, et pour la coopération policière, d'autre part. Cet accès a été établi par deux règlements distincts [règlements (UE) 2019/817 et 2019/818], ainsi que l'explique la Commission européenne dans les propositions relatives à ces instruments, 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 [...]».

27. Dans ce contexte, le CEPD recommande que le **considérant 17** de la recommandation **fasse également référence aux dispositions relatives à la protection des données des instruments portant création des agences et offices de l'Union concernés par l'accord envisagé.** Le cadre juridique de l'UE en matière de protection des données se compose en effet de plusieurs sources juridiques différentes, parmi lesquelles une série de dispositions du droit dérivé de l'Union qui s'appliquent à des transferts spécifiques de données, interdisant en principe les transferts vers des organisations internationales et ne les autorisant qu'à titre dérogatoire dans des conditions strictes[29].

28. En ce qui concerne **Europol**, le CEPD invite le Conseil à veiller à ce que l'accord envisagé ne descende pas en dessous du niveau des mesures de sauvegarde de la protection des données prévues par le règlement Europol (lequel fait explicitement référence à la coopération et à l'échange d'informations, y compris de données à caractère personnel, entre Interpol et Europol)

et par l'accord bilatéral en vigueur. À titre d'illustration, le point c) ii) de l'annexe prévoit que «*[l]'accord doit prévoir la possibilité d'indiquer, lors du transfert des données, toute restriction d'accès ou d'utilisation, y compris une restriction relative au transfert, à l'effacement ou à la destruction des données*». En ce qui concerne ces restrictions, l'article 19, paragraphe 2, du règlement Europol dispose également que, *«[l]orsque la nécessité d'appliquer ces limitations apparaît après la fourniture des informations, [les organisations internationales] en informent Europol. Europol se conforme à ces limitations.*» **Cette obligation d'information devrait également figurer dans l'accord envisagé**. Le point iv) de l'annexe dispose que «[l*]'accord doit préciser les critères au regard desquels seront indiquées la fiabilité de la source et l'exactitude des données*». Toutefois, le règlement Europol contient déjà une disposition spécifique sur la fiabilité et l'exactitude de la source des informations émanant d'un État membre (article 29), laquelle précise, en vertu du paragraphe 5*, que «[l]e présent article s'applique mutatis mutandis lorsqu'Europol reçoit des données ou des informations [...] d'une organisation internationale* [...]». **Les directives de négociation devraient être modifiées de façon à préciser que l'accord envisagé ne devrait pas porter atteinte aux critères énoncés dans le règlement Europol qui portent sur la fiabilité et l'exactitude de la source d'information**[30]. **Dans le même ordre d'idées, en ce qui concerne les autres agences et organes inclus dans la recommandation, d'autres modifications seront nécessaires pour veiller à ce que les dispositions pertinentes relatives à la responsabilité de l'exactitude des informations fournies dans le cadre de leurs mandats respectifs ne soient pas compromises par le futur accord UE-Interpol.**

29. En ce qui concerne **Eurojust**, les articles 47 et 56 (Principes généraux pour les transferts de données opérationnelles à caractère personnel vers des pays tiers ou à des organisations internationales) fixent également des exigences spécifiques et obligatoires pour la coopération impliquant le transfert de données à caractère personnel vers une organisation internationale, y compris des règles strictes en matière de transferts ultérieurs.

30. En ce qui concerne le **Parquet européen**, conformément à l'article 80 (Principes généraux applicables aux transferts de données opérationnelles à caractère personnel) du règlement du Parquet européen, «[l]*e Parquet européen ne peut transférer des données opérationnelles à caractère personnel vers un pays tiers ou à une organisation internationale, sous réserve du respect des autres dispositions du présent règlement, en particulier de l'article 53, que lorsque les conditions définies aux articles 80 à 83 sont respectées*».

31. **Qui plus est**, le CEPD souligne qu'il importe de prévoir des mesures de sauvegarde suffisantes pour garantir que les informations transmises par Interpol sont **correctes et complètes**, étant donné qu'elles seront utilisées pour prendre des décisions concernant des personnes (par exemple, dans le cadre de l'ETIAS, les personnes pourraient se voir refuser l'entrée sur le territoire de l'UE).

