Avis du Contrôleur européen de la protection des données

sur la Communication de la Commission au Conseil et au Parlement européen sur «Les armes à feu et la sécurité intérieure dans l'Union européenne: protéger les citoyens et déjouer les trafics illicites»

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

vu la Charte des droits fondamentaux de l'Union européenne, et en particulier 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],

vu le règlement (CE) n° 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[2], et en particulier son article 28, paragraphe 2,

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 21 octobre 2013, la Commission a adopté la Communication au Conseil et au Parlement européen sur «Les armes à feu et la sécurité intérieure dans l'Union européenne: protéger les citoyens et déjouer les trafics illicites» (désignée ci-après «la Communication»)[4]. Le CEPD se réjouit d'avoir été consulté sur cette Communication avant son adoption, ainsi que d'avoir eu la possibilité de remettre des observations informelles à la Commission.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.01.2001, p. 1.
[3] JO L 350 du 30.12.2008, p. 60.
[4] COM(2013) 716 final.

1.2. Objectif et portée de la Communication

2. La Communication établit la stratégie de l'Union européenne pour déjouer les trafics illicites d'armes à feu. Dans cette mesure, elle propose une politique intégrée axée sur quatre priorités:
   - protéger le marché licite des armes civiles;
   - réduire le nombre d'armes à feu détournées tombant aux mains de criminels;
   - accroître la pression exercée sur les marchés criminels;
   - améliorer la connaissance grâce au renseignement.

3. Pour atteindre ces priorités, différentes tâches sont envisagées, dont certaines peuvent impliquer le traitement de données à caractère personnel et, par conséquent, avoir un impact sur la protection des données des individus:
   - l'établissement d'une norme européenne en matière de marquage: des données à caractère personnel pourraient faire partie des données marquées sur l'arme à feu;
   - une simplification des règles d'octroi des permis de détention d'armes à feu et la possibilité d'exiger des examens médicaux et vérifications judiciaires comme une condition d'achat et de détention licites de toute arme à feu. Les examens médicaux impliquent le traitement de données relatives à la santé des individus. Les données médicales sont des données sensibles au sens de l'article 8 de la directive 95/46/CE, qui requiert une protection spécifique[5], et elles sont donc soumises à des exigences encore plus strictes en matière de protection des données. Les vérifications judiciaires impliquent le traitement de données à caractère personnel relatives à des infractions, condamnations pénales ou mesures de sécurité, ainsi qu'un accès aux casiers judiciaires, qui ne peuvent intervenir que sous le contrôle d'une autorité officielle (tel que prévu à l'article 8, paragraphe 5, de la directive 95/46/CE). Quant à l'enregistrement et au contrôle obligatoires des courtiers, la création d'une nouvelle base de données impliquant le traitement des données à caractère personnel des courtiers doit respecter les principes clés en matière de protection des données, y compris la justification de la nécessité de sa création et de la proportionnalité du traitement, ainsi que de son intrusion dans la vie privée;
   - l'étude de solutions technologiques, telles que des capteurs biométriques lorsque des données à caractère personnel sont stockées dans l'arme à feu afin de garantir que l'arme ne puisse être utilisée que par son propriétaire. Le traitement de données biométriques est soumis à des garanties strictes en matière de protection des données, ainsi qu'à des exigences strictes qui seront expliquées dans le présent avis;
   - la promotion de la coopération transfrontière pour mettre un terme à la détention et à la circulation illégales d'armes à feu, notamment par la collecte coordonnée et le partage d'informations sur la criminalité liée aux armes à feu, associant la police, les gardes-frontières et les autorités douanières. L'accès

[5] Voir arrêts de la Cour de justice de l'Union européenne (la «Cour de justice») du 8 avril 1992, Commission/Allemagne, C-62/90, Rec. p. I-2575, point 23, et du 5 octobre 1994, X/Commission, C-404/92 P, Rec. p. I-4737, point 17; et arrêts de la Cour européenne des droits de l'homme du 17 juillet 2008, I c. Finlande (recours n° 20511/03), point 38 et du 25 novembre 2008, Armonas c. Lituanie (recours n° 36919/02), point 40.

aux bases de données de la police et des douanes est strictement réglementé, comme il sera rappelé ci-dessous;

- le traçage des armes à feu utilisées par des criminels pour les identifier, ainsi que la personne ayant acheté l'arme. Cette mesure, si elle implique le traitement de données à caractère personnel, devra fournir des garanties spécifiques en matière de protection des données;
- la collecte de données plus précises et plus complètes sur la criminalité liée aux armes à feu par l'utilisation des outils informatiques existants, tels que le système d'information Schengen de deuxième génération (SIS II), le système d'information des douanes, le système d'information d'Europol et iARMS (l'outil d'INTERPOL). Comme indiqué ci-dessus, l'accès à une base de données existante de la police et des douanes est soumis à des règles strictes en matière de protection des données.

