

CONCOURS EXTERNE
DE TECHNICIEN PRINCIPAL
DE POLICE TECHNIQUE ET SCIENTIFIQUE
DE LA POLICE NATIONALE

SESSION 2019

ÉPREUVE ÉCRITE D'ÉTUDE D'UN DOSSIER DOCUMENTAIRE
EN LIEN AVEC LA POLICE TECHNIQUE ET SCIENTIFIQUE

Durée de l'épreuve : 2 heures – Coefficient : 1

Il vous appartient de vous assurer que le sujet en votre possession comporte la totalité des pages (20 pages).

Il vous est demandé de répondre avec clarté à chaque question, sur votre feuille de composition (coin gommé).

Sous peine d'annulation de leur épreuve, les candidats ne devront faire apparaître **aucun signe ou mention** pouvant permettre l'identification des copies et intercalaires.

*Epreuve écrite d'étude d'un dossier documentaire
en lien avec la police technique et scientifique*

Dossier documentaire

**La coopération européenne en matière de
police technique et scientifique**

DOCUMENT 1 – 5 pages

Décision 2008/615/JAI du 23 juin 2008 - extrait du journal officiel de l'union européenne

DOCUMENT 2 – 3 pages

Décision-cadre 2009/905/JAI du 30/11/2009 relative à l'accréditation des prestataires de services de police scientifique menant des activités de laboratoire – extrait du journal officiel de l'union européenne

DOCUMENT 3 – 1 page

Extrait du code de la sécurité intérieure – article L235-1

DOCUMENT 4 – 3 pages

Chapitre 2 du traité du 27 mai 2005 relatif à l'approfondissement de la coopération transfrontalière.

DOCUMENT 5 – 2 pages

Le fichier des empreintes digitales ouvert aux policiers étrangers – Le Monde.fr du 10/02/2011

DOCUMENT 6 – 1 page

La division des relations internationales– article du 13/12/2011

DOCUMENT 7 – 2 pages

Extrait du décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur

Vous répondrez aux questions suivantes

1. a) Sur quelles bases légales reposent les échanges de données dactyloscopiques et génétiques (3 pts)
b) Quelles en ont été les conséquences pour la police technique et scientifique française ? (2 pts)
2. En vous basant sur les documents et vos connaissances personnelles, citez les principaux acteurs français impliqués dans cette coopération (2 pts)
3. Quelles sont, dans le cadre des échanges de données des fichiers de PTS, les préconisations en matière de protection des données personnelles ? (4 pts)
4. Énumérez les avantages et les inconvénients de ces échanges (4 pts)
5. Selon vous, quels seraient les axes d'amélioration dans ces échanges ? (3 pts)

La présentation et l'orthographe sont notées sur 2 points

III

(Actes pris en application du traité UE)

ACTES PRIS EN APPLICATION DU TITRE VI DU TRAITÉ UE

DÉCISION 2008/615/JAI DU CONSEIL

du 23 juin 2008

relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 30, paragraphe 1, points a) et b), son article 31, paragraphe 1, point a), son article 32 et son article 34, paragraphe 2, point c),

vu l'initiative du Royaume de Belgique, de la République de Bulgarie, de la République fédérale d'Allemagne, du Royaume d'Espagne, de la République française, du Grand-Duché de Luxembourg, du Royaume des Pays-Bas, de la République d'Autriche, de la République de Slovénie, de la République slovaque, de la République italienne, de la République de Finlande, de la République portugaise, de la Roumanie et du Royaume de Suède,

vu l'avis du Parlement européen ⁽¹⁾,

considérant ce qui suit:

- (1) À la suite de l'entrée en vigueur du traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale («traité de Prüm»), la présente initiative est présentée, en concertation avec la Commission européenne et conformément aux dispositions du traité sur l'Union européenne, dans le but d'intégrer, en substance, les dispositions du traité de Prüm dans le cadre juridique de l'Union européenne.
- (2) Les conclusions du Conseil européen de Tampere d'octobre 1999 ont confirmé la nécessité de renforcer l'échange d'informations entre les autorités compétentes des États membres aux fins de la détection des infractions et des enquêtes en la matière.
- (3) Dans le programme de La Haye de novembre 2004 qui vise à renforcer la liberté, la sécurité et la justice dans l'Union européenne, le Conseil européen a déclaré être persuadé que cet objectif passe par une approche innovante de l'échange transfrontalier d'informations en matière répressive.
- (4) Le Conseil européen a dès lors affirmé que l'échange de ces informations devrait obéir aux conditions s'appliquant au principe de disponibilité. Selon ce principe, tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre, les services répressifs de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées, en tenant compte des exigences des enquêtes en cours dans cet autre État.
- (5) Le Conseil européen a fixé au 1^{er} janvier 2008 la date limite pour atteindre cet objectif dans le cadre du programme de La Haye.
- (6) La décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ⁽²⁾ fixe déjà les règles en vertu desquelles les services répressifs des États membres peuvent échanger d'une manière rapide et efficace des informations et des renseignements afin de mener des enquêtes pénales ou des opérations policières de collecte de renseignement.
- (7) Le programme de La Haye visant à renforcer la liberté, la sécurité et la justice précise également que les nouvelles technologies devraient être exploitées pleinement et qu'un accès réciproque aux banques de données nationales devrait également être prévu, tout en stipulant que de nouvelles bases de données européennes centralisées ne devraient être créées que sur la base d'études qui en auront démontré la valeur ajoutée.

(1) Avis du 10 juin 2007 (non encore paru au Journal officiel).

(2) JO L 386 du 29.12.2006, p. 89.