32. **Le CEPD recommande en outre d'inclure** dans l'annexe au minimum les mesures de sauvegarde suivantes:

- l'accord envisagé devrait préciser **quand et dans quelles circonstances des décisions individuelles automatisées sont** autorisées (ou non) [**lettre viii), point c)**];

- **de plus amples détails sont nécessaires sur l'obligation d'Interpol de notifier en cas de violation de données à caractère personnel** [**lettre ix), point c)**]. Le texte dans sa version actuelle ne précise pas qui doit informer qui, ni qui informe les personnes concernées. En fonction de la nature de la violation de données à caractère personnel, il convient de préciser quand et si Interpol doit informer les autorités compétentes (par

exemple, l'agence de l'UE qui a communiqué les informations, son organe de contrôle) et, le cas échéant, les personnes concernées. En outre, l'accord devrait inclure une description des informations minimales à fournir lors de la notification de la violation (à l'organe de contrôle et à la personne concernée); et

– **il convient de fournir davantage de détails opérationnels sur les mesures techniques et organisationnelles prises pour assurer la sécurité** des données à caractère personnel, notamment sur la manière dont la confidentialité des communications électroniques serait assurée.

33. En ce qui concerne l'«**échange d'informations opérationnelles**» avec Interpol, la recommandation ne précise pas suffisamment les modalités, conditions, limites et portée des données transférées à Interpol, y compris les données à caractère personnel. Cette question est aggravée par la possibilité de **transferts ultérieurs** d'Interpol vers d'autres organisations internationales ou des pays tiers, y compris ceux pour lesquels aucune décision d'adéquation n'a été prise, conformément au **point c), lettre x),** de l'annexe. En effet, en ce qui concerne les données à caractère personnel transférées par les agences et organes de l'UE, conformément à l'article 46 du règlement (UE) 2018/1725, un transfert de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert à une organisation internationale ne peut avoir lieu que si, sous réserve des autres dispositions dudit règlement, les conditions définies dans le chapitre V de ce même règlement, sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ d'une organisation internationale vers un autre pays tiers ou à une autre organisation internationale, de manière à ce que le niveau de protection des personnes physiques garantit par ledit règlement ne soit pas compromis.

34. Plus particulièrement, **le CEPD recommande d'inclure dans les directives de négociation les mesures de sauvegarde portant sur les transferts ultérieurs:**

– le fait que le transfert de données à caractère personnel sera soumis à des **obligations de confidentialité**; et

– le fait que les données à caractère personnel ne seront pas utilisées pour demander, **prononcer ni exécuter une peine de mort ou toute forme de traitement cruel et inhumain**[31].

35. Par ailleurs, des **dérogations** sont prévues à l'article 50 du règlement (UE) 2018/1725 pour autoriser l'exécution d'un transfert en dépit de l'absence de décision d'adéquation ou de mesures de sauvegarde appropriées, si cela est nécessaire pour protéger les intérêts vitaux d'une personne. Toutefois, ce n'est que lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement et elle ne prévoit pas de dérogation aux fins de prévenir une menace grave et immédiate pour la sécurité publique. En outre, aucune dérogation n'est prévue en ce qui concerne le transfert de données opérationnelles au titre de l'article 94 du règlement (UE) 2018/1725. Ce n'est que dans le cadre de la directive (UE) 2016/680 qu'une dérogation fondée sur la sécurité publique d'un État membre ou d'un pays tiers est prévue [article 38, paragraphe 1, point c)]. **Le CEPD recommande donc de limiter l'application des dérogations pour les transferts ultérieurs aux cas déjà autorisés pour les agences et organes de l'UE concernés lors du transfert des données à caractère personnel.** Sur ce point, le CEPD rappelle une fois encore qu'il est nécessaire de veiller au respect **des exigences spécifiques établies par les règlements portant création de l'agence ou de l'office de l'UE concerné**.

