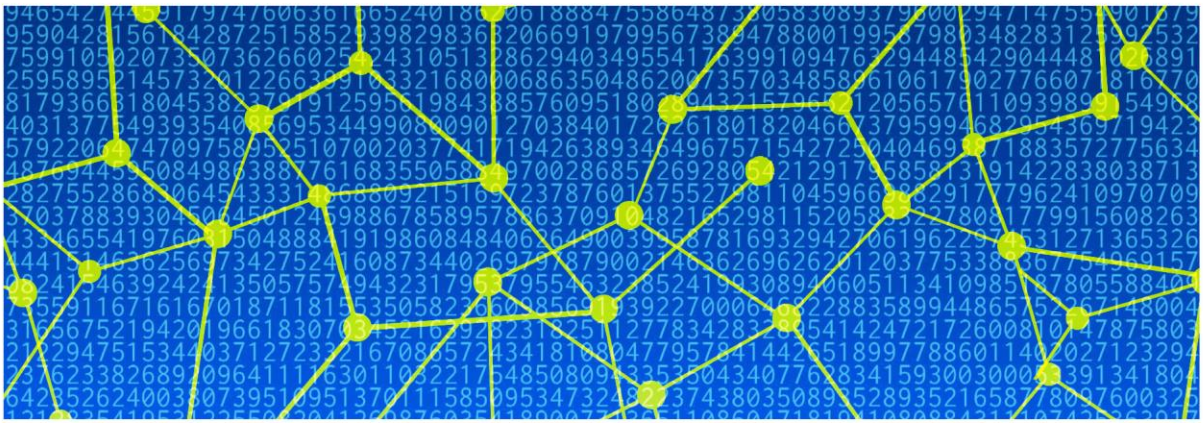

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 2/2018

Avis du CEPD sur huit mandats de négociation en vue de la conclusion d'accords internationaux autorisant l'échange de données entre Europol et des pays tiers

EDPS

14 mars 2018

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[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 vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, «[l]orsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel», de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mandat spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

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 dans le secteur répressif, conformément à l'action nº 5 de la stratégie du CEPD: «Intégrer la protection des données dans les politiques internationales».

Synthèse

La Commission a publié huit recommandations suggérant au Conseil d'autoriser l'ouverture de négociations entre l'Union européenne et, respectivement, l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie en vue de conclure des accords internationaux sur l'échange de données à caractère personnel entre Europol et les autorités de ces huit pays tiers compétentes pour lutter contre les formes graves de criminalité et le terrorisme. Ces accords internationaux constitueraient le cadre juridique nécessaire pour autoriser Europol à transférer des données à caractère personnel aux autorités de ces pays tiers. Les annexes de ces recommandations fixent les directives du Conseil pour négocier chacun des huit accords internationaux envisagés et établissent les mandats confiés à la Commission.

Les accords internationaux autorisant Europol et les pays tiers à coopérer et à échanger des données à caractère personnel doivent satisfaire aux principes de nécessité et de proportionnalité prévus à l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne. Ils doivent établir un juste équilibre entre la nécessité de lutter contre les formes graves de criminalité et le terrorisme et la protection efficace des données à caractère personnel et autres droits fondamentaux garantis par la charte. Le CEPD formule des recommandations pour garantir le respect de ces exigences élevées.

En outre, le règlement Europol fixe des règles spécifiques concernant les transferts de données effectués par Europol en dehors de l'Union européenne. Europol pourrait transférer régulièrement des données vers un pays tiers sur la base d'un accord international contraignant conclu entre l'Union européenne et le pays tiers en question, à condition qu'un tel accord offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et des droits fondamentaux des personnes. Dans le présent avis, le CEPD énonce également des recommandations générales afin de garantir que les accords négociés offriront des garanties appropriées au sens du règlement Europol.

De même, le CEPD formule des observations générales et des recommandations spécifiques relatives aux annexes des recommandations de la Commission et aux directives qui y sont fixées, que le Conseil adressera à la Commission pour négocier les accords internationaux avec les pays tiers pour lesquels une coopération avec Europol est envisagée.

Enfin, le CEPD est prêt à donner des conseils supplémentaires tant au cours des négociations qu'avant la finalisation de ces huit accords internationaux.

TABLE DES MATIÈRES

1. INTRODUCTION ET CONTEXTE 5

2. RÔLE DU CEPD 6

3. RECOMMANDATIONS GÉNÉRALES 7

3.1. NÉCESSITÉ ET PROPORTIONNALITÉ DES TRANSFERTS DE DONNÉES EFFECTUÉS PAR EUROPOL VERS LES PAYS TIERS 7

3.2. OFFRE DE GARANTIES APPROPRIÉES EN VERTU DU RÈGLEMENT EUROPOL 8

4. RECOMMANDATIONS SPÉCIFIQUES 10

4.1. LIMITATION ET DÉTERMINATION DES FINALITÉS DES TRANSFERTS DE DONNÉES EFFECTUÉS PAR EUROPOL 11

a) Détermination des finalités des transferts de données 11

b) Limitation du traitement ultérieur des données transférées par l'autorité destinataire 12

4.2. TRANSFERTS ULTÉRIEURS 12

4.3. LIMITATIONS SPÉCIFIQUES DU TRAITEMENT DES INFORMATIONS TRANSFÉRÉES PAR EUROPOL 12

4.4. SURVEILLANCE PAR UNE AUTORITÉ INDÉPENDANTE 13

4.5. DROITS DES PERSONNES CONCERNÉES 13

4.6. TRANSFERT DE CATÉGORIES PARTICULIÈRES DE DONNÉES 14

4.7. CONSERVATION DES DONNÉES 15

4.8. SUSPENSION OU DÉNONCIATION DES ACCORDS INTERNATIONAUX EN CAS DE VIOLATION 15

5. CONCLUSION 15

NOTES 18

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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1], et 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)[2],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[3], et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[4], et 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[5],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

Le règlement Europol[6] fixe des règles spécifiques concernant les transferts de données effectués par Europol en dehors de l'Union européenne. Son article 25, paragraphe 1, énumère un certain nombre de fondements juridiques sur lesquels Europol pourrait s'appuyer pour transférer en toute légalité des données aux autorités de pays tiers. L'un de ces fondements serait une décision d'adéquation de la Commission adoptée conformément à l'article 36 de la directive (UE) 2016/680[7], selon laquelle le pays tiers vers lequel Europol transfère des données assure un niveau de protection adéquat. Étant donné qu'il n'existe pas actuellement de telles décisions d'adéquation, un autre fondement sur lequel Europol pourrait s'appuyer pour transférer régulièrement des données vers un pays tiers serait un cadre approprié résultant de la conclusion d'un accord international contraignant entre l'Union européenne et le pays tiers destinataire.

