EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
La voix des avocats européens
Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Position du CCBE sur la proposition de règlement 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

6/05/2021

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million d'avocats européens. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.

En décembre 2020, la Commission européenne a publié une proposition de règlement 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 définit les nouveaux pouvoirs à conférer à Europol pour traiter des données à caractère personnel « *pour soutenir une enquête pénale donnée, Europol peut traiter des données à caractère personnel ne relevant pas des catégories de personnes concernées énumérées à l'annexe II* » (article 18 bis), pour transmettre des données opérationnelles à caractère personnel à une autre institution, un autre organe ou un autre organisme de l'Union « *si elles sont nécessaires à l'exécution légitime de missions de cette autre institution ou de cet autre organe ou organisme de l'Union* » (article 24), pour recevoir des données à caractère personnel directement de parties privées et traiter ces données à caractère personnel « *en vue de prévenir la diffusion de contenus en ligne liés au terrorisme ou à l'extrémisme violent en situation de crise* » (article 26 bis), et pour traiter des données à caractère personnel à des fins de recherche et d'innovation (article 33 bis).

L'objectif du présent document est que le CCBE expose sa position par rapport à un certain nombre d'aspects de la proposition.

A. Commentaires généraux

Tout d'abord, le CCBE observe que les concepts de « sécurité nationale », de « lutte contre le terrorisme », de prévention de « l'extrémisme violent », ainsi que l'invocation d'un prétendu besoin de faire face à des situations de crise sont souvent utilisés par les États et d'autres autorités pour justifier une prétendue nécessité d'obtenir l'accès à des données à caractère personnel. Un des problèmes majeurs à cet égard est l'absence de définition commune internationalement acceptée de ces termes (« sécurité nationale », « terrorisme », « extrémisme », etc.), ce qui fait qu'il est difficile pour les tribunaux de s'assurer que les mesures de surveillance sont conformes à un critère strict de ce qui est nécessaire et proportionné. Le CCBE a déjà abordé la question dans ses recommandations sur la protection des droits fondamentaux dans le contexte de la sécurité nationale[1].

[1] Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale », pages 2 et 26.

Le CCBE estime que tout accès direct ou indirect aux données à caractère personnel des citoyens entrepris par un État doit s'inscrire dans les limites de l'état de droit. Étant donné qu'il constituerait une ingérence dans les droits fondamentaux, il doit être proportionnel et, en particulier, être limité au minimum en ce qui concerne l'étendue de la surveillance et la période de conservation des données[2].

À cet égard, le CCBE rappelle que la Cour européenne des droits de l'homme (ci-après la « **CEDH** ») a jugé que la simple conservation de données relatives à la vie privée d'un individu, indépendamment de leur utilisation ultérieure, constitue une ingérence au sens de l'article 8 de la Convention européenne des droits de l'homme, qui garantit le droit au respect de la vie privée et familiale, du domicile et de la correspondance[3]. Pour sa part, la Cour de justice de l'Union européenne (ci-après la « **CJUE** ») considère que l'accès à des données à caractère personnel en vue de leur conservation ou de leur utilisation porte atteinte au droit fondamental au respect de la vie privée garanti par l'article 7 de la Charte des droits fondamentaux de l'UE (ci-après « la Charte »). Un tel traitement de données à caractère personnel entre également dans le champ d'application de l'article 8 de la Charte étant donné qu'il constitue un traitement de données à caractère personnel au sens de cet article et, partant, doit nécessairement satisfaire aux exigences de protection des données prévues à cet article[4]. En outre, les deux juridictions considèrent que l'accès aux données à caractère personnel par une autorité publique constitue une ingérence supplémentaire[5]. **Par conséquent, l'accès à des données à caractère personnel, leur conservation et leur utilisation ultérieure par des autorités publiques telles que les services répressifs dans le cadre de mesures de surveillance ne doivent pas dépasser les limites de ce qui est strictement nécessaire, apprécié à la lumière de la Charte, pour être justifiés dans une société démocratique.**