36. Les directives de négociation se bornent à énoncer, au **point c), lettre x)**, de l'annexe, que «*les transferts ultérieurs d'informations d'Interpol à d'autres organisations internationales ou vers des pays tiers ne doivent être autorisés qu'aux fins de l'accord, doivent être soumis à des conditions appropriées*», tandis que, par exemple, l'article 23, paragraphe 7, du **règlement Europol** dispose que «[l]*es transferts ultérieurs de données à caractère personnel détenues par Europol, [...] et les organisations internationales sont interdits,* ***à moins qu'Europol ne les ait explicitement autorisés au préalable***» (caractères gras ajoutés). L'article 47 du règlement **Eurojust** prévoit des mesures de sauvegarde en matière de transferts ultérieurs, sur lesquelles l'accord envisagé devra être aligné. Plus particulièrement, l'article 47, paragraphe 6, du règlement Eurojust dispose clairement que «*[l]orsque [...] des organisations internationales ont reçu des données à caractère personnel d'Eurojust, le transfert ultérieur de ces données à un tiers est interdit, sauf si toutes les conditions suivantes sont remplies:*

(a) Eurojust a obtenu le consentement préalable de l'État membre qui a fourni ces données;

(b) Eurojust a donné son consentement explicite après examen des circonstances de l'espèce;

(c) le transfert ultérieur a lieu uniquement dans un but précis qui n'est pas incompatible avec la finalité pour laquelle les données ont été transmises» (caractères gras ajoutés).

37. Qui plus est, l'article 80, paragraphe 1, point e), du **règlement du Parquet européen** dispose que, «*en cas de transfert ultérieur vers un autre pays tiers ou à une autre organisation internationale, par un pays tiers ou une organisation internationale, le Parquet européen exige du pays tiers ou de l'organisation internationale qu'il lui demande une autorisation préalable pour ce transfert ultérieur, autorisation que le Parquet européen ne peut accorder qu'après avoir dûment pris en considération l'ensemble des facteurs pertinents, y compris la gravité de l'infraction pénale, la finalité pour laquelle les données opérationnelles à caractère personnel ont été transférées initialement et le niveau de protection des données à caractère personnel dans le pays tiers ou au sein de l'organisation internationale vers lequel/laquelle les données opérationnelles à caractère personnel sont transférées ultérieurement*».

38. Pour finir, le CEPD note que le **point e) de l'annexe** à la recommandation prévoit la possibilité de suspendre ou de dénoncer l'accord en question. **Le CEPD recommande de préciser dans le mandat que l'accord devrait prévoir cette possibilité en cas de violation de ses dispositions relatives aux données à caractère personnel par l'une des parties et que les données à caractère personnel relevant du champ d'application de l'accord transférées avant sa suspension ou sa dénonciation peuvent continuer à être traitées conformément à l'accord.**

4. Sur la base juridique de la future décision du Conseil

39. Il ressort de l'exposé des motifs de la recommandation[32] que l'objet du futur accord relèverait notamment du domaine des instruments relatifs à la protection des données (article 16 du TFUE). Les visas du préambule de la recommandation ne font toutefois pas référence à la base juridique matérielle de l'acte juridique.

40. Conformément à l'article 296, deuxième alinéa, du TFUE et à la jurisprudence constante de la CJUE[33], le CEPD s'interroge sur le fait que les visas cités dans le préambule de la recommandation font certes référence aux bases juridiques procédurales appropriées, mais ne font pas de la même manière référence aux bases juridiques matérielles pertinentes.

41. **Le CEPD recommande que les visas cités dans le préambule de la recommandation fassent non seulement référence à la base juridique procédurale adéquate mais également à la base juridique matérielle pertinente, notamment à l'article 16 du TFUE.** Il s'ensuit de l'annexe portant sur les directives de négociation que la Commission devrait poursuivre plusieurs objectifs simultanément lors des négociations en vue de l'accord envisagé, parmi lesquels garantir le respect des droits fondamentaux inscrits dans la Charte, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel afin de permettre le transfert des données à caractère personnel en toute légalité. De cette manière, l'accord envisagé serait directement en rapport avec les objectifs visés par l'article 16 du TFUE.

42. Le CEPD rappelle que, dans un contexte répressif similaire, la Cour de justice de l'Union européenne a conclu que «*la décision du Conseil relative à la conclusion de l'accord envisagé [entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers] doit être fondée conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), TFUE*»[34].

5. Conclusions

43. Le CEPD se félicite que l'accord devrait garantir le strict respect des droits fondamentaux et observer les principes qui sont consacrés par la Charte, en particulier le droit à la vie privée et familiale, prévu à l'article 7 de la Charte, le droit à la protection des données à caractère personnel, prévu à l'article 8 de la Charte, et le droit à un recours effectif et à accéder à un tribunal impartial, consacrés par l'article 47 de la Charte.

