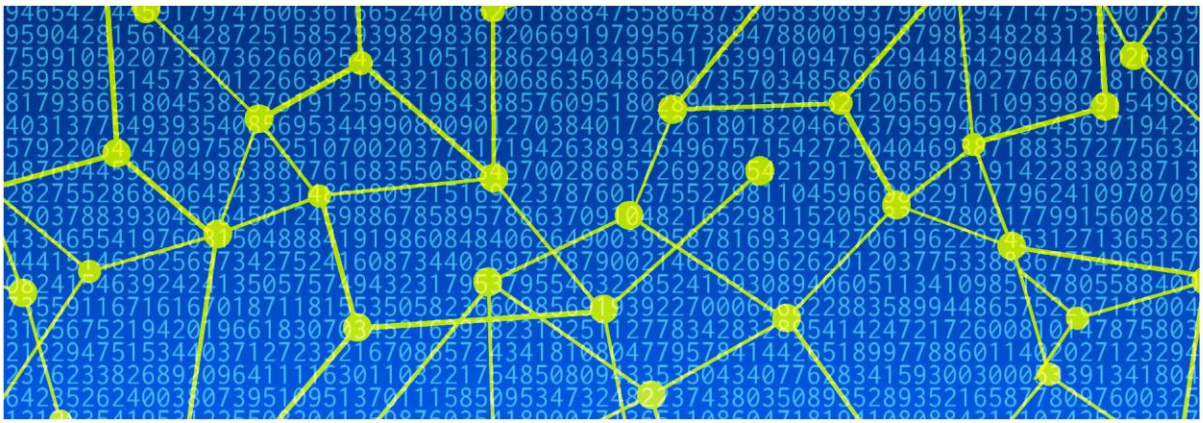

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 4/2021

Avis du CEPD sur la proposition de modification du règlement Europol

EDPS

8 mars 2021

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

Conformément à 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». Par ailleurs, en vertu de l'article 57, paragraphe 1, point g), du règlement susvisé, 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 a été rendu par le CEPD, dans le délai de huit semaines à compter de la réception de la demande de consultation prévu à l'article 42, paragraphe 3, du règlement (UE) 2018/1725, vu l'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel de la proposition de la Commission relative au règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794, en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation.

Résumé analytique

Le 9 décembre 2020, la Commission européenne a présenté une proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation. La proposition législative vise à renforcer et, dans certains, cas, à étendre le mandat d'Europol afin de répondre à l'évolution de la situation en matière de sécurité et à des menaces en constante mutation et de plus en plus complexes.

Le CEPD comprend que les autorités répressives ont besoin de disposer des meilleurs outils techniques et juridiques possibles pour s'acquitter de leurs tâches, à savoir détecter, enquêter et prévenir les infractions et autres menaces à la sécurité publique. En outre, il est convaincu qu'il n'existe pas de conflit intrinsèque et inconciliable entre la sécurité et les droits fondamentaux, y compris le droit à la protection des données. Par conséquent, le présent avis vise à donner une évaluation juste et objective de la nécessité et de la proportionnalité des mesures proposées, ainsi qu'à formuler un certain nombre de recommandations spécifiques en vue d'assurer un juste équilibre entre les valeurs et les intérêts en jeu.

Les enquêtes pénales et les opérations de renseignement en matière pénale incluent de plus en plus fréquemment la collecte et le traitement d'ensembles de données vastes et complexes par les autorités répressives. Si le CEPD prend note avec satisfaction des garanties qui accompagnent les dérogations proposées dans ces cas, il craint que les exceptions aux règles actuelles en matière de protection des données, qui s'appliquent à Europol, puissent, en réalité, devenir la règle. Il recommande dès lors que le règlement Europol définisse plus précisément les situations et les conditions dans lesquelles Europol peut recourir aux dérogations proposées. En outre, même dans ces cas, le traitement de données à caractère personnel par l'Agence devrait être parfaitement conforme aux principes et obligations généraux énoncés au chapitre IX du règlement (UE) 2018/1725.

S'agissant des possibilités légales élargies permettant à Europol de coopérer avec les parties privées, notamment dans le cas d'ensembles de données relevant de la compétence de plusieurs autorités ou ne pouvant être rattachés à la compétence d'une ou plusieurs autorités spécifiques, le CEPD apprécie qu'elles soient contrebalancées par des garanties spécifiques, telles que l'interdiction de transferts de données systémiques, massifs ou structurels. Dans le même temps, le CEPD recommande que cette restriction importante soit appliquée à tous les échanges entre Europol et les parties privées, où qu'elles se trouvent, à l'intérieur ou en dehors de l'Union. Le CEPD estime également que le rôle et les responsabilités juridiques exacts d'Europol, en tant que prestataire de services pour les autorités nationales et, partant, en tant que sous-traitant, devraient être précisés dans un acte juridique contraignant. En outre, il juge nécessaire d'évaluer les risques potentiels pour la sécurité que pose l'ouverture de l'infrastructure de communication d'Europol à une utilisation par des parties privées.

Le CEPD attache également une attention particulière à l'utilisation envisagée par Europol de données à caractère personnel à des fins de recherche et d'innovation. Dans le même temps, il est parfaitement conscient que l'alternative, à savoir qu'Europol et les autorités répressives nationales s'appuient sur des outils et des produits mis au point par des fournisseurs externes souvent établis en dehors de l'UE, représente clairement des risques beaucoup plus grands pour les droits fondamentaux. Néanmoins, le CEPD est d'avis que la définition de la nouvelle finalité du traitement est trop vague et il recommande que la portée des activités de recherche et d'innovation soit précisée dans un document contraignant.

Le CEPD se réjouit de la proposition de renforcement accru du cadre d'Europol en matière de protection des données et la soutient pleinement, notamment l'application directe des règles horizontales, énoncées au chapitre IX du règlement (UE) 2018/1725, au traitement de données opérationnelles par l'Agence. Cela marque également une étape importante vers une harmonisation complète du cadre de la protection des données pour toutes les institutions, organes et agences de l'UE, que le CEPD n'a cessé de demander.