Une telle ingérence devient particulièrement dangereuse lorsqu'on accède à des données et à des communications qui bénéficient d'une protection spéciale en vertu de la loi. C'est clairement le cas des communications entre les avocats et leurs clients, puisque, dans tous les États membres de l'UE, la loi protège de la divulgation les informations communiquées à titre confidentiel entre les avocats et leurs clients[6]. En outre, cette protection est, en matière contentieuse, un élément essentiel pour garantir le droit à un procès équitable garanti par l'article 6 de la Convention européenne des droits de l'homme, qui est un droit absolu et, en toutes matières, un principe fondamental de l'état de droit. **Par conséquent, le CCBE est particulièrement préoccupé par les effets que toute mesure de l'UE sur l'accès d'Europol aux données à caractère personnel pourrait avoir sur le secret professionnel ou le *legal professional privilege*.**

Un autre problème lié à l'accès aux données des avocats conservées en ligne est la difficulté actuelle de déterminer à l'avance si les données relèvent du secret professionnel ou du *legal professional privilege*. Le CCBE reconnaît que les fournisseurs d'accès à Internet n'ont pas encore les moyens, ou, s'ils les ont, seulement de manière très limitée, de reconnaître si les données demandées par les

---

2 La Cour de justice de l'UE a récemment rendu des arrêts dans les affaires La Quadrature du Net e.a. et Privacy International (C-511/18, 512/18, 520/18 et 623/17), confirmant l'importance accordée par la Cour à la protection des données et l'interprétation stricte de la possibilité de déroger à l'obligation de l'État d'assurer la confidentialité des données pour des raisons de sécurité nationale. La Cour a confirmé que toute dérogation doit toujours être limitée à ce qui est strictement nécessaire et accompagnée de garanties effectives. En particulier, il a été jugé que le droit de l'UE s'oppose à une législation nationale exigeant d'un fournisseur de services de communications électroniques qu'il procède à une transmission ou à une conservation générale et indifférenciée de données aux fins de la lutte contre la criminalité. Voir également les recommandations 02/2020 du Comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, paragraphes 20-22.

3 CEDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, requêtes 30562/04 et 30566/04, §67.

4 CJUE, 16 juillet 2020, Data Protection Commissioner c. Facebook Ireland Limited et Maximillian Schrems, Affaire C-311/18, §170.

5 CJUE, 8 avril 2014, Digital Rights Ireland, affaires C-293/12 et C-594/12 ; CEDH, 26 mars 1987, Leander c. Suède, requête 9248/81, §48.

6 Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance, p. 10

services répressifs relèvent du secret professionnel[7] : il est donc possible que l'accès à des données protégées soit accordé, conduisant à des violations du secret professionnel ou du *legal professional privilege*.

Sur cette question, la CJUE a reconnu que : « *une transmission des données relatives au trafic et des données de localisation à des autorités publiques à des fins sécuritaires est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte.* ***De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel »***[8]**.**

À cet égard, le CCBE souligne que les fournisseurs d'accès à Internet ou les services répressifs et Europol devraient être tenus de s'assurer que les technologies utilisées pour recueillir, traiter et échanger des données à caractère personnel entre eux garantissent qu'il n'y a aucune interférence avec tout type de données relevant du secret professionnel. En tout état de cause, les services répressifs devraient être tenus d'utiliser tous les moyens technologiques disponibles pour écarter le matériel relevant du secret professionnel ou du *legal professional privilege* du champ des opérations de surveillance ou du recueil, de la conservation, du traitement et du transfert des données à caractère personnel. Le développement d'une telle technologie doit être une priorité absolue.

En vue d'informer les législateurs et les décideurs politiques des normes à respecter afin de garantir que les principes essentiels du secret professionnel et du *legal professional privilege* ne soient pas remis en cause, il est proposé de formuler les recommandations suivantes, fondées sur les Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance[9].

1. Nécessité d'un contrôle législatif

Le CCBE considère que toute activité de surveillance entreprise par les services répressifs doit être réglementée avec une spécificité et une transparence adéquates. Ce principe doit s'appliquer à Europol. Par conséquent, toute mesure européenne relative aux pouvoirs d'Europol en matière d'accès aux données à caractère personnel doit être soumise à un contrôle législatif efficace dans un cadre réglementaire clair[10].