44. Il convient cependant de préciser dans le mandat que l'accord devrait inclure les trois niveaux de conformité suivants:

- de manière générale, avec la Charte;
- avec la législation horizontale pertinente en matière de protection des données: avec le règlement (UE) 2018/1725, la directive (UE) 2016/680 et le règlement (UE) 2016/679;
- avec les exigences et garanties spécifiques en matière de protection des données prévues dans les actes de base instituant les agences ou systèmes informatiques de l'UE.

45. En outre, l'objectif consistant à soutenir une coopération (existante et à venir) importante entre l'UE et Interpol au moyen d'un instrument juridique unique rend l'accord envisagé très hétérogène par nature, englobant un large éventail d'activités. Le CEPD insiste dès lors sur la nécessité d'une analyse d'impact approfondie et souligne que cette approche ne devrait pas conduire à affaiblir les libertés et droits fondamentaux des personnes physiques, plus particulièrement leurs droits à la protection des données et à la vie privée.

46. En l'absence de décision d'adéquation concernant Interpol, l'accord envisagé pourrait constituer une base juridique permettant le transfert de données à caractère personnel à Interpol à la condition qu'il soit juridiquement contraignant et opposable à toutes les parties à l'accord et qu'il s'accompagne de mesures de sauvegarde appropriées en matière de protection des données.

47. Le CEPD estime que la mise en place de mesures de sauvegarde appropriées implique que l'accord international conclu avec Interpol devrait:

- veiller au respect des mesures de sauvegarde introduites dans la législation existante de l'UE pour ce qui concerne le transfert par les agences et organes de l'UE concernés et les transferts ultérieurs de données à caractère personnel, y compris les dispositions spécifiques relatives aux transferts de données opérationnelles par Europol et le Parquet européen. Plus particulièrement, dans le contexte des transferts ultérieurs, il convient de prévoir explicitement que les données à caractère personnel transférées par l'UE à Interpol ne seront pas utilisées pour demander, prononcer ni exécuter une peine de mort ou toute forme de traitement cruel et inhumain;

- préciser explicitement qu'il n'y aura pas d'accès réciproque, direct ou indirect, d'Interpol aux bases de données de l'UE;

- préciser quand et dans quelles circonstances des décisions individuelles automatisées sont autorisées (ou non);

- offrir davantage de détails sur l'obligation d'Interpol de notifier une violation de données à caractère personnel;

- fournir davantage de détails opérationnels sur les mesures techniques et organisationnelles prises pour assurer la sécurité des données à caractère personnel.

48. Qui plus est, le CEPD recommande de préciser dans le mandat la possibilité de suspendre ou de dénoncer l'accord en cas de violation de ses dispositions relatives aux données à caractère personnel par l'une des parties et que les données à caractère personnel relevant du champ d'application de l'accord transférées avant sa suspension ou sa dénonciation peuvent continuer à être traitées conformément à l'accord.

49. Pour finir, le CEPD recommande que les visas cités dans le préambule de la décision du Conseil fassent non seulement référence à la base juridique procédurale adéquate mais également à la base juridique matérielle pertinente, notamment à l'article 16 du TFUE.

Bruxelles, le 25 mai 2021

Wojciech Rafał WIEWIÓROWSKI

[signature électronique]