- (8) Pour que la coopération internationale soit réelle, il est primordial que des informations précises puissent être échangées de manière rapide et efficace. Pour cela, il y a lieu de prévoir des procédures favorisant des échanges de données rapides, efficaces et peu coûteux. Aux fins de l'utilisation conjointe des données, ces procédures devraient respecter le principe de responsabilité et prévoir des garanties appropriées quant à l'exactitude et à la sécurité des données pendant leur transmission et leur conservation, ainsi que des modalités d'enregistrement des échanges de données et des restrictions à l'utilisation des informations échangées.
- (9) Ces conditions sont remplies par le traité de Prüm. Pour que tous les États membres satisfassent aux exigences de fond du programme de La Haye dans les délais qui y sont fixés, les parties essentielles du traité de Prüm devraient, en substance, devenir applicables à l'ensemble des États membres.
- (10) La présente décision contient donc des dispositions fondées sur les dispositions principales du traité de Prüm et destinées à améliorer l'échange d'informations, qui permettent aux États membres d'accorder aux autres États membres des droits d'accès à leurs fichiers automatisés d'analyses ADN, à leurs systèmes automatisés d'identification dactyloscopique et à leurs registres d'immatriculation des véhicules. Dans le cas de données extraites de fichiers nationaux d'analyse ADN et de systèmes automatisés d'identification dactyloscopique, un système «hit-no hit» (de concordance/non-concordance) devrait permettre à l'État membre qui effectue une consultation de demander, dans un second temps, des données à caractère personnel bien précises à l'État membre gestionnaire du dossier et, le cas échéant, de demander des informations complémentaires par le biais des procédures d'entraide judiciaire, notamment celles adoptées conformément à la décision-cadre 2006/960/JAI.
- (11) Cela accélérerait considérablement les procédures existantes qui permettent aux États membres de savoir si un autre État membre quel qu'il soit dispose ou non des informations dont ils ont besoin et, dans l'affirmative, de déterminer lequel.
- (12) La comparaison transfrontalière des données devrait conférer une nouvelle dimension à la lutte contre la criminalité. Les informations obtenues par comparaison des données devraient ouvrir aux États membres de nouvelles perspectives quant aux méthodes d'enquête et jouer ainsi un rôle crucial en matière d'aide aux services répressifs et aux autorités judiciaires des États membres.
- (13) La règle est de mettre en réseau des bases de données nationales des États membres.
- (14) Sous certaines conditions, les États membres devraient pouvoir fournir des données, à caractère personnel ou non, de façon à améliorer l'échange d'informations aux fins de la prévention des infractions pénales et du maintien de l'ordre et de la sécurité publics en liaison avec des manifestations de grande envergure revêtant une dimension transfrontalière.
- (15) Dans le cadre de la mise en œuvre de l'article 12, les États membres peuvent décider de donner la priorité à la lutte contre la criminalité grave, en tenant compte des capacités techniques limitées disponibles pour la transmission de données.
- (16) Outre l'amélioration des échanges d'informations, il est nécessaire de réglementer les autres formes de coopération plus étroite entre les services de police, en particulier par le biais d'opérations conjointes de sécurité (telles que des patrouilles communes).
- (17) Une coopération policière et judiciaire plus étroite en matière pénale doit aller de pair avec le respect des droits fondamentaux, en particulier du droit au respect de la vie privée et du droit à la protection des données à caractère personnel, que garantiraient des arrangements particuliers en matière de protection des données, qui devraient être adaptés à la nature spécifique des différentes formes d'échange de données. Ces arrangements en matière de protection des données devraient tenir particulièrement compte de la nature spécifique de l'accès en ligne transfrontalier aux bases de données. Étant donné que, avec l'accès en ligne, il n'est pas possible pour l'État membre gestionnaire du dossier de réaliser des contrôles préalables, il conviendrait de mettre en place un système garantissant qu'une vérification ultérieure est bien effectuée.
- (18) Le système «hit-no hit» (de concordance/non-concordance) crée une structure de comparaison de profils anonymes, dans le cadre de laquelle des données à caractère personnel supplémentaires ne sont échangées qu'après une concordance, leur transmission et leur réception étant régies par la législation nationale, y compris les règles d'assistance juridique. Ce mécanisme garantit un système adéquat de protection des données, étant entendu que la transmission de données à caractère personnel à un autre État membre exige un niveau suffisant de protection des données de la part de l'État membre destinataire.
- (19) Compte tenu des importants échanges d'informations et de données qui découlent d'une coopération policière et judiciaire plus étroite, la présente décision vise à garantir un niveau approprié de protection des données. Elle respecte le niveau de protection prévu pour le traitement des données à caractère personnel dans la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et dans son protocole additionnel du 8 novembre 2001, ainsi que les principes énoncés dans la recommandation n° R (87) 15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

- (20) Les dispositions en matière de protection des données contenues dans la présente décision comprennent également des principes relatifs à la protection des données, qu'il était nécessaire de mentionner, compte tenu de l'absence d'une décision-cadre sur la protection des données dans le troisième pilier. Cette décision-cadre devrait s'appliquer à l'ensemble du domaine de la coopération policière et judiciaire en matière pénale, à condition que son niveau de protection des données ne soit pas inférieur à la protection prévue par la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et par son protocole additionnel du 8 novembre 2001, et elle tient compte de la recommandation n° R (87) 15 du 17 septembre 1987 du comité des ministres aux États membres visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police, même si ces données ne font pas l'objet d'un traitement automatique.
- (21) Étant donné que les objectifs de la présente décision, notamment l'amélioration des échanges d'informations dans l'Union européenne, ne peuvent pas être réalisés de manière suffisante par les États membres agissant isolément, en raison du caractère transnational de la lutte contre la criminalité et des questions de sécurité, et peuvent donc, en raison de l'interdépendance des États membres dans ces domaines, être mieux réalisés au niveau communautaire, la Communauté peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité instituant la Communauté européenne et visé à l'article 2 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé à l'article 5 du traité CE, la présente décision n'exécède pas ce qui est nécessaire pour atteindre ces objectifs.
- (22) La présente décision respecte les droits fondamentaux et observe les principes définis notamment dans la Charte des droits fondamentaux de l'Union européenne,

DÉCIDE:

CHAPITRE 1

GÉNÉRALITÉS

Article premier

Objet et champ d'application

Par la présente décision, les États membres visent à approfondir la coopération transfrontalière dans les matières relevant du titre VI du traité, en particulier l'échange d'informations entre les services chargés de la prévention des infractions pénales et des enquêtes en la matière. À cet effet, la présente décision contient des règles dans les domaines suivants:

- dispositions relatives aux conditions et aux procédures applicables au transfert automatisé des profils ADN, des données dactyloscopiques et de certaines données nationales relatives à l'immatriculation des véhicules (chapitre 2);
- dispositions relatives aux conditions de transmission de données en liaison avec des manifestations de grande envergure revêtant une dimension transfrontalière (chapitre 3);

- dispositions relatives aux conditions de transmission d'informations en vue de prévenir les infractions terroristes (chapitre 4);
- dispositions relatives aux conditions et aux procédures applicables à l'approfondissement de la coopération policière transfrontalière par le biais de diverses mesures (chapitre 5).

CHAPITRE 2

ACCÈS EN LIGNE ET DEMANDES DE SUIVI

SECTION 1

Profils ADN

Article 2

Création de fichiers nationaux d'analyses ADN

1. Les États membres créent et conservent des fichiers nationaux d'analyses ADN aux fins des enquêtes relatives aux infractions pénales. Le traitement des données conservées dans ces fichiers en vertu de la présente décision s'effectue conformément au droit national applicable au traitement.

2. Aux fins de la mise en œuvre de la présente décision, les États membres garantissent la disponibilité de données indexées provenant de leurs fichiers nationaux d'analyses ADN visés dans la première phrase du paragraphe 1. Ces données indexées ne contiennent que les profils ADN issus de la partie non codante de l'ADN et une référence. Les données indexées ne contiennent aucune donnée permettant l'identification directe de la personne concernée. Les données indexées qui ne peuvent être attribuées à aucun individu (profils ADN non identifiés) doivent être reconnaissables comme telles.