4. La protection des données semble donc être l'un des points essentiels découlant de cette Communication.

1.3. Objectif et portée de l'avis

5. La Commission ayant l'intention de présenter des propositions législatives en 2015, le CEPD soulignera et expliquera, dans le présent avis, les implications en termes de protection des données des mesures envisagées dans la Communication. Ce faisant, le CEPD souhaite s'assurer que les aspects liés à la protection des données soient dûment pris en compte dans les futures propositions législatives dans ce domaine. À cette fin, il rappellera le cadre légal européen applicable à la protection des données, donnera des indications sur le moment où il est le plus opportun d'en tenir compte et indiquera les conséquences de la conformité requise, mesure par mesure.

2. OBSERVATIONS GÉNÉRALES

2.1. Le cadre européen applicable à la protection des données

2.1.1. Les protections consacrées aux articles 7 et 8 de la Charte

6. Comme expliqué ci-dessus, certaines des priorités et tâches énoncées dans la Communication de la Commission nécessiteront la mise en place de nouveaux traitements et/ou la modification de traitements existants. Le partage de données à caractère personnel, y compris de données sensibles, sera encouragé.

7. Une telle collecte de données à caractère personnel constituera donc une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, tels qu'ils sont consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (désignée ci-après «la Charte»). L'article 7 de la Charte, qui est similaire à l'article 8 de la Convention européenne des droits de l'homme (CEDH)[6], prévoit un droit général au respect de la vie privée et familiale et protège les individus contre toute ingérence des autorités publiques. L'article 8 de la Charte confère à une personne le droit que ses données à caractère personnel ne soient traitées que si certaines exigences essentielles sont

[6] Conseil de l'Europe, STCE n° 5, 4.11.1950.

satisfaites. Ces exigences essentielles sont énoncées à l'article 8, paragraphes 2 et 3, de la Charte:

- les données à caractère personnel doivent être traitées loyalement et licitement, à des fins spécifiques;
- la transparence doit être garantie, en donnant aux personnes concernées des droits d'accès et de rectification des données les concernant;
- la conformité aux règles doit faire l'objet d'un contrôle par une autorité indépendante.

8. Tandis que l'article 7 protège l'individu contre toute ingérence par l'Union européenne et par les États membres mettant en œuvre le droit communautaire, l'article 8 confère une protection ex ante à l'individu selon certaines normes à chaque fois que ses données sont traitées, peu importe par qui. Les deux approches sont différentes et complémentaires.

9. À cet égard, le CEPD se réjouit du fait qu'il soit indiqué, en conclusion de la Communication, que les tâches envisagées seront exécutées dans le respect des libertés et des droits fondamentaux consacrés dans la Charte, y compris les droits au respect de la vie privée et à la protection des données à caractère personnel.

2.1.2. Le droit en matière de protection des données applicable aux mesures proposées par la Commission concernant les armes à feu

10. Il est essentiel de faire explicitement référence au droit communautaire applicable en matière de protection des données dans tous les futurs actes législatifs européens qui seront présentés suite à la Communication chaque fois qu'ils contiennent des mesures impliquant le traitement de données à caractère personnel. Le CEPD recommande qu'une telle référence soit insérée dans une disposition matérielle de ces propositions.

11. La plupart des propositions qui seront présentées suite à cette Communication impliquerait le traitement de données à caractère personnel par des autorités policières et douanières à des fins de prévention et de détection des infractions pénales, ainsi que d'enquêtes et de poursuites en la matière. Chaque fois qu'un tel traitement intervient dans le contexte de la coopération entre les autorités de plusieurs États membres, la décision-cadre 2008/977/JAI du Conseil trouve application. Lorsque le traitement est effectué uniquement au niveau national, les règles nationales en matière de protection des données sont applicables. Elles peuvent découler de la directive 95/46/CE si l'État membre a appliqué les règles en matière de protection des données à des affaires pénales; dans les autres cas, elles pourraient découler des principes énoncés dans la Convention n° 108/1981 du Conseil de l'Europe[7].

12. En outre, si des bases de données européennes sont créées pour lesquelles les institutions et organes communautaires réaliseront tout ou partie du traitement (telles que la base de données des courtiers), les règles énoncées dans le règlement (CE) n° 45/2001 trouveront aussi application.

[7] Conseil de l'Europe, STCE n° 108/1981, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28.01.1981.

2.2. La nécessaire prise en considération opportune des principes clés en matière de protection des données

13. Dans la mesure du possible, les exigences relatives à la protection des données doivent être prises en considération à un stade précoce du processus législatif.

14. Le CEPD comprend que l'objectif de cette Communication n'est pas de traiter en détail certains points spécifiques. Toutefois, comme déjà exposé/évoqué plus haut, cette Communication proposant des mesures qui entraîneront la création de nouveaux traitements de données à caractère personnel ou la modification de traitements existants, il serait utile qu'elle attire l'attention sur les considérations en jeu en matière de protection des données. Cela aiderait à garantir que ces points soient évoqués suffisamment à l'avance afin que les mesures devant être adoptées à l'issue de la Communication soient conformes au droit en matière de protection des données.