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 119 du 4.5.2016, p. 89.
[3] JO L 295 du 21.11.2018, p. 39.
[4] Statut de l'O.I.P.C.-Interpol [I/CONS/GA/1956 (2017)].
[5] Communication de la Commission au Parlement européen, au Conseil européen, au Comité économique et social européen et au Comité des régions relative à la stratégie de l'UE pour l'union de la sécurité, Bruxelles, 24.7.2020, COM(2020) 605 final.
[6] COM(2021) 177 final.
[7] Page 8.
[8] 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) (le «règlement Europol»). Ainsi que cela est indiqué dans l'exposé des motifs, un accord de coopération avec Interpol qui prévoit l'échange de données à caractère personnel a déjà été conclu en 2001, bien avant l'entrée en vigueur du règlement Europol. Toutefois, l'accord ne permet pas à Europol d'accéder directement ou indirectement aux informations et aux bases de données d'Interpol, et notamment aux notices contenant des informations sur les terroristes. En outre, l'Agence ne peut échanger des informations avec Interpol et avoir accès à ses bases de données pour l'exécution de ses tâches que par l'intermédiaire de l'officier de liaison d'Interpol détaché auprès d'elle ou de son officier de liaison détaché auprès d'Interpol. Cet accord a été complété ultérieurement par plusieurs documents relatifs à la coopération approuvés par les organisations ou conclus entre elles, concernant, par exemple, la coopération par l'intermédiaire des officiers de liaison et l'établissement, la mise en œuvre et l'exploitation d'une ligne de communication sécurisée pour l'échange d'informations.
[9] Après l'adoption des règlements relatifs à l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas, à savoir 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 (JO L 135 du 22.5.2019, p. 27) et 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 (JO L 135 du 22.5.2019, p. 85).
[10] Frontex désigne l'Agence européenne de garde-frontières et de garde-côtes. Règlement (UE) 2019/1896 du Parlement européen et du Conseil du 13 novembre 2019 relatif au corps européen de garde-frontières et de garde-côtes et abrogeant les règlements (UE) nº 1052/2013 et (UE) 2016/1624 (JO L 295 du 14.11.2019, p. 1) (le «règlement Frontex»).
[11] 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); proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 767/2008, le règlement (CE) nº 810/2009, le règlement (UE) 2017/2226, le règlement (UE) 2016/399, le règlement (UE) XX/2018 [règlement sur l'interopérabilité] et la décision 2004/512/CE et abrogeant la décision 2008/633/JAI du Conseil (COM/2018/302 final) et voir accord politique: https://data.consilium.europa.eu/doc/document/ST-5537-2021-INIT/en/pdf
[12] Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen (JO L 283 du 31.10.2017, p. 1) (le «règlement du Parquet européen»).
[13] Conformément à l'article 54 du règlement Frontex, le contingent permanent du corps de garde-frontières et de garde-côtes européens se compose de quatre catégories de personnel opérationnel. La catégorie 1 comprend les membres du personnel statutaire déployés en tant que membres des équipes dans des zones d'opération, conformément à l'article 55 dudit règlement. L'Agence contribue au contingent permanent en mettant à disposition des membres de son personnel statutaire (catégorie 1) destinés à être déployés dans des zones d'opération en tant que membres des équipes accomplissant les tâches et exerçant les compétences prévues à l'article 82 dudit règlement. Leurs missions comprennent la lutte contre la criminalité transfrontalière et le terrorisme.
[14] Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO L 295 du 21.11.2018, p. 138) (le règlement «Eurojust»).
[15] À ce jour, 22 États membres contribuent à une coopération renforcée dans le cadre de la création du Parquet européen.
[16] Voir, par exemple, dans le contexte des propositions de la Commission visant à modifier les instruments juridiques des systèmes d'information de l'UE à la suite de l'adoption du règlement (UE) 2018/1240 portant création d'un système

européen d'information et d'autorisation concernant les voyages (ETIAS), l'étude d'impact de substitution ciblée demandée par la commission LIBE du Parlement européen:
https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)642808.

[17] Voir le Guide du CEPD pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf
et les Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, à l'adresse: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[18] À cet égard, voir l'avis 1/15 de la Cour de justice de l'Union européenne (ci-après la «CJUE») (grande chambre) du 26 juillet 2017, accord PNR UE-Canada, EU:C:2017:592, points 77 et 78: «77. Si l'examen d'un acte de l'Union démontre que ce dernier poursuit une double finalité ou qu'il a une double composante et si l'une de celles-ci est identifiable comme étant principale ou prépondérante, tandis que l'autre n'est qu'accessoire, l'acte doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou la composante principale ou prépondérante. À titre exceptionnel, s'il est établi, en revanche, que l'acte poursuit à la fois plusieurs objectifs ou a plusieurs composantes qui sont liés de façon indissociable, sans que l'un soit accessoire par rapport à l'autre, de telle sorte que différentes dispositions des traités sont applicables, une telle mesure doit être fondée sur les différentes bases juridiques correspondantes (arrêt du 14 juin 2016, Parlement/Conseil, C-263/14, EU:C:2016:435, point 44 et jurisprudence citée).
78. Toutefois, le recours à une double base juridique est exclu lorsque les procédures prévues pour l'une et l'autre de ces bases sont incompatibles (arrêt du 6 novembre 2008, Parlement/Conseil, C-155/07, EU:C:2008:605, point 37 et jurisprudence citée)».