À cet égard, le CCBE met l'accent sur le fait que les concepts de sécurité nationale/extrémisme/terrorisme/crise en tant qu'éléments justificatifs du traitement des données à caractère personnel devraient être définis de manière suffisamment précise et claire. La proposition prévoit qu'Europol puisse échanger des données à caractère personnel avec des parties privées dans le cadre de la réponse à des crises, conformément au nouvel article 26 bis. L'objectif de cette disposition est d'empêcher la diffusion de contenus liés au terrorisme ou à l'extrémisme violent dans les situations de crise. La proposition ne définit cependant pas en particulier ce qu'est une situation de crise, ni le terrorisme, ni l'extrémisme violent. Le CCBE estime

---

7 Discussions menées entre le CCBE et EURO-ISPA (Association européenne des fournisseurs de services Internet, https://www.euroispa.org/about/).

8 CJUE, 6 octobre 2020, Privacy International, Affaire C-623/17, §72.

9 Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale », pages 2 et 22.

10 Ceci est conforme à la position du Comité européen de la protection des données, telle qu'elle est exposée dans les Recommandations 02/2020 du Comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance (paragraphes 26-31).

que la proposition doit prévoir des dispositions plus claires et précises en ce qui concerne les justifications du recueil, du traitement et de l'échange de données à caractère personnel.

Le pouvoir d'accès aux données à caractère personnel doit être réglementé avec la même spécificité et transparence. **Le CCBE considère que l'accès aux données à caractère personnel ne devrait être autorisé que lorsqu'Europol, en tant qu'organisme souhaitant entreprendre une surveillance, peut établir qu'il existe des raisons impérieuses donnant lieu à un degré de suspicion suffisant pour justifier l'interception[11]. Ces raisons devraient être clairement définies.**

À cet égard, le CCBE se réfère à la jurisprudence la plus récente de la CJUE, selon laquelle « Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général. »[12]

Au-delà du cadre réglementaire, le CCBE considère que des contrôles législatifs et un contrôle démocratique efficaces doivent être mis en place pour évaluer politiquement l'activité d'Europol et le traitement des données à caractère personnel ou des données relevant du secret professionnel ou du *legal professional privilege*. À cet égard, le CCBE fait remarquer que, conformément à l'article 88 du TFUE, le règlement Europol prévoit un groupe de contrôle parlementaire conjoint (article 51), dont les membres proviennent à la fois des parlements nationaux et du Parlement européen. La proposition renforce ce contrôle en prévoyant qu'Europol devrait fournir chaque année au groupe de contrôle parlementaire conjoint des informations sur l'utilisation de ses outils et capacités supplémentaires ainsi que sur les résultats obtenus (considérant 40, modification de l'article 51, paragraphe 3).

Cependant, le CCBE considère que le contrôle législatif actuel et les dispositions de renforcement proposées ne sont pas suffisants pour assurer un contrôle démocratique efficace des activités d'Europol. En ce qui concerne les risques et les menaces pour les droits fondamentaux causés par le traitement des données à caractère personnel de la part des services répressifs et d'Europol, les pouvoirs de contrôle conférés au groupe de contrôle parlementaire conjoint devraient être renforcés de manière à aller au-delà du pouvoir de questionner ou d'être informé des activités d'Europol. Le règlement devrait prévoir des pouvoirs et des responsabilités plus concrets pour le groupe de contrôle parlementaire conjoint, ainsi que des sanctions efficaces et d'autres conséquences appropriées en cas de constatation d'une violation des droits fondamentaux.

2. Autorisation judiciaire préalable, contrôle indépendant et recours effectifs

Selon les nouveaux articles 26 §6a, et 26 bis §5 proposés, Europol peut demander aux États membres d'obtenir des données à caractère personnel auprès de parties privées conformément à leur législation applicable, afin de les partager avec Europol, à condition que les données à caractère personnel demandées se limitent strictement à ce qui est nécessaire à Europol. Il est précisé que « les *États membres veillent à ce que leurs autorités nationales compétentes puissent légalement traiter ces*

---

[11] De même, le Comité européen de la protection des données exige que « la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées » (Recommandations 02/2020 du Comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, para. 32-38).

[12] CJUE, 6 octobre 2020, La Quadrature du Net e.a., affaires C-511/18, C-512/18 et C-520/18, §140. Voir également CJUE, 2 mars 2021, H.K. c. Prokuratuur, affaire C-746/18, §45.

demandes conformément à leur droit national afin de fournir à Europol les informations nécessaires à la réalisation de ses objectifs ».

