EUROPEAN DATA PROTECTION SUPERVISOR

Avis 11/2017

Avis du CEPD sur la proposition de règlement relatif au système ECRIS-TCN

12 décembre 2017

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE. Le contrôleur est chargé, en vertu de l'article 41, paragraphe 2, du règlement (CE) nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, […] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et « […] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Le contrôleur européen et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'être plus constructifs et proactifs, et ils ont publié en mars 2015 une stratégie quinquennale exposant la manière dont ils entendaient mettre en œuvre ce mandat et en rendre compte.

Le présent avis s'inscrit dans le cadre de la mission du CEPD, qui consiste à conseiller les institutions de l'UE sur les implications de leurs politiques en matière de protection des données et à encourager l'élaboration responsable de politiques, conformément à l'action nº 9 de la stratégie du CEPD : «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD estime que le respect des exigences en matière de protection des données est une condition préalable et un vecteur clés pour garantir l'échange efficace de renseignements sur les antécédents judiciaires des ressortissants de pays tiers dans les domaines de la liberté, de la sécurité et de la justice.

Résumé

Le système ECRIS actuel, établi par la décision-cadre 2009/315/JAI du Conseil, encourage l'échange d'informations sur les condamnations pénales, principalement dans le contexte de la coopération judiciaire. L'ECRIS peut également être utilisé à d'autres fins que dans le cadre des procédures pénales, conformément au droit national de l'État membre requis et de l'État membre requérant. Si le système ECRIS actuel peut être utilisé pour des ressortissants de pays tiers (*third country nationals* ou «TCN» en anglais), son efficacité est remise en question. C'est la raison pour laquelle des améliorations se justifient.

L'efficacité de l'ECRIS pour des ressortissants de pays tiers a été soulignée dans le programme européen en matière de sécurité et est devenue une priorité législative pour 2017. Déjà en 2016, la Commission avait adopté une proposition de directive modifiant la législation en vigueur et introduisant des améliorations pour les ressortissants de pays tiers au moyen d'un système décentralisé fonctionnant sur la base d'un index-filtre contenant les empreintes digitales stockées sous la forme de modèles hachés. Cette solution s'est heurtée à des problèmes techniques. La proposition de règlement relative au système ECRIS-TCN, adoptée le 29 juin 2017, porte création d'une base de données européenne centralisée dans laquelle sont stockées des informations contribuant à établir l'identité des ressortissants de pays tiers, notamment leurs empreintes et images faciales. Cette base de données devrait permettre d'effectuer des recherches fondées sur la concordance/non-concordance («hit/no hit») et d'identifier l'État membre détenant des informations sur les condamnations pénales de ressortissants de pays tiers. En outre, la proposition d'un système ECRIS-TCN centralisé se justifie en partie par le fait qu'il devrait favoriser l'interopérabilité future des systèmes européens à grande échelle dans les domaines de la liberté, de la sécurité et de la justice.

Le CEPD suit ce dossier depuis le début des négociations pour la création du système ECRIS. Il a déjà émis deux avis et reconnu l'importance d'un échange efficace des informations, qu'il s'agisse, indifféremment, de ressortissants européens ou de ressortissants de pays tiers. Cette position reste inchangée.

Le présent avis aborde certains problèmes particuliers que soulève la proposition de règlement. S'il y a lieu, il renvoie à la proposition de directive, les deux propositions se voulant complémentaires. Le CEPD relève quatre préoccupations majeures et formule d'autres recommandations supplémentaires, lesquelles sont davantage détaillées dans le présent avis. En somme, le système ECRIS ayant été adopté par l'Union européenne avant le Traité de Lisbonne, le CEPD recommande que ces nouvelles propositions de directive et de règlement rendent le système conforme aux normes requises par l'article 16 du TFUE et la Charte des droits fondamentaux de l'Union européenne, notamment au regard des exigences de limitation légale des droits fondamentaux.

La nécessité d'un système européen centralisé devrait faire l'objet d'une analyse d'impact qui devrait également prendre en considération l'impact de la concentration de l'administration de toutes les bases de données européennes de grande envergure dans les domaines de la liberté, de la sécurité et de la justice au sein d'une seule et unique agence. Il serait prématuré d'anticiper l'interopérabilité dans ce contexte, cette notion devant tout d'abord être juridiquement définie et sa conformité avec les principes de protection des données garantie.

Les finalités du traitement des données auxquelles tendent les systèmes ECRIS et ECRIS-TCN, outre dans le contexte des procédures pénales, doivent être définies clairement, en accord avec le principe de limitation de la finalité dans le cadre de la protection des données. Cela vaut également pour l'accès par les instances de l'Union qui doit aussi être évalué à la lumière du droit à l'égalité de traitement des citoyens de l'Union et des ressortissants de pays tiers. Il doit être démontré que tout accès par les instances de l'Union est nécessaire, adapté, conforme à la finalité de l'ECRIS et strictement limité aux tâches incombant à ces instances européennes dans le cadre de leur mission.

Le traitement de données à caractère personnel en cause, très sensibles par nature, doit respecter rigoureusement le principe de nécessité : une concordance (« *hit* ») ne doit être déclenchée que lorsque l'État membre requis est autorisé en vertu de son droit national à fournir des informations sur les condamnations pénales à d'autres fins que dans le cadre de procédures pénales. La portée du traitement des empreintes digitales doit être limitée, et ce traitement ne doit survenir que lorsque l'identité d'un ressortissant d'un pays tiers donné ne peut être confirmée par d'autres méthodes. S'agissant des images faciales, le CEPD recommande la conduite - ou la mise à disposition (si elle a déjà été conduite) - d'une évaluation basée sur des données probantes de la nécessité de collecter de telles données et de les utiliser à des fins de vérifications ou d'identification.

La proposition de règlement qualifie, à tort, l'eu-LISA de sous-traitant. Le CEPD préconise de désigner l'eu-LISA et les autorités centrales des États membres responsables conjoints du traitement. Il recommande par ailleurs de mentionner clairement, dans une disposition de base, que l'eu-LISA pourra être tenue responsable de toute violation de cette proposition de règlement et du règlement n° 45/2001.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

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

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

vu la décision-cadre du Conseil 2008/977/JAI du 27 novembre 2008 sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[4], et 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 ou de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[5],

A ADOPTÉ L'AVIS SUIVANT :

1. INTRODUCTION ET CONTEXTE

1. Le 29 juin 2017, la Commission européenne a publié une proposition de règlement portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides, qui vise à compléter et à soutenir le système européen d'information sur les casiers judiciaires (système ECRIS-TCN), et modifiant le règlement (UE) nº 1077/2011 (ci-après «la proposition de règlement»)[6]. Cette proposition s'accompagne d'un document d'analyse connexe[7]. Le même jour, la Commission européenne a adopté le premier Rapport statistique sur les échanges, au moyen du système européen d'information sur les casiers judiciaires (ECRIS), d'informations extraites des casiers judiciaires entre les États membres, comme prévu par l'article 7 de la décision 2009/316/JAI du Conseil.[8]

2. La proposition de règlement vise à améliorer les échanges d'informations sur les ressortissants de pays tiers et les citoyens de l'Union qui possèdent également la nationalité d'un pays tiers. Le principe fondamental du système ECRIS existant réside dans le fait que les informations relatives aux condamnations pénales de ressortissants de l'Union européenne peuvent être obtenues auprès de l'État membre dont ces personnes sont des nationaux, qui conserve toutes les condamnations pénales indépendamment du lieu de l'Union européenne où elles ont été prononcées. En ce qui concerne les ressortissants de pays tiers, chaque État membre conserve les condamnations prononcées sur son territoire; aussi une demande d'informations doit être adressée à tous les États membres. De l'avis de la Commission, si le système ECRIS doit être utilisé systématiquement pour extraire des informations sur des ressortissants de pays tiers, répondre aux «demandes générales» génère une charge administrative et des coûts élevés. Les États membres se montrent réticents à utiliser le système, - selon le Rapport statistique, 10 % des demandes concernant des ressortissants de pays tiers[9] - et, de ce fait, les antécédents judiciaires des ressortissants de pays tiers ne sont pas toujours accessibles comme envisagé[10]. L'amélioration de l'efficacité du système ECRIS en ce qui concerne les ressortissants de pays tiers est accélérée par le programme européen en matière de sécurité[11] et constitue l'une des priorités législatives pour 2017[12].