Un mandat renforcé d'Europol devrait toujours aller de pair avec un contrôle accru. Le CEPD demande donc une harmonisation complète de ses pouvoirs de contrôle à l'égard d'Europol avec les pouvoirs généraux conférés au CEPD par le règlement (UE) 2018/1725 et applicables aux autres institutions, organes et agences de l'UE, y compris le Parlement européen, le Conseil et la Commission. Cette harmonisation serait conforme à la volonté du législateur de l'Union et contribuerait également à éviter un traitement différencié des organes de l'Union et à les mettre dans une situation plus ou moins privilégiée.

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 (le «règlement général sur la protection des données»)[1],

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 (le «RPDUE»)[2], et notamment son article 42, paragraphe 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[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. L'Agence de l'Union européenne pour la coopération des services répressifs (Europol) a été créée par le règlement (UE) 2016/794 du Parlement européen et du Conseil (ci-après le «règlement Europol») en vue de soutenir et de renforcer l'action des autorités compétentes des États membres et leur coopération mutuelle en matière de prévention des formes graves de criminalité transfrontière, de terrorisme et d'autres activités criminelles portant atteinte aux intérêts communs de l'Union et de lutte contre ces phénomènes. Le règlement Europol a remplacé l'acte juridique de base précédent, à savoir la décision 2009/371/JAI du Conseil[4], et a confié au CEPD la tâche de contrôler la licéité du traitement de données à caractère personnel par Europol à compter du 1er mai 2017.

2. Le 9 décembre 2020, la Commission européenne a adopté une proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation[5].

3. La proposition a été incluse dans le programme de travail de la Commission pour 2020 en tant qu'initiative législative visant à «renforce[r] le mandat d'Europol afin d'intensifier la coopération policière opérationnelle». Il s'agit également d'une action clé de la stratégie de l'UE pour l'union de la sécurité, adoptée en juillet 2020[6]. En outre, la proposition législative fait partie d'un train de mesures annoncées par la Commission le 9 décembre 2020 en vue de renforcer la réponse de l'Union à la menace terroriste[7].

4. La proposition a pour objet de renforcer et, le cas échéant, d'étendre le mandat d'Europol dans le cadre de sa mission et de ses tâches telles qu'énoncées à l'article 88 du traité sur le fonctionnement de l'Union européenne (TFUE). Les trois principaux domaines couverts par la proposition sont explicitement mentionnés dans le titre du projet de règlement, à savoir la coopération avec les parties privées, l'appui opérationnel aux enquêtes pénales et la recherche et l'innovation. Toutefois, un certain nombre de modifications supplémentaires ont été apportées à d'autres aspects importants du travail d'Europol, tels que le régime juridique relatif à la protection des données, les transferts de données vers des pays tiers, l'introduction de signalements dans le système d'information Schengen, etc. Ce dernier point fait l'objet d'une proposition législative distincte[8], sur laquelle le CEPD a également été consulté et qu'il a commentée dans un autre avis.

5. Selon l'exposé des motifs, la proposition législative répond à l'évolution de la situation en matière de sécurité et à des menaces en constante mutation et de plus en plus complexes, notamment l'exploitation par des groupes criminels de la transformation numérique, des nouvelles technologies et de la crise de la COVID-19. Dans ce contexte, la Commission rappelle plusieurs déclarations politiques récentes du Conseil et du Parlement européen, qui abordent spécifiquement la nécessité de renforcer davantage le mandat et les capacités d'Europol[9].

6. Le CEPD a été consulté de manière informelle par la Commission à plusieurs reprises tout au long du processus d'élaboration de la proposition législative et pour la dernière fois le 25 novembre 2020, et il a transmis ses observations informelles. Il se réjouit que son avis ait été sollicité à un stade précoce de la procédure et encourage la Commission à maintenir cette bonne pratique. De plus, le 9 octobre 2020, le CEPD a organisé un webinaire d'experts intitulé «La réforme d'Europol du point de vue de la protection des données», l'accent étant mis en particulier sur l'alignement des dispositions relatives à la protection des données du règlement Europol sur les règles générales relatives au traitement des données opérationnelles à caractère personnel.

7. Le CEPD a été officiellement consulté par la Commission le 7 janvier 2021 sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 et a adopté le présent avis conformément à l'article 42, paragraphe 3, du règlement (UE) 2018/1725.

2. OBSERVATIONS GÉNÉRALES

8. L'application cohérente des règles de protection des données au sein de l'espace de liberté; de sécurité et de justice ainsi que l'identification des divergences dans les normes de traitement des données opérationnelles à caractère personnel dans l'UE comptent au nombre des principaux objectifs de la stratégie du CEPD pour la période 2020-2024 «Façonner un avenir numérique plus sûr: une nouvelle stratégie pour une nouvelle décennie»[10]. En sa qualité de conseiller des institutions, organes et organismes de l'Union, chargé de faire appliquer les règles en matière de protection des données et de la vie privée, le CEPD occupe une position idéale pour contrôler que leurs compétences sont définies et utilisées dans le plein respect du cadre juridique et des droits fondamentaux des particuliers.

9. Le CEPD comprend que les autorités répressives ont besoin de disposer des meilleurs outils techniques et juridiques possibles pour s'acquitter de leurs tâches, à savoir détecter, enquêter et prévenir les infractions et autres menaces à la sécurité publique. Le droit à la

protection des données n'est pas un droit absolu et des ingérences peuvent être justifiées, pour autant qu'elles restent limitées à ce qui est nécessaire et proportionné dans une société démocratique, conformément à l'article 52, paragraphe 1, de la Charte des droits fondamentaux.

10. Le CEPD est convaincu qu'il n'existe pas de conflit intrinsèque et irréconciliable entre la sécurité et les droits fondamentaux, y compris le droit à la protection des données. Au lieu d'examiner le problème sous l'angle d'une dichotomie abstraite et assez erronée, il estime que la meilleure approche consiste à procéder à une évaluation juste et objective de la nécessité et de la proportionnalité des mesures proposées. À cet égard, le CEPD se réjouit que la Commission ait utilisé la boîte à outils sur la nécessité et les lignes directrices sur la proportionnalité élaborées par le CEPD[11] lors de la réalisation de l'analyse d'impact qui accompagne la proposition législative[12].