À cet égard, le CCBE observe qu'une **autorisation préalable accordée par un tribunal** doit être requise pour tout accès aux données à caractère personnel par les services répressifs. **La Cour européenne des droits de l'homme et la CJUE ont précisé à de nombreuses reprises que toute ingérence dans le droit à la vie privée et à la protection des données doit être soumise à un système de contrôle effectif, indépendant et impartial[13].**

La législation doit garantir que les **données à caractère personnel obtenues sans autorisation judiciaire préalable spécifique sont irrecevables devant les tribunaux.** En outre, il est nécessaire d'exiger la destruction de tout matériel intercepté considéré comme ayant été acquis illégalement. Par ailleurs, **toute donnée à caractère personnel interceptée légalement doit être utilisée uniquement dans le but pour lequel l'autorisation a été accordée**.

À cet égard, le CCBE souligne que la proposition ne doit permettre à Europol de contourner ni la nécessité d'une autorisation judiciaire préalable ni le système de contrôle indépendant et impartial qui sont des garanties essentielles[14].

En outre, afin de fournir une protection juridique efficace contre la surveillance illégale, il est nécessaire que des **voies de recours**[15] soient mises à la disposition des citoyens dont les données ont été traitées. En particulier, une fois qu'il a été révélé que des mesures de surveillance ont été prises, les citoyens doivent avoir le droit d'être informés des données qui ont été collectées et traitées et doivent pouvoir contester la légalité de ces mesures devant un juge. En outre, des sanctions appropriées doivent être imposées aux personnes et aux agences qui ont entrepris une surveillance illégale.

Le CCBE fait remarquer que le règlement Europol prévoit que les personnes concernées peuvent déposer une plainte auprès du Contrôleur européen de la protection des données en cas de traitement irrégulier de données à caractère personnel par Europol (article 47). En outre, toute personne ayant subi un préjudice du fait d'un traitement illégal de données a le droit d'être indemnisée par Europol, conformément à l'article 340 TFUE, et a le droit d'intenter une action contre Europol devant la CJUE ou devant les tribunaux nationaux contre les États membres.

Toutefois, le CCBE considère que ces recours devraient être renforcés, au sein même d'Europol, afin de permettre aux personnes concernées d'exercer leurs droits au titre des articles 7 et 8 de la Charte d'être informées du traitement de leurs données, de demander l'accès à leurs données à caractère personnel ayant fait l'objet d'un traitement et, si cela est nécessaire, de faire rectifier ou effacer ces données, ainsi que de disposer d'un recours effectif devant un tribunal.

Le respect de l'état de droit et du secret professionnel/*legal professional privilege* doit être un **principe primordial** dans le cadre de toute mesure européenne relative à la surveillance et, en particulier, à l'accès aux données à des fins de sécurité et de répression. En outre, la loi doit prévoir une **protection explicite du secret professionnel et du *legal professional privilege***, en leur accordant toujours le plus haut niveau de protection.

---

13 CEDH, 1978, Klass et autres c. Allemagne, requête 5029/71 ; CJUE, La Quadrature du Net, §189.

14 Comité européen de la protection des données, Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020.

15 Recommandations 02/2020 du Comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, paragraphes 43 à 47.

Dans le cas où l'accès aux données relatives aux communications avocat-client est accordé dans des circonstances exceptionnelles, le CCBE souligne qu'il doit y avoir un contrôle juridictionnel[16] indépendant à tous les stades de la procédure de surveillance, au cas par cas. Le juge qui supervise la mise en œuvre de l'interception doit être différent du juge qui l'a autorisée.

En outre, lorsque des données relevant du secret professionnel ou du *legal professional privilege* sont interceptées à tort sans autorisation, ces données doivent être effacées immédiatement, qu'elles soient liées ou non à l'affaire concernée. En cas de doute sur la nature protégée des données, Europol devrait séparer les données concernées et effectuer les contrôles nécessaires avant tout traitement.