15. La consultation des parties prenantes, que la Commission entend réaliser avant la présentation de ses propositions législatives en 2015, est une autre bonne opportunité de mettre en pratique les principes clés en matière de protection des données. Le CEPD recommande, par exemple, que les points suivants soient évoqués: la nécessité du traitement, les catégories de données nécessaires pour atteindre les objectifs poursuivis, la détermination des personnes compétentes ayant «besoin d'en connaître» qui peuvent accéder aux données. Les professionnels impliqués au quotidien dans la lutte contre le trafic d'armes à feu sont effectivement les mieux positionnés pour déterminer avec certitude quelles données sont nécessaires et quelles données semblent inutiles pour atteindre leur objectif. Le CEPD recommande également de consulter le groupe d'experts européens en armes à feu sur ces questions de protection des données.

16. Le CEPD se tient disponible pour fournir tous conseils, en particulier pendant ces consultations des parties prenantes. Dans cette perspective, il se réjouit de savoir qu'il sera consulté sur la collecte de données plus précises et plus complètes concernant la criminalité liée aux armes à feu dans l'Union européenne et dans le monde[8].

17. En outre, il rappelle qu'il doit impérativement être consulté sur tout acte législatif qui sera rédigé en vertu de cette Communication dès lors qu'il implique le traitement de données à caractère personnel, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

18. Par ailleurs, pour chaque proposition législative envisagée, l'impact des mesures proposées sur le droit à la protection des données à caractère personnel devrait être mesuré sur la base d'une analyse d'impact spécifique en matière de protection des données. Les résultats de cette analyse d'impact aideront à définir les exigences en matière de protection des données devant être spécifiées dans chaque proposition, le cas échéant.

[8] Voir Communication page 19, priorité 4, tâche 1.

2.3. La nécessaire spécification de ces exigences en matière de protection des données dans les futurs actes législatifs

19. Si, conformément à cette Communication, la Commission doit proposer un acte législatif impliquant le traitement de données à caractère personnel, celui-ci devra respecter des exigences en matière de protection des données et indiquer des garanties à cet égard, en tenant dûment compte du droit applicable en la matière pour cette proposition. Plus précisément:

- Pour toute situation dans laquelle un traitement de données à caractère personnel est envisagé, le CEPD recommande d'évaluer, dans l'analyse d'impact, la nécessité et la proportionnalité du traitement en tenant compte de l'ingérence dans le droit de l'individu au respect de la vie privée et des exigences en matière de protection des données à caractère personnel. Par exemple, avant d'envisager la création d'une nouvelle base de données, il convient de déterminer si un outil existant ou un outil moins intrusif ne permettrait pas d'atteindre l'objectif poursuivi, si des données à caractère personnel sont nécessaires ou si des données anonymisées pourraient suffire. S'il est prévu de rendre une base de données accessible au public, il convient de déterminer si un moyen moins intrusif pourrait permettre d'atteindre le même objectif.

- Suite à une telle évaluation, conformément au principe de limitation des finalités, la finalité pour laquelle des données sont collectées doit être précisée dans l'acte législatif et, si nécessaire, définie plus en détail. Il convient de souligner que les données collectées pour une finalité ne doivent pas être utilisées pour toute autre finalité incompatible, sans autorité légale compétente. Par exemple, dans le contexte de la lutte contre le trafic d'armes à feu, si une base de données de courtiers est mise en place pour lutter contre le courtage illicite, ce concept doit être clairement défini et la base de données ne doit pas être utilisée à d'autres fins. Il ne serait notamment pas acceptable de l'utiliser pour garantir une concurrence loyale entre les courtiers.

- Des garanties concrètes devraient être insérées dans l'acte législatif pour assurer le respect des principes en matière de protection des données. Par exemple, la liste des données devant être collectées devrait être précisée autant que possible, tout en gardant à l'esprit que seules les données strictement nécessaires pour atteindre l'objectif poursuivi devraient être collectées (principe de minimisation des données). Dans cette perspective, si la création d'une base de données des courtiers en armes à feu est considérée comme l'outil le plus pertinent pour atteindre l'objectif de lutte contre le courtage illicite d'armes à feu, seules les données nécessaires pour identifier ces courtiers devraient être conservées dans la base de données. Les données relatives à leurs antécédents médicaux, à leurs convictions religieuses, voire à leur origine ethnique, ne sont pas nécessaires pour atteindre cet objectif. Par conséquent, ces données ne doivent pas être traitées dans la base de données.

- Comme exposé ci-dessus, des garanties strictes s'appliquent en cas de traitement de données sensibles. Par exemple, si le traitement de données relatives à la santé est prévu dans le cadre de l'octroi de permis de détention d'armes à feu, l'accès à ces données doit être restreint à un professionnel de santé soumis au secret professionnel.

- Les données ne doivent pas être conservées plus longtemps que nécessaire pour atteindre l'objectif défini. Par conséquent, des périodes de conservation devraient être mises en place et le choix d'une certaine durée de conservation devrait être justifié. Pour reprendre l'exemple d'une base de données des courtiers, le futur acte législatif devra préciser la durée de conservation nécessaire pour atteindre l'objectif poursuivi. Il pourrait indiquer, par exemple, que les données seront conservées tant que la personne exerce comme courtier et jusqu'à X années après la cessation de son activité de courtier.