Le 20 décembre 2017, la Commission a adopté huit recommandations[8] de décisions du Conseil autorisant l'ouverture de négociations en vue d'accords internationaux entre l'Union européenne et huit pays tiers de la région du Proche-Orient et de l'Afrique du Nord (MENA), à savoir l'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie. Ces accords internationaux constitueraient le cadre juridique nécessaire à l'échange de données à caractère personnel entre Europol et les autorités de ces pays tiers compétentes pour lutter contre les formes graves de criminalité et le terrorisme.

La Commission estime qu'il est nécessaire de renforcer la coopération entre Europol et ces huit pays compte tenu de la stratégie politique de l'Union européenne exposée dans le programme européen en matière de sécurité[9], les conclusions du Conseil[10] et la stratégie globale pour la politique étrangère et de sécurité de l'Union européenne[11], ainsi que des besoins opérationnels d'Europol et des autorités répressives dans l'ensemble de l'Union européenne. Ces huit pays tiers ont également été identifiés dans le onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective[12]. La coopération avec les pays de la région MENA est envisagée dans le contexte de la région prise dans son ensemble[13]. L'instabilité qui règne actuellement dans cette région, notamment la situation en Syrie et en Iraq, fait peser sur la sécurité de l'Union européenne une importante menace à long terme. Cela concerne tant la lutte efficace contre le terrorisme et la criminalité organisée qui s'y rapporte que les problèmes liés aux migrations tels que l'aide à l'immigration irrégulière et la traite des êtres humains. La coopération avec les autorités répressives locales est également cruciale pour venir à bout de ces problèmes.

Conformément à la procédure prévue à l'article 218 du traité sur le fonctionnement de l'Union européenne (TFUE), la Commission sera chargée de négocier ces accords internationaux avec les pays tiers au nom de l'Union européenne. Avec ces huit recommandations, la Commission cherche à obtenir l'autorisation du Conseil de l'Union européenne (Conseil) pour entamer les négociations avec les huit pays tiers concernés. Une fois les négociations terminées et en vue de conclure formellement ces accords, le Parlement européen devra approuver les textes des accords négociés, tandis que le Conseil devra signer les accords.

2. RÔLE DU CEPD

Le considérant 35 du règlement Europol dispose que «[l]e cas échéant et conformément au règlement (CE) nº 45/2001[14] [...], la Commission devrait pouvoir consulter le Contrôleur européen de la protection des données (CEPD) avant et pendant la négociation d'un accord international» entre l'Union européenne et un pays tiers afin d'autoriser l'échange de données entre Europol et les autorités de ce pays tiers. Le CEPD fait observer qu'il n'a pas été consulté par la Commission sur les huit recommandations et leurs annexes avant leur adoption (mais seulement après leur adoption).

Les annexes de ces recommandations sont de la plus haute importance, car elles fixent les directives du Conseil pour négocier chacun de ces accords internationaux et établissent les mandats confiés à la Commission. Elles visent notamment à déterminer les besoins opérationnels d'Europol qui justifieraient la conclusion d'accords internationaux en vue de l'échange de données avec ces huit pays tiers. Elles devraient également inclure toutes les exigences en matière de protection des données que ces accords internationaux devraient respecter. Étant donné que le CEPD est devenu le seul contrôleur d'Europol le 1er mai 2017 et que, conformément au règlement (CE) nº 45/2001, le CEPD est également le conseiller des institutions de l'Union européenne sur les politiques et les législations relatives à la protection des données, les accords internationaux sur l'échange de données entre Europol et les pays tiers sont particulièrement importants, eu égard au rôle que le CEPD joue en tant que contrôleur de l'agence et que conseiller en matière de protection des données. Pour ces raisons, conformément au considérant 35 du règlement Europol, le CEPD est prêt à donner des conseils supplémentaires à la Commission tant au cours des négociations qu'avant la finalisation de chacun de ces huit accords internationaux.

3. RECOMMANDATIONS GÉNÉRALES

3.1. Nécessité et proportionnalité des transferts de données effectués par Europol vers les pays tiers

Le CEPD se félicite de l'attention accordée à la protection des données dans les annexes des huit recommandations de la Commission.

Le CEPD comprend qu'Europol souhaite renforcer sa coopération avec les pays tiers afin de lutter contre les formes graves de criminalité et le terrorisme. Néanmoins, la nécessité et la proportionnalité des accords internationaux envisagés pour autoriser Europol à transférer régulièrement des données à caractère personnel aux autorités compétentes des huit pays tiers en question doivent être évaluées. Étant donné que les transferts de données à caractère personnel vers des pays tiers portent atteinte aux droits des personnes au respect de la vie privée et à la protection des données garantis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), les exigences de nécessité et de proportionnalité du traitement envisagé doivent être évaluées conformément à l'article 52, paragraphe 1, de la charte. En outre, chaque accord international doit établir un juste équilibre entre la nécessité de lutter contre les formes graves de criminalité et le terrorisme et la protection efficace des données à caractère personnel et autres droits fondamentaux.

Le CEPD se félicite que l'exposé des motifs de chacune des recommandations précise le contexte politique dans le pays tiers en question, y compris ses relations avec l'Union européenne, et les besoins opérationnels exigeant un renforcement de la coopération entre le pays tiers et Europol. Dans ce contexte, la deuxième phrase de la directive 2 de chacune des annexes précise quelque peu les finalités du transfert de données à caractère personnel par Europol vers le pays tiers en question. Cependant, **le CEPD estime que ces finalités devraient être définies plus précisément**. Pour permettre une évaluation approfondie et au cas par cas de la nécessité et de la proportionnalité, **nous recommandons de restreindre et de différencier davantage les besoins de transfert en fonction de la situation particulière de chaque pays tiers et de la réalité sur le terrain**. **Le champ d'application de chaque accord international et les finalités pour lesquelles Europol transférera des données vers chaque pays tiers devraient être davantage précisés en conséquence dans les annexes**.