11. Le renforcement du mandat d'Europol devrait également être examiné sous un angle politique plus large. D'une part, un rôle plus important et proactif d'Europol dans la prévention des formes graves de criminalité et l'instruction en la matière s'inscrit dans la tendance stratégique à protéger de façon plus affirmée les intérêts communs de l'Union, ce qui a conduit à la création du Parquet européen, à la transformation de Frontex en un corps européen de garde-frontières et de garde-côtes et de l'EASO en une Agence de l'Union européenne pour l'asile. D'autre part, il soulève la question de savoir si le cadre juridique régissant le contrôle d'Europol et les voies de recours juridiques existantes sont suffisants et adéquats pour le nouveau rôle de l'Agence.

12. Le CEPD souligne que tout changement législatif devrait tenir compte de la nécessité d'adopter les dispositions qui s'imposent pour atteindre le juste équilibre entre les valeurs et les intérêts en jeu. En particulier, un mandat renforcé devrait toujours aller de pair avec un contrôle accru d'Europol. Le CEPD encourage également le législateur de l'Union à rechercher des solutions pérennes dans un monde en mutation rapide.

13. Le CEPD observe que l'un des éléments clés du système de garanties, conçu pour contrebalancer les pouvoirs renforcés d'Europol, est l'extension du rôle du CEPD, notamment en ce qui concerne l'évaluation de la proportionnalité et de la licéité du traitement des données à caractère personnel provenant de pays tiers (article 18*bis*, paragraphe 4), l'approbation de la prolongation de la période maximale pour l'analyse préalable des mégadonnées (article 18, paragraphe 5*bis*) ou le suivi des projets de recherche et d'innovation [article 33*bis*, paragraphe 1, point b)]. Bien que le CEPD ne fuie pas devant une responsabilité supplémentaire, il tient à insister sur le fait que **la mise en œuvre effective des nouvelles tâches impose de disposer des ressources nécessaires, tant humaines que techniques**[13]. Plus cruciales encore que le nombre de personnes disponibles sont les compétences des experts, qui devraient couvrir un très large éventail de questions, allant des enquêtes pénales et de la coopération policière à l'analyse des mégadonnées et à l'intelligence artificielle. Il en va de même des autorités de contrôle nationales qui, conformément à l'article 44, paragraphe 2, effectueraient des inspections communes en collaboration avec le CEPD.

14. Le présent avis contient également des recommandations spécifiques destinées à s'assurer que les limitations des droits et libertés fondamentaux des personnes concernées, notamment les droits à la protection des données et de la vie privée, dans le cadre de la lutte contre les formes graves de criminalité et le terrorisme, sont limitées au strict nécessaire[14].

3. RECOMMANDATIONS SPÉCIFIQUES

3.1. Coopération avec les parties privées

15. À l'heure actuelle, Europol est autorisé à échanger des données à caractère personnel avec des parties privées sous réserve de conditions spécifiques, conformément à l'article 26 du règlement (UE) 2016/794. Les modifications proposées élargissent les possibilités légales de ces échanges, en particulier dans le cas d'ensembles de données relevant de plusieurs juridictions ou ne pouvant pas être rattachées à une ou plusieurs juridictions.

16. Un nouvel élément de la proposition est l'appui apporté par Europol aux États membres pour empêcher la diffusion à grande échelle, par l'intermédiaire de plateformes en ligne, de contenus à caractère terroriste relatifs à des événements réels en cours ou récents, représentant des atteintes à la vie ou à l'intégrité physique ou appelant à des atteintes imminentes à la vie ou à l'intégrité physique. À cette fin, Europol servirait de canal d'échange de données à caractère personnel avec des parties privées, notamment des hachages, des adresses IP ou des URL en rapport avec ces contenus (nouvel article 26 *bis*)

17. Le CEPD se félicite du choix de la Commission de rejeter comme non proportionnées les autres options stratégiques, qui auraient permis à Europol d'interroger des bases de données gérées par des parties privées ou de demander directement, de sa propre initiative, des données à caractère personnel détenues par ces dernières. En outre, de tels pouvoirs n'auraient pas été compatibles avec la limitation prévue à l'article 88, paragraphe 3, TFUE, qui exclut l'application de mesures coercitives par Europol.

18. Le CEPD observe également avec satisfaction que, pour contrebalancer les nouveaux pouvoirs d'Europol, la proposition maintient les garanties spécifiques existantes, comme l'exigence de nécessité «absolue» ou «stricte» (article 26, paragraphe 5), et en introduit de nouvelles, telles que l'**interdiction de transferts systémiques, massifs ou structurels** (article 26, paragraphe 6, dernier alinéa). Toutefois, étant donné que ce dernier point ne concerne que les cas de transferts internationaux à des parties privées établies en dehors de l'UE, **le CEPD recommande que cette garantie s'applique également aux transferts à des parties privées établies dans l'Union**.

19. Le CEPD est d'avis que le rôle et les responsabilités juridiques exacts d'Europol, lorsqu'il agit en tant que prestataire de services aux autorités nationales en offrant son infrastructure d'échanges de données entre les États membres et les parties privées, ne sont pas suffisamment clairs. En fait, la seule orientation relative à ce point est fournie dans une note en bas de page de l'analyse d'impact, où la Commission considère que «[e]n pareils cas, Europol agit comme sous-traitant plutôt que comme responsable du traitement»[15]. Or, le règlement Europol actuel ne définit pas la notion de «sous-traitant». Dès que l'article 3 et le chapitre IX du RPDUE seront directement applicables à Europol (voir le point 3.1 du présent avis), l'Agence devra se conformer aux conditions et aux obligations incombant à un sous-traitant en vertu de l'article 87 du RPDUE. Par conséquent, eu égard également au principe de responsabilité, **le CEPD rappelle qu'en vertu de l'article 87, paragraphe 3, du RPDUE, un certain nombre d'éléments obligatoires devraient être prévus dans un acte juridique contraignant en vertu du droit de l'Union ou du droit des États membres**[16].