- L'autorité/l'organe responsable du traitement des données (ou le «responsable du traitement») devrait être identifié. En conséquence, ce dernier sera chargé de mettre à jour les données et d'en garantir la sécurité. Dans l'exemple de la base de données des courtiers, cela se traduirait par/impliquerait l'identification de l'autorité/l'organe responsable de la gestion de la base de données et de sa sécurité. Cette autorité/cet organe serait aussi l'interlocuteur des personnes concernées exerçant leurs droits.

- Des dispositions matérielles devraient être insérées pour définir les modalités selon lesquelles les droits de la personne concernée (en particulier accès, modification et suppression) seront exercés. Dans notre exemple, cela impliquerait d'insérer une clause particulière précisant que le courtier dont les données sont traitées dispose d'un droit d'accès, de modification et de suppression (dans certaines circonstances particulières) des données traitées à son sujet. La clause devrait désigner l'interlocuteur et donner ses coordonnées ou garantir que le courtier puisse facilement les obtenir.

- L'accès aux données traitées devrait être limité aux collaborateurs de l'autorité/l'organe ayant «besoin d'en connaître». S'agissant de la base de données des courtiers, le futur acte législatif devrait préciser que seuls des agents autorisés ont accès aux données.

- La sécurité physique et logique des données traitées devrait être assurée.

2.4. La mise en œuvre d'instruments internationaux au niveau européen

20. Le CEPD relève que la Communication prévoit la mise en œuvre du traité sur le commerce des armes et des normes internationales sur le contrôle des armes

légères (désignées ci-après les «ISACS») des Nations Unies, ainsi que l'appui sur l'Instrument international de traçage[9].

21. Ces instruments encouragent le traitement de données à caractère personnel telles que, par exemple, des registres de courtiers en armes à feu et des registres nationaux d'autorisations d'exportation pour le traité sur le commerce des armes, ainsi que la collecte et l'analyse centralisées de données sur les armes légères et de petit calibre illicites récupérées qui sont utiles pour le traçage de ces armes conformément aux ISACS.

22. Le CEPD insiste sur le fait que la mise en œuvre de ces instruments internationaux au niveau européen devrait être conforme au droit communautaire en matière de protection des données, lorsque cela est pertinent.

3. OBSERVATIONS SPÉCIFIQUES

3.1. Le futur établissement d'une norme européenne en matière de marquage

23. La Commission entend étudier la faisabilité d'une norme européenne en matière de marquage pour toutes les armes (priorité 1, tâche 2). Le CEPD relève que la norme commune de marquage consistera à imprimer ou graver une marque commune sur des armes à feu, ce qui permettra de les reconnaître et de les tracer. Il souligne que la note de bas de page 40 - qui précise les éléments qui seront inclus sur les marquages, selon le choix du fabricant et les prescriptions légales nationales, - ne fait pas référence aux informations personnelles du propriétaire, mais mentionne le fabricant.

24. Le CEPD recommande à la Commission de préciser dans la proposition législative pertinente si des informations personnelles, et si oui celles de quelle personne, seront traitées dans le cadre de ce marquage. Cela est particulièrement important dans la mesure où aucune autre précision n'est apportée quant aux données à caractère personnel qui devront être collectées et conservées dans le cadre de cette procédure de marquage et où l'instrument international de traçage auquel renvoie cette initiative n'en énumère aucune.

3.2. Octroi de permis de détention d'armes à feu et traitement de données relatives à la santé et aux infractions

25. Comme indiqué ci-dessus, la prise en considération opportune d'exigences en matière de protection des données et leur spécification dans le futur acte législatif sont particulièrement importantes au regard de certains des traitements envisagés dans la Communication, qui impliquent la collecte de données sensibles.

26. La Commission entend évaluer les avantages de la demande d'examens médicaux et de vérifications de casiers judiciaires comme condition d'achat et de détention licites de toute arme à feu[10].

[9] Instrument international visant à permettre aux États de procéder à l'identification et au traçage rapides et fiables des armes légères et de petit calibre, adopté par l'Assemblée générale de l'Organisation des Nations Unies le 8 décembre 2005.

[10] Voir page 13, tâche 3, deuxième paragraphe de la Communication.

27. Le CEPD tient à attirer l'attention de la Commission sur le fait que les données relatives à la santé et à l'origine ethnique (évoquées dans la priorité 3) sont considérées comme des données sensibles (article 6 de la décision-cadre 2008/977/JAI du Conseil et article 8 de la directive 95/46/CE) et, en tant que telles, sont soumises à des conditions de traitement strictes. En outre, le traitement de données relatives aux infractions est limité aux autorités officielles compétentes et peut, dans certains cas exceptionnels, être effectué par un tiers, à condition qu'il agisse sous leur contrôle (comme prévu à l'article 8, paragraphe 5, de la directive 95/46/CE). Le CEPD recommande de tenir compte de ces conditions particulières dans la rédaction d'actes législatifs relatifs à l'octroi de permis de détention d'armes à feu. En tout état de cause, le traitement de données relatives à la santé, à l'origine ethnique et aux infractions doit être prévu par la législation et satisfaire aux exigences de l'article 6 de la décision-cadre 2008/977/JAI du Conseil et de l'article 8 de la directive 95/46/CE.