Les transferts de données à caractère personnel vers des pays tiers afin de prévenir et de combattre les formes graves de criminalité transnationale et le terrorisme pourraient avoir une incidence significative sur la vie des personnes concernées. Les transferts envisagés concernent des informations personnelles recueillies dans le cadre d'enquêtes pénales et traitées ensuite par Europol pour produire des renseignements en matière criminelle. Les transferts de ces informations permettront éventuellement de mettre les personnes concernées sous les projecteurs des services répressifs des pays tiers destinataires et pourraient servir dans le cadre de poursuites pour crimes graves engagées devant les juridictions des pays destinataires et en vertu de leur droit national. **Le CEPD recommande de réaliser de nouvelles analyses d'impact afin d'évaluer en profondeur les risques que présentent les transferts de données à caractère personnel vers chaque pays tiers pour les droits des personnes au respect de la vie privée et à la protection des données, mais aussi pour les autres libertés et droits fondamentaux garantis par la charte, de manière à pouvoir définir précisément les garanties nécessaires.**

Enfin, le CEPD ne dispose pas d'informations concernant le niveau de protection des données à caractère personnel garanti dans les pays tiers pour lesquels une coopération avec Europol est envisagée. Le CEPD se félicite que la Commission encourage[15] tous les pays tiers qui ne l'ont pas encore fait[16] et pour lesquels une coopération avec Europol est envisagée à adhérer à la convention 108 du Conseil de l'Europe[17] dans la directive 8 des annexes. Le CEPD invite la Commission à rassembler ces informations, qui seront importantes pour établir des accords internationaux adaptés à chaque pays tiers en tenant compte de l'état de leur législation en matière de protection des données.

3.2. Offre de garanties appropriées en vertu du règlement Europol

Étant donné qu'il n'existe actuellement pas de décision d'adéquation de la Commission conformément à l'article 36 de la directive (UE) 2016/680, l'article 25, paragraphe 1, point a), du règlement Europol ne peut servir de fondement pour qu'Europol transfère des données vers les pays tiers envisagés[18]. L'autre fondement sur lequel Europol peut s'appuyer pour transférer régulièrement[19] des données vers un pays tiers est un cadre juridique approprié résultant de la conclusion d'un accord international contraignant entre l'Union européenne et le pays tiers destinataire «offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et des droits fondamentaux des personnes» [article 25, paragraphe 1, point b)]. La Commission recommande d'adopter des décisions du Conseil pour autoriser l'ouverture de négociations en vue de la conclusion de tels accords internationaux conformément à l'article 25, paragraphe 1, point b). La question reste de savoir ce que le règlement Europol entend exactement par «offrant des garanties appropriées».

Avant toute chose, le CEPD tient à rappeler une norme de droit de l'Union concernant les accords internationaux conclus par l'Union européenne, à savoir le respect des droits fondamentaux. La Cour de justice de l'Union européenne (CJUE) a constaté à l'égard des accords internationaux conclus par l'Union européenne que «les obligations qu'impose un accord international ne sauraient avoir pour effet de porter atteinte aux principes constitutionnels du traité CE, au nombre desquels figure le principe selon lequel tous les actes communautaires doivent respecter les droits fondamentaux, ce respect constituant une condition de leur légalité»[20]. Non seulement la charte garantit le respect de la vie privée et familiale (article 7), mais elle a également élevé la protection des données au rang de droit fondamental dans le droit de l'Union (article 8). Par conséquent, le CEPD estime que l'offre de garanties suffisantes au regard du droit à la protection des données exige, en premier lieu, que **les pays tiers vers lesquels Europol transférera des données à caractère personnel respectent pleinement l'article 8 de la charte, notamment le principe de limitation de la finalité, le droit d'accès, le droit de rectification et le contrôle par une autorité indépendante, comme la charte le prévoit expressément**.

En outre, la CJUE a récemment défini les conditions dans lesquelles un accord international peut servir de base juridique pour les transferts de données à caractère personnel dans son avis 1/15[21] sur l'accord international relatif au transfert des données des dossiers passagers (PNR) vers le Canada, rendu en juillet 2017. La CJUE a jugé qu'«un transfert de données à caractère personnel depuis l'Union vers un pays tiers ne peut avoir lieu que si ce pays assure un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union» et que «[c]ette exigence vaut, de même, dans le cas de la communication des données PNR depuis le Canada vers d'autres pays tiers, [...] afin d'éviter que le niveau de protection prévu par cet accord puisse être contourné par des transferts de données à caractère personnel vers d'autres pays tiers et de garantir la continuité du niveau de

protection offert par le droit de l'Union[22]». **Par conséquent, il résulte de l'avis 1/15 que le niveau de protection résultant des accords internationaux envisagés avec les pays tiers sur l'échange de données à caractère personnel entre Europol et leurs autorités nationales compétentes devrait, de la même façon** (que l'accord entre l'Union européenne et le Canada sur le transfert des données PNR)**, être essentiellement équivalent au niveau de protection offert par le droit de l'Union.**

En outre, si le règlement Europol établit des règles autonomes en matière de protection des données spécifiques à Europol, son considérant 40 indique clairement qu'elles devraient être, dans le même temps, «cohérentes avec d'autres instruments pertinents en matière de protection des données applicables au domaine de la coopération policière dans l'Union», en particulier «la directive (UE) 2016/680 [...], ainsi que la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe et sa recommandation nº R (87) 15». **Par conséquent, le CEPD estime que de nouvelles exigences peuvent être déduites de la directive (UE) 2016/680 pour déterminer si un accord international avec un pays tiers offre en effet des garanties suffisantes.** L'article 37 de la directive (UE) 2016/680 prévoit que les transferts qui ne sont pas fondés sur une décision d'adéquation ne devraient être autorisés que lorsque «des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant[23]» (comme le règlement Europol) ou lorsque «le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel». Le considérant 71 apporte davantage de précisions et énonce trois critères à prendre en considération pour évaluer l'existence de telles garanties appropriées dans un contexte répressif:

- le fait que le transfert de données à caractère personnel sera soumis à des obligations de confidentialité;
- le principe de spécificité, ce qui garantit que les données ne seront pas traitées à des fins autres que celles pour lesquelles elles ont été transférées; et
- le fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain.