20. Le CEPD s'inquiète également des répercussions pratiques possibles du nouveau paragraphe 6 *ter* de l'article 26. Compte tenu de l'engagement de la Commission en vertu duquel «[p]our qu'Europol exerce son mandat avec efficacité et succès, il est essentiel que tous les traitements de données qu'il effectue *par l'intermédiaire de son infrastructure* se déroulent avec le niveau le plus élevé de protection des données»[17] (soulignement ajouté), **le CEPD recommande qu'Europol procède à une évaluation des risques potentiels pour la sécurité que pose l'ouverture de son infrastructure à une utilisation par des parties privées et, si nécessaire, qu'il mette en œuvre les mesures de prévention et d'atténuation appropriées**.

3.2. Traitement d'ensembles de données vastes et complexes

21. À l'heure actuelle, les enquêtes pénales et les opérations de renseignement en matière pénale incluent de plus en plus fréquemment la collecte et le traitement d'ensembles de données vastes et complexes par les autorités répressives. Le traitement de vastes ensembles de données représente donc désormais une partie importante du travail d'Europol en vue de produire des renseignements en matière pénale. Toutefois, alors que le traitement de ces informations pourrait être licite au regard du droit national, le règlement Europol est actuellement plus restrictif. En particulier, Europol ne peut traiter que des informations relatives à certaines catégories de personnes, à savoir les suspects, les contacts et l'entourage, les victimes, les témoins ou les informateurs, et certaines catégories de données (article 18, paragraphe 5, et annexe II B du règlement Europol).

22. En raison de l'incohérence entre les pratiques d'Europol relatives aux vastes ensembles de données et le cadre juridique en vigueur, le CEPD a décidé d'adresser un avertissement à Europol en septembre 2020[18]. La décision portait spécifiquement sur les questions juridiques soulevées par le traitement de vastes ensembles de données, à savoir l'absence de la base juridique nécessaire ainsi que l'application du principe de minimisation des données. Dans le même temps, il convient de garder à l'esprit que l'analyse de mégadonnées soulève un certain nombre d'autres défis en termes de protection des données à caractère personnel, notamment la limitation de la finalité, la minimisation des données, la qualité des données, la limitation de la durée de conservation, la transparence, etc.[19].

23. Le CEPD note que la proposition s'efforce de résoudre le problème juridique structurel détecté en introduisant une «analyse préalable» des ensembles de données vastes et complexes reçus dans le seul but de déterminer si ces données relèvent des catégories de personnes concernées et des catégories de données à caractère personnel visées à l'article 18, paragraphe 5, et à l'annexe II B du règlement Europol (nouveau paragraphe 5 *bis* de l'article 18). En outre, le traitement préalable des données est limité à une période maximale d'un an, qui peut être prolongée dans des cas justifiés, moyennant l'autorisation préalable du CEPD.

24. Le CEPD se réjouit des garanties qui accompagnent l'«analyse préalable» proposée, qui sont généralement conformes aux principes de limitation de la finalité et de limitation de la conservation en matière de protection des données, ainsi que du fait que ce nouveau type de traitement est interprété comme une dérogation aux règles générales. Le CEPD est toutefois d'avis qu'il doit être limité aux seuls cas où le transfert des États membres à Europol et le traitement ultérieur de vastes ensembles de données par l'Agence est effectivement une nécessité objective. En d'autres termes, **la dérogation visée à l'article 18, paragraphe 5 *bis* ne devrait pas devenir la règle**.

25. Le CEPD se pose également des questions sur la manière dont la possibilité légale de prolonger la période maximale d'analyse préalable prévue au paragraphe 5 *bis* va fonctionner dans la pratique. Compte tenu de l'absence de critères spécifiques ou, à tout le moins, d'indications générales sur ce qui devrait être considéré comme des «cas justifiés», l'autorisation préalable de la prolongation par le CEPD pourrait, en fait, se transformer en «approbation» des demandes de l'Agence. Par ailleurs, le rapport entre la nouvelle dérogation prévue à l'article 18, paragraphe 5 *bis*, et la dérogation existante prévue au paragraphe 6 dudit article n'est pas totalement clair. Les deux dispositions prévoient «un traitement temporaire des données» (analyse préalable) à des fins similaires, mais pas identiques. Par conséquent, **le CEPD recommande que le règlement définisse plus précisément les cas dans lesquels Europol pourrait appliquer la dérogation prévue au paragraphe 5 *bis* ou quand l'Agence peut demander une prolongation de la période maximale d'un an. En outre, l'interaction entre les paragraphes 5 *bis* et 6 de l'article 18 devrait être clarifiée.**

3.3. Traitement de données à l'appui d'une enquête pénale spécifique

26. Le traitement d'informations proposé par Europol à l'appui des enquêtes pénales spécifiques prévu par le nouvel article 18 *bis* est une autre réponse au «défi des mégadonnées», qui a conduit à l'avertissement donné par le CEPD à Europol. Il s'agit aussi de la modification du cadre juridique qui aura l'impact le plus important sur la protection des données à caractère personnel, dans la mesure où elle permettra un vaste traitement de données en dehors de la liste des catégories de données à caractère personnel figurant à l'annexe II et au-delà des délais de conservation actuels prévus par le règlement Europol.

27. Le CEPD est conscient du fait que certains États membres pourraient ne pas disposer des outils, de l'expertise et des ressources informatiques nécessaires à l'analyse d'ensembles de données vastes et complexes dans le cadre d'une enquête pénale et pourraient donc s'adresser à Europol pour lui demander de l'aide. S'il convient, de manière générale, d'encourager et de soutenir la mise en commun d'expertise et de capacités au niveau de l'Union lorsqu'il s'agit d'enquêtes complexes, telles que celles relatives à la cybercriminalité ou au terrorisme, le CEPD craint que la large dérogation par rapport aux garanties existantes en matière de minimisation des données et de limitation de leur durée de conservation prévues par le règlement Europol puisse, dans la pratique, menacer le système actuel de contrôles et d'équilibres qui régit le traitement des données à caractère personnel par l'Agence.