28. Le CEPD insiste donc sur la nécessité de veiller à ce que des garanties en matière de protection des données soient appliquées concrètement à ce domaine spécifique et que ces garanties soient spécifiquement énoncées dans le futur acte législatif. En particulier, si le projet est confirmé, la proposition législative devrait indiquer de façon stricte/précisément la finalité du traitement et la restriction d'accès aux données aux seules personnes concernées ayant besoin de les connaître et soumises à des obligations au secret professionnel.

29. En outre, le CEPD suggère que la proposition législative contienne les éléments suivants:
    - Les «examens médicaux» et les «vérifications du casier judiciaire» devraient être définis. Les données pouvant être/susceptibles d'être traitées à ces fins devraient être énumérées de façon stricte, et des procédures de contrôle devraient être spécifiées de manière claire.
    - Les raisons médicales/légales de refus d'un permis devraient être indiquées clairement.
    - Il convient de veiller à ce qu'aucune décision ne soit prise sans intervention humaine et à ce que les droits des personnes concernées (tels que développés/qu'énumérés/que stipulés ci-dessus) soient respectés.
    - Les examens médicaux et le certificat en résultant ne devraient être réalisés et délivrés que par un professionnel de santé. Seules des autorités officielles autorisées devraient procéder aux vérifications du casier judiciaire.

3.3. L'enregistrement et le contrôle obligatoires des courtiers en armes à feu[11]

30. Le CEPD recommande que la nécessité et la proportionnalité de cette mesure soient suffisamment établies avant sa mise en œuvre. Il conseille également qu'une analyse d'impact de la protection des données soit réalisée et que des garanties adéquates soient insérées dans le futur acte législatif sur la base de cette analyse.

[11] Voir priorité 1, tâche 3, page 13.

3.4. «Armes intelligentes»: l'utilisation éventuelle de capteurs biométriques

31. Le CEPD relève que la Commission étudiera «des solutions technologiques, par exemple des capteurs biométriques, lorsque des données à caractère personnel sont stockées dans l'arme à feu, afin de garantir que l'arme ne puisse être utilisée que par son propriétaire légal»[12]. Une telle technologie pourrait être obligatoire pour des armes à feu vendues légalement dans l'Union européenne afin d'empêcher toute utilisation illicite suite à un vol ou une perte.

32. Les données biométriques, de par leur nature même, concernent directement un individu et, par conséquent, constituent des données à caractère personnel. Une condition préalable à l'utilisation de données biométriques est la définition claire de la finalité pour laquelle les données biométriques sont collectées et traitées, qui tienne compte des risques pour la protection des libertés et des droits fondamentaux des individus. Dans son avis sur l'évolution des technologies biométriques[13], le groupe de travail «Article 29» a insisté sur le fait que «*en règle générale, l'utilisation de la biométrie pour des exigences générales de sécurité de biens et de personnes ne peut être considérée comme un intérêt légitime qui l'emporte sur les droits et libertés fondamentaux de la personne concernée. Au contraire, le traitement de données biométriques ne peut se justifier en tant qu'outil nécessaire assurant la sécurité de biens ou de personnes, lorsqu'il existe des preuves objectives et documentées de l'existence concrète d'un risque considérable. À cet effet, le responsable du traitement doit prouver que les circonstances spécifiques posent un risque considérable concret, qu'il doit évaluer très soigneusement. Afin de respecter le principe de proportionnalité, le responsable du traitement doit, en présence d'une de ces situations à haut risque, vérifier si d'éventuelles mesures alternatives pourraient être tout aussi efficaces mais moins intrusives au regard de la finalité poursuivie, et choisir ces alternatives. L'existence de ces circonstances doit également être régulièrement contrôlée. Sur la base des résultats de cet examen, toute opération de traitement des données qui se révèle ne plus être justifiée doit être suspendue ou arrêtée*»[14].

33. Le CEPD relève que la Commission évoque le risque considérable associé au détournement d'armes à feu pour justifier le traitement de données biométriques. Une telle justification pourrait permettre le traitement d'empreintes digitales, à condition toutefois que la Commission apporte des preuves concrètes de ce risque dans la proposition pertinente. De même, le CEPD se réjouit de l'intention de spécifier les modalités de conservation des données biométriques, à savoir dans l'arme à feu. Cette solution, qui n'implique pas la création d'une base de données centrale des empreintes digitales des propriétaires d'armes à feu, semble légitime et acceptable, tandis que la conservation dans une base de données centrale aurait nécessité une justification plus solide.