3. Chaque État membre informe le secrétariat général du Conseil des fichiers nationaux d'analyses ADN auxquels s'appliquent les articles 2 à 6, ainsi que des conditions régissant la consultation automatisée visée à l'article 3, paragraphe 1, conformément à l'article 36.

Article 3

Consultation automatisée de profils ADN

1. Aux fins d'enquête en matière d'infractions pénales, les États membres autorisent les points de contact nationaux des autres États membres, visés à l'article 6, à accéder aux données indexées de leurs fichiers d'analyses ADN, avec la possibilité de procéder à des consultations automatisées par comparaison de profils ADN. La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. Si une consultation automatisée révèle des concordances entre un profil ADN transmis et les profils ADN enregistrés dans le fichier consulté de l'État membre destinataire, le point de contact national de l'État membre effectuant la consultation reçoit de manière automatisée les données indexées pour lesquelles une concordance a été mise en évidence. Si aucune concordance ne peut être mise en évidence, notification en est faite de manière automatisée.

Article 4

Comparaison automatisée de profils ADN

1. Aux fins d'enquêtes en matière d'infractions pénales, les États membres comparent d'un commun accord, par l'intermédiaire de leurs points de contact nationaux, les profils ADN non identifiés avec tous les profils ADN provenant des données indexées des autres fichiers nationaux d'analyses ADN. La transmission et la comparaison se font de manière automatisée. Les profils ADN non identifiés ne sont transmis aux fins de comparaison que lorsque le droit national de l'État membre requérant prévoit une telle transmission.

2. Si la comparaison visée au paragraphe 1 permet à un État membre de mettre en évidence une concordance entre des profils ADN transmis et le contenu de son propre fichier d'analyse ADN, il communique sans délai au point de contact national de l'autre État membre les données indexées pour lesquelles une concordance a été mise en évidence.

Article 5

Transmission d'autres données à caractère personnel et d'autres informations

Si les procédures prévues aux articles 3 et 4 révèlent une concordance de profils ADN, la transmission d'autres données disponibles à caractère personnel et d'autres informations relatives aux données indexées est régie par le droit national de l'État membre requis, y compris les dispositions relatives à l'entraide judiciaire.

Article 6

Point de contact national et mesures d'exécution

1. Aux fins de la transmission des données prévues aux articles 3 et 4, chaque État membre désigne un point de contact national. Les compétences des points de contact nationaux sont régies par le droit national qui leur est applicable.

2. Les mesures d'exécution visées à l'article 33 règlent les détails techniques des procédures prévues aux articles 3 et 4.

Article 7

Prélèvement de matériel génétique et transmission de profils ADN

Si, dans le cadre d'une enquête ou d'une procédure judiciaire en cours, le profil ADN d'une personne déterminée présente sur le territoire de l'État membre requis fait défaut, ce dernier accorde l'entraide judiciaire en prélevant et en analysant le matériel génétique de cette personne ainsi qu'en transmettant le profil ADN ainsi obtenu, à condition:

- a) que l'État membre requérant indique à quelles fins cette procédure est nécessaire;
- b) que l'État membre requérant présente une ordonnance ou un mandat relatif à l'enquête, émis par l'autorité compétente, conformément au droit national de cet État

membre, et montrant que les conditions préalables au prélèvement et à l'analyse du matériel génétique seraient réunies dans l'hypothèse où la personne en question aurait été présente sur le territoire de l'État membre requérant, et

- c) que les conditions préalables prévues par le droit de l'État membre requis en matière de prélèvement et d'analyse du matériel génétique ainsi que de transmission du profil ADN obtenu sont réunies.

SECTION 2

Données dactyloscopiques

Article 8

Données dactyloscopiques

Aux fins de la mise en œuvre de la présente décision, les États membres veillent à la disponibilité des données indexées provenant du fichier regroupant les systèmes automatisés nationaux d'identification par empreintes digitales créés en vue de la prévention et des enquêtes en matière d'infractions pénales. Ces données indexées ne contiennent que des données dactyloscopiques et un numéro de référence. Les données indexées ne contiennent aucune donnée permettant l'identification directe de la personne concernée. Les données indexées qui ne peuvent être rattachées à aucune personne (données dactyloscopiques non identifiées) doivent être reconnaissables en tant que telles.

Article 9

Consultation automatisée de données dactyloscopiques

1. Aux fins de prévention et d'enquête en matière d'infractions pénales, les États membres autorisent les points de contact nationaux des autres États membres, visés à l'article 11, à accéder aux données indexées des systèmes automatisés d'identification par empreintes digitales qu'ils ont créés à cet effet, avec la possibilité de procéder à des consultations automatisées par comparaison de données dactyloscopiques. La consultation n'est possible que cas par cas et dans le respect du droit national de l'État membre requérant.

2. La confirmation d'une concordance formelle entre une donnée dactyloscopique et une donnée indexée détenue par l'État membre gestionnaire du fichier est établie par le point de contact national de l'État membre requérant au moyen d'une transmission automatisée des données indexées nécessaires à une attribution claire.

Article 10

Transmission d'autres données à caractère personnel et d'autres informations

Si la procédure prévue à l'article 9 révèle une concordance des données dactyloscopiques, la transmission d'autres données à caractère personnel et d'autres informations, relatives aux données indexées, est régie par le droit national de l'État membre requis, y compris les dispositions relatives à l'entraide judiciaire.

*Article 11***Point de contact national et mesures d'exécution**

1. Aux fins de la transmission de données prévue à l'article 9, chaque État membre désigne un point de contact national. Les compétences des points de contact nationaux sont régies par le droit national qui leur est applicable.

2. Les mesures d'exécution visées à l'article 33 règlent les modalités techniques de la procédure prévue à l'article 9.

SECTION 3

Données relatives à l'immatriculation des véhicules*Article 12***Consultation automatisée de données relatives à l'immatriculation des véhicules**

1. Aux fins de la prévention et de l'enquête en matière d'infractions pénales, et dans le cadre du traitement d'autres infractions relevant de la compétence des tribunaux ou du ministère public de l'État membre effectuant la consultation, ainsi que dans le cadre du maintien de la sécurité publique, les États membres autorisent les points de contact nationaux des autres États membres, visés au paragraphe 2, à accéder aux données nationales suivantes relatives à l'immatriculation des véhicules, avec la possibilité de procéder, cas par cas, à une consultation automatisée:

- a) les données relatives aux propriétaires ou aux détenteurs, et
- b) les données relatives aux véhicules.

Les consultations nécessitent un numéro de châssis complet ou un numéro d'immatriculation complet. La consultation n'est possible que dans le respect du droit national de l'État membre effectuant ladite consultation.

2. Aux fins de la transmission des données en vertu du paragraphe 1, chaque État membre désigne un point de contact national pour les demandes qui lui sont adressées. Les compétences des points de contact nationaux sont régies par le droit national qui leur est applicable. Les mesures d'exécution visées à l'article 33 règlent les détails techniques de la procédure.