28. L'impact potentiel de la mesure proposée est reconnu dans l'analyse d'impact qui accompagne la proposition législative, y compris la nécessité de «tenir pleinement compte des droits fondamentaux et, notamment le droit à la protection des données à caractère personnel». L'option stratégique retenue (option 4) est présentée comme une «exception limitée et justifiée», qui s'appliquerait «à titre exceptionnel»[20]. Dans le même ordre d'idées, le dix-huitième considérant de la proposition législative prévoit deux évaluations parallèles de la nécessité et de la proportionnalité du traitement du dossier d'enquête par Europol, qui seraient réalisées par l'État membre concerné et par l'Agence. Néanmoins, ces garanties importantes ne subsistent que dans les dispositions non contraignantes susvisées et n'apparaissent pas dans le libellé de l'article 18 *bis*.

29. Eu égard aux observations qui précèdent, **le CEPD recommande d'introduire des garanties efficaces à l'article 18 *bis* afin de faire en sorte que cette dérogation soit appliquée à titre exceptionnel et d'éviter ainsi le risque que l'exception devienne la règle. À cet effet, le règlement modifié devrait établir certaines conditions et/ou seuils, tels que l'ampleur, la complexité, le type ou l'importance des enquêtes.** Ces garanties légales devraient ensuite être précisées par le conseil d'administration d'Europol, conformément à l'article 18 *bis*, paragraphe 2, deuxième alinéa.

30. En outre, **le CEPD souligne que le traitement de données à caractère personnel au titre de la dérogation prévue à l'article 18 *bis* devrait toujours être conforme aux principes et obligations généraux énoncés au chapitre IX du RPDUE**.

3.4. Utilisation de données à des fins de recherche et d'innovation

31. La recherche et l'innovation à des fins répressives constituent un autre domaine dans lequel la proposition législative entend élargir le mandat et le rôle d'Europol. Compte tenu de l'évolution des menaces pour la sécurité et de l'exploitation de la transformation numérique et des nouvelles technologies par les criminels, la modification proposée a pour objectif d'appuyer la réponse au niveau de l'UE en dotant les autorités répressives des outils nécessaires pour contrer ces menaces.

32. Le CEPD prend note des différents arguments avancés à l'appui du choix stratégique consistant à attribuer à Europol un rôle de premier plan dans le domaine de la recherche et de l'innovation. À cet égard, le CEPD tient à insister sur les normes communes élevées, la transparence renforcée ainsi que la souveraineté technologique et l'autonomie stratégique de l'UE en matière de sécurité intérieure. L'alternative – à savoir qu'Europol et les autorités répressives nationales s'appuient sur des outils et des produits mis au point par des fournisseurs externes, très souvent établis en dehors de l'UE – représente clairement des risques nettement plus grands, notamment en ce qui concerne les droits fondamentaux au respect de la vie privée et à la protection des données[21].

33. Compte tenu du fait que le développement de nouvelles technologies nécessite très souvent le traitement d'un grand volume de données, par exemple pour l'entraînement des algorithmes, le défi principal consiste à savoir comment garantir la stricte nécessité et la proportionnalité de ce traitement[22]. Sur ce point, le CEPD se félicite de l'introduction d'un certain nombre de garanties spécifiques dans le nouvel article 33 *bis*, notamment l'obligation de procéder à «une analyse d'impact relative à la protection des données en ce qui concerne les risques pour *l'ensemble des droits et libertés* des personnes concernées, *y compris de tout biais éventuel*» (soulignement ajouté). La liste des garanties énumérées à l'article 33 *bis* ne devrait toutefois pas être considérée comme exhaustive, mais uniquement comme un minimum et tous les autres principes pertinents en matière de protection des données devraient aussi être pleinement pris en compte, notamment la minimisation des données, la protection de la vie privée dès la conception et par défaut, etc. Dans le même temps, le CEPD estime que la portée de la finalité du nouveau traitement, énoncée à l'article 18, paragraphe 2, point e), est trop large. Par conséquent, **le CEPD recommande que la portée des activités de recherche et d'innovation soit mieux définie dans le règlement Europol, par exemple en associant clairement ces activités aux tâches d'Europol, et également précisée dans un document contraignant, par exemple un document adopté par le conseil d'administration d'Europol, qui pourrait être mis à jour ultérieurement, si nécessaire**.

34. De plus, l'analyse d'impact accompagnant la proposition législative prévoit la participation d'Europol au déploiement de la stratégie européenne pour les données, en tant qu'acteur majeur de la mise en place et de l'utilisation de l'espace européen des données de sécurité, et tient compte également du livre blanc de la Commission sur l'intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance. Gardant à l'esprit les risques accrus découlant du traitement à grande échelle de données et de l'utilisation d'algorithmes dans le domaine répressif, **le CEPD estime que les observations et recommandations formulées dans ses avis sur la stratégie européenne pour les données[23] et sur le livre blanc sur l'intelligence artificielle[24], valent aussi pleinement pour la recherche et l'innovation menées par Europol**, en particulier en ce qui concerne l'application des principes régissant la protection des données, les interdictions relatives à l'utilisation de données à caractère personnel sensibles à d'autres fins, la responsabilité et l'application dans le cadre de l'UE, l'identification biométrique à distance, etc.

3.5. Renforcement de la coopération d'Europol avec les pays tiers

35. Le CEPD relève que, contrairement aux intentions initiales[25], les modifications du règlement Europol concernant les transferts internationaux de données sont assez limitées. En effet, le seul élément nouveau est la possibilité légale, prévue à l'article 25, paragraphe 5, pour le directeur exécutif d'Europol d'autoriser des *catégories* de transferts de données à caractère personnel vers des pays tiers dans des situations particulières et au cas par cas.