Le CEPD estime que ces critères devraient être appliqués mutatis mutandis pour déterminer si les accords internationaux autorisant l'échange de données entre Europol et les huit pays tiers concernés offrent des garanties suffisantes. En ce qui concerne le troisième critère du considérant 71, le CEPD souligne qu'aucun des pays tiers en question (à l'exception d'Israël) n'a aboli la peine de mort et que seuls certains d'entre eux (à savoir le Maroc, l'Algérie et la Tunisie) ont adopté un moratoire sur la peine de mort.

En outre, le règlement Europol vise à garantir un niveau élevé de protection des données tout en tenant compte des spécificités des activités d'Europol en tant que «centre névralgique de l'Union pour l'échange d'informations» dans la lutte contre le terrorisme et les formes graves de criminalité organisée et centre de soutien des opérations de répression. **Par conséquent, les garanties spécifiques qui sont prévues à cet effet dans le règlement Europol devraient se retrouver dans les accords internationaux conclus avec les pays tiers afin d'offrir des garanties suffisantes au sens du règlement Europol.** À cet égard, le CEPD souligne que le règlement Europol attribue différentes responsabilités en matière de protection des données aux fournisseurs d'informations, tels que les États membres, et à Europol, lorsqu'ils traitent les données fournies pour l'une des finalités légitimes énumérées dans le règlement Europol (article 18). Les États membres sont responsables de la qualité des données fournies [article 38, paragraphe 2, point a)], c'est-à-dire qu'elles doivent être exactes et tenues à jour, ainsi que de

la légalité du transfert [article 38, paragraphe 5, point a)]. Cette répartition des responsabilités en matière de protection des données entre Europol et les fournisseurs d'informations devrait être prise en considération lors de la définition du régime offrant des garanties suffisantes dans chacun des accords internationaux. Le règlement Europol attache également une grande importance au respect du principe de limitation de la finalité. En outre, les fournisseurs d'informations peuvent également appliquer des limitations supplémentaires à l'utilisation des données par Europol et d'autres bénéficiaires (article 19, paragraphe 2). En ce sens, l'article 25 du règlement Europol mentionne explicitement l'obligation de se conformer à ces limitations spécifiques en ce qui concerne l'utilisation ultérieure des données. Les futurs accords internationaux entre l'Union européenne et les pays tiers pour l'échange de données d'Europol devraient ainsi garantir l'application effective de ces limitations.

Enfin, les accords internationaux en question devraient offrir des garanties suffisantes non seulement au regard de la protection des données, mais aussi des autres libertés et droits fondamentaux des personnes. Les accords internationaux autoriseront les transferts de données à caractère personnel collectées dans le cadre d'enquêtes pénales. Ces données seront utilisées dans le pays destinataire pour ordonner des mesures spécifiques de surveillance, pour procéder à des arrestations, pour fournir des preuves dans le cadre de poursuites pénales et, enfin, pour imposer des sanctions pénales. Les transferts envisagés de données à caractère personnel vers les pays tiers en question pourraient donc avoir des incidences sur d'autres droits fondamentaux reconnus au titre I «Dignité» de la charte (c'est-à-dire le droit à la dignité humaine, le droit à la vie, le droit à l'intégrité de la personne, l'interdiction de la torture et des peines ou traitements inhumains ou dégradants) et au titre VI «Justice» (c'est-à-dire le droit à un recours effectif et à accéder à un tribunal impartial, le droit à la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité des délits et des peines, le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction). À cet égard, le CEPD fait observer que certains des pays tiers pour lesquels une coopération avec Europol est envisagée ont violé ces droits fondamentaux. Le Comité des Nations unies contre la torture a relevé de graves manquements dans certains de ces pays en ce qui concerne des cas signalés de torture et de mauvais traitements, les conditions des lieux de détention, l'utilisation de preuves obtenues sous la contrainte, l'absence de garanties fondamentales pour les détenus et les conditions de vie dans les camps de réfugiés[24]. Compte tenu de la volonté permanente de l'Union européenne de promouvoir et de défendre activement les droits de l'homme dans ses relations avec des pays tiers, le **CEPD insiste sur le fait que les garanties essentielles s'appliquent également dans le cadre des enquêtes pénales et que les garanties prévues dans les futurs accords internationaux avec Europol doivent tenir compte, au cas par cas, des risques prévisibles que ces transferts pourraient présenter**.

4. RECOMMANDATIONS SPÉCIFIQUES

Le CEPD souhaite exprimer les observations générales et les recommandations spécifiques suivantes sur les directives de négociation figurant dans les annexes des recommandations. Ces observations sont sans préjudice des recommandations supplémentaires que le CEPD pourrait formuler sur la base d'informations complémentaires et des dispositions des projets d'accords durant les négociations.

Le principe de protection des données et les garanties de protection des données à caractère personnel des personnes physiques que le CEPD examinera ci-dessous sont, en grande partie,

mentionnés en termes généraux dans les directives de négociation. Néanmoins, le CEPD tient à insister sur la nécessité de fournir des garanties qui soient à la fois concrètes, spécifiques et rigoureuses. Compte tenu du contexte répressif et des risques potentiels que ces transferts de données pourraient présenter pour les personnes concernées, **les garanties prévues dans ces accords internationaux avec les pays tiers devraient prévenir et atténuer ces risques de manière satisfaisante**. En outre, **ces garanties devraient être claires et effectives afin de respecter pleinement le droit primaire de l'Union et être conformes à l'avis 1/15 de la CJUE**[25].

4.1. Limitation et détermination des finalités des transferts de données effectués par Europol

La limitation de la finalité est un principe fondamental des cadres de l'Union en matière de protection des données. À cet égard, le règlement Europol établit qu'«elle contribue notamment à la transparence, à la sécurité juridique et à la prévisibilité, et revêt une importance particulièrement grande dans le domaine de la coopération entre services répressifs, dans lequel les personnes concernées ignorent habituellement que leurs données à caractère personnel sont collectées et traitées et où l'utilisation de données à caractère personnel peut avoir une incidence considérable sur la vie et les libertés des personnes physiques[26]». Plus précisément, la limitation de la finalité exige, d'une part, que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes et, d'autre part, qu'elles ne soient pas traitées ultérieurement de manière incompatible avec ces finalités.

a) Détermination des finalités des transferts de données

L'article 18 du règlement Europol fournit une liste de finalités des activités de traitement de données effectuées par Europol, considérées comme légitimes[27]. Pour les analyses opérationnelles, les finalités des activités de traitement de données doivent être davantage précisées dans les décisions d'ouverture des projets d'analyse opérationnelle (article 18, paragraphe 3)[28].