3. La proposition de règlement vient compléter la proposition de directive présentée par la Commission du 19 janvier 2016 en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), qui modifie la décision-cadre 2009/315/JAI du Conseil existante et remplace la décision 2009/316/JAI du Conseil (ci-après la «proposition de directive»).

4. Le point commun de ces deux propositions réside dans la création d'un système pour l'identification des États membres détenant des informations sur les condamnations pénales des ressortissants de pays tiers et des citoyens de l'Union européenne qui possèdent également la nationalité d'un pays tiers. La proposition de directive prévoyait un système décentralisé, ce qui signifie qu'il n'existera pas une base de données européenne unique, mais que chaque État membre tiendra à jour un dossier dit «index-filtre». Ce dossier devait être alimenté au moyen d'informations sur les ressortissants de pays tiers qui auraient été anonymisées et extraites des casiers judiciaires des États membres avant d'être communiquées à l'ensemble des États membres. Les États membres auraient ensuite fait concorder leurs propres données avec les données du terrain et pu découvrir, selon qu'il y ait ou non concordance, l'identité des États membres détenant des informations au sujet de la condamnation pénale d'un ressortissant de pays tiers. Si la proposition de directive prévoyait déjà le traitement des empreintes digitales, le recours aux empreintes digitales ayant été considéré comme l'une des options envisageables dans l'Analyse d'impact 2016, la proposition de règlement, elle, rend leur utilisation obligatoire. La Commission explique que les attaques terroristes ont accéléré l'encouragement de l'utilisation systématique des empreintes digitales à des fins d'identification[13]. Une fois la proposition de directive adoptée, une étude de faisabilité a révélé qu'il n'existe actuellement aucune technologie aboutie permettant de confronter une empreinte digitale à plusieurs autres au moyen de modèles hachés.

5. La proposition de règlement, pour répondre aux problèmes techniques rencontrés, envisage plutôt un système centralisé incluant des données alphanumériques, des empreintes digitales

et des images faciales des ressortissants de pays tiers. Les données alphanumériques et les empreintes digitales pourraient être utilisées pour identifier les ressortissants de pays tiers et les images faciales, à des fins de vérification dans un premier temps puis, lorsque la technologie sera plus aboutie, à des fins d'identification également. L'«autorité centrale» de l'État membre de condamnation saisit les données dans le système ECRIS TCN local, lequel transmet ces données vers un système centralisé de l'UE. Selon qu'il y a ou non concordance, l'État membre requérant peut identifier l'État ou les États membre(s) qui détien(nen)t des informations sur les antécédents judiciaires d'un ressortissant d'un pays tiers, puis demander à obtenir ces informations en utilisant le système ECRIS existant, tel qu'amélioré par la proposition de directive. Lorsque les empreintes digitales sont utilisées à des fins d'identification, toute donnée alphanumérique correspondante peut être communiquée également. La gestion de la base de données européenne est confiée à l'eu-LISA et, à cette fin, la proposition de règlement modifie le règlement n° 1077/2011 portant création de l'eu-LISA.

6. Par ailleurs, la solution d'un système centralisé est replacée dans le contexte de l'interopérabilité prévue entre tous les systèmes d'information pour la gestion de la sécurité, des frontières et des flux migratoires. En réalité, parmi les motifs invoqués pour justifier le choix d'un système centralisé, l'interopérabilité est mise en avant, plutôt que les problèmes techniques rencontrés[14]. Le système ECRIS est également inscrit dans la feuille de route du Conseil visant à renforcer les échanges d'informations, la gestion des informations et la recherche de l'interopérabilité[15]. L'interopérabilité avec le système ECRIS est également prévue dans la proposition ETIAS[16].

7. Une fois alignées l'une sur l'autre, les deux propositions devraient être complémentaires. Si la proposition de règlement doit aborder les problèmes liés au système centralisé, la proposition de directive doit régler les problèmes d'ordre général liés au fonctionnement du système ECRIS pour les ressortissants de pays tiers comme pour les citoyens de l'Union européenne[17]. La Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a adopté le Rapport sur la proposition de directive en 2016[18], tandis qu'en ce qui concerne la proposition de règlement, le projet de rapport a été adopté le 30 octobre 2017.[19] Le Conseil a d'abord suspendu les négociations relatives à la proposition de directive à la suite de la demande, adressée par des États membres à la Commission lors du Conseil du 9 juin 2016, de présenter une proposition en vue de la création d'un système centralisé[20] et procède actuellement à l'examen des deux propositions en parallèle[21].

8. Le système ECRIS-TCN constitue une initiative importante qui traite des systèmes d'information dans les domaines de la liberté, de la sécurité et de la justice. Le CEPD suit ce dossier depuis le début des négociations pour la création du système ECRIS. Le premier avis relatif au système ECRIS a été publié en 2006[22], puis validé par la décision-cadre 2009/315/JAI du Conseil. Plus tard, en 2016, le CEPD, dans son avis 3/2016, a tenu compte de la proposition de directive[23].

9. Dans ses deux avis, le CEPD a reconnu l'importance d'échanges d'informations extraites du casier judiciaire de personnes ayant été condamnées qui soient efficaces, ainsi que la nécessité qu'un système puisse fonctionner efficacement pour des ressortissants de pays tiers, particulièrement dans le contexte de l'adoption du programme européen en matière de sécurité[24]. Sa position reste inchangée.

10. Le présent avis s'appuie sur l'avis 3/2016 et aborde certains problèmes particuliers que soulève la proposition de règlement. Le cas échéant, l'avis fait également référence à la proposition de directive. Au chapitre 2, le CEPD expose ses principales inquiétudes et formule des recommandations quant aux réponses à y apporter. Les inquiétudes et recommandations supplémentaires pour de plus amples améliorations sont décrites au chapitre 3.

2. RECOMMANDATIONS PRINCIPALES

2.1 Création d'une base de l'Union européenne centralisée

11. Dans la proposition de directive, la Commission a opté pour une solution décentralisée s'appuyant sur la création d'un index-filtre. Malgré des coûts plus élevés, cette option était privilégiée à l'époque, notamment en raison de la duplication des données dans une base de données centralisée et des règles supplémentaires de protection des données que le système centralisé impliquerait[25].

12. En revanche, la proposition de règlement fait le choix de la création d'un système centralisé. Comme cela a été mentionné plus haut (voir points 5 et 6), les raisons justifiant le changement de la solution technique sont liées à l'absence d'une technologie aboutie à l'appui de l'index-filtre prévu par lequel une solution centralisée permettra de garantir l'interopérabilité future avec d'autres systèmes dans les domaines de la liberté, de la sécurité et de la justice. L'exposé des motifs énonce que «les objectifs de l'initiative ne pourraient pas être atteints aussi facilement dans le cadre d'une approche décentralisée»[26], que «[c]ette option s'est révélée la plus efficiente et techniquement moins complexe et plus facile à entretenir que les autres»[27] et que le choix d'un système centralisé est «justifié et proportionné, étant donné que la différence de traitement (entre les ressortissants de pays tiers et les citoyens européens] n'entraîne pas d'inconvénients majeurs pour les RPT»[28]. Cela est expliqué de façon plus détaillée puisque «pour les [ressortissants de pays tiers], les conséquences sont les mêmes, que leurs données soient conservées à l'échelle européenne ou par les autorités nationales, étant donné que l'utilisation des données se limite, dans les deux cas, à l'identification des États membres qui détiennent effectivement des informations concernant les condamnations» [traduction libre].[29] Contrairement au raisonnement présenté dans l'Analyse d'impact jointe à la proposition de directive, la Commission affirme désormais que le système centralisé permet une répartition des données à caractère personnel moins large parmi les États membres, la pseudonymisation n'étant pas nécessaire puisque l'accès au système centralisé fait l'objet de contrôles stricts[30]. Pour ce qui concerne les aspects de la protection des données, la Commission précise que des garanties, telles que des limitations des droits d'accès et de la finalité, des fichiers journaux, une infrastructure sécurisée de communication, des limitations de la conservation conformément au droit national et l'application du règlement n° 45/2001 sont envisagées.