3. Garanties essentielles applicables au transfert de données à caractère personnel à des parties privées

Selon les nouveaux articles 26 §5 et 26 §6 proposés, Europol peut transmettre ou transférer des données à caractère personnel à des parties privées, établies à l'intérieur ou à l'extérieur de l'UE, au cas par cas dans plusieurs situations et dans le respect des exigences de nécessité absolue et stricte. Une autorisation spécifique du directeur exécutif d'Europol est demandée si la partie privée concernée n'est pas établie au sein de l'Union et des conditions doivent être remplies pour accorder cette autorisation. En particulier, les données à caractère personnel ne sont pas transférées si le directeur exécutif détermine que les libertés et droits fondamentaux de la personne concernée l'emportent sur l'intérêt public du transfert. En outre, les transferts ne doivent être ni systématiques, ni massifs ni structurels. Les garanties spécifiques prévues dans la proposition ont été saluées par le Contrôleur européen de la protection des données[17].

Le CCBE rappelle que la personne concernée dont les données à caractère personnel sont transférées vers un pays tiers doit bénéficier d'un niveau de protection essentiellement équivalent à celui qui est garanti au sein de l'Union européenne[18]. Par conséquent, tout transfert de données à caractère personnel à des parties privées effectué par Europol, au sein ou en dehors de l'UE, doit respecter les garanties européennes essentielles susmentionnées, reconnues par le Conseil de l'UE pour la protection des données :

- **le transfert doit être fondé sur des règles claires, précises et accessibles ;**
- **la nécessité et la proportionnalité par rapport aux objectifs légitimes poursuivis doivent être démontrées ;**
- **un contrôle juridictionnel indépendant doit être assuré ;**
- **la personne concernée doit disposer de voies de recours efficaces.**

En outre, le CCBE considère que des garanties supplémentaires doivent figurer dans la proposition concernant le transfert ou la transmission par Europol de données à caractère personnel à des parties privées, au-delà de celles prévues par le règlement proposé et la législation européenne sur la protection des données. Le CCBE souligne que tout transfert de données à caractère personnel à des parties privées doit tenir dûment compte des droits de la défense et du droit à un procès équitable. En tout état de cause, Europol doit veiller à ce que les données à caractère personnel relevant du secret professionnel ou du *legal professional privilege* ne soient pas transférées.

---

16 Recommandations 02/2020 du Comité européen de la protection des données sur les garanties essentielles européennes pour les mesures de surveillance, paragraphe 39.

17 Avis du Contrôleur européen de la protection des données sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021, point 18.

18 CJUE, 16 juillet 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, point 96.

En outre, avant toute transmission de données à caractère personnel à des parties privées, Europol doit s'assurer que les données sont adéquates, pertinentes et à jour. Cette condition revêt une grande importance lorsque, par exemple, les données concernent des informations relatives à une infraction pénale pour laquelle la personne concernée a été acquittée.

Comme le recommande le Contrôleur européen de la protection des données dans son avis sur la proposition, ces garanties doivent s'appliquer aux transmissions à des parties privées au sein ou à l'extérieur de l'UE[19].

B. Les nouveaux pouvoirs d'Europol en matière de recherche et d'innovation

Le CCBE considère que le pouvoir de recherche et d'innovation proposé doit être lié à des garanties solides, en particulier sur la transparence et le contrôle, notamment pour ce qui est du Contrôleur européen de la protection des données.

1. Développement de technologies reposant sur l'intelligence artificielle pour les services répressifs

Selon le considérant (38), « *Europol devrait jouer un rôle clé en aidant les États membres à développer de nouvelles solutions technologiques fondées sur l'intelligence artificielle, dont pourraient bénéficier les services répressifs nationaux dans toute l'Union*. »

Le CCBE considère qu'Europol ne devrait pas prendre la tête du développement de nouvelles solutions technologiques reposant sur l'intelligence artificielle pour les services répressifs. En effet, le CCBE souligne que de nombreux débats sont encore nécessaires pour évaluer de manière critique le rôle que les outils d'intelligence artificielle devraient jouer, le cas échéant, dans le domaine de l'application de la loi et de la justice pénale. S'il est possible que l'utilisation de l'intelligence artificielle puisse contribuer à la prévention ou à la résolution de crimes, les risques de partialité et de discrimination à l'encontre de certains groupes de la société sont élevés, et la menace d'une surveillance de masse par les systèmes d'intelligence artificielle représente un risque pour les sociétés ouvertes et pluralistes.