36. Le CEPD comprend que la modification proposée vise à assouplir davantage la coopération internationale, notamment dans le cadre d'une enquête pénale. Cependant, la signification exacte des «*catégories* de transferts» visées à l'article 25, paragraphe 5, n'est pas tout à fait claire, pas plus que la différence entre ces catégories et la «*série* de transferts» visée au paragraphe 6. En outre, dans l'analyse d'impact accompagnant la proposition législative, la Commission admet une «sous-utilisation» des fondements juridiques des transferts déjà prévus dans le règlement Europol[26].
37. Le CEPD souligne que l'absence de clarté quant à ce qui pourrait être inclus dans «une catégorie de transferts» crée des risques potentiels pour la protection des données à caractère personnel des personnes concernées, en particulier si, dans la pratique, l'Agence donne une interprétation large à cette notion. L'analyse d'impact indique en effet que «[c]ela permet des transferts [...] *liés à l'infraction en cause* lorsque *l'enquête le nécessite*»[27] (soulignement ajouté). Toutefois, comme expliqué précédemment dans le présent avis, l'analyse d'impact est un document non contraignant et ne suffit pas à garantir la clarté et la sécurité juridiques nécessaires. Par conséquent, **le CEPD recommande que le sens de l'expression «catégories de transferts» et la distinction avec les «séries de transferts» soient précisés et clarifiés davantage dans le règlement Europol**.

38. En outre, la proposition législative prévoit la «*suppression*» de la phrase suivante à l'article 25, paragraphe 8: «Lorsqu'un transfert est effectué en vertu du paragraphe 5, ce transfert est documenté et la documentation est mise à la disposition du CEPD, sur demande. La documentation comporte un relevé de la date et de l'heure du transfert et des informations sur l'autorité compétente destinataire, sur la justification du transfert et sur les données opérationnelles à caractère personnel transférées». Or, le paragraphe 8 actuel ne contient pas ce texte. En outre, l'objectif de cette phrase semble être d'introduire une

garantie supplémentaire. Par conséquent, **le CEPD considère qu'il s'agit d'une erreur technique et recommande de remplacer le mot «supprimé» par «ajouté»**.

3.6. Renforcement du cadre de protection des données

39. Le règlement Europol adopté en 2016 prévoit un régime autonome de protection des données, propre à Europol. Le RPDUE adopté par la suite a introduit un chapitre distinct, contenant des règles générales applicables au traitement des données opérationnelles à caractère personnel par les organes, organismes et agences de l'Union dans l'exercice d'activités qui relèvent de la coopération judiciaire en matière pénale et de la coopération policière. Europol et le Parquet européen ont toutefois conservé leurs régimes autonomes de protection des données, soumis à un examen juridique de la Commission au plus tard le 30 avril 2022[28].

40. Le CEPD se réjouit de la proposition de renforcer davantage le cadre d'Europol en matière de protection des données et la soutient pleinement, et, en particulier, l'application directe du chapitre IX et de l'article 3 du RPDUE au traitement de données opérationnelles par l'Agence. Cela marque également une étape importante vers une harmonisation complète du cadre de la protection des données pour toutes les institutions, organes et agences de l'UE, que le CEPD n'a cessé de demander[29] et qui guide les propositions de réforme du cadre de protection des données depuis 2009[30].

41. Dans le même temps, le CEPD relève qu'un élément important fait toujours défaut: l'harmonisation des pouvoirs du CEPD vis-à-vis d'Europol avec les pouvoirs généraux du CEPD prévus à l'article 58 du RPDUE. À titre d'exemple, à l'heure actuelle, le CEPD n'est pas habilité à ordonner à Europol de mettre les opérations de traitement en conformité avec les dispositions du RPDUE, d'infliger une amende administrative en vertu de l'article 66 du RPDUE en cas de non-conformité ou d'ordonner la suspension des transferts de données vers un destinataire établi dans un État membre, un pays tiers ou une organisation internationale[31].

42. Le fait que le chapitre IX du RPDUE ne contienne pas de dispositions *sui generis* sur le contrôle montre clairement que le législateur de l'Union n'a pas eu l'intention d'établir un régime de contrôle distinct pour les données opérationnelles à caractère personnel. Ce choix stratégique est expressément confirmé au onzième considérant du RPDUE, qui dispose qu'«[a]fin de réduire la fragmentation juridique, les règles spécifiques en matière de protection des données applicables au traitement de données opérationnelles à caractère personnel par les organes ou organismes de l'Union lorsqu'ils exercent des activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou 5, du traité sur le fonctionnement de l'Union européenne **devraient être conformes aux [...] dispositions du présent règlement relatives à un contrôle indépendant, aux voies de recours, à la responsabilité et aux sanctions**» (caractères gras ajoutés). Dans le même contexte, l'article 98, paragraphe 1, point c), du RPDUE invite spécifiquement la Commission à «identifier les divergences qui sont susceptibles de donner lieu à une fragmentation juridique de la législation en matière de protection des données dans l'Union», lorsqu'elle réexamine les actes juridiques qui régissent le traitement de données opérationnelles à caractère personnel par les organes ou organismes de l'Union.

43. Outre les arguments juridiques susvisés, il convient d'ajouter qu'il n'est que juste que l'ensemble des institutions, organes et agences de l'UE soient soumis aux mêmes pouvoirs

de contrôle du CEPD, étant donné que toute différenciation mettrait certains d'entre eux dans une position plus ou moins privilégiée. Par conséquent, conformément à la volonté clairement affichée du législateur de l'UE, **le CEPD demande que ses pouvoirs de contrôle à l'égard d'Europol soient alignés sur les pouvoirs que l'article 58 du RPDUE confère au CEPD. À cet effet, les paragraphes 3 et 4 actuels de l'article 43 «Contrôle par le CEPD» du règlement (UE) 2016/794 devraient être supprimés, de sorte que les dispositions de l'article 58 du RPDUE s'appliquent directement**.

44. Le CEPD relève également que le nouvel article 37 *bis* proposé «Droit à la limitation du traitement» n'est pas suffisamment clair et précis en ce qui concerne les possibilités légales de traiter des données à caractère personnel soumises à une limitation. Outre les deux finalités énoncées à l'article 82, paragraphe 3, du règlement (UE) 2018/1725, auxquelles l'article 37 *bis* fait expressément référence, à savoir vérifier l'exactitude des données à caractère personnel et l'utilisation de données comme preuves, la proposition législative en introduit une nouvelle: «la protection des droits de la personne concernée ou d'une autre personne physique ou *morale*» (soulignement ajouté). Le CEPD considère que cette formulation est trop large et pourrait, dans la pratique, priver la limitation du traitement des données à caractère personnel de l'effet escompté. En outre, elle créerait une fragmentation juridique supplémentaire de la législation en matière de protection des données dans l'Union. Par conséquent, **le CEPD recommande que la nouvelle finalité proposée à l'article 37 *bis* soit supprimée et que la limitation du traitement de données à caractère personnel par Europol soit directement régie par la disposition de l'article 82 du règlement (UE) 2018/1725**.