13. Il est clair qu'un système centralisé constitue un nouveau système de traitement des données en ce qu'il assure la conservation de données à caractère personnel. Il constitue en soi un risque pour la protection des données à caractère personnel en ce qu'il devrait permettre de recueillir une importante quantité de données. Une violation des données, une perte accidentelle de données ou toute autre action illégale sur les données est susceptible d'avoir un impact beaucoup plus important qu'un incident local, qui n'affecterait qu'une partie de ce qu'un système décentralisé ne ferait. La conception et la mise en œuvre de mesures de sécurité communes dans l'ensemble des points de stockage locaux pourraient également limiter les inconvénients associés et inhérents dans des modèles répartis. Qui plus est, le système centralisé envisagé implique une duplication des données à caractère personnel détenues localement pour le même objectif.

14. Le CEPD rappelle que toute mesure conduisant au traitement de données à caractère personnel constitue une limitation des droits fondamentaux tels qu'ils sont consacrés à l'article 8 de la Charte. Pour être légale, la limitation doit satisfaire aux conditions prévues à l'article 52, paragraphe 1, de la Charte. La nécessité et la proportionnalité d'une mesure envisagée sont des éléments fondamentaux de cet examen. Plus particulièrement, la nécessité requiert notamment que la mesure traite efficacement le problème, soit la moins attentatoire possible aux droits fondamentaux par rapport à d'autres mesures alternatives, et qu'il y ait des éléments de preuve objectifs et vérifiables de l'efficacité et de la nature moins intrusive de la mesure envisagée. Les problèmes associés aux garanties et aux coûts supplémentaires sont examinés dans le cadre de la proportionnalité au sens strict et surviennent donc après que la nécessité d'une mesure proposée ait été dûment établie. Dans ce contexte, nous faisons référence au «Guide pour l'évaluation de la nécessité» émis par le CEPD afin de prodiguer quelques conseils pratiques au législateur de l'Union[31].

15. Des éléments de preuve permettant d'attester qu'une base de données centralisée constitue la solution la moins intrusive et que d'autres solutions ne présentent pas la même efficacité font défaut. Par exemple, on ne dispose d'aucune explication complémentaire concernant les problèmes techniques rencontrés lors de l'utilisation du système ECRIS, ni quant à savoir si ces problèmes pourraient être résolus efficacement à l'avenir, par exemple au moyen d'une meilleure gestion des opérations. Compte tenu du fait que le premier rapport d'examen consacré au système ECRIS fait état de progrès en matière de connexion à ECRIS, 24 % des interconnexions restant toujours à établir[32], rien ne permet de justifier de manière adéquate pourquoi l'infrastructure actuelle du système ECRIS ne peut être encore améliorée de façon à rendre possibles des demandes sortantes automatisées et des réponses entrantes en provenance des casiers judiciaires nationaux à la manière du modèle Prüm[33].

16. S'agissant des coûts occasionnés par les différentes solutions, les estimations pour une solution décentralisée sont établies sur la base du choix coûteux prévu dans la proposition de directive, à savoir la mise en place de l'index-filtre avec des empreintes digitales hachées[34]. Une comparaison des coûts doit être établie par rapport aux systèmes décentralisés alternatifs actuels (notamment le système Prüm précité) plutôt que par rapport à l'hypothétique solution d'index-filtre. En outre, les coûts ne peuvent devenir un facteur significatif pour juger de la licéité de la limitation des droits fondamentaux. Le CEPD observe également que les aspects financiers n'ont pas empêché la Commission d'opter pour la solution décentralisée en 2016.

17. La solution du système centralisé suggérée n'a pas été accompagnée d'une analyse d'impact appropriée, bien qu'il s'agisse d'une condition importante de la politique de la Commission afin de mieux légiférer[35], et d'une condition préalable essentielle lorsque des droits fondamentaux sont en jeu[36]. En lieu et place, la Commission s'est appuyée sur l'Analyse d'impact menée en 2016 et a suggéré la solution qui avait été rejetée à cette époque. L'impact associé au fait de confier l'hébergement et la gestion du système centralisé à l'eu-LISA doit également être évalué dans le contexte de la concentration dans une seule et unique agence de la gestion opérationnelle de tous les systèmes informatiques européens de grande envergure dans les domaines de la liberté, de la sécurité et de la justice. Dans son récent avis sur la proposition de l'eu-LISA, le CEPD a mis ce risque en exergue et critiqué le fait que des initiatives importantes dans ce domaine ne s'accompagnent pas d'une analyse d'impact.

18. Enfin, l'objectif de garantir l'interopérabilité du système ECRIS-TCN avec d'autres systèmes informatiques européens de grande envergure dans les domaines de la liberté, de la sécurité et de la justice, ne justifie pas, à lui seul, la nécessité d'une solution centralisée, ni des données prévues pour le traitement (voir la section 2.3). Les objectifs et finalités de l'interopérabilité doivent être clairement définis et leur impact sur les droits fondamentaux à la vie privée et à la protection des données doit être soigneusement évalué avant d'utiliser à nouveau cette notion pour étayer une nouvelle proposition législative. De plus, les finalités des systèmes interconnectés devraient être clairement définies et leur nécessité et proportionnalité établies (voir la section 2.2) avant que la notion d'interopérabilité ne puisse être exploitée pour concevoir un cadre plus cohérent et plus homogène. Le CEPD a récemment publié une déclaration et un document de synthèse sur l'interopérabilité qui n'en demeurent pas moins fort pertinents dans le contexte de la présente proposition de règlement[37].

19. Le CEPD rappelle donc **la nécessité d'un élément de preuve objectif étayant la nécessité de créer un système européen centralisé. Dans ce contexte, l'impact de l'interopérabilité sur les droits fondamentaux doit d'abord être examiné et ses finalités clairement définies au regard de la finalité du système ECRIS.** Une analyse d'impact appropriée sur les droits fondamentaux à la vie privée et à la protection des données doit accompagner la proposition de règlement. **Plus particulièrement, l'impact de la concentration de tous les systèmes au sein d'une seule et même agence nécessite d'être analysé.**

2.2 Finalité du système ECRIS-TCN et conditions de l'utilisation des informations relatives aux condamnations pénales

20. La finalité de la proposition de règlement consiste à permettre l'identification des États membres détenant des informations sur les casiers judiciaires de ressortissants de pays tiers. Les données figurant dans le système ne doivent être traitées qu'à cette fin[38]. Cependant, certaines règles vont au-delà de cette finalité. Les finalités de l'utilisation des informations relatives aux condamnations pénales ne sont pas modifiées par une disposition de base dans la proposition de directive: les informations doivent être utilisées dans le cadre de procédures pénales et à toute autre fin conforme au droit national de l'État membre requérant et dans les limites du droit national de l'État membre requis.

21. Cependant, le deuxième considérant de la proposition de règlement et de directive stipule que les informations relatives aux condamnations doivent également être prises en considération pour prévenir de nouvelles infractions. De la même manière, le projet de rapport sur la proposition de règlement élaboré par la Commission des libertés civiles, de la justice et des affaires intérieures ajoute également un considérant (2 bis) selon lequel les autorités compétentes doivent tenir compte des condamnations antérieures pour les décisions mettant fin au séjour régulier, ainsi que pour les décisions de retour et d'interdiction d'entrée qui visent des ressortissants de pays tiers constituant une menace pour l'ordre public, la sécurité publique ou la sécurité nationale[39]. La proposition de règlement n'entendant pas modifier la finalité et les conditions d'utilisation du système ECRIS, ni traiter de questions d'ordre général abordées dans la proposition de directive, les considérants 2 et 2 bis doivent être supprimés. Le considérant doit également être supprimé dans la proposition de directive en ce qu'il pourrait être perçu, à tort, comme une nouvelle obligation d'utilisation du système ECRIS et serait en contradiction avec la règle actuelle de l'article 9, paragraphe 3, de la décision-cadre 2009/315/JAI du Conseil qui n'est pas modifiée. Partant, les États membres peuvent, sans obligation aucune, utiliser des informations sur les condamnations pénales dans l'unique but de prévenir une menace immédiate et sérieuse à la sécurité publique.