34. Le CEPD recommande néanmoins une évaluation prudente des conséquences du traitement proposé en matière de protection des données. Entre autres, il insiste sur la nécessité de préciser le type de données biométriques visant à identifier le

[12] Voir priorité 2, tâche 2, page 15.
[13] Avis 3/2012 sur l'évolution des technologies biométriques, 00720/12/FR WP 193, adopté le 27 avril 2012.
[14] Voir avis 3/2012, page 14.

propriétaire. Il recommande également d'indiquer dans la proposition les mesures de sécurité qui devraient être mises en place pour garantir l'accès aux données conservées et pour empêcher la manipulation, ainsi que de définir la façon dont les empreintes digitales conservées seront modifiées en cas de changement de propriétaire de l'arme à feu.

3.5. Fournir des orientations aux agents des services répressifs[15] et le traitement de données liées à l'origine ethnique du détenteur de l'arme à feu

35. Le CEPD recommande que l'application et, si nécessaire, la mise à jour des lignes directrices élaborées par le Conseil pour normaliser les procédures concernant les enquêtes transfrontières relatives à des armes à feu saisies ou récupérées ayant servi à des activités criminelles[16] soient conformes aux exigences en matière de protection des données pour toute situation dans laquelle le traitement de données à caractère personnel est envisagé. En particulier, il relève que les procédures présentées par le Conseil, ainsi que les modèles suggérés, impliquent la collecte de données à caractère personnel concernant le détenteur de l'arme à feu et, plus précisément, la collecte de son «origine ethnique»[17] ainsi que des références à ses antécédents judiciaires (qui sont des catégories spéciales de données, comme expliqué au point 3.2 ci-dessus). Pourtant, il n'est fait aucune mention de la protection des données dans ces lignes directrices, alors même que la décision-cadre 2008/977/JAI du Conseil s'applique.

36. En particulier, il convient de tenir dûment compte de l'article 6 de la décision-cadre du Conseil, consacré au traitement de catégories spéciales de données, qui dispose que le «*traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique (...) n'est autorisé que lorsque cela est strictement nécessaire et lorsque des garanties adéquates sont prévues par la législation nationale*». À cet égard, le CEPD recommande d'évaluer la nécessité du traitement de données liées à l'origine ethnique du détenteur de l'arme à feu pour la réalisation de l'objectif poursuivi. Il conseille également que des références aux règles visées dans la décision-cadre du Conseil soient insérées dans ces lignes directrices lorsqu'elles seront mises à jour.

3.6. Coopération transfrontière pour mettre un terme à la détention et à la circulation illégales d'armes à feu

37. Le CEPD relève que le projet de coopération transfrontière pour mettre un terme à la détention et à la circulation illégales d'armes à feu comprendra la collecte coordonnée et le partage d'informations sur la criminalité liée aux armes à feu, associant la police, les gardes-frontières et les autorités douanières, tant dans les États membres qu'au-delà des frontières[18]. Il comprend que ce projet impliquera

[15] Voir priorité 3, tâche 1.
[16] Voir note de bas de page 53, page 14.
[17] Voir page 13 de la recommandation du Conseil relative à une procédure standard applicable dans les États membres aux fins des enquêtes transfrontières menées par les services de police concernant les filières d'approvisionnement en armes à feu saisies ou récupérées ayant servi à des activités criminelles. http://register.consilium.europa.eu/doc/srv?l=FR&t=PDF&gc=true&sc=false&f=ST%2010000%202007%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F07%2Fst10%2Fst10000.fr07.pdf.
[18] Voir priorité 3, tâche 2.

très probablement la collecte et le partage de données à caractère personnel concernant des suspects, des victimes et, potentiellement, des courtiers dans des bases de données transfrontières nationales et européennes.

38. En conséquence, le CEPD souhaite souligner que la décision-cadre 2008/977/JAI du Conseil s'appliquera à ces traitements et que des garanties spécifiques doivent être développées lorsque des transferts de données vers des pays tiers sont prévus. Le traitement de données à caractère personnel au niveau européen, quant à lui, devra être conforme aux garanties en matière de protection des données édictées par le règlement (CE) n° 45/2001.

39. De même, la Commission encourage un suivi concerté des signalements relatifs à des armes à feu dans le système d'information Schengen.

40. Le CEPD se réjouit de l'objectif ainsi poursuivi par la Commission, à savoir encourager et améliorer l'utilisation des bases de données existantes, plutôt que suggérer la création de nouvelles bases, conformément à la considération sous-jacente selon laquelle de nouvelles bases de données devraient être créées uniquement lorsque cela s'avère nécessaire à l'objectif poursuivi[19].

41. À cet égard, il souligne que l'échange transfrontalier d'informations entre les autorités officielles au sein de l'Union européenne devrait impliquer, autant que possible, l'utilisation des canaux sécurisés existants.

3.7. Un répertoire central en ligne rassemblant des informations factuelles concernant la balistique et les types d'armes

42. Le CEPD relève la possibilité d'établir un répertoire central en ligne des informations factuelles concernant la balistique et les types d'armes, dont la gestion serait confiée à Europol. Il comprend que ce répertoire n'impliquerait pas le traitement de données à caractère personnel et recommande donc que cela soit précisé lorsque cela est pertinent, si cette idée se traduit par une action législative concrète.