La directive 2 de chacune des annexes limite la coopération menée entre Europol et les autorités des pays tiers en vertu des futurs accords internationaux aux formes de criminalité et aux infractions pénales connexes relevant de la compétence d'Europol. Elle précise ensuite les finalités de cette coopération en énumérant différentes formes de criminalité pour chacun des accords. La directive 3, point a), précise en outre que «[l]es finalités du traitement de données à caractère personnel par les parties dans le contexte de l'accord seront clairement et précisément énoncées et ne dépasseront pas ce qui est nécessaire dans des cas particuliers afin de prévenir et de combattre le terrorisme et les infractions pénales visées dans l'accord».

Compte tenu de l'importance particulière que le règlement Europol accorde à la limitation de la finalité, **le CEPD recommande de définir de manière plus précise les finalités des transferts dans la directive 2 de chacune des annexes des accords**. **À cette fin, le CEPD recommande plus précisément de:**

- définir clairement dans les accords internationaux les listes des infractions au sujet desquelles des données à caractère personnel seront échangées. En particulier, les accords devraient définir de manière claire et précise les activités couvertes par ces formes de criminalité, ainsi que les personnes, les groupes et les organisations susceptibles d'être affectés par le transfert;

- communiquer à l'avance aux autorités chargées de superviser la mise en œuvre de l'accord la liste des projets d'analyse opérationnelle d'Europol auxquels les pays tiers concernés participeront, ainsi que les conditions d'une telle participation;
- définir clairement les termes «cas particuliers» dans les accords internationaux, de façon à pouvoir déterminer la nécessité et la proportionnalité des transferts. Il est difficile d'établir si ces termes font référence à des enquêtes pénales ou à des opérations de renseignement criminel ciblant des personnes physiques particulières considérées comme suspectes, s'ils couvrent également des personnes physiques qui sont des victimes, des témoins ou des contacts et s'ils pourraient justifier des transferts massifs de données (par exemple, en rapport à une liste de jeunes voyageant vers un pays tiers en question qui sont suspectés d'être radicalisés).

b) Limitation du traitement ultérieur des données transférées par l'autorité destinataire

La directive 3, point b), des annexes limite le traitement de données à caractère personnel «pour les seules finalités pour lesquelles elles auront été transférées». Le CEPD souligne que le respect de ce principe est étroitement lié au champ de compétences des bénéficiaires dans les pays tiers destinataires. Pour garantir le respect du principe de limitation de la finalité, le champ de compétences des autorités des pays tiers destinataires auxquelles Europol transmettra des données et qui traiteront ces données devrait être clairement défini afin de s'assurer qu'elles sont également compétentes au regard des finalités du transfert. En ce sens, l'article 4, paragraphe 2, de la directive (UE) 2016/680 autorise le traitement ultérieur, par le même ou par un autre responsable du traitement, pour l'une des finalités de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, autre que celles pour lesquelles les données à caractère personnel ont été collectées à condition que le traitement soit nécessaire et proportionné à cette autre finalité et *que le destinataire soit autorisé à traiter ces données à caractère personnel pour une telle finalité* conformément au cadre juridique régissant ses activités. Par conséquent, le CEPD **recommande que les accords internationaux comprennent une liste exhaustive des autorités compétentes des pays tiers destinataires vers lesquels Europol transférera des données, ainsi qu'une brève description de leurs compétences**. **De telles informations devraient également apparaître dans l'une des directives des annexes.**

4.2. Transferts ultérieurs

Le CEPD signale l'existence d'une incohérence entre la directive 3, point b) («[l]es données à caractère personnel transférées par Europol conformément à l'accord seront traitées [...] pour les seules finalités pour lesquelles elles auront été transférées») et la directive 3, point h) («les transferts ultérieurs d'informations d'autorités compétentes de [le pays tiers] à d'autres autorités en [le même pays] ne seront autorisés qu'aux fins de l'accord et seront soumis à des conditions et garanties appropriées») des annexes. **La directive 3, point h), des annexes devrait être plus restrictive que les «fins de l'accord» et limiter les transferts ultérieurs d'autorités compétentes du pays tiers à d'autres autorités du même pays aux finalités initiales du transfert effectué par Europol.**

4.3. Limitations spécifiques du traitement des informations transférées par Europol

L'article 19, paragraphes 2 et 3, du règlement Europol offre aux États membres et aux autres fournisseurs d'informations à Europol, ainsi qu'à Europol elle-même, la possibilité de notifier

toute limitation de l'accès aux données, ainsi que de leur utilisation, transfert, effacement ou destruction, et oblige Europol à se conformer à ces limitations. Les futurs accords internationaux conclus entre l'Union européenne et les pays tiers en question autorisant l'échange de données entre Europol et les autorités compétentes de ces pays ne peuvent ignorer les limitations que les États membres et d'autres fournisseurs ont imposées à l'accès aux données qu'ils ont partagées avec Europol et à leur utilisation. Les accords internationaux avec les pays tiers devraient dès lors garantir l'application effective de ces limitations[29]. Pour le moment, la directive 3, point b), des annexes n'exige que d'offrir à «Europol la possibilité d'indiquer, au moment du transfert de données, toute limitation de l'accès ou de l'utilisation, y compris en ce qui concerne leur transfert, effacement ou destruction». **Le CEPD recommande de renforcer la formulation de cette directive de façon à établir qu'Europol indiquera, au moment du transfert de données, toute limitation existante du traitement ultérieur de ces données. Les accords internationaux devraient obliger les autorités compétentes des pays tiers en question à respecter ces limitations et à préciser comment le respect de ces limitations sera appliqué dans la pratique.**