45. Le CEPD note que la proposition remplace le modèle actuel de contrôle coordonné d'Europol, exercé par un comité de coopération composé des autorités de contrôle des États membres, par le modèle unique de contrôle coordonné prévu à l'article 62 du RPDUE et, respectivement, le comité de contrôle de la coordination du comité européen de la protection des données. Le CEPD est convaincu que ce changement, qui vise à apporter une plus grande cohérence et à harmoniser davantage le contrôle des agences de l'UE et des systèmes d'information à grande échelle, apportera encore d'autres possibilités d'exploiter les compétences et l'expérience des autorités de contrôle nationales.

3.7. Autres éléments

3.7.1. Transmission de données opérationnelles à caractère personnel aux institutions, organes et organismes de l'Union

46. La proposition législative actualise les règles actuelles de l'article 24 sur le transfert de données opérationnelles à caractère personnel par Europol aux institutions, organes et organismes de l'Union. Le CEPD se réjouit du fait que la nouvelle disposition précise davantage les conditions de ces transferts, en particulier les exigences de licéité et de nécessité. Dans le même temps, le CEPD observe que la règle générale énoncée à l'article 71, paragraphe 2, du règlement (UE) 2018/1725, applicable au traitement par le même ou par un autre responsable du traitement de l'UE pour des finalités autres que celles pour lesquelles les données opérationnelles à caractère personnel ont été collectées, établit une exigence supplémentaire de proportionnalité, qui fait défaut dans la proposition. Par conséquent, **le CEPD invite le législateur à aligner les conditions applicables aux transferts de données à d'autres organes de l'Union prévues à l'article 24 du**

règlement Europol sur les règles générales énoncées à l'article 71, paragraphe 2, du règlement (UE) 2018/1725, notamment l'exigence de proportionnalité.

3.7.2. Analyse opérationnelle conjointe entre Europol et les États membres

47. Un autre changement juridique visant à réglementer les activités de traitement qui sont apparues dans la pratique et n'étaient pas initialement prévues dans le règlement Europol, concerne les analyses opérationnelles conjointes entre Europol et les États membres (article 20, paragraphe 2 *bis*, et considérant 20). Comme indiqué précédemment dans le présent avis, le CEPD est favorable à la mise en commun des ressources et des compétences au niveau de l'Union en matière de lutte contre les formes graves de criminalité et le terrorisme. Dans le même temps, il estime que les dispositions légales pertinentes pourraient encore être améliorées dans un souci de clarté et de sécurité juridiques.

48. Dans ce contexte, le CEPD observe que la notion d'«analyses opérationnelles conjointes» n'est mentionnée qu'au vingtième considérant et n'est pas définie dans les dispositions légales du règlement Europol. En outre, les règles juridiques applicables au traitement des données à caractère personnel dans le cadre de ces analyses opérationnelles conjointes sont ambiguës. Le vingtième considérant, dernière phrase, indique que [t]out traitement de données à caractère personnel effectué par les États membres dans le cadre d'une analyse opérationnelle conjointe devrait respecter les règles et garanties énoncées dans le présent règlement», ce qui correspond également à l'article 18, paragraphe 4, du règlement Europol. Parallèlement, l'article 20, paragraphe 3, dispose que les États membres peuvent avoir accès et procéder à un traitement ultérieur des informations conformément à leur droit national. Par conséquent, **le CEPD recommande que la notion d'«analyse opérationnelle conjointe» et les règles juridiques applicables au traitement de données à caractère personnel soient clairement définies dans le règlement Europol et pas uniquement dans l'exposé des motifs**.

4. CONCLUSIONS

49. À la lumière des considérations qui précèdent, le CEPD émet les recommandations suivantes:

Sur la coopération avec les parties privées

- l'interdiction des transferts systémiques, massifs ou structurels (article 26, paragraphe 6, dernier alinéa) devrait s'appliquer à tous les échanges avec des parties privées, y compris au sein de l'UE;
- les obligations incombant à Europol lorsqu'il agit en tant que sous-traitant/prestataire de services, en particulier les éléments obligatoires visés à l'article 87, paragraphe 3, du règlement (UE) 2018/1725, devraient être énoncées dans un acte juridique contraignant relevant du droit de l'Union ou du droit des États membres;
- le CEPD recommande qu'Europol procède à une évaluation des risques potentiels pour la sécurité que pose l'ouverture de son infrastructure à une utilisation par des parties privées et, si nécessaire, qu'il mette en œuvre les mesures de prévention et d'atténuation appropriées.

Sur le traitement d'ensembles de données vastes et complexes, notamment à l'appui d'enquêtes pénales spécifiques

- le règlement Europol devrait prévoir des garanties suffisantes pour que les dérogations visées à l'article 8, paragraphe 5 *bis*, et à l'article 18 *bis* ne deviennent pas la règle dans la pratique;
- le règlement Europol devrait définir plus précisément les cas dans lesquels Europol pourrait appliquer la dérogation prévue à l'article 18, paragraphe 5 *bis*, ou quand l'Agence peut demander une prolongation de la période maximale d'un an. En outre, l'interaction entre les paragraphes 5 *bis* et 6 de l'article 18 devrait être clarifiée.
- l'article 18 *bis* devrait fixer des conditions et des seuils supplémentaires pour le traitement par Europol de données ne relevant pas des catégories de personnes concernées énumérées à l'annexe II à l'appui d'une enquête pénale spécifique, tels que l'ampleur, la complexité, le type ou l'importance de l'enquête;
- le traitement de données à caractère personnel au titre des dérogations prévues à l'article 18, paragraphe 5 *bis*, et de l'article 18 *bis* devrait toujours être conforme aux principes et obligations généraux énoncés au chapitre IX du règlement (UE) 2018/1725.