CHAPITRE 3

MANIFESTATIONS MAJEURES*Article 13***Transmission de données à caractère non personnel**

Aux fins de la prévention des infractions pénales et du maintien de l'ordre et de la sécurité publiques lors de manifestations majeures à dimension transfrontalière, notamment dans le domaine sportif ou en rapport avec des réunions du Conseil européen, les États membres se transmettent les données à caractère non personnel nécessaires à cet effet, tant sur demande que de leur propre

initiative, et dans le respect du droit national de l'État membre qui transmet les données.

*Article 14***Transmission de données à caractère personnel**

1. Aux fins de la prévention des infractions pénales et du maintien de l'ordre et de la sécurité publiques lors de manifestations de grande envergure à dimension transfrontalière, notamment dans le domaine sportif ou en rapport avec des réunions du Conseil européen, les États membres se transmettent des données à caractère personnel, tant sur demande que de leur propre initiative, lorsque des condamnations définitives ou d'autres circonstances font présumer que les personnes concernées vont commettre des infractions pénales dans le cadre de ces manifestations ou qu'elles présentent un danger pour l'ordre et la sécurité publiques, pour autant que la transmission de ces données soit autorisée en vertu du droit national de l'État membre qui transmet les données.

2. Les données à caractère personnel ne peuvent être traitées qu'aux fins visées au paragraphe 1 et pour les manifestations précises en vue desquelles elles ont été communiquées. Les données transmises doivent être effacées immédiatement, dès lors que les objectifs visés au paragraphe 1 ont été atteints ou ne sont plus réalisables. En tout état de cause, les données transmises doivent être effacées après un an au plus tard.

*Article 15***Point de contact national**

Aux fins de la transmission des données prévue aux articles 13 et 14, chaque État membre désigne un point de contact national. Les compétences des points de contact nationaux sont régies par le droit national qui leur est applicable.

CHAPITRE 4

MESURES VISANT À PRÉVENIR LES INFRACTIONS TERRORISTES*Article 16***Transmission d'informations aux fins de prévention des infractions terroristes**

1. Aux fins de la prévention des infractions terroristes, les États membres peuvent, conformément au droit national, dans des cas particuliers, sans même en avoir reçu la demande, transmettre aux points de contact nationaux des autres États membres, visés au paragraphe 3, les données à caractère personnel et les informations visées au paragraphe 2, dans la mesure où cela est nécessaire au regard de circonstances particulières laissant présumer que les personnes concernées vont commettre les infractions visées aux articles 1^{er}, 2 et 3 de la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme (1).

(1) JO L 164 du 22.6.2002, p. 3.

III

(Actes pris en application du traité UE)

ACTES PRIS EN APPLICATION DU TITRE VI DU TRAITÉ UE

DÉCISION-CADRE 2009/905/JAI DU CONSEIL

du 30 novembre 2009

relative à l'accréditation des prestataires de services de police scientifique menant des activités de laboratoire

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 30, paragraphe 1, points a) et c), et son article 34, paragraphe 2, point b),

vu l'initiative du Royaume de Suède et du Royaume d'Espagne⁽¹⁾,

vu l'avis du Parlement européen,

considérant ce qui suit:

- (1) L'Union européenne s'est fixé pour objectif de maintenir et de développer un espace de liberté, de sécurité et de justice dans lequel un niveau élevé de sécurité doit être assuré par une action en commun des États membres dans le domaine de la coopération policière et judiciaire en matière pénale.
- (2) Cet objectif doit être réalisé par la prévention de la criminalité et la lutte contre ce phénomène, grâce à une coopération plus étroite entre les services répressifs des États membres, tout en respectant les principes et les règles relatifs aux droits de l'homme, aux libertés fondamentales et à l'état de droit, sur lesquels l'Union est fondée et qui sont communs à tous les États membres.
- (3) L'échange d'informations et de renseignements sur la criminalité et les activités criminelles est essentiel pour permettre aux services répressifs de prévenir et de déjouer la criminalité ou les activités criminelles, et d'enquêter sur celles-ci. L'action en commun dans le domaine de la coopération policière au titre de l'article 30, paragraphe 1, point a), du traité implique la nécessité d'un traitement des informations pertinentes dans le respect des dispositions appropriées en matière de protection des données à caractère personnel.

(4) L'échange accru d'informations concernant les preuves scientifiques et le recours accru, dans le cadre des procédures judiciaires d'un État membre, à des preuves émanant d'un autre État membre, mettent en évidence la nécessité d'établir des normes communes concernant les prestataires de services de police scientifique.

(5) À l'heure actuelle, les informations livrées par les procédures d'expertise dans un État membre peuvent donner lieu à certaines incertitudes dans un autre État membre quant à la manière dont les pièces ont été utilisées, aux méthodes employées et à l'interprétation des résultats.

(6) Au point 3.4, point h), du plan d'action du Conseil et de la Commission mettant en œuvre le programme de La Haye visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne⁽²⁾, les États membres ont souligné la nécessité de définir des normes de qualité applicables aux laboratoires médico-légaux en 2008 au plus tard.

(7) Il importe tout particulièrement d'instaurer des normes communes concernant les prestataires de services de police scientifique relatives aux données à caractère personnel sensibles telles que les profils ADN et les données dactyloscopiques.

(8) En vertu de l'article 7, paragraphe 4, de la décision 2008/616/JAI du Conseil du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière⁽³⁾, les États membres prennent les mesures nécessaires pour garantir l'intégrité des profils ADN mis à la disposition des autres États membres ou transmis pour comparaison, et pour faire en sorte que ces mesures soient conformes aux normes internationales, telles que la norme ISO/CEI 17025, intitulée «Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais» (ci-après dénommée «ISO/CEI 17025»).

(1) JO C 174 du 28.7.2009, p. 7.

(2) JO C 198 du 12.8.2005, p. 1.

(3) JO L 210 du 6.8.2008, p. 12.