4.4. Surveillance par une autorité indépendante

Alors que le CEPD est l'autorité indépendante chargée de contrôler les activités de traitement de données effectuées par Europol, y compris le transfert de données vers des pays tiers, il est également nécessaire de garantir une surveillance indépendante efficace une fois que les données ont été transférées dans les pays tiers destinataires. Le CEPD rappelle que tant l'article 16 TFUE que l'article 8, paragraphe 3, de la charte prévoient une garantie essentielle du droit à la protection des données, à savoir le contrôle exercé par une autorité indépendante. Le CEPD se félicite dès lors que la directive 3, point j), des annexes exige que les futurs accords internationaux garantissent «un système de surveillance par une ou plusieurs autorités publiques indépendantes chargées de la protection des données, investies de pouvoirs d'enquête et d'intervention efficaces pour surveiller [et] pour agir en justice [, et qui ont] le pouvoir de connaître des réclamations de personnes physiques». En outre, les autorités publiques chargées de cette surveillance indépendante devraient être investies de ces pouvoirs sur toutes les autorités auxquelles Europol transférera des données en vertu des accords internationaux.
Le CEPD rappelle que, conformément à la jurisprudence de la CJUE[30], une autorité de contrôle indépendante au sens de l'article 8, paragraphe 3, de la charte est une autorité capable de prendre des décisions indépendamment de toute influence extérieure, directe ou indirecte. Une telle autorité de contrôle doit non seulement être indépendante des parties qu'elle contrôle, mais elle ne doit pas non plus être «subordonnée à une autorité de tutelle, dont elle peut recevoir des instructions», car cela signifierait qu'elle «n'est donc pas à l'abri de toute influence extérieure susceptible d'orienter ses décisions»[31].

4.5. Droits des personnes concernées

Le CEPD se félicite que la directive 3, point d), des annexes exige que les futurs accords internationaux assurent «des droits opposables pour les personnes physiques dont les données à caractère personnel sont traitées, en définissant des règles relatives au droit d'accès, de rectification et d'effacement, y compris les motifs spécifiques pouvant autoriser d'éventuelles limitations nécessaires et proportionnées».

Avant toute chose, le CEPD tient à rappeler que les droits d'accès et de rectification sont inscrits à l'article 8, paragraphe 2, de la charte en tant qu'éléments essentiels du droit à la

protection des données. Si l'exercice des droits des personnes concernées est généralement limité dans le contexte répressif afin d'éviter de compromettre les enquêtes en cours, la possibilité pour les personnes concernées d'exercer leurs droits devrait exister dans la pratique et ne pas rester purement théorique, même s'il est limité ou confié à un tiers de confiance dans des situations dans lesquelles l'exercice de ces droits est refusé pour protéger des informations sensibles en matière répressive (comme c'est le cas dans le règlement Europol).

En outre, le CEPD prend note du fait que les annexes n'incluent aucune directive concernant le droit à l'information. Le droit à l'information est également de la plus haute importance, car il permet l'exercice d'autres droits en matière de protection des données, y compris le droit à un recours, et garantit un traitement loyal des données[32]. Les personnes concernées n'ont généralement aucune connaissance du fait que leurs données sont traitées (ou transférées) à des fins répressives. Le règlement Europol ne prévoit aucune obligation pour Europol d'informer à l'avance les personnes concernées qu'elle traite des informations à caractère personnel les concernant. Les personnes concernées doivent exercer leur droit d'accès pour savoir si Europol traite des données les concernant. Néanmoins, dans son récent avis 1/15, la CJUE a jugé qu'«il importe que les passagers aériens soient informés du transfert de leurs données PNR vers le Canada et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques», considérant qu'«une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données PNR les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la [c]harte, un recours effectif devant un tribunal»[33]. **Par conséquent, le CEPD recommande d'inclure le droit à l'information dans les annexes, exigeant que les futurs accords internationaux prévoient des obligations de transparence pour les autorités des pays tiers auxquelles Europol transférera des données.**

4.6. Transfert de catégories particulières de données

La directive 3, point c), des annexes établit que le transfert de catégories particulières de données doit être interdit «à moins qu'il ne soit strictement nécessaire et proportionné dans des cas particuliers pour prévenir les infractions pénales [...] ou lutter contre celles-ci [...] et sous réserve de garanties appropriées», et que le transfert de données concernant des catégories spécifiques de personnes concernées doit également être assorti de garanties spécifiques. Le CEPD estime que, si les futurs accords internationaux conclus avec les pays tiers en question autorisent le transfert de catégories particulières de données vers ces pays, ils devraient contenir des dispositions spécifiques garantissant qu'elles bénéficient d'un niveau de protection des données comparable à celui prévu par les dispositions spécifiques imposées à Europol. Le règlement Europol soumet le traitement de catégories particulières de données et le traitement de données concernant des catégories spécifiques de personnes concernées (c'est-à-dire les victimes, les témoins, les contacts, les informateurs et les personnes de moins de 18 ans) aux principes de strictes nécessité et proportionnalité (article 30, paragraphes 1 et 2[34]).

En outre, le CEPD souligne que, dans la mesure où les futurs accords internationaux prévoient que des catégories particulières de données peuvent être transférées vers les pays tiers en question, la Cour de justice a jugé dans l'avis 1/15 que tout transfert de ces données sensibles nécessiterait «**une justification précise et particulièrement solide, tirée de motifs autres que la protection de la sécurité publique contre le terrorisme et la criminalité transnationale grave**»[35]. En l'absence d'une telle justification, la Cour a jugé, concernant le

Canada, que les dispositions de l'accord sur le transfert de données sensibles et sur le traitement et la conservation de ces données étaient incompatibles avec les droits fondamentaux.[36]

4.7. Conservation des données

La directive 3, point b), des annexes dispose que les données à caractère personnel transférées «ne seront pas conservées plus longtemps que ce qui est nécessaire aux finalités pour lesquelles elles auront été transférées». La directive 3, point e), exige en outre que les accords définissent les règles de conservation, de réexamen, de correction et d'effacement de données à caractère personnel. À cet égard, le CEPD tient à souligner que le règlement Europol prévoit un régime élaboré de conservation des données qui repose à la fois sur des règles détaillées en matière de conservation des données[37] et sur des garanties techniques et procédurales, garantissant que les obligations de conservation sont respectées dans la pratique[38]. L'article 31 impose à Europol de réexaminer la nécessité et la proportionnalité de la conservation des données tous les trois ans. Cette obligation est sans préjudice des différents délais de conservation communiqués par les fournisseurs de données lors de l'envoi des données à Europol, qui sont obligatoires pour Europol. Toute décision de conserver les données au-delà des trois premières années doit être dûment justifiée et les raisons doivent être consignées. En outre, l'article 31, paragraphe 6, du règlement Europol prévoit une série de dérogations à l'obligation d'effacer les données. Europol est également tenue d'effacer les données qui ont été effacées dans les systèmes du fournisseur de données dès qu'elle en est informée. Europol devrait également être en mesure d'informer les tiers que les données qui leur ont été communiquées ou transférées seront effacées de ses systèmes.