22. En outre, l'article 7, paragraphe 1, de la proposition de règlement impose l'obligation aux autorités centrales des États membres d'utiliser le système ECRIS-TCN pour identifier les États membres détenant des informations sur le casier judiciaire de la personne en question. En revanche, l'utilisation du système ECRIS pour des ressortissants de l'Union européenne n'est pas obligatoire en vertu de l'article 6, paragraphe 1, de la décision-cadre 2009/315/JAI qui ne sera pas modifiée par la proposition de directive. Cette obligation renforce le traitement de données à caractère personnel et donnerait lieu à une situation d'inégalité de traitement entre les citoyens européens et les ressortissants de pays tiers, y compris des personnes bénéficiant de la double nationalité européenne/non européenne. Ce dernier cas pose tout particulièrement le problème de l'égalité de traitement et de la non-discrimination des ressortissants de l'UE[40]. Une justification plus détaillée apparaît donc nécessaire.

23. L'article 7, paragraphes 2 et 3, permet à Europol, à Eurojust et au Parquet européen d'accéder au système ECRIS-TCN dans le cadre de l'exercice de leurs missions légales. Eurojust aura accès au système, en plus de l'accomplissement de ses tâches statutaires, afin de servir d'interlocuteur pour les demandes émises par des pays tiers. Le projet de rapport sur la proposition de règlement élaboré par la commission des libertés civiles, de la justice et des affaires intérieures ajoute également l'Agence européenne de garde-frontières et de garde-côtes aux autorités devant bénéficier d'un accès au système[41].

24. Le CEPD estime qu'il est justifié de désigner Eurojust en tant qu'interlocuteur pour les demandes émises par des pays tiers, conformément à l'article 14. Le rôle d'Eurojust se limitant ici à servir d'interlocuteur, une règle prévoyant des garanties supplémentaires doit être ajoutée afin de veiller à ce que les données soient utilisées à cette fin uniquement et soient effacées immédiatement après que la demande a été transmise à l'État membre concerné.

25. En ce qui concerne l'accès par les instances susmentionnées, le CEPD observe que ni la proposition de règlement, ni le projet de rapport sur la proposition de règlement élaboré par la commission des libertés civiles, de la justice et des affaires intérieures pour ce qui concerne l'Agence européenne de garde-frontières et de garde-côtes, ne justifient d'aucune manière la nécessité d'un tel accès, ni les lacunes par rapport à l'utilisation du système ECRIS actuel. Le système ECRIS a principalement été créé à des fins de coopération judiciaire et ces règles établies dans la proposition de règlement semblent étendre cette finalité au maintien de l'ordre et à la gestion des flux migratoires. La règle existante de l'article 9, paragraphe 3, de la décision-cadre 2009/315/JAI du Conseil fixe la limite à la prévention d'un danger immédiat et sérieux pour la sécurité publique. L'accès d'Europol, d'Eurojust, du Parquet européen et de l'Agence européenne de garde-frontières et de garde-côtes au système ECRIS-TCN doit aussi être conforme au droit à l'égalité de traitement des citoyens de l'UE et des ressortissants de pays tiers. Les tâches particulières qui leur incombent dans le cadre de leur mandat et les conditions d'accès, y compris les catégories d'infractions, et la désignation d'une autorité centrale chargée de formuler les demandes doivent aussi être clairement définies et limitées à ce qui est strictement nécessaire[42]. À titre d'exemple, s'agissant d'Eurojust, seul le membre national peut accéder aux casiers judiciaires nationaux conformément à l'article 9, paragraphe 3, de la décision 2002/187/JAI. De la même manière, l'article 47, paragraphe 1, de la Proposition SIS sur la coopération policière et judiciaire consacré à l'accès par Eurojust aux données du SIS prévoit un accès par l'intermédiaire des membres nationaux et précise les tâches pour lesquelles un tel accès est accordé[43]. L'accès par Europol (à des fins de maintien de l'ordre) doit être davantage justifié conformément à la finalité du système ECRIS, puis être limité à ce qui est strictement nécessaire.

26. Dernier point mais non le moindre, des informations peuvent être demandées en vertu de l'article 7, paragraphe 1, de la proposition de règlement à toutes fins, en plus d'une procédure pénale, qui sont conformes à la législation nationale de l'État membre requérant. De telles informations peuvent être communiquées dès lors que la demande se conforme également au droit national de l'État membre requis, ainsi que le stipule l'article 9, paragraphe 2, de la décision-cadre 2009/315/JAI du Conseil en vigueur. Ni la proposition de règlement, ni la proposition de directive ne modifient cette finalité ou les conditions d'utilisation des informations relatives aux casiers judiciaires. Cependant, une définition aussi étendue de la finalité, laissée à la discrétion des États membres, ne respecte pas le principe de limitation de la finalité et la jurisprudence constante arrêtée entre-temps sur les critères d'une limitation légale des droits fondamentaux[44]. Cela s'applique d'autant plus que la proposition de règlement établit une nouvelle base de données européenne centralisée et que le traitement dans la proposition de directive concerne des données hautement sensibles, à savoir des données relatives à des casiers judiciaires, traitement qui, s'il ne fait pas l'objet de conditions strictes et clairement définies, peut avoir un sérieux impact sur les personnes concernées. Une législation qui ne prévoit pas de règles claires et précises régissant la portée et l'application de la mesure envisagée ne résistera pas à un contrôle juridictionnel, étant donné qu'elle est dépourvue de prévisibilité, porte atteinte à la sécurité juridique et que la nécessité de la mesure législative ne peut pas non plus être démontrée. La spécification des finalités pourrait être formulée dans la proposition de directive, de sorte que la législation envisagée traite de la demande du législateur à la Commission pour évaluer la relation entre la directive 2016/680 et les textes adoptés avant

que cette directive ne soit adoptée, afin qu'une protection des données à caractère personnel soit garantie de manière homogène dans l'ensemble de l'Union[45].

27. **Le CEPD recommande donc de tenir compte des exigences relatives à une limitation légale des droits fondamentaux et d'offrir un niveau de protection cohérent avec celui de la Charte des droits fondamentaux de l'Union européenne et l'article 16 du TFUE: À cette fin, les finalités autres que celles concernant les procédures pénales pour lesquelles les systèmes ECRIS et ECRIS-TCN sont envisagés, doivent être analysées afin de déterminer si elles sont nécessaires et proportionnelles et clairement définies, en accord avec le principe de la limitation de la finalité dans le cadre de la protection des données. Par ailleurs, l'accès au système ECRIS-TCN par les instances de l'Union doit être conforme à la finalité du système ECRIS actuel et respecter le droit à l'égalité de traitement des citoyens de l'Union européenne et des ressortissants de pays tiers. Il doit en outre être limité aux tâches qui incombent à ces instances dans le cadre de leur mandat, pour lesquelles un accès s'avère strictement nécessaire. Tout élargissement prévu des finalités actuelles doit être entériné par une disposition de base (un considérant ne suffit pas).**

2.3 Traitement de données sensibles par nature

28. La proposition de règlement prévoit la conservation de données alphanumériques et biométriques, c'est-à-dire d'empreintes digitales et d'images faciales, dans le système centralisé. La recherche dans le système d'informations judiciaires détenues par un État membre au sujet d'un ressortissant d'un pays tiers donné sera effectuée sous la forme d'une recherche fondée sur la concordance/non-concordance des empreintes digitales et/ou des données alphanumériques. Pour l'heure, les images faciales seront utilisées pour vérifier l'identité et, une fois la technologie plus aboutie, elles serviront également à l'identification (recherche d'une image parmi l'ensemble des images). Les données biométriques doivent être conservées par les États membres dans tous les cas, sans aucune autre condition. Les empreintes digitales devront être relevées sur les dix doigts. En cas de concordance, le système doit automatiquement informer l'autorité compétente de l'État membre ou des États membres détenant des informations sur le casier judiciaire du ressortissant de pays tiers concerné[46].