3.8. Plan de collecte de données sur les armes à feu[20]

43. La Communication souligne que des informations sur des armes saisies peuvent être enregistrées par la police dans ses bases de données et par les douanes dans leurs bases de données. En outre, le système commun de gestion des risques, le système d'information des douanes et le système d'information d'Europol ne sont pas interopérables. Les tâches proposées par la Commission pour lutter contre l'absence de traçage des armes à feu en résultant comprennent le développement d'un plan de collecte de données sur les armes à feu et une solution pratique permettant à des experts des armes à feu d'interroger toutes les bases de données à la recherche d'armes à feu perdues ou volées au moyen d'une seule opération.

[19] Voir, en particulier, avis du CEPD du 18 juillet 2013 sur les propositions de règlement établissant un système d'entrée/sortie (EES) et de règlement établissant un programme d'enregistrement des voyageurs (RTP), disponible en anglais dans la rubrique Consultation du site internet du CEPD, www.edps.europa.eu.
[20] Voir priorité 4: améliorer la connaissance de la situation grâce au renseignement.

44. S'agissant de la première tâche consistant à développer un plan de collecte de données sur les armes à feu, le CEPD considère que cela impliquera forcément la collecte de données à caractère personnel et, par conséquent, il se réjouit de savoir qu'il doit être consulté, de même que d'autres parties prenantes. Cela garantira que les exigences en matière de protection des données, y compris le principe de minimisation des données (seules les données strictement nécessaires à l'objectif poursuivi doivent être collectées) et le besoin de définir une période commune et justifiée de conservation des données, sont pris en compte en amont et lors de la création du plan de collecte des données.

45. S'agissant de la seconde tâche d'interrogation de bases de données à la recherche d'armes à feu perdues ou volées, y compris Europol, CIS, SIS II et iARMS[21], le CEPD reconnaît la légitimité du besoin d'échange d'informations entre des experts des armes à feu, qu'il s'agisse de policiers, de gardes-frontières ou d'agents des douanes.

46. La Commission suggère que des applications nationales des services répressifs soient mises à jour pour permettre au gestionnaire du dossier de créer, d'actualiser ou de supprimer des enregistrements au moyen d'une seule opération, ce qui garantirait que les enregistrements soient corrects dans les registres nationaux, le SIS II et iArms. Le CEPD comprend l'objectif poursuivi, qui améliorerait très probablement l'exactitude des données, mais il tient à souligner que ces développements doivent intervenir conformément aux règles existantes concernant l'accès aux bases de données susmentionnées.

47. Le CEPD insiste pour limiter l'accès à ces bases de données aux autorités compétentes et, au sein de celles-ci, aux seuls agents ayant «besoin d'en connaître». Il recommande également que la traçabilité de l'accès de ces agents désignés aux bases de données soit assurée par l'attribution d'identifiants et de mots de passe individuels. À cet égard, il se réjouit que le règlement (CE) n° 1987/2006[22] et la décision 2007/533/JAI du Conseil[23] limitent déjà cet accès et prévoient une traçabilité. Il se réjouit également du fait que l'accès à iARMS et la traçabilité soient couverts par la partie 3 des règles d'INTERPOL en matière de traitement de données.

48. En outre, si l'accès de nouvelles entités aux bases de données susmentionnées devait être envisagé, cette extension des droits d'accès devrait intervenir sur le fondement d'une base légale spécifique, par voie d'amendement de la base légale actuelle.

49. Enfin, le CEPD recommande de clarifier les modalités de l'opération unique sur la base de laquelle la création, la mise à jour et la suppression de registres interviendraient simultanément dans des registres nationaux, le SIS II et iARMS.

[21] Système de gestion de l'enregistrement et du traçage des armes illicites d'INTERPOL.
[22] Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).
[23] Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), article 10, points b) et f).

50. Selon la Communication, «toute déclaration de perte ou de vol d'une arme à feu devrait donner lieu à un signalement dans le SIS II et dans le système iARMS»[24]. À cet égard, le CEPD se réjouit que ces deux bases de données impliquent une traçabilité totale des actions effectuées dans le registre par l'agent qui réagira au signalement ou utilisera l'outil de recherche. Cela permettra de garantir le respect du principe de limitation des finalités et la conformité aux mesures strictes de sécurité.

51. La Communication indique également que «*les États membres devraient veiller à ce que tous les utilisateurs finaux aient accès aux outils de recherche actuellement disponibles qui leur permettent d'introduire une requête unique pour interroger les registres nationaux, le SIS II et iARMS, l'ensemble des résultats s'affichant sur l'écran de ces utilisateurs*»[25]. Le CEPD rappelle que seuls les utilisateurs finaux initialement autorisés à accéder aux registres nationaux, au SIS II et à iARMS devraient utiliser ces outils de recherche et que les résultats s'affichant sur l'écran de ces utilisateurs devraient uniquement prendre la forme d'une réponse de concordance/non-concordance.

4. CONCLUSIONS

52. Le CEPD se réjouit que la Communication précise que les mesures prévues seront mises en œuvre en toute conformité avec les droits à la vie privée et à la protection des données à caractère personnel. Toutefois, il souligne que le traitement de données à caractère personnel devrait être reflété à un stade précoce de la procédure législative et, de préférence, également au stade d'adoption de communications par la Commission. Cela aiderait à garantir que les questions de protection des données soient évoquées suffisamment à l'avance afin que les mesures adoptées soient conformes au droit en matière de protection des données.