4.8. Suspension ou dénonciation des accords internationaux en cas de violation

Le CEPD note que la directive 5 des annexes des recommandations prévoit la possibilité de suspendre ou de dénoncer les accords internationaux en question. De la même façon que les décisions d'adéquation existantes fondées sur l'article 25 de la directive 95/46/CE actuelle, et que l'article 36, paragraphe 5, de la directive (UE) 2016/680 concernant les décisions d'adéquation à des fins répressives, le CEPD estime qu'il est de la plus haute importance d'inclure la possibilité de suspendre ou de dénoncer ces accords internationaux avec les pays tiers en cas de violation de leurs dispositions par les autorités répressives des pays tiers destinataires. À cet égard, le CEPD souligne également le rôle primordial de l'autorité indépendante chargée de surveiller l'application des futurs accords internationaux afin de détecter les violations. En outre, **le CEPD recommande de préciser que les données à caractère personnel qui relèvent du champ d'application de l'accord et qui ont été transférées avant la suspension ou la dénonciation dudit accord peuvent continuer à être traitées conformément aux dispositions de l'accord**.

5. CONCLUSION

Le CEPD se félicite de l'attention accordée à la protection des données dans les annexes des recommandations de la Commission du 20 décembre 2017 qui constitueront le mandat de la Commission pour négocier, au nom de l'Union européenne, les accords internationaux respectifs avec chacun des huit pays de la région MENA pour lesquels une coopération avec Europol est envisagée.

La nécessité et la proportionnalité des accords internationaux envisagés pour autoriser Europol à transférer régulièrement des données aux autorités compétentes des huit pays tiers en question

doivent faire l'objet d'une évaluation approfondie afin de garantir le respect de l'article 52, paragraphe 1, de la charte. Pour permettre une telle évaluation en profondeur et au cas par cas, le CEPD recommande de restreindre et de différencier davantage les besoins de transfert en fonction de la situation particulière de chaque pays tiers et de la réalité sur le terrain. Le champ d'application de chaque accord international et les finalités des transferts vers chaque pays tiers devraient être précisés en conséquence dans les annexes. Le CEPD recommande de réaliser de nouvelles analyses d'impact afin de mieux évaluer les risques que présentent les transferts de données vers ces pays tiers pour les droits des personnes physiques au respect de la vie privée et à la protection des données, mais aussi pour les autres libertés et droits fondamentaux garantis par la charte, de manière à définir précisément les garanties nécessaires.

Le CEPD note que, conformément à l'article 25, paragraphe 1, point b), du règlement Europol, Europol pourrait transférer régulièrement des données vers un pays tiers en concluant un accord international contraignant entre l'Union européenne et le pays tiers destinataire, à condition qu'un tel accord offre des garanties suffisantes. Le CEPD estime que l'«offre de garanties suffisantes» au sens du règlement Europol implique que les accords internationaux conclus avec les pays tiers:

- garantissent que les pays tiers destinataires respectent pleinement l'article 8 de la charte, en particulier le principe de limitation de la finalité, le droit d'accès, le droit de rectification et le contrôle par une autorité indépendante expressément prévue par la charte;
- se conforment à l'avis 1/15 de la CJUE en veillant à ce que le niveau de protection résultant de ces accords soit essentiellement équivalent au niveau de protection offert par le droit de l'Union;
- appliquent mutatis mutandis les critères énoncés au considérant 71 de la directive (UE) 2016/680, à savoir le fait que les transferts de données à caractère personnel sont soumis à des obligations de confidentialité, le principe de spécificité et le fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou mettre à exécution une condamnation à la peine de mort ou toute forme de traitement cruel et inhumain;
- reprennent les garanties spécifiques prévues dans le règlement Europol, telles que les limitations spécifiées par les fournisseurs d'informations; et
- appliquent des garanties essentielles dans le cadre des enquêtes pénales et prévoient des garanties qui tiennent compte, au cas par cas, des risques prévisibles que les transferts vers ces pays tiers pourraient présenter au regard d'autres libertés et droits fondamentaux.

Outre ces recommandations générales, les recommandations et observations formulées par le CEPD dans le présent avis portent sur les aspects spécifiques suivants des futurs accords internationaux à négocier avec les pays de la région MENA dans le cadre des mandats de négociation:

- les principes de limitation et de détermination des finalités des transferts de données effectués par Europol;
- les transferts ultérieurs effectués par les autorités compétentes des pays tiers en question;
- les limitations du traitement des informations transmises par Europol aux autorités compétentes des pays tiers;
- la surveillance par une autorité indépendante dans les pays tiers;
- les droits des personnes concernées;

- le transfert de catégories particulières de données aux autorités compétentes des pays tiers;
- la conservation des données transférées par Europol; et
- la possibilité de suspendre et de dénoncer les accords internationaux en cas de violation de leurs dispositions.

Bruxelles, le 14 mars 2018

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

NOTES

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 119 du 4.5.2016, p. 1.
[3] JO L 8 du 12.1.2001, p. 1.
[4] JO L 350 du 30.12.2008, p. 60.
[5] JO L 119 du 4.5.2016, p. 89.
[6] 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, ci-après le «règlement Europol».
[7] 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.
[8] Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Royaume hachémite de Jordanie sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités jordaniennes compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 798 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la République de Turquie sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités turques compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 799 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la République libanaise sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités libanaises compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 805 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et l'État d'Israël sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités israéliennes compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 806 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la Tunisie sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités tunisiennes compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 807 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et le Royaume du Maroc sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités marocaines compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 808 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la République arabe d'Égypte sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités égyptiennes compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 809 final; recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et la République algérienne démocratique et populaire sur l'échange de données à caractère personnel entre l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et les autorités algériennes compétentes pour lutter contre les formes graves de criminalité et le terrorisme, COM(2017) 811 final.
[9] Communication de la Commission du 28 avril 2015 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Le programme européen en matière de sécurité, COM(2015) 185 final.
[10] Conclusions du Conseil du 19 juin 2017 sur l'action extérieure de l'UE en matière de lutte contre le terrorisme, document 10384/17.
[11] Vision partagée, action commune: Une Europe plus forte – Une stratégie globale pour la politique étrangère et de sécurité de l'Union européenne, disponible à l'adresse: https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_fr_version.pdf.
[12] Communication de la Commission du 18 octobre 2017 au Parlement européen, au Conseil européen et au Conseil – Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 608 final.