29. Les données à caractère personnel envisagées pour le traitement sont sensibles par nature. Les données biométriques s'inscrivent dans des catégories particulières de données, conformément au règlement général sur la protection des données et à la directive 2016/680[47]. Les données relatives à des antécédents judiciaires, même si elles ne relèvent pas de catégories particulières de données, sont soumises à des garanties spécifiques.

30. Les informations fournies sous la forme d'une concordance sont des données à caractère personnel qui sont de nature sensible, étant donné qu'elles révèlent déjà qu'une personne a fait l'objet d'une condamnation judiciaire, quand bien même la nature de sa condamnation exacte n'est pas décrite dans le système centralisé et n'est pas communiquée automatiquement à l'autorité compétente requérante d'un État membre. Au contraire, ces informations ne sont pas divulguées lorsque le système ECRIS actuel est utilisé pour

demander des informations à d'autres fins que pour une procédure pénale. La réponse standardisée aux demandes, conformément à l'annexe à la décision-cadre 2009/315/JAI du Conseil, prévoit que «selon les conditions prévues par la législation de l'État membre requis, il ne peut être donné suite aux demandes introduites à des fins autres qu'une procédure pénale». Une telle recherche fondée sur la concordance/non-concordance ne placerait donc pas les citoyens européens et les ressortissants de pays tiers sur un même pied d'égalité. Même si l'article 22, paragraphe 1, de la proposition de règlement dispose que les données figurant dans le système central ne font l'objet d'un traitement qu'aux fins de l'identification du ou des État(s) membre(s) détenant des informations sur les casiers judiciaires, il ne peut être garanti que le simple fait de connaître l'existence d'une condamnation pénale n'aurait aucun impact négatif sur les ressortissants de pays tiers et ne serait pas à l'origine de **comportements discriminatoires. Les informations ne seraient pas utiles non plus si elles ne pouvaient être totalement récupérées et, partant, cela serait contraire au principe de qualité des données** (à savoir, seules les données à caractère personnel qui sont nécessaires aux fins indiquées peuvent être traitées)[48]. La proposition de règlement devrait plutôt prévoir qu'une concordance ne soit déclenchée qu'aux fins pour lesquelles le ou les État(s) membre(s) requis est/sont autorisé(s) à fournir des informations en vertu de son/leur droit national. La mise en œuvre du système d'une telle façon permettrait également de se conformer à l'importante obligation de la protection des données dès la conception et par défaut, ainsi que l'exposent la directive 2016/680 et la proposition de règlement sur la protection des données par les institutions de l'UE[49].

31. Le traitement des empreintes digitales interfère non seulement avec le droit à la protection des données à caractère personnel, mais également avec le droit à la vie privée, ainsi que l'ont clairement exprimé la CJUE et la CEDH[50]. Le CEPD a reconnu à plusieurs reprises les avantages apportés par l'utilisation des données biométriques, tout en soulignant toujours que, par la nature même de telles données, ces avantages dépendraient de l'application de garanties plus strictes[51].

32. S'il est possible de concevoir que, dans certains cas, les données alphanumériques ne permettent pas d'aboutir à une identification sûre, cela ne justifie pas la nécessité d'utiliser systématiquement des empreintes digitales à des fins d'identification lorsque l'identité du ressortissant de pays tiers peut être confirmée par d'autres méthodes. Les documents d'identité délivrés par un nombre de pays tiers de plus en plus important présentent des éléments de sécurité élevés. En outre, les permis de séjour émis par les États membres doivent comporter des éléments de sécurité, notamment des données biométriques[52]. La nécessité d'utiliser systématiquement des empreintes digitales n'est pas étayée non plus par les données statistiques relatives à l'utilisation du système ECRIS au cours des cinq dernières années. Selon le rapport de la Commission, de 1 à 3 % des réponses seulement ont permis d'identifier plusieurs personnes[53]. Même si ce chiffre devait s'appliquer à 10 % des demandes qui concernent des ressortissants de pays tiers, il n'est pas révélateur d'un problème majeur lié à l'identification des ressortissants de pays tiers. En conséquence, l'utilisation des empreintes digitales devrait uniquement être réservée à l'identification des ressortissants de pays tiers si l'identité du ressortissant de pays tiers ne peut être confirmée par d'autres méthodes. Une approche similaire est adoptée à l'article 42 de la proposition de règlement sur le SIS dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale[54].

33. Par ailleurs, le CEPD, dans son avis 3/2016, a souligné les différentes traditions judiciaires dans les États membres au regard du traitement des empreintes digitales, selon la gravité des infractions. Si l'absence d'harmonisation des pratiques judiciaires est mentionnée dans la proposition de directive, la proposition de règlement introduit l'obligation pour les États membres de traiter les données biométriques sans fixer aucun seuil pour les infractions. Le CEPD recommande donc de limiter davantage le traitement des données biométriques aux infractions graves et répertoriées.

34. En guise d'élément de qualité des données supplémentaire, et afin d'éviter toute «dérive des missions» par rapport aux finalités pour lesquelles les données sont collectées dans d'autres bases de données au niveau national, les empreintes digitales, ainsi que d'autres données biométriques, doivent uniquement être conservées lorsqu'elles sont impliquées dans des procédures pénales ou peuvent être utilisées à cette fin. À cet effet, il convient d'ajouter une règle à l'article 5 de la proposition de règlement.

35. Enfin, le CEPD observe que la proposition de règlement ne fournit aucune explication quant au choix d'utiliser un deuxième identifiant biométrique, à savoir les images faciales, et de l'utiliser non seulement à des fins de vérification de l'identité d'un ressortissant de pays tiers, mais également aux fins d'identifier ledit ressortissant (recherche permettant de confronter l'image faciale à plusieurs autres) à partir du moment où la technologie sera plus aboutie. Le CEPD estime qu'une évaluation basée sur des données probantes de la nécessité et de la proportionnalité aurait dû être menée avant d'inclure de telles données dans le système ECRIS-TCN et de définir la finalité de leur utilisation[55]

36. **Le CEPD recommande dès lors d'ajouter des conditions appropriées pour que le traitement des données à caractère personnel soit en accord avec le principe de nécessité. Une concordance ne doit être déclenchée que lorsque l'État membre requis est autorisé en vertu de son droit national à fournir des informations sur les condamnations pénales à d'autres fins que dans le cadre de procédures pénales. La portée du traitement des empreintes digitales doit être limitée et ce traitement ne doit survenir que lorsque l'identité d'un ressortissant d'un pays tiers donné ne peut être confirmée par d'autres méthodes. S'agissant des images faciales, le CEPD recommande la conduite ou la mise à disposition d'une évaluation basée sur des données probantes de la nécessité d'inscrire de telles données et de les utiliser à des fins de vérifications ou d'identification.**

2.4 Qualification de l'eu-LISA en tant que sous-traitant et responsabilité de l'agence

37. L'article 21 de la proposition de règlement indique que chaque autorité centrale de l'État membre doit être considérée comme le responsable du traitement, l'eu-LISA devant être considérée comme le sous-traitant des données conformément au règlement (CE) nº 45/2001. Cependant, l'eu-LISA aura à sa charge le développement du système ECRIS-TCN (article 11, paragraphe 1). Pour ce faire, l'eu-LISA doit définir l'architecture matérielle du système, notamment ses spécifications techniques, selon laquelle les représentants des États membres, réunis au sein d'un conseil de gestion du programme, doivent veiller à la bonne gestion de la phase de conception et de développement (article 11, paragraphe 5). L'eu-LISA veille, en coopération avec les États membres, à l'utilisation permanente de la meilleure technologie disponible (article 11, paragraphe 10). La gestion

opérationnelle du système incombe à l'eu-LISA, qui est aussi responsable de la sécurité du système (article 13, paragraphe 2, et article 17, paragraphes 1 et 2). L'eu-LISA doit en outre développer et tenir à jour un mécanisme de contrôle de la qualité des données (article 11, paragraphe 13).