53. Le CEPD recommande que les aspects de protection des données qui sont pertinents pour les mesures proposées en lien avec les armes à feu soient évoqués lors de la consultation des parties prenantes à laquelle procèdera la Commission. Il conseille également de consulter le groupe d'experts européens en armes à feu sur les questions de protection des données.

54. S'agissant des futures propositions législatives devant être présentées par la Commission suite à cette Communication, le CEPD recommande qu'une référence explicite au droit européen applicable en matière de protection des données soit insérée à chaque fois qu'elles impliquent le traitement de données à caractère personnel. Ceci devrait être fait sous forme de disposition matérielle dédiée dans ces propositions. Conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, le CEPD doit être consulté sur les propositions qui impliquent le traitement de données à caractère personnel.

55. Dans le présent avis, le CEPD a mis en évidence les exigences en matière de protection des données qui s'appliquent à la lutte contre le trafic illicite d'armes à feu. Il recommande que tout futur acte législatif dans ce domaine tienne compte des exigences en matière de protection des données, telles que la nécessité, la

[24] Voir priorité 4, tâche 1, page 20.
[25] Voir priorité 4, tâche 1, page 20.

proportionnalité, la limitation des finalités, le principe de minimisation des données, les catégories spéciales de données, la période de conservation des données, les droits des personnes concernées et la sécurité du traitement. Il conseille également de réaliser une analyse d'impact de la protection des données qui contribuera à spécifier les garanties en la matière devant être insérées dans chaque proposition, le cas échéant.

56. Plus spécifiquement, le CEPD formule les recommandations suivantes:

- Tout futur acte législatif concernant l'établissement d'une norme européenne en matière de marquage devrait préciser si des données à caractère personnel seront traitées et, si oui, lesquelles et au sujet de qui;

- S'agissant de l'octroi de permis de détention d'armes à feu, la nécessité de traiter des données médicales et ethniques, ainsi que celle des vérifications du casier judiciaire, devraient être évaluées, et les conditions dans lesquelles ces catégories spéciales de données peuvent être traitées devraient être respectées, tel que prévu à l'article 6 de la décision-cadre 2008/977/JAI du Conseil et à l'article 8 de la directive 95/46/CE. Le futur acte législatif devrait contenir des garanties spécifiques, notamment: indiquer la finalité du traitement, énumérer les types exacts de données qui peuvent être traitées, restreindre l'accès aux données sensibles aux seules personnes pertinentes ayant besoin de les connaître et soumises à une obligation de secret professionnel (telles qu'un professionnel de santé, des autorités officielles autorisées), garantir que les motifs médicaux / ethniques / judiciaires de refus d'un permis soient clairement indiqués et préciser les modalités d'exercice des droits des personnes concernées;

- La nécessité et la proportionnalité de l'enregistrement et du contrôle obligatoires des courtiers en armes à feu devraient être suffisamment établies avant la mise en œuvre de la mesure;

- S'agissant de la possibilité d'utiliser des capteurs biométriques sur des armes intelligentes, la preuve des risques pour la sécurité justifiant l'utilisation de données biométriques devrait être apportée dans la proposition pertinente. La proposition devrait indiquer les types de données biométriques devant être traitées et les mesures de sécurité régissant l'accès aux données, la prévention de la manipulation des données et les conditions de mise à jour des données biométriques en cas de changement de propriétaire;

- La mise à jour des orientations fournies aux agents des services répressifs devrait inclure des références aux règles énoncées dans la décision-cadre 2008/977/JAI du Conseil, en particulier concernant le traitement de catégories spéciales de données. Il conseille également d'évaluer la nécessité du traitement de données liées à l'origine ethnique du détenteur de l'arme à feu;

- S’agissant de la coopération transfrontière, l’échange transfrontalier d’informations entre les autorités officielles au sein de l’Union européenne devrait impliquer, autant que possible, l’utilisation des canaux sécurisés existants;

- Si un répertoire central en ligne rassemblant des informations factuelles concernant la balistique et les types d’armes est créé, l’acte législatif pertinent devrait mentionner l’absence de traitement de données à caractère personnel;

- S’agissant du plan de collecte de données sur les armes à feu, il conviendrait de veiller à ce que les nouvelles fonctionnalités introduites dans les registres nationaux, le SIS II et iARMS soient conformes aux règles existantes/en vigueur relatives à l’accès à ces bases de données. Tout projet d’extension de l’accès à ces bases de données à d’autres entités/utilisateurs devrait nécessiter la modification de la base légale actuelle. L’accès à l’outil de recherche dans ces bases de données devrait être réservé aux utilisateurs autorisés, et les résultats de ces recherches devraient prendre la forme d’une réponse de concordance/non-concordance.

Fait à Bruxelles, Belgique, le 17 février 2014

(signé)

Giovanni BUTTARELLI
Contrôleur européen adjoint de la protection des données