[19] Voir l'étude demandée par la commission DROI du Parlement européen, «Misuse of Interpol's red notices and impact on human rights, recent developments» (Utilisation abusive des notices rouges d'Interpol et incidence sur les droits de l'homme, évolutions récentes), janvier 2019, disponible à l'adresse:
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf

[20] Voir l'avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, EU:C:2017:592.

[21] Caractères gras ajoutés. Voir considérant 7 de la recommandation.

[22] Points 3) et 6) de l'annexe à la recommandation.

[23] Par exemple, à la suite de l'analyse d'impact sur les droits fondamentaux de substitution, supra, note 16.

[24] Règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes (code frontières Schengen) (JO L 77 du 23.3.2016, p. 1).

[25] Page 5.

[26] Ils sont répertoriés à l'adresse: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en

[27] Considérant 29 du règlement Eurojust.

[28] Pour ce qui concerne la protection des données: Directive (UE) 2016/680 en cas d'échange de données à caractère personnel par les autorités compétentes des États membres 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 avec Interpol; règlement (UE) 2016/679 en cas d'échange de données à caractère personnel par les autorités publiques d'autres États membres avec Interpol, règlement (UE) 2018/1725 en cas d'échange de données à caractère personnel par les institutions, bureaux, agences et organes de l'UE avec Interpol, et notamment son chapitre IX, article 94, en cas de transfert de données opérationnelles à caractère personnel à Interpol par des organes et organismes de l'Union exerçant des activités relevant du champ d'application du chapitre 4 ou du chapitre 5 du titre V du TFUE (coopération judiciaire en matière pénale ou coopération policière), ainsi que des dispositions spécifiques relatives à la protection des données figurant dans des instruments distincts, tels que les règlements Europol.

[29] Voir, par exemple, l'article 31 du règlement (CE) nº 767/2008 du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur des visas de court séjour (JO L 218 du 13.8.2008, p. 60).

[30] L'article 29, paragraphes 1 et 2, Évaluation de la fiabilité de la source et de l'exactitude des informations, du règlement Europol
dispose ce qui suit:
«*1. La fiabilité de la source des informations émanant d'un État membre est évaluée, dans la mesure du possible, par l'État membre qui les fournit, en utilisant les codes d'évaluation des sources suivants:*
(A): il n'existe aucun doute quant à l'authenticité, à la fiabilité et à la compétence de la source, ou l'information provient d'une source qui s'est révélée fiable dans tous les cas;
(B): l'information provient d'une source qui s'est révélée fiable dans la plupart des cas;
(C): l'information provient d'une source qui s'est révélée non fiable dans la plupart des cas;
(X): la fiabilité de la source ne peut être évaluée.
2. L'exactitude des informations émanant d'un État membre est évaluée, dans la mesure du possible, par l'État membre qui les fournit, en utilisant les codes d'évaluation des informations suivants:
(1): aucun doute n'est permis quant à l'exactitude de l'information;

(2): la source a eu directement connaissance de l'information, mais le fonctionnaire qui la transmet n'en a pas eu directement connaissance;
(3): la source n'a pas eu directement connaissance de l'information, mais celle-ci est corroborée par d'autres informations déjà enregistrées;
(4): la source n'a pas eu directement connaissance de l'information et celle-ci ne peut être corroborée d'aucune manière».

[31] Voir le considérant 71 de la directive (UE) 2016/680 en ce qui concerne les critères à prendre en considération lors de l'évaluation de l'existence de mesures de sauvegarde appropriées dans un contexte répressif en l'absence d'une décision d'adéquation.

[32] Voir la section 3, p. 9, de la recommandation.

[33] Voir l'arrêt du 25 octobre 2017, Commission européenne/Conseil de l'Union européenne, affaire C-687/15, EU:C:2017:803, points 48 et suivants.

[34] Avis 1/15 du 26 juillet 2017, Accord PNR UE-Canada, EU:C:2017:592, point 232.