38. Plusieurs points de la proposition de règlement s'appuient sur le futur règlement qui devrait remplacer le règlement n° 45/2001. Conformément au règlement général sur la protection des données, l'article 2, sous d), définit la notion de responsable du traitement et l'article 28 clarifie les responsabilités des responsables conjoints du traitement. Lorsque deux entités ou plus déterminent conjointement les finalités et les méthodes du traitement, elle sont alors qualifiées de responsables conjoints du traitement.

39. En 2010 déjà, le groupe de travail «Article 29» sur la protection des données avait formulé des orientations sur les notions de responsable du traitement, de responsables conjoints du traitement et de sous-traitant. D'après ces dernières, la notion de responsable du traitement est une notion autonome de la législation européenne sur la protection des données et fonctionnelle, en ce sens qu'elle vise à attribuer les responsabilités sur la base de l'influence factuelle plutôt qu'en s'appuyant sur une analyse formelle.[56]

40. À plusieurs reprises, le CEPD a souligné les conséquences de la répartition des rôles entre divers acteurs dans les bases de données de l'Union européenne à grande échelle et a recommandé que lorsqu'un acteur définit indépendamment les finalités ou les méthodes du traitement de données, il doit être considéré comme un responsable du traitement plutôt que comme un sous-traitant[57]. Lorsque plusieurs acteurs contribuent ainsi aux finalités et/ou méthodes de traitement, comme cela est le cas en l'espèce, ils doivent être considérés comme des responsables conjoints du traitement.

41. Étant donné que la notion de responsable du traitement implique une approche fonctionnelle des responsabilités de chacune des parties, conformément aux critères définis par la législation européenne en matière de protection des données, la désignation par tout autre instrument législatif d'un responsable du traitement ou d'un sous-traitant ne doit pas enfreindre ces critères.

42. Par ailleurs, avec la répartition des rôles telle qu'énoncée dans la proposition de règlement, les États membres peuvent être reconnus responsables, en tant que responsables du traitement, de questions échappant à leurs compétences (par exemple, la façon dont l'eu-LISA gère la sécurité des informations dans le système centralisé et la transmission sécurisée des données depuis et vers le système centralisé). **Le CEPD préconise donc de désigner l'eu-LISA et les autorités centrales des États membres responsables conjoints du traitement.**

43. L'article 18 de la proposition de règlement établit la responsabilité d'un État membre et le droit de toute personne ou d'un État membre à recevoir une réparation au titre de tout dommage subi à la suite d'une opération de traitement illicite ou de toute action incompatible avec cette proposition de règlement. **Puisque les principaux instruments légaux en matière de protection des données s'appliquent également aux opérations de traitement, à savoir la directive 2016/680 et le règlement nº 45/2001 et son**

règlement successeur, il convient d'ajouter une référence à ces derniers dans l'article 18.

44. Enfin, si l'article 18 tient compte de la responsabilité des États membres, il ne prend pas en considération celle de l'eu-LISA. Cela pourrait donner lieu à une imprécision et contredire d'autres dispositions de la proposition de règlement confirmant l'application du règlement nº 45/2001 et de son règlement successeur. Il transfère également la charge de la preuve aux États membres, qui doivent établir que l'entité responsable d'une violation donnée est l'eu-LISA.

45. **Le CEPD suggère dès lors d'ajouter à l'article 18 une règle similaire à celle relative aux États membres s'agissant de la responsabilité de l'eu-LISA en cas d'infraction à l'une des règles exposées dans cette proposition de règlement ainsi que dans le règlement nº 45/2001.**

3. RECOMMANDATIONS COMPLÉMENTAIRES

3.1 Référence à la directive 2016/680 et au règlement nº 45/2001

46. Le CEPD estime que le fait de se référer de manière sélective à l'application de la directive 2016/680 et au règlement nº 45/2001 porte atteinte à la sécurité juridique et risque d'omettre certaines dispositions importantes. À titre d'exemple, l'article 25 sur les voies de recours en cas de refus des demandes d'accès, de rectification et d'effacement des données de la personne concernée, constitue un sous-groupe des voies de recours dont la personne concernée peut se prévaloir au titre des articles 52 et 54 de la directive 2016/680.

47. **Le CEPD préconise donc d'éviter la répétition inutile de certaines règles et, conformément au considérant 23, d'inclure dans l'article 2 une disposition de base sur l'applicabilité générale de la directive 2016/680 et du règlement nº 45/2001.**

3.2 Droits des personnes concernées

48. Le CEPD accueille avec satisfaction les règles supplémentaires exposées aux articles 23 et 24 concernant l'exercice du droit d'accès et du droit de rectification et d'effacement, tels qu'énoncés dans les articles 14 et 16 de la directive 2016/680. Plus particulièrement, il se félicite que les ressortissants de pays tiers puissent adresser leur demande à un État membre, de la coopération des États membres concernés et de la coopération des autorités de contrôle nationales ainsi que des délais stricts impartis pour répondre à de telles demandes. Le CEPD recommande en outre les modifications ci-après:

49. Le titre actuel de l'article 23 de la version anglaise doit reprendre les mêmes termes que ceux employés dans la directive 2016/680 : il convient ainsi de remplacer le terme « *deletion* » (suppression) par «*erasure*» (effacement).

50. La formulation de l'article 23, paragraphe 2, semble faire référence uniquement au droit de rectification et d'effacement, étant donné qu'il est question de contrôler l'exactitude des données ainsi que la licéité du traitement. Les délais fixés et la coopération entre l'État

membre requis et l'État membre de condamnation ne s'appliqueraient dès lors qu'à l'égard dudit droit. **En conséquence, il y a lieu d'ajouter une règle sur la coopération des ces États membres et sur le délai de réponse aux demandes d'accès.**

51. Dans l'article 24, paragraphe 3, la formulation «l'État membre qui a transmis les données» doit être modifiée de façon à utiliser la même terminologie que celle employée à l'article 23, à savoir «l'État membre auquel la demande a été présentée».

52. Enfin, suite à la recommandation précitée (voir chapitre 3.1) visant à éviter toute répétition inutile de certaines règles de la directive 2016/680, le CEPD suggère de reconsidérer l'utilité de l'article 25.

3.3 Statistiques, fichier central et contrôle

53. Le CEPD salue la disposition de l'article 30, paragraphe 1, qui énonce que la règle d'accès aux données par l'eu-LISA ne vaut qu'à des fins d'établissement de rapports et statistiques ne permettant aucune identification individuelle. Pourtant, en raison des éventuels risques résiduels d'identification, le même degré de sécurité doit s'appliquer également pour ce fichier.

54. Selon la proposition de règlement, aux fins susmentionnées, l'eu-LISA doit créer un fichier central. À cet égard, le CEPD rappelle ses avis précédents sur l'eu-LISA[58], l'EES[59], l'ETIAS[60] et le SIS[61], dans lesquels il mettait vivement en garde contre le fait que la solution proposée pour générer des statistiques imposerait une lourde charge à l'eu-LISA, qui devrait gérer et sécuriser de manière appropriée un deuxième fichier, en plus des données de production réelle dans le système centralisé. Cela entraînerait également la duplication inutile des données et supposerait des risques supplémentaires pour le CEPD qui devrait alors superviser ce deuxième fichier. **Le CEPD préconiserait une solution qui, au lieu de rendre nécessaire un fichier central supplémentaire, imposerait à l'eu-LISA de développer des fonctions permettant aux États membres, à la Commission, à l'eu-LISA et aux agences autorisées d'extraire automatiquement et directement les statistiques demandées des systèmes centralisés.**

55. Contrairement à l'article 30, paragraphe 1, la formulation actuelle de l'article 34, paragraphes 1 et 2, ne permet pas d'établir clairement si l'eu-LISA, dans le cadre de sa mission de contrôle et d'évaluation du système, doit bénéficier d'un accès aux informations contenant des données à caractère personnel. **Dans la mesure où un tel accès aux données à caractère personnel est nécessaire, la formulation doit être alignée sur celle de l'article 30, paragraphe 1, et prévoir un accès aux données à caractère personnel sans permettre l'identification individuelle.**

3.4 Sécurité des données

56. Conformément à l'article 22 du règlement nº 45/2001, le degré de sécurité à garantir doit être «approprié au regard des risques». La même approche est observée dans l'article 32, paragraphe 1, du règlement général sur la protection des données et dans l'article 29, paragraphe 1, de la directive 2016/680. En conséquence, lorsque le projet de proposition évoque la «sécurité», comme dans l'article 11, paragraphe 11, point b), l'article 13, paragraphe 2, l'article 17, paragraphe 1 et l'article 30, paragraphe 3, il convient d'effectuer l'ajout respectif.