- (9) Les profils ADN et les données dactyloscopiques ne sont pas utilisés uniquement dans le cadre de procédures pénales. Leur rôle est également déterminant pour l'identification des victimes, en particulier après des catastrophes.
- (10) L'accréditation des prestataires de services de police scientifique menant des activités de laboratoire représente une étape importante vers un échange plus sûr et plus efficace des informations de police scientifique au sein de l'Union.
- (11) L'accréditation est octroyée par l'organisme national d'accréditation qui dispose d'une compétence exclusive pour évaluer si un laboratoire satisfait aux exigences fixées par des normes harmonisées. La compétence d'un organisme d'accréditation lui est conférée par l'État. Le règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits (*) compte des dispositions précises concernant la compétence de ces organismes nationaux d'accréditation. L'article 7 dudit règlement, notamment, régit l'accréditation transfrontalière dans les cas où l'accréditation peut être demandée auprès d'un autre organisme national d'accréditation.
- (12) L'absence d'accord permettant d'appliquer une norme d'accréditation commune pour l'analyse des preuves scientifiques est une lacune à laquelle il faudrait remédier; il y a donc lieu d'adopter un instrument juridiquement contraignant concernant l'accréditation de tous les prestataires de services de police scientifique menant des activités de laboratoire. L'accréditation apporte les garanties indispensables que les activités des laboratoires sont menées dans le respect des normes internationales pertinentes, en particulier la norme ISO/CEI 17025 et des lignes directrices applicables en la matière.
- (13) La norme d'accréditation permet à tout État membre de demander, s'il le souhaite, l'application de normes complémentaires aux activités des laboratoires relevant de son ressort territorial.
- (14) L'accréditation contribuera à l'instauration d'une confiance mutuelle dans la validité des principales méthodes analytiques utilisées. Toutefois, elle ne mentionne pas la méthode qu'il convient d'utiliser, mais indique seulement que celle-ci doit être adaptée à l'objectif poursuivi.
- (15) Toute mesure prise en dehors d'un laboratoire sort du champ d'application de la présente décision-cadre. Par exemple, ni la prise des données dactyloscopiques, ni les mesures prises sur la scène de l'incident ou la scène de crime, ni les analyses de police scientifique effectuées en dehors des laboratoires ne relèvent de son champ d'application.
- (16) La présente décision-cadre n'a pas pour objet d'harmoniser les réglementations nationales relatives à l'appréciation judiciaire des preuves scientifiques.

- (17) La présente décision ne porte pas atteinte à la validité, établie conformément aux réglementations nationales applicables, des résultats des activités de laboratoire menées avant sa mise en œuvre, même si le fournisseur de services de police scientifique n'a pas été accrédité comme étant conforme aux exigences de la norme ISO/CEI 17025.

A ARRÊTÉ LA PRÉSENTE DÉCISION-CADRE:

Article premier

Objectif

1. La présente décision-cadre a pour objectif de garantir que les résultats d'activités de laboratoire menées dans un État membre par des fournisseurs de services de police scientifique accrédités soient reconnus par les autorités chargées de la prévention et du dépistage des infractions pénales ou des enquêtes en la matière comme étant aussi fiables que les résultats d'activités de laboratoire menées par des fournisseurs de services de police scientifique accrédités conformément à la norme ISO/CEI 17025 dans tout autre État membre.
2. À cette fin, les fournisseurs de services de police scientifique menant des activités de laboratoire sont accrédités par un organisme national d'accréditation certifiant leur conformité à la norme ISO/CEI 17025.

Article 2

Champ d'application

La présente décision-cadre s'applique aux activités de laboratoire ayant pour but d'établir:

- a) des profils ADN; et
- b) des données dactyloscopiques.

Article 3

Définitions

Aux fins de la présente décision-cadre, on entend par:

- a) «activité de laboratoire», toute mesure prise dans un laboratoire dans le cadre de la détection et de la recherche de traces sur des objets, de l'élaboration, de l'analyse et de l'interprétation de preuves scientifiques, dans le but d'obtenir des avis d'experts ou d'échanger des preuves scientifiques;
- b) «résultats des activités des laboratoires», tous les résultats analytiques et l'interprétation s'y rapportant directement;
- c) «prestataire de services de police scientifique», toute organisation, publique ou privée, qui mène des activités de laboratoire de police scientifique à la demande des autorités répressives ou judiciaires compétentes;

(*) JO L 218 du 13.8.2008, p. 30.

- d) «organisme national d'accréditation», l'organisme exclusivement chargé, dans un État membre, de l'accréditation, qui tire son autorité de cet État ainsi qu'il ressort du règlement (CE) n° 765/2008;
- e) «profil ADN», un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci);
- f) «données dactyloscopiques», les images d'empreintes digitales, images d'empreintes digitales latentes, d'empreintes de paumes de mains, d'empreintes de paumes de mains latentes, ainsi que des modèles de telles images (points caractéristiques codés).

Article 4

Accréditation

Les États membres veillent à ce que les fournisseurs de services de police scientifique menant des activités de laboratoire soient accrédités par un organisme national d'accréditation comme étant conformes à la norme ISO/CEI 17025.

Article 5

Reconnaissance des résultats

1. Chaque État membre fait en sorte que les résultats des fournisseurs de services de police scientifique menant des activités de laboratoire dans d'autres États membres soient reconnus par ses autorités chargées de la prévention et de la détection des infractions pénales et des enquêtes en la matière comme étant aussi fiables que les résultats des fournisseurs de services de police scientifique menant des activités de laboratoire accrédités conformément à la norme ISO/CEI 17025.
2. La présente décision-cadre est sans préjudice des règles nationales en matière d'appréciation judiciaire des preuves.

Article 6

Coûts

1. Chaque État membre supporte les coûts publics résultant de la présente décision-cadre conformément aux dispositions nationales.
2. La Commission examine les modalités d'une aide financière prélevée sur le budget général de l'Union européenne pour

les projets nationaux et transnationaux destinés à contribuer à la mise en œuvre de la présente décision-cadre, notamment pour l'échange d'expérience, la diffusion du savoir-faire et les essais d'aptitude.

Article 7

Mise en œuvre

1. Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre en ce qui concerne les profils ADN au plus tard le 30 novembre 2013.
2. Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre en ce qui concerne les données dactyloscopiques au plus tard le 30 novembre 2015.
3. Les États membres communiquent au secrétariat général du Conseil et à la Commission le texte des dispositions transposant dans leur droit national les obligations qui leur sont imposées par la présente décision-cadre au plus tard le 30 mai 2016.
4. Sur la base des informations visées au paragraphe 3 et d'autres informations fournies par les États membres sur demande, la Commission soumet au Conseil, avant le 1^{er} juillet 2018, un rapport sur la mise en œuvre et l'application de la présente décision-cadre.
5. Le Conseil examine, avant la fin de l'année 2018, dans quelle mesure les États membres se sont conformés à la présente décision-cadre.

Article 8

Entrée en vigueur

La présente décision-cadre entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 30 novembre 2009.

Par le Conseil

La présidente

B. ASK

Extrait du Code de la sécurité intérieure

Article L235-1

- Créé par Ordonnance n°2012-351 du 12 mars 2012 - Annexe, v. init.

Les données contenues dans les traitements automatisés de données à caractère personnel gérés par les services de police et de gendarmerie nationales peuvent être transmises, dans le cadre des engagements internationaux régulièrement introduits dans l'ordre juridique interne, à des organismes de coopération internationale en matière de police judiciaire ou à des services de police étrangers, qui représentent un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées

Les services de police et de gendarmerie nationales peuvent recevoir des données contenues dans les traitements gérés par les organismes de coopération internationale en matière de police judiciaire ou les services de police étrangers dans le cadre des engagements prévus au présent article.