Par conséquent, les outils reposant sur l'intelligence artificielle pour l'application de la loi ne devraient être introduits que lorsqu'il existe des garanties suffisantes contre toute forme de partialité ou de discrimination. Toutes les mesures de surveillance accrue doivent être soigneusement mises en balance avec les effets qu'elles peuvent avoir sur une société ouverte et pluraliste. À cet égard, il n'appartient pas à Europol, en tant qu'agence européenne chargée de faire respecter la loi, de jouer un rôle clé dans la promotion d'une intelligence artificielle éthique, digne de confiance et centrée sur l'humain, sous réserve de garanties solides en termes de sécurité, de sûreté et de droits fondamentaux. Si des technologies reposant sur l'intelligence artificielle doivent être développées pour les systèmes judiciaires et répressifs au niveau européen, il devrait d'abord incomber au législateur européen de mettre en place les garanties susmentionnées de manière ouverte et transparente.

2. Champ d'application des activités de recherche et d'innovation d'Europol

Selon **l'article 18, paragraphe 2, point e)**, proposé, Europol pourrait traiter les données à caractère personnel aux fins des « *activités de recherche et d'innovation relatives à des questions relevant du*

[19] Avis du Contrôleur européen de la protection des données sur la proposition de modification du règlement Europol, avis 4/2021, 8 mars 2021, point 18.

présent règlement pour l'élaboration, l'entraînement, l'expérimentation et la validation d'algorithmes pour la mise au point d'outils ».

Le CCBE constate que le Contrôleur européen de la protection des données, dans son avis sur la proposition de modification du règlement Europol, a conclu que le champ d'application de la nouvelle finalité de traitement de la recherche et de l'innovation est défini de manière trop large dans le nouvel article 18 §2 (e)[20]. Le CCBE est d'accord avec cette conclusion.

Compte tenu des risques élevés de partialité et des menaces de surveillance de masse, le champ d'application des activités de recherche et d'innovation d'Europol doit être clairement défini dans la proposition en indiquant notamment les objectifs poursuivis, les activités ciblées des services répressifs, les outils à développer et leurs utilisations prévues.

3. Garanties et contrôle des activités de recherche et d'innovation d'Europol (nouvel article 33 bis)

Le CCBE observe que des garanties supplémentaires ont été prévues dans le nouvel article 33 bis concernant le traitement des données à caractère personnel par Europol dans le cadre de la recherche et de l'innovation. En outre, Europol est tenu de conserver une description complète et détaillée du traitement et du raisonnement qui sous-tend la formation, le test et la validation des algorithmes afin de garantir la transparence et de vérifier l'exactitude des résultats.

En ce qui concerne le contrôle des activités de recherche et d'innovation d'Europol, la proposition prévoit que tout projet est soumis à l'autorisation préalable du directeur exécutif d'Europol, à partir d'une description de l'activité de traitement envisagée précisant la nécessité du traitement ; d'une description de la période de conservation ; des conditions d'accès aux données ; d'une **évaluation des effets sur la protection des données des risques pour tous les droits et libertés des personnes concernées, y compris de toute partialité dans le résultat, et des mesures envisagées pour faire face à ces risques**. En outre, avant le lancement d'un projet de traitement de données à caractère personnel à des fins de recherche et d'innovation, le Contrôleur européen de la protection des données doit être informé.

Le CCBE considère que les garanties prévues dans la proposition sont nécessaires. Toutefois, celles-ci ne sont pas suffisantes et ne constituent qu'un minimum. Le CCBE estime que l'autorisation préalable des projets de recherche et d'innovation devrait émaner d'une autorité indépendante. Le directeur exécutif d'Europol ne devrait pas être le seul à décider si un projet doit être lancé ou non, ni le seul à réaliser une analyse d'impact sur la protection des données de risques pour les droits et libertés des personnes concernées, dont les risques de partialité.

Cette tâche pourrait être confiée au Contrôleur européen de la protection des données. Le CCBE constate que le règlement Europol prévoit déjà à l'article 43(f) la possibilité pour le Contrôleur européen de la protection des données d'imposer une interdiction temporaire ou définitive des traitements effectués par Europol qui sont en violation des dispositions régissant le traitement des données à caractère personnel. Cependant, compte tenu des risques et menaces que cela représente pour les droits et libertés, une telle évaluation ne devrait pas être postérieure au lancement d'un nouveau projet de recherche et d'innovation d'Europol.