57. Une suppression automatique des données à l'expiration de la période de conservation permet de renforcer le respect du principe de limitation de la conservation. **Le CEPD recommande donc de prévoir la suppression automatique à l'article 8, paragraphe 2, ainsi qu'à l'article 10, paragraphe 1, après le point j).**

58. Enfin, des règles sur la sécurité des données similaires à celles appliquées aux États membres au titre de l'article 17, paragraphe 3, doivent être mentionnées dans l'article 16 pour les organes de l'Union, en prenant en considération leur rôle tel qu'envisagé de n'accéder qu'au système ECRIS-TCN.

3.5 Rôle du CEPD

59. Le CEPD salue le fait que les autorités de contrôle nationales puissent accéder à tous les locaux nationaux liés au système ECRIS-TCN, ainsi que cela est prévu à l'article 26, paragraphe 4. Il accueille aussi favorablement la règle sur la surveillance coordonnée en faisant référence à la proposition de règlement abrogeant le règlement nº 45/2001.

60. Le CEPD représente l'autorité chargée de la protection des données qui supervise l'agence eu-LISA. Si le CEPD dispose de la compétence nécessaire pour obtenir toutes les informations pertinentes auprès des institutions, organes et agences de l'UE, la procédure doit être **perfectionnée en incluant le CEPD dans la liste des destinataires des rapports que l'eu-LISA présentera à la Commission ou au Conseil et au Parlement en vertu de l'article 34.**

61. Le CEPD ayant de toute façon également accès aux fichiers journaux conformément à l'article 47, paragraphe 2, point a), du règlement nº 45/2001, une disposition similaire à l'article 29, paragraphe 6, consacrée à l'accès par les autorités de contrôle nationales, devrait être ajoutée à l'article 29, paragraphe 5.

62. Par souci de clarté, toute référence à l'application du règlement nº 45/2001, similaire à l'application de la directive 2016/680 pour les États membres, doit être mentionnée dans le considérant 23.

63. Pour finir, un contrôle efficace ne peut être assuré que lorsque des ressources adéquates sont mises à la disposition des autorités de contrôle nationales et au CEPD sans distinction. Nous suggérons donc d'inclure une disposition à l'article 27, similaire à l'article 26, paragraphe 3, exigeant de l'autorité budgétaire de l'UE qu'elle veille à ce que le CEPD dispose de ressources adéquates.

3.6 Autorités de contrôle nationales

64. L'article 26, paragraphe 1, fait uniquement référence à l'article 6 concernant la licéité du traitement des données à caractère personnel à laquelle l'autorité de contrôle nationale doit veiller. Les autorités de contrôle nationales sont toutefois compétentes pour garantir la conformité des données à caractère personnel susceptibles d'être traitées conformément à la proposition de règlement, notamment les données visées à l'article 5 et les fichiers journaux. **Il y a donc lieu de modifier la formulation actuelle, par exemple en supprimant l'expression «énumérées à l'article 6».**

65. L'article 19 et l'article 27, paragraphe 2, distinguent deux types d'autorités de contrôle, à savoir l'« autorité de contrôle » et l'« autorité de contrôle nationale ». La signification de ces deux entités doit être précisée et, si nécessaire, la référence à l'« autorité de contrôle » doit être supprimée.

3. CONCLUSION

66. À l'issue d'une analyse approfondie de la proposition ECRIS-TCN, le CEPD formule les recommandations suivantes :

67. Au moment de créer une nouvelle base de données européenne centralisée et de modifier la législation relative au système ECRIS existante, le CEPD préconise de prendre en considération les exigences de la Charte des droits fondamentaux de l'Union européenne imposant une limitation légale des droits fondamentaux et de prévoir un degré de protection des données à caractère personnel suffisant dans le contexte de la proposition de règlement.

68. Plus particulièrement, le CEPD rappelle la nécessité de produire des éléments de preuve objectifs de la nécessité d'instaurer un système centralisé au niveau européen. Dans ce contexte, l'interopérabilité doit d'abord être analysée par rapport à son impact sur les droits fondamentaux et ses finalités doivent être clairement définies au regard des finalités du système ECRIS. Une analyse d'impact appropriée sur les droits fondamentaux à la vie privée et à la protection des données doit accompagner la proposition de règlement pour ce qui concerne cet aspect, ainsi que pour ce qui concerne la concentration de tous les systèmes au sein d'une seule et même agence.

69. La création d'une nouvelle base de données européenne centralisée et la modification de la législation relative au système ECRIS existante doivent respecter les critères de limitation légale des droits fondamentaux, conformément à une jurisprudence constante. À cette fin, les finalités du traitement des données autres que celles concernant les procédures pénales pour lesquelles ECRIS et ECRIS-TCN sont envisagés doivent être analysées du point de vue de leur nécessité et de leur proportionnalité, mais aussi être définies clairement, en accord avec le principe de limitation de la finalité dans le cadre de la protection des données. Par ailleurs, l'accès au système ECRIS-TCN par des instances de l'Union telles qu'Europol doit être conforme à la finalité du système ECRIS actuel et respecter le droit à une égalité de traitement des citoyens européens et des ressortissants de pays tiers. Il doit en outre être limité aux tâches qui incombent à ces instances dans le cadre de leur mission, pour lesquelles un accès répond à des impératifs de stricte nécessité. Tout élargissement envisagé des finalités actuelles doit être entériné par une disposition de base (un considérant ne suffit pas).

70. Puisque le système ECRIS-TCN implique le traitement de données à caractère personnel très sensibles par nature, le CEPD invite à préciser les conditions appropriées pour traiter des données à caractère personnel dans le respect du principe de nécessité: une concordance (« *hit* ») ne doit être déclenchée que lorsque l'État membre requis est autorisé en vertu de son droit national à fournir des informations sur les condamnations pénales à d'autres fins que dans le cadre de procédures pénales. La portée du traitement des empreintes digitales doit être limitée et ce traitement ne doit survenir que lorsque l'identité d'un ressortissant d'un pays tiers donné ne peut être confirmée par d'autres méthodes. S'agissant des images faciales, le CEPD recommande la réalisation ou la mise à disposition d'une évaluation

basée sur des données probantes de la nécessité d'inscrire de telles données et de les utiliser à des fins de vérifications et/ou d'identification.

71. En outre, l'eu-LISA et les autorités centrales des États membres doivent être désignées en tant que responsables conjoints du traitement des données, étant donné qu'elles ont la responsabilité commune de définir les finalités et les méthodes des activités de traitement envisagées. La désignation de l'eu-LISA en tant que sous-traitant ne refléterait pas adéquatement la situation actuelle et ne contribuerait pas à garantir un degré élevé de protection des données, ou encore ne serait pas favorable aux intérêts légitimes des États membres. De plus, la proposition relative au système ECRIS-TCN doit mentionner clairement la responsabilité de l'eu-LISA en cas de violation de cette proposition de règlement ou d'infraction au règlement nº 45/2001.

72. Outre les principales préoccupations recensées ci-dessus, les recommandations exprimées par le CEPD dans le présent avis ont trait à l'amélioration des dispositions suggérées portant sur:

    - les références à l'applicabilité de la directive 2016/680 et du règlement nº 45/2001;
    - les droits des personnes concernées;
    - les statistiques, le fichier central et le contrôle;
    - la sécurité des données;
    - le rôle du CEPD;
    - les autorités de contrôle nationales.

73. Le CEPD reste disponible pour apporter des conseils supplémentaires sur les propositions de règlement et de directive, ainsi que sur tout acte délégué ou d'exécution susceptible d'être adopté en vertu des instruments proposés, et portant sur le traitement de données à caractère personnel.