T R A I T É
du 27 mai 2005**dit Traité de Prüm**

ENTRE LE ROYAUME DE BELGIQUE, LA RÉPUBLIQUE FÉDÉRALE D'ALLEMAGNE,
LE ROYAUME D'ESPAGNE, LA RÉPUBLIQUE FRANÇAISE, LE GRAND-DUCHÉ
DE LUXEMBOURG, LE ROYAUME DES PAYS-BAS ET LA RÉPUBLIQUE D'AUTRICHE
RELATIF À L'APPROFONDISSEMENT DE LA COOPÉRATION TRANSFRONTALIÈRE,
NOTAMMENT EN VUE DE LUTTER CONTRE LE TERRORISME, LA CRIMINALITÉ
TRANSFRONTALIÈRE ET LA MIGRATION ILLÉGALE
(ENSEMBLE DEUX ANNEXES ET UNE DÉCLARATION)

Chapitre 2 – Profils ADN, données dactyloscopiques et autres données**Article 2 – Création de fichiers nationaux d'analyse ADN**

(1) Les Parties contractantes s'engagent à créer et à gérer des fichiers nationaux d'analyse ADN en vue de la poursuite d'infractions pénales. Le traitement des données enregistrées dans ces fichiers en vertu du présent Traité s'effectuera, sous réserve des autres dispositions du présent Traité, conformément au droit national applicable au processus de traitement en question.

(2) En vue de la mise en oeuvre du présent Traité, les Parties contractantes garantissent que des données indexées se référant au contenu des fichiers nationaux d'analyse ADN visés au paragraphe 1^{er}, 1^{re} phrase, sont disponibles. Ces données indexées ne contiennent que les profils ADN (*) issus de la partie non codante de l'ADN ainsi qu'une référence. Les données indexées ne doivent contenir aucune donnée permettant l'identification directe de la personne concernée. Les données indexées qui ne peuvent être attribuées à aucune personne (traces ouvertes) doivent être reconnaissables en tant que telles.

(3) Lors du dépôt de l'instrument de ratification, d'acceptation, d'approbation ou d'adhésion, chaque Partie contractante désigne les fichiers nationaux d'analyse ADN auxquels les articles 2 à 6 s'appliquent, ainsi que les conditions régissant la consultation automatisée sur la base de l'article 3, paragraphe 1^{er}.

(*) Pour l'Allemagne, les profils ADN en vertu du présent Traité s'appellent Identifizierungsmuster (modèles d'identification ADN).

Article 3 – Consultation automatisée de profils ADN

(1) Les Parties contractantes autorisent les points de contact nationaux des autres Parties contractantes, visés à l'article 6, à accéder, en vue de poursuivre des infractions pénales, aux données indexées de leurs fichiers d'analyse ADN, et ce avec le droit de procéder à une consultation automatisée à l'aide d'une comparaison des profils ADN. La consultation ne peut s'opérer qu'au cas par cas et dans le respect du droit national de la Partie contractante qui effectue ladite consultation.

(2) Si, dans le cadre d'une consultation automatisée, une concordance entre un profil ADN transmis et un profil ADN enregistré dans le fichier de la Partie contractante destinataire est constatée, le point de contact national ayant lancé la consultation est informé par voie automatisée de l'existence d'une concordance et de la référence. Si aucune concordance ne peut être constatée, communication en est faite de manière automatisée.

Article 4 – Comparaison automatisée de profils ADN

(1) Les Parties contractantes comparent, par l'intermédiaire de leurs points de contact nationaux et d'un commun accord, les profils ADN de leurs traces ouvertes avec tous les profils ADN provenant des données indexées des autres fichiers nationaux d'analyse ADN en vue de poursuivre des infractions pénales. La transmission et la comparaison s'opèrent de manière automatisée. La transmission visant à comparer des profils ADN des traces ouvertes ne s'opère que dans les cas où une telle transmission est prévue par le droit national de la Partie contractante requérante.

(2) Si, lors de la comparaison prévue au paragraphe 1^{er}, une Partie contractante constate que des profils ADN transmis correspondent à ceux contenus dans son propre fichier d'analyse ADN, elle communique sans délai au point de contact national de l'autre Partie contractante les données indexées pour lesquelles une concordance a été constatée.

Article 5 – Transmission d'autres données à caractère personnel et d'autres informations

En cas de constatation de concordance de profils ADN dans le cadre de la procédure prévue aux articles 3 et 4, la transmission d'autres données à caractère personnel se rapportant aux données indexées ainsi que d'autres informations s'opère en vertu du droit national de la Partie contractante requise, y compris les dispositions relatives à l'entraide judiciaire.

Article 6 – Point de contact national et accord d'exécution

(1) Chaque Partie contractante désigne un point de contact national pour la transmission de données en vertu des articles 3 et 4. Les compétences du point de contact national sont régies par le droit national qui lui est applicable.

(2) Un accord d'exécution au sens de l'article 44 règle les détails techniques des procédures décrites aux articles 3 et 4.

Article 7 – Prélèvement de matériel génétique et transmission de profils ADN

Si, dans le cadre d'une procédure d'enquête ou d'une procédure judiciaire en cours, le profil ADN d'une personne déterminée qui se trouve sur le territoire de la Partie contractante requise fait défaut, cette dernière accorde l'entraide judiciaire en prélevant et en analysant le matériel génétique de cette personne ainsi qu'en transmettant le profil ADN obtenu, lorsque :

1. La Partie contractante requérante communique le but pour lequel cette procédure est nécessaire ;
2. La Partie contractante requérante présente une ordonnance ou un acte d'enquête, émis par l'autorité compétente, requis en vertu de son droit national, faisant ressortir que les conditions pour le prélèvement et l'analyse du matériel génétique seraient réunies dans l'hypothèse où la personne en question se trouverait sur le territoire de la Partie contractante requérante, et
3. Les conditions préalables au prélèvement et à l'analyse du matériel génétique ainsi qu'à la transmission du profil ADN obtenu sont réunies en vertu du droit de la Partie contractante requise.

Article 8 – Données dactyloscopiques

En vue de la mise en oeuvre du présent Traité, les Parties contractantes garantissent que des données indexées soient disponibles concernant le contenu des systèmes automatisés nationaux d'identification dactyloscopique créés en vue de la prévention et de la poursuite d'infractions pénales. Ces données indexées ne contiennent que des données dactyloscopiques et une référence. Les données indexées ne doivent contenir aucune donnée permettant l'identification directe de la personne concernée. Les données indexées qui ne peuvent être attribuées à aucune personne (traces ouvertes) doivent être reconnaissables en tant que telles.

Article 9 – Consultation automatisée de données dactyloscopiques

(1) Les Parties contractantes autorisent le point de contact national des autres Parties contractantes, visé à l'article 11, à accéder, en vue de prévenir et de poursuivre des infractions pénales, aux données indexées de leurs systèmes automatisés d'identification dactyloscopique créés à cette fin, et ce avec le droit de procéder à une consultation automatisée à l'aide d'une comparaison des données dactyloscopiques. La consultation ne peut s'opérer qu'au cas par cas et dans le respect du droit national de la Partie contractante qui effectue ladite consultation.