Sur l'utilisation de données à des fins de recherche et d'innovation

- la portée des activités de recherche et d'innovation devrait être mieux définie dans le règlement Europol et précisée dans un document contraignant, qui pourrait être mis à jour ultérieurement.

Sur la coopération d'Europol avec les pays tiers

- la signification de l'expression «catégories de transferts» visée à l'article 25, paragraphe 5, et la distinction par rapport à la «série de transferts» visée au paragraphe 6 du même article devraient être précisées et clarifiées davantage dans le règlement Europol.

Sur le cadre de protection des données applicable à Europol

- les pouvoirs de contrôle du CEPD à l'égard d'Europol devraient être pleinement alignés sur les pouvoirs généraux conférés au CEPD par l'article 58 du règlement (UE) 2018/1725;
- la nouvelle finalité proposée à l'article 37 *bis* devrait être supprimée et la limitation du traitement de données à caractère personnel par Europol devrait donc être directement régie par l'article 82 du règlement (UE) 2018/1725.

Sur les autres éléments de la proposition

- les conditions applicables aux transferts de données à d'autres organes de l'Union prévues à l'article 24 du règlement Europol devraient être alignées sur les règles générales énoncées à l'article 71, paragraphe 2, du règlement (UE) 2018/1725, notamment l'exigence de proportionnalité;
- la notion d'«analyse opérationnelle conjointe» et les règles juridiques applicables au traitement de données à caractère personnel dans le cadre d'une telle analyse devraient être clairement définies dans le règlement Europol.

Bruxelles, le 8 mars 2021

Wojciech Rafał WIEWIÓROWSKI
(signature électronique)

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol) (JO L 121 du 15.5.2009, p. 37).
[5] COM(2020) 796 final.
[6] COM(2020) 605 final (24.7.2020).
[7] https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_2326
[8] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2018/1862 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale en ce qui concerne l'introduction de signalements par Europol, COM(2020) 791 final.
[9] Voir, notamment, la résolution du Parlement européen du 10 juillet 2020 sur une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme (2020/2686(RSP), les conclusions du Conseil sur la coopération d'Europol avec les parties privées du 2 décembre 2019 ou la déclaration des ministres de l'Intérieur de l'UE («Plan d'action en dix points sur l'avenir d'Europol») du 21 octobre 2020.
[10] https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en
[11] Contrôleur européen de la protection des données: Évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel: boîte à outils (11.4.2017), Contrôleur européen de la protection des données: Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel (19.12.2019).
[12] Voir le rapport d'analyse d'impact, partie 2, SWD(2020) 543 final (en anglais).
[13] Au point 4 «INCIDENCE BUDGÉTAIRE» de la proposition législative, la Commission estime qu'Europol aura besoin d'un budget supplémentaire d'environ 180 millions d'EUR et d'approximativement 160 postes supplémentaires pour l'ensemble de la période couverte par le cadre financier pluriannuel pour exécuter son mandat révisé. Toutefois, aucune estimation de ce type n'a été calculée pour le CEPD.
[14] Voir les arrêts rendus dans les affaires jointes C-293/12 et C-594/12, DRI, point 52; l'affaire C-73/07, Satakunnan Markkinapörssi et Satamedia, point 56; et les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke et Eifert, points 77 et 86.
[15] Note en bas de page 69, Rapport d'analyse d'impact, partie 1, page 13, SWD(2020) 543 final (en anglais).
[16] Pour un complément d'informations, voir Lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725
[17] Rapport d'analyse d'impact, partie 1, page 9, SWD(2020) 543 final (en anglais).
[18] https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en
[19] Voir aussi l'avis préliminaire du CEPD «Vie privée et compétitivité à l'ère de la collecte de données massives» de mars 2014.
[20] Voir le rapport d'analyse d'impact, partie 1, page 51, SWD(2020) 543 final (en anglais).
[21] L'utilisation de l'application «Clearview AI» par certaines autorités répressives de l'UE est une illustration évidente de ce risque.
[22] On pourrait établir un parallèle avec la conclusion de la Cour de justice de l'UE dans son avis 1/2015 sur l'accord concernant les dossiers passagers entre l'UE et le Canada, dans lequel la Cour a conclu que «l'utilisation systématique des données [PNR] aux fins de vérifier la fiabilité et l'actualité des modèles et des critères préétablis [...] ou de définir de nouveaux modèles et critères [...] doit être considérée comme ne dépassant pas les limites du strict nécessaire». De même, l'utilisation de données opérationnelles à caractère personnel, collectées et stockées légalement par Europol, afin de développer des outils et de fournir des solutions pour faciliter la lutte contre les formes graves de criminalité et le terrorisme, pourrait être justifiée, si elle s'accompagne de garanties efficaces et appropriées.
[23] https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_fr.pdf
[24] https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf
[25] Voir l'analyse d'impact initiale, Ares(2020)2555219.
[26] Voir le rapport d'analyse d'impact, partie 2, annexe 7, pages 109 et 110, SWD(2020) 543 final (en anglais).
[27] Idem.
[28] Voir l'article 2, paragraphe 3, et l'article et 98, du règlement (UE) 2018/1725.

[29] Voir, notamment, l'avis du CEPD du 14 janvier 2011 sur la communication de la Commission intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», ainsi que l'avis 5/2017 du CEPD sur le renforcement des règles de protection des données pour les institutions et organes de l'UE

[30] Dans sa communication sur «Une approche globale de la protection des données à caractère personnel dans l'Union européenne» [COM(2010)609 final], la Commission a conclu que l'Union a besoin d'une politique plus exhaustive et cohérente sur le droit fondamental à la protection des données à caractère personnel. Dans le domaine répressif, la Commission a souligné une nouvelle fois en 2012 que le nouveau cadre réformé de l'UE en matière de protection des données vise donc à garantir un niveau élevé et cohérent de protection des données afin de renforcer la confiance mutuelle entre les autorités policières et judiciaires des différents États membres (et des institutions, organes et organismes de l'Union), contribuant ainsi davantage à la libre circulation des données et à une coopération efficace entre autorités policières et judiciaires [communication de la Commission «Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle», COM(2012)09 final].

[31] Voir l'article 58, paragraphe 2, points e), i) et j), du règlement (UE) 2018/1725.