[13] Voir le mémorandum d'accord de toutes les recommandations de la Commission de décisions du Conseil déposées le 20 décembre 2017, à l'exception de celle concernant Israël.
[14] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO L 8 du 12.1.2001, p. 1.
[15] Directive 8 des annexes des recommandations concernant l'Algérie, l'Égypte, Israël, la Jordanie et le Liban; voir également la communication de la Commission du 10 janvier 2017 au Parlement européen et au Conseil sur l'échange et la protection de données à caractère personnel à l'ère de la mondialisation, COM(2017) 7 final, p. 11, dans laquelle la Commission encourage l'adhésion des pays tiers à la convention 108 du Conseil de l'Europe et à son protocole additionnel.
[16] Pour l'heure, la Turquie en tant qu'État membre du Conseil de l'Europe a signé la convention 108, la Tunisie en tant qu'État tiers a adhéré à la convention 108 et le Maroc en tant qu'État tiers a été invité à y adhérer. L'Algérie, l'Égypte, Israël, la Jordanie et le Liban ne se sont pas engagés dans ce processus.
[17] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, STE nº 108.
[18] Le CEPD n'a connaissance d'aucune intention à court terme de la Commission d'entamer des discussions avec ces pays tiers et de procéder à des évaluations approfondies de leurs systèmes juridiques en vue de l'adoption de telles décisions d'adéquation.
[19] L'article 25, paragraphe 5, du règlement Europol prévoit des dérogations pouvant être utilisées au cas par cas pour les transferts individuels; elles ne peuvent être applicables aux transferts systématiques, en masse ou structurels. L'article 25, paragraphe 6, prévoit également des dérogations pour une série de transferts qui doivent être dûment justifiés et documentés et effectués en accord avec le CEPD.
[20] Affaires jointes C-402/05 P et C-415/05 P, Kadi/Conseil, ECLI:EU:C:2008:461, point 285.
[21] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592.
[22] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 214; voir également point 93 de l'avis 1/15.
[23] Dans le cas de l'article 37 de la directive (UE) 2016/680, les instruments juridiquement contraignants sont ceux conclus entre les États membres et les pays tiers.
[24] Voir les derniers rapports du Comité des Nations unies contre la torture disponibles à l'adresse suivante: http://www.ohchr.org/FR/Countries/MENARegion/Pages/LBIndex.aspx.
[25] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, en particulier le point 134, dans lequel la Cour juge que «[m]ême si les moyens visant à garantir un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union [...], ces moyens doivent néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union».
[26] Considérant 26 du règlement Europol.
[27] Il s'agit des finalités suivantes: recoupements, analyses de nature stratégique ou thématique, analyses opérationnelles et facilitation de l'échange d'informations entre les États membres, Europol, d'autres organes de l'Union, des pays tiers et des organisations internationales.
[28] Les projets d'analyse opérationnelle sont des plates-formes dans lesquelles une analyse opérationnelle peut être effectuée afin d'appuyer des enquêtes pénales et des opérations de renseignement criminel menées au niveau international contre des cibles déterminées. Ils sont définis par Europol en fonction des besoins opérationnels des États membres dans le cadre de la lutte transfrontalière contre les formes graves de criminalité relevant de la compétence d'Europol. Ces plates-formes peuvent porter en particulier sur une forme de criminalité couvrant un ou plusieurs types de criminalité; elles peuvent couvrir une zone géographique donnée ou se concentrer sur des structures, des phénomènes ou des incidents particuliers de criminalité qui, en raison de leur taille, de leur complexité ou de leur incidence, nécessitent l'adoption d'une approche spécifique.
[29] Dans le cadre du système d'analyse actuellement mis en place par Europol, l'application effective des limitations est réglementée par l'utilisation de codes de traitement qui lient tous les États membres et les autres fournisseurs d'informations.
[30] Voir affaire C-518/07, Commission/Allemagne, ECLI:EU:C:2010:125, point 25; affaire C-614/10, Commission/Autriche, ECLI:EU:C:2012:631, points 36 et 37; affaire C-288/12, Commission/Hongrie, ECLI:EU:C:2014:237, point 48; affaire C-362/14, Maximillian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650, point 41.
[31] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 230.
[32] Affaire C-201/14, Smaranda Bara e.a./Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală, ECLI:EU:C:2015:638, en particulier les points 32 et 33 dans lesquels la Cour estime que «cette exigence d'information des personnes concernées par le

traitement de leurs données personnelles est d'autant plus importante qu'elle est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées [...] et de leur droit d'opposition au traitement desdites données» et que «[c]es informations concernent l'identité du responsable du traitement de ces données, les finalités de ce traitement ainsi que toute information supplémentaire nécessaire pour assurer un traitement loyal des données».

[33] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 220.

[34] Dans la pratique, ces dispositions sont mises en œuvre grâce à une évaluation spécifique faite dans le cadre de la décision d'ouverture de chaque projet d'analyse opérationnelle. Tous les participants au projet d'analyse opérationnelle ont accès à ces informations conformément aux règles définies à l'article 20 du règlement Europol.

[35] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 165.

[36] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 167.

[37] Par exemple, l'obligation pour Europol de conserver les données d'une manière permettant d'établir leur source (article 38, paragraphe 1) ou l'obligation de consigner dans des journaux toutes les opérations de traitement des données (article 40, paragraphe 1).

[38] Par exemple, l'obligation pour Europol de transmettre sur demande les journaux au CEPD, au délégué à la protection des données d'Europol ou à l'unité nationale concernée dans le cadre d'une enquête particulière (article 40, paragraphe 2).