(2) L'établissement définitif d'un lien entre une donnée dactyloscopique et une donnée indexée de la Partie contractante gestionnaire du fichier est réalisé par le point de contact national de la Partie ayant réalisé la consultation sur la base des données indexées transmises en mode automatisé et nécessaires à une attribution univoque.

Article 10 – Transmission d'autres données à caractère personnel ainsi que d'autres informations

En cas de constatation de concordance de données indexées dans le cadre de la procédure prévue à l'article 9, la transmission d'autres données à caractère personnel se rapportant aux données indexées ainsi que d'autres informations s'opère en vertu du droit national de la Partie contractante requise, y compris les dispositions relatives à l'entraide judiciaire.

Article 11 – Point de contact national et accord d'exécution

(1) Chaque Partie contractante désigne un point de contact national pour la transmission de données en vertu de l'article 9. Les compétences du point de contact national sont régies par le droit national qui lui est applicable.

(2) Un accord d'exécution au sens de l'article 44 règle les détails techniques de la procédure décrite à l'article 9.

10 février 2011

Le fichier des empreintes digitales ouvert aux policiers étrangers

Le fichier automatisé des empreintes digitales (FAED) du ministère de l'intérieur sera désormais accessible aux douaniers, mais également par des « *agents d'organismes de coopération internationale en matière de police judiciaire ou par des agents des services de police ou de justice d'Etats étrangers* ».

La CNIL s'inquiète des modalités de cette extension : le décret prévoit en effet que le gouvernement ne sera plus tenu de lui demander son avis lorsqu'il voudra élargir à d'autres organismes ou pays l'accès à ce fichier.

Le décret, paru au Journal Officiel ce jeudi 9 février, précise que seuls des « *agents spécialement habilités* » pourront accéder au fichier, sur demande préalable motivée, et que le gestionnaire du traitement mettra en place « *un dispositif permettant de retracer, par enregistrement informatique, la consultation du fichier* ».

Cet élargissement des modalités de consultation du fichier des empreintes digitales s'inscrit dans le cadre du Traité de Prüm (également appelé « *Schengen III* » ou « *Schengen plus* »), signé en 2005 par la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche) et qui, au nom de la lutte contre le terrorisme, l'immigration illégale et la criminalité, « *prévoit l'échange de données génétiques, d'empreintes digitales et de données à caractère personnel, la constitution de patrouilles policières communes ainsi que d'autres formes d'intervention (gardes armés à bord des aéronefs, assistance lors d'événements de grande envergure, etc.)* ».

L'avis de la CNIL regrette cela dit que, profitant de l'occasion, le gouvernement prévoit d'écarter la CNIL des futures extensions du domaine de ce fichier : Si la commission prend donc acte de ces nouveaux destinataires des données enregistrées dans le FAED, elle relève que le projet de décret revêt un caractère plus général en permettant la consultation du traitement par les agents des services de police ou de justice d'Etats étrangers dans les conditions prévues « *par tout acte pris en application du titre V du traité sur le fonctionnement de l'Union européenne et poursuivant des buts analogues, en tout ou partie, à ceux du traité mentionné au 1° [traité de Prüm]* » ainsi que « *par tout engagement liant la France à des organismes internationaux ou à des Etats étrangers, aux fins et dans les conditions définies à l'article 24 de la loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure* ».

Le gardien de la vie privée « *relève en outre que la rédaction projetée par le ministère de l'intérieur aurait pour conséquence de ne plus avoir à modifier le texte réglementaire relatif au FAED en cas d'adoption de nouveaux actes européens, ou de signature de nouveaux accords bilatéraux ou multilatéraux, permettant l'échange de données dactyloscopiques, sauf si les Etats étrangers n'assurent pas un niveau de protection des données suffisant* » : Dès lors, la commission sera simplement tenue informée de tout changement affectant les destinataires du traitement et les

transferts de données à caractère personnel envisagés.

Dans la mesure où elle n'a connaissance ni du contenu de ces accords ni des pays concernés, et eu égard à la sensibilité des informations susceptibles d'être transmises et aux garanties spécifiques qui doivent être prises pour assurer la protection des données biométriques, et des empreintes digitales en particulier, la commission émet donc de sérieuses réserves quant à la possibilité qui pourrait ainsi être donnée d'élargir la liste des destinataires du FAED en conséquence de l'entrée en vigueur de nouveaux engagements internationaux.

Le précédent du fichier génétique

Ce n'est pas la première fois que la CNIL alerte le gouvernement, en vain, sur les risques de dérives ou de « *function creep* » (détournement d'usage, en français), du nom donné à ces processus qui sont détournés de leurs finalités premières, entraînant des dommages collatéraux qui n'avaient pas suffisamment été anticipés (voir Safari et la (nouvelle) chasse aux Français) : Elle relève qu'elle a déjà formulé ces demandes, notamment dans le cadre du décret relatif à l'accès d'Etats étrangers au FNAEG, et qu'elle n'a pas été suivie par le Gouvernement.

Cependant, dans la mesure où la rédaction projetée du décret relatif au FAED aurait pour conséquence de priver la commission de l'exercice de certains de ses pouvoirs de contrôle a priori sur la mise en œuvre de nouveaux transferts de données, qui ne seraient pas soumis à l'avis de la CNIL, elle estime qu'il convient que le ministère de l'intérieur prenne les mesures nécessaires afin de garantir que ces nouveaux transferts respectent pleinement les droits des personnes à l'égard des traitements automatisés de données à caractère personnel.

En résumé : ce n'est plus tant la CNIL qui veillera à la protection des données personnelles des fichiers d'empreintes génétiques et digitales, mais le ministère de l'Intérieur... Une nouvelle attaque en règle contre la CNIL, qui, successivement, a récemment tenté de décapiter la CNIL pour interdire à un homme politique d'influence de pouvoir la présider, avant de l'attaquer au portefeuille (voir La CNIL dans le collimateur de la Cour des comptes).

Initialement créé pour prévenir la récidive des criminels sexuels, le FNAEG a depuis été étendu à la quasi-totalité des crimes et délits (137, pour être précis, et à l'exception notables des crimes financiers) : Au 31 décembre 2009, onze ans après sa création, le FNAEG compte 1 276 769 profils génétiques, soit près de 2% de la population française. 280 399 personnes y figurent en tant que personnes condamnées (leur empreinte sera conservée quarante ans), et 934 112 en tant que « mises en cause dans des affaires judiciaires » (la conservation est alors de vingt-cinq ans), ce à quoi il convient de rajouter 62 258 « traces non identifiées ».

Près de 75% des gens dont l'ADN est fiché, en France, sont donc toujours « *présumés innocents* » de ce pour quoi ils ont un jour été suspectés, mis en cause, et fichés (voir Objectif: fichier l'ADN de toute la population).