Bruxelles,

Giovanni BUTTARELLI
Contrôleur européen de la protection des données

Notes

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 119 du 4.5.2016, p. 1.
[3] JO L 8 du 12.1.2001, p. 1.
[4] JO L 350 du 30.12.2008, p. 60.
[5] JO L 119 du 4.5.2016, p. 89.
[6] COM(2017) 344 final.
[7] SWD(2017) 248 final.
[8] COM(2017) 341 final. Ce Rapport s'accompagne d'un document de travail des services de la Commission, SWD(2017) 242 final.
[9] COM(2017) 341 final, p. 15-16.
[10] Exposé des motifs de la proposition, COM(2017) 344 final, p. 2.
[11] COM(2015) 185 final
[12] Déclaration commune sur les priorités législatives de l'Union européenne pour l'année 2017, https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-legislative-priorities-2017-jan2017_fr.pdf
[13]Exposé des motifs de la proposition, COM(2017) 344 final, p. 3 ; Document analytique connexe, SWD(2017) 248 final, p. 3
[14] Exposé des motifs de la proposition, COM(2017) 344 final, pp. 3, 5, 9.
[15] Feuille de route en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures, 9368/1/16, http://data.consilium.europa.eu/doc/document/ST-9368-2016-REV-1/fr/pdf; premier rapport du Conseil du 8 novembre 2016, http://statewatch.org/news/2016/dec/eu-council-info-exhang-interop-sop-13554-REV-1-16.pdf; deuxième rapport du Conseil du 11 mai 2017, http://www.statewatch.org/news/2017/may/eu-council-information-management-strategy-second-implementation-report-8433-17.pdf;
[16] COM(2016) 731 final.
[17] Exposé des motifs de la proposition, COM(2017) 344 final, p. 4.
[18] A8-0219/2016.
[19] PE 612.310v01-00.
[20] Résultats de la session du Conseil (JAI), 9979/16, http://data.consilium.europa.eu/doc/document/ST-9979-2016-INIT/fr/pdf .
[21] Voir l'ordre du jour du Conseil Coreper du 29 novembre 2017, http://data.consilium.europa.eu/doc/document/CM-5236-2017-INIT/en/pdf .
[22] Avis du CEPD concernant la proposition de décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres [COM(2005) 690 final], JO C 313/26, 20.12.2006, https://edps.europa.eu/sites/edp/files/publication/06-05-29_criminal_records_fr.pdf.
[23] Avis 3/2016 du CEPD sur le système ECRIS, https://edps.europa.eu/sites/edp/files/publication/16-04-13_ecris_fr.pdf.
[24] Avis 3/2016 du CEPD relatif au système ECRIS, p. 12, et référence supplémentaire 38 dans l'avis du CEPD de 2006.
[25] Analyse d'impact, SWD(2016) 4 final, p. 29.
[26] Exposé des motifs de la proposition, COM(2017) 344 final, p. 6.
[27] Exposé des motifs de la proposition, COM(2017) 344 final, p. 9.
[28] Exposé des motifs de la proposition, COM(2017) 344 final, p. 9.
[29] Document d'analyse connexe, SWD(2017) 248 final, p. 10.
[30] Document d'analyse connexe, SWD(2017) 248 final, p. 12.
[31] CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.
[32] COM(2017) 341 final, p. 4.
[33] La décision Prüm principale (2008/615/JAI) requiert des États membres qu'ils établissent des règles et des procédures pour la recherche automatisée et le transfert de «données de référence» détenues dans les fichiers nationaux d'analyse ADN: il s'agit de données contenant des profils ADN individuels susceptibles d'être utilisés pour établir une correspondance, ainsi que de données relatives à des empreintes digitales et de certaines données sur l'immatriculation de véhicules. Une deuxième décision (2008/616/JAI) décrit des mesures techniques

détaillées pour appliquer la décision Prüm principale et inclut, par exemple, des orientations sur les critères techniques permettant d'établir des profils ADN.

[34] Document d'analyse connexe, SWD(2017) 248 final, p. 14.

[35] Communications de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Améliorer la réglementation pour obtenir de meilleurs résultats - Un enjeu prioritaire pour l'UE et Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne - Mieux légiférer

[36] CEPD, Avis 9/2017 sur la proposition de règlement relatif à eu-LISA, https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu_lisa_opinion_fr.pdf

[37] Déclaration du CEPD du 15 mai 2017 sur le concept d'interopérabilité dans le domaine de la migration, de l'asile et de la sécurité, disponible en anglais à l'adresse : https://edps.europa.eu/data-protection/our-work/publications/other-documents/interoperability-field-migration-asylum-and_en; CEPD, Document de synthèse sur l'interopérabilité des systèmes d'information au sein de l'espace de liberté, de sécurité et de justice, https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_fr_0.pdf.

[38] Articles 1er et 2 et article 22, paragraphe 1, de la proposition de règlement relative au système ECRIS-TCN.

[39] Troisième amendement du projet de rapport élaboré par M. Daniel Dalton, membre du Parlement européen.

[40] Voir, à ce sujet, l'avis 3/2016 du CEPD sur le système ECRIS.

[41] Amendement 23 du projet de rapport élaboré par M. Daniel Dalton, membre du Parlement européen.

[42] Voir, par exemple, l'article 30 de la Proposition de règlement portant création d'un système d'entrée/sortie, COM(2016) 194 final, sur la désignation d'un point d'accès central en charge de gérer l'accès d'Europol. Aucune modification n'a été apportée à l'article 30 par le Parlement européen qui a adopté sa position en première lecture le 25 octobre 2017, P8_TA(2017)0412.

[43] Article 47, paragraphe 1, de la proposition SIS sur la coopération policière et judiciaire, COM(2016) 883 final. Pour ce qui concerne l'accès de l'Agence européenne de garde-frontières et de garde-côtes au SIS, voir l'avis 7/2017 du CEPD sur la nouvelle base juridique du système d'information Schengen, points 25 et 28.

[44] CJUE, Digital Rights Ireland Ltd, C-293/12, points 54 et 60 ; CJUE avis 1/15, point 141.

[45] Considérant 94 de la directive (UE) n° 680/2016 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, d'enquête, de détection et de poursuite des infractions pénales ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

[46] Article premier, paragraphe l, article 5, article 7, paragraphes 3 et 5, du projet de proposition de règlement, COM(2017) 344 final.

[47] Voir l'article 9 du règlement 2016/679 et l'article 10 de la directive 2016/680.

[48] Voir aussi CEPD, Document de synthèse sur l'interopérabilité des systèmes d'information au sein de l'espace de liberté, de sécurité et de justice, https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_fr_0.pdf.

49 Article 20 de la directive 2016/680 et article 27 de la proposition de règlement 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, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, COM(2017) 8 final.

[50] CEDH. S. et Marper c. Royaume-Uni, points 68, 84 et 85 ; CJUE, C-291/12, M. Schwarz/Stadt Bochum, points 26 et 27.

[51] Avis 6/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 37 et note de pied de page 53.

[52] FRA Opinion concerning the exchange of information on third-country nationals under a possible future system complementing the European Criminal Records Information Sytem, 4 décembre 2015, p. 17.

[53] Document de travail des services de la Commission qui accompagne le Rapport de la Commission au Parlement européen et au Conseil sur les échanges, au moyen du système européen d'information sur les casiers judiciaires (ECRIS), d'informations extraites des casiers judiciaires entre les États membres, SWD(2017) 242 final, section 1.8, p. 11.

[54] COM(2016) 883 final

[55] Voir aussi CEPD, Avis 7/2016 sur le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin), points 19 à 23 ; CEPD, Avis 7/2017 du CEPD sur la nouvelle base juridique du système d'information Schengen, points 17 et 18.

[56] Groupe de travail «Article 29», Avis 1/2010 sur les notions de «responsable du traitement» et «sous-traitant», p. 32.

[57] CEPD, Avis 3/2017 sur la proposition de création d'un système ETIAS, point 83 à 87 ; CEPD, Avis 6/2016 sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 49.

[58] CEPD, Avis 9/2017 sur l'eu-LISA.
[59] Avis 6/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne, point 70.
[60] CEPD, Avis 3/2017 sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS), point 108.
[61] CEPD, Avis 7/2017 sur la nouvelle base juridique du système d'information Schengen, point 36.