En outre, le CCBE souligne que, pour les raisons expliquées ci-dessus, le groupe de contrôle parlementaire conjoint devrait être informé au cas par cas avant le lancement de tout projet de recherche et d'innovation. De tels projets devraient également être menés de manière transparente, non seulement en ce qui concerne les résultats de la recherche mais également en

[20] Avis du Contrôleur européen de la protection des données sur la proposition de modification du règlement Europol, avis 4/2021, 8 mars 2021, point 33.

ce qui concerne l'ensemble du processus. Les parties prenantes, y compris la profession d'avocat, qui sont concernées par l'utilisation des outils pour les services répressifs, devraient être informées de chaque projet envisagé et être consultées à son sujet.

C. Remarques finales

Enfin, le CCBE attire l'attention sur le rapport du Contrôleur européen de la protection des données (CEPD) daté du 17 septembre 2020, qui a donné lieu à un « avertissement » formel à l'encontre d'Europol à la suite du traitement potentiellement illégal des données à caractère personnel d'un grand nombre de personnes innocentes.

Selon le rapport, Europol reçoit de grandes quantités de données des services répressifs nationaux et d'ailleurs et, afin d'utiliser ces données pour des enquêtes judiciaires, a adopté des moyens et des méthodes qui ne sont pas conformes à la législation régissant l'agence.

Le résultat, selon le Contrôleur européen de la protection des données, est (traduction libre) :

« (...) une situation dans laquelle de grandes quantités de données à caractère personnel dont il n'est pas certain qu'elles soient conformes aux exigences établies par (...) le règlement Europol, sont conservées sur les systèmes d'Europol pendant plusieurs années. En tant que tel, le stockage continu de données à caractère personnel susceptibles de dépasser les limites contenues dans ces articles porte atteinte au principe de minimisation des données (...) »

Le rapport souligne qu'Europol traite très probablement de manière illégale les données à caractère personnel d'un grand nombre, en réalité inconnaissable, de personnes : *« (...) il est fort probable qu'Europol traite continuellement des données à caractère personnel de personnes pour lesquelles il n'est pas autorisé à le faire et conserve des catégories de données à caractère personnel qui vont au-delà de la liste restrictive prévue dans (…) le règlement Europol. Bien que le nombre exact ne puisse être quantifié, l'augmentation de l'utilisation du (...) observée ces dernières années montre clairement que la quantité de grands ensembles de données partagés par les États membres avec Europol augmente rapidement. »*

Le rapport expose ensuite ce que cela signifie pour les individus : *« Le traitement de données concernant des personnes dans une base de données répressive de l'UE peut avoir de profondes conséquences sur les personnes concernées. Sans une mise en œuvre adéquate du principe de minimisation des données et des garanties spécifiques contenues dans le règlement Europol, les personnes concernées courent le risque d'être liées à tort à une activité criminelle dans toute l'UE, avec tous les dommages potentiels pour leur vie personnelle et familiale, leur liberté de mouvement et leur profession que cela implique. »*

Le CCBE exhorte instamment Europol et les institutions européennes compétentes, avant tout autre processus législatif, à répondre aux préoccupations susmentionnées en apportant une réponse adéquate, notamment en définissant les mesures et politiques nécessaires qu'ils prévoient d'entreprendre afin de résoudre le problème du traitement illégal des données à caractère personnel qui se pose.

Le CCBE constate par ailleurs que le règlement Europol doit être évalué par la Commission européenne d'ici le 1er mai 2022. L'article 68 prévoit que cette évaluation porte notamment sur les effets, l'efficacité et l'efficience d'Europol et de ses méthodes de travail. Cette évaluation est la meilleure occasion d'entreprendre une analyse approfondie du règlement en ce qui concerne la compatibilité des activités d'Europol avec les droits fondamentaux. Le CCBE considère en conséquence que l'adoption de la proposition visant à renforcer le mandat d'Europol, à la suite de l'avertissement du Contrôleur européen des données, est prématurée et hâtive.