Créé en 1987, le FAED répertoriait, lui, les empreintes digitales de 3 451 622 individus au 31 janvier 2010. Aucune donnée ne permet de savoir, par contre, combien sont de simples suspects, et combien ont été condamnés. Les empreintes sont conservées 25 ans durant. 300 fonctionnaires français environ y ont accès à ce jour. Ce à quoi il conviendra donc de rajouter un certain nombre de leurs homologues étrangers.

La division des relations internationales

13 décembre 2011

La direction centrale de la police judiciaire a fêté en 2007 son centenaire. En charge de la lutte contre le crime organisé et le grand banditisme, elle a toujours su s'adapter aux nouvelles formes de criminalité qui ont opportunément profité de l'explosion des nouveaux moyens de transport et de communication. L'internationalisation du crime était née.

Les outils internationaux de coopération policière, créés entre 1923 (Interpol) et la fin des années quatre-vingt dix (*convention de l'accord de Schengen et le SIS, convention Europol puis traité de Lisbonne transformant l'organisation en agence européenne*) sont une première réponse à la menace que fait peser de plus en plus le crime international sur la sécurité de nos démocraties.

La direction centrale de la police judiciaire s'est donc dotée, parallèlement avec la mise en place d'offices centraux, d'une division des relations internationales (DRI) dont l'une des missions fondamentales est de coordonner la coopération policière opérationnelle, jusque-là éclatée entre différentes entités. Le BCN France a été créé en 1928, suivi du bureau Sirène France en 1995 et de l'unité nationale Europol (UNE) en 1996 (*expressément mentionnées par l'art. D8-2 du CPP*).

La division des relations internationales, rattachée directement au cabinet du directeur central de la police judiciaire depuis 2004, se positionne donc aujourd'hui comme l'élément moteur en charge de la coopération policière internationale à caractère opérationnel. Dans un contexte aujourd'hui interministériel (*Police nationale, Gendarmerie nationale, Douane et Justice*), la DRI est au service de l'ensemble des services de sécurité français lorsqu'ils sont amenés à utiliser les canaux institutionnels (*demandes de coopération, exécution d'un mandat d'arrêt européen, observation transfrontalière...*).

La proximité avec l'autorité judiciaire du fait du détachement d'une mission justice, émanation du bureau d'entraide pénal international (BEPI) de la Chancellerie, est également un gage d'efficacité dans le traitement de certaines requêtes nécessitant l'aval d'un magistrat (*demandes d'extradition, MAE, ...*).

La DRI est placée sous l'autorité d'un commissaire divisionnaire, assisté d'un adjoint. Elle s'articule autour :

- d'une section de coopération opérationnelle de police (SCCOPOL) en charge de l'échange d'informations H24 7/7 ayant à sa tête un commissaire de police et un officier supérieur de la gendarmerie nationale ;
- d'un service en charge des actions de coopération européenne et internationale (SCACEI) chargé plus particulièrement du cadre institutionnel lié au fonctionnement des trois canaux que sont INTERPOL, EUROPOL et SCHENGEN ;
- d'une section de gestion administrative, comprenant notamment une cellule informatique et un pool de traduction vient compléter le dispositif.

La mission de la DRI est plus globalement de faciliter l'utilisation, par les services répressifs, de tous les outils de coopération disponibles. C'est le cas notamment de la Décision PRÛM sur l'ADN, les empreintes dactyloscopiques et les fichiers nationaux d'immatriculation des véhicules (EUCARIS).

Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur

NOR: INTD8700094D
Version consolidée au 15 août 2013

Le Premier ministre,

Sur le rapport du garde des sceaux, ministre de la justice, du ministre de la défense, du ministre de l'intérieur et du ministre délégué auprès du ministre de l'intérieur, chargé de la sécurité,

Vu le code de procédure pénale ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 78-774 du 17 juillet 1978 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 ;

Vu le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'Etat, la défense et la sécurité publiques de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'avis de la Commission nationale de l'informatique et des libertés ;

Après avis du Conseil d'Etat (section de l'intérieur),

Article 1

- Modifié par Décret n°2011-157 du 7 février 2011 - art. 1

Est autorisé, dans les conditions prévues au présent décret, le traitement automatisé de traces et empreintes digitales et palmaires en vue de faciliter la recherche et l'identification, par les services de la police nationale et de la gendarmerie nationale, ainsi que par le service national de la douane judiciaire, des auteurs de crimes et de délits et de faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie.

Article 2

Ce traitement est mis en oeuvre par la direction centrale de la police judiciaire au ministère de l'intérieur. Il porte la dénomination de fichier automatisé des empreintes digitales.

Article 3

- Modifié par Décret n°2005-585 du 27 mai 2005 - art. 3 JORF 29 mai 2005

Peuvent être enregistrées :

1° Les traces relevées dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire, d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte prévue par les articles 74-1 ou 80-4 du code de procédure pénale ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire ;

2° Les empreintes digitales et palmaires relevées dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire, lorsqu'elles concernent des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteur ou comme complice, à la commission d'un crime ou d'un délit ou des personnes, mises en cause dans une procédure pénale, dont l'identification certaine s'avère nécessaire ;

3° Les empreintes digitales et palmaires relevées dans les établissements pénitentiaires, en application du code de procédure pénale, en vue de s'assurer de manière certaine de l'identité des détenus qui font l'objet d'une procédure pour crime ou délit et d'établir les cas de récidive ;

4° Les traces et les empreintes digitales et palmaires transmises par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers en application d'engagements internationaux.

Article 9-1 (transféré)

- Créé par Décret n°2005-585 du 27 mai 2005 - art. 10 JORF 29 mai 2005
 - Transféré par Décret n°2011-157 du 7 février 2011 - art. 3

Article 9-1

- Modifié par Décret n°2011-157 du 7 février 2011 - art. 4

Par dérogation aux articles 8 et 9, les données enregistrées dans le fichier automatisé des empreintes digitales peuvent être consultées, en vue notamment de faire l'objet de rapprochements, par les agents d'organismes de coopération internationale en matière de police judiciaire ou par les agents des services de police ou de justice d'Etats étrangers, aux fins et dans les conditions prévues :

1° Par le traité relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé à Prüm le 27 mai 2005 ;

2° Par tout acte pris en application du titre V du traité sur le fonctionnement de l'Union européenne et poursuivant des buts analogues, en tout ou partie, à ceux du traité mentionné au 1° ;

3° Par tout engagement liant, aux fins et dans les conditions définies à l'article **24 de la loi n° 2003-239 du 18 mars 2003** sur la sécurité intérieure, la France à des organismes internationaux ou à des Etats étrangers, lorsque ces organismes et ces Etats assurent à la vie privée, aux libertés et aux droits fondamentaux des personnes à l'égard de données à caractère personnel un niveau de protection suffisant au sens de **l'article 68 de la loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés.