

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 Slovaquie, 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'excède 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

- 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.
- 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

- 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.
- 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 publics 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 publics 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 publics, 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.

2. Les données à transmettre comportent les noms, prénoms, date et lieu de naissance ainsi qu'une description des circonstances qui sont à l'origine de la présomption visée au paragraphe 1.

3. Chaque État membre désigne un point de contact national chargé de l'échange de données avec les points de contact nationaux des autres États membres. Les compétences des points de contact nationaux sont régies par le droit national qui leur est applicable.

4. L'État membre qui transmet les données peut, conformément au droit national, fixer des conditions d'utilisation de ces données et informations par l'État membre qui les reçoit. Ce dernier est tenu de respecter lesdites conditions.

CHAPITRE 5

AUTRES FORMES DE COOPÉRATION

Article 17

Opérations conjointes

1. Afin d'intensifier la coopération policière, les autorités compétentes désignées par les États membres peuvent, dans le cadre du maintien de l'ordre et de la sécurité publics ainsi que de la prévention des infractions pénales, mettre en place des patrouilles communes et prévoir d'autres formes d'opérations communes, dans le cadre desquelles des fonctionnaires ou d'autres agents de l'autorité publique, désignés par les États membres («fonctionnaires»), participent aux opérations sur le territoire d'un autre État membre.

2. En tant qu'État membre d'accueil, chaque État membre peut, conformément à son droit national et avec l'accord de l'État membre d'origine, confier des compétences de puissance publique à des fonctionnaires d'autres États membres participant à des opérations communes, ou admettre, pour autant que le droit de l'État membre d'accueil le permette, que des fonctionnaires d'autres États membres exercent leurs compétences de puissance publique conformément au droit de l'État membre d'origine. Ces compétences de puissance publique ne peuvent être exercées que sous l'autorité et, en règle générale, en présence de fonctionnaires de l'État membre d'accueil. Les fonctionnaires des autres États membres sont soumis au droit national de l'État membre d'accueil. L'État membre d'accueil assume la responsabilité de leurs actes.

3. Les fonctionnaires participant à des opérations communes sont soumis aux instructions de l'autorité compétente de l'État membre d'accueil.

4. Les États membres communiquent les déclarations visées à l'article 36 en y exposant les aspects pratiques de la coopération.

Article 18

Assistance en liaison avec des manifestations de masse, des catastrophes et des accidents graves

Les autorités compétentes des États membres se portent mutuellement assistance, dans le respect de leur droit national,

en liaison avec des manifestations de masse et d'autres événements similaires de grande envergure, ainsi que des catastrophes et des accidents graves, dans le but de prévenir des infractions pénales et de maintenir l'ordre et la sécurité publics en:

- a) se notifiant, dès que possible, les événements de ce type ayant des implications transfrontalières et en échangeant toute information pertinente à cet égard;
- b) prenant et en coordonnant sur leur territoire les mesures policières qui s'imposent lors d'événements ayant des implications transfrontalières;
- c) mettant, autant que possible, fonctionnaires, spécialistes, conseillers et équipements à la disposition de l'État membre qui en fait la demande et sur le territoire duquel l'événement est survenu.

Article 19

Utilisation des armes, munitions et équipements

1. Les fonctionnaires d'un État membre qui participent à une opération commune sur le territoire d'un autre État membre en vertu de l'article 17 ou 18 peuvent y porter leur uniforme de service national. Ils peuvent porter les armes, munitions et équipements qui leur sont permis au titre du droit national de l'État membre d'origine. L'État membre d'accueil peut interdire le port de certaines armes, de certaines munitions et de certains équipements par les fonctionnaires d'un État membre d'origine.

2. Les États membres communiquent les déclarations visées à l'article 36, dans lesquelles ils énumèrent les armes, munitions et équipements qui ne peuvent être utilisés qu'en cas de légitime défense de soi-même ou d'autrui. Le fonctionnaire de l'État membre d'accueil, qui dirige effectivement l'opération, peut autoriser, cas par cas et dans le respect du droit national, l'utilisation d'armes, de munitions et d'équipements à des fins plus larges que celles indiquées ci-dessus. L'utilisation des armes, munitions et équipements est régie par le droit de l'État membre d'accueil. Les autorités compétentes se tiennent informées des armes, munitions et équipements autorisés ainsi que des conditions de leur utilisation.

3. Si les fonctionnaires d'un État membre ont recours à des véhicules pour une intervention menée, au titre de la présente décision, sur le territoire d'un autre État membre, ils sont soumis aux mêmes règles de circulation routière que les fonctionnaires de l'État membre d'accueil, y compris en ce qui concerne les règles de priorité et les éventuelles prérogatives de puissance publique.

4. Les États membres communiquent les déclarations visées à l'article 36, dans lesquelles ils exposent les aspects pratiques de l'utilisation des armes, munitions et équipements.

*Article 20***Protection et assistance**

Les États membres sont tenus d'accorder aux fonctionnaires d'autres États membres qui franchissent leurs frontières la même protection et assistance dans l'exercice de leurs fonctions qu'à leurs propres fonctionnaires.

*Article 21***Règles générales en matière de responsabilité civile**

1. Lorsque les fonctionnaires d'un État membre se trouvent en mission sur le territoire d'un autre État membre en vertu de l'article 17, leur État membre est responsable des dommages qu'ils causent pendant le déroulement de la mission, conformément au droit de l'État membre sur le territoire duquel ils opèrent.

2. L'État membre sur le territoire duquel les dommages visés au paragraphe 1 sont causés assume la réparation de ces dommages dans les conditions applicables aux dommages causés par ses propres agents.

3. Dans le cas visé au paragraphe 1, l'État membre dont les fonctionnaires ont causé des dommages à quiconque sur le territoire d'un autre État membre rembourse intégralement à ce dernier les sommes qu'il a versées aux victimes ou à leurs ayants droit.

4. Lorsque des fonctionnaires d'un État membre se trouvent en mission sur le territoire d'un autre État membre en vertu de l'article 18, cet État membre est responsable, conformément à son droit national, des dommages qu'ils causent pendant le déroulement de la mission.

5. Lorsque les dommages visés au paragraphe 4 résultent d'une négligence grave ou d'une faute intentionnelle, l'État membre d'accueil peut s'adresser à l'État membre d'origine afin que celui-ci rembourse les sommes qu'il a versées aux victimes ou à leurs ayants droit.

6. Sans préjudice de l'exercice de ses droits à l'égard des tiers et à l'exception du paragraphe 3, chaque État membre renonce, dans le cas prévu au paragraphe 1, à demander à un autre État membre le remboursement du montant des dommages qu'il a subis.

*Article 22***Responsabilité pénale**

Les fonctionnaires d'un État membre opérant sur le territoire d'un autre État membre au titre de la présente décision sont assimilés aux fonctionnaires de l'État membre d'intervention en ce qui concerne les infractions pénales qu'ils commettraient ou dont ils seraient victimes, sauf disposition contraire figurant dans un autre accord liant les États membres concernés.

*Article 23***Relation de travail**

Les fonctionnaires d'un État membre opérant sur le territoire d'un autre État membre au titre de la présente décision restent soumis aux dispositions du droit du travail qui s'appliquent dans leur État membre, notamment en matière disciplinaire.

CHAPITRE 6

DISPOSITIONS GÉNÉRALES RELATIVES À LA PROTECTION DES DONNÉES*Article 24***Définitions et champ d'application**

1. Aux fins de la présente décision, on entend par:
 - a) «traitement de données à caractère personnel»: toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, la lecture, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion ainsi que le verrouillage, l'effacement ou la destruction de données. Aux fins de la présente décision, le terme «traitement» englobe également la notification de l'existence ou de l'absence d'une concordance;
 - b) «consultation automatisée»: l'accès direct à une banque de données automatisée d'une autre autorité avec réponse entièrement automatisée à la demande de la consultation;
 - c) «marquage»: l'apposition d'une marque sur des données à caractère personnel enregistrées sans chercher à limiter leur traitement futur;
 - d) «verrouillage»: le marquage de données à caractère personnel enregistrées en vue de limiter leur traitement futur.
2. Les dispositions qui suivent sont applicables aux données qui sont ou qui ont été transmises en vertu de la présente décision, pour autant que les chapitres précédents n'en disposent pas autrement.

*Article 25***Niveau de protection des données**

1. En ce qui concerne le traitement de données à caractère personnel qui sont ou qui ont été transmises en vertu de la présente décision, chaque État membre garantit dans son droit national un niveau de protection des données correspondant au moins à celui qui est prévu 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, ainsi que par son protocole additionnel du 8 novembre 2001, et tient à cet égard compte de la recommandation n° R (87) 15 du 17 septembre 1987 du comité des ministres du Conseil de l'Europe aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, et ce également lorsque les données ne sont pas traitées en mode automatisé.

2. La transmission de données à caractère personnel prévue par la présente décision ne peut avoir lieu qu'après la mise en œuvre du présent chapitre dans le droit national sur le territoire des États membres concernés par cette transmission. Le Conseil décide à l'unanimité si cette condition a été remplie.

3. Le paragraphe 2 ne s'applique pas aux États membres dans lesquels la transmission de données à caractère personnel prévue par la présente décision a déjà commencé conformément au traité du 27 mai 2005 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»).

Article 26

Finalités de l'utilisation

1. L'État membre destinataire ne peut traiter les données à caractère personnel qu'aux fins pour lesquelles les données lui ont été transmises en vertu de la présente décision. Le traitement à d'autres fins n'est admissible qu'avec l'autorisation préalable de l'État membre gestionnaire des données et dans le respect du droit national de l'État membre destinataire. L'autorisation peut être délivrée pour autant que le droit national de l'État membre gestionnaire des données permette ce traitement à ces autres fins.
2. L'État membre effectuant la consultation ou la comparaison des données ne peut procéder à un traitement des données transmises en vertu des articles 3, 4 et 9 que pour:
 - a) déterminer la concordance entre les profils ADN ou les données dactyloscopiques comparés;
 - b) préparer et introduire une demande d'entraide administrative ou judiciaire conformément au droit national, en cas de concordance de ces données;
 - c) effectuer une journalisation conformément à l'article 30.

L'État membre gestionnaire du fichier ne peut traiter les données qui lui ont été transmises conformément aux articles 3, 4 et 9 que si ce traitement est nécessaire pour réaliser une comparaison, donner une réponse automatisée à la demande ou effectuer la journalisation en vertu de l'article 30. Les données transmises sont effacées immédiatement après la comparaison ou la réponse automatisée, à moins que la poursuite du traitement aux fins visées au premier alinéa, points b) et c), ne soit nécessaire.

3. L'État membre gestionnaire du fichier ne peut utiliser les données transmises conformément à l'article 12 que si cette utilisation est nécessaire pour répondre par la voie automatisée à la demande ou pour effectuer la journalisation prévue à l'article 30. Les données transmises sont effacées immédiatement après l'obtention de la réponse automatisée, à moins que la poursuite du traitement en vue de la journalisation prévue à l'article 30 ne soit nécessaire. L'État membre effectuant la consultation ne peut utiliser les données obtenues dans le cadre de la réponse qu'aux fins de la procédure pour laquelle la consultation a eu lieu.

Article 27

Autorités compétentes

Les données à caractère personnel transmises ne peuvent être traitées que par les autorités, organes et tribunaux chargés d'une tâche servant à réaliser l'une des finalités visées à l'article 26. En particulier, des données ne peuvent être transmises à d'autres autorités qu'avec l'autorisation préalable de l'État membre ayant transmis les données et dans le respect du droit national de l'État membre destinataire.

Article 28

Exactitude, actualité et durée de conservation des données

1. Les États membres assurent l'exactitude et l'actualité des données à caractère personnel. S'il ressort ex officio ou d'une communication de la personne concernée que des données inexactes ou qui n'auraient pas dû être transmises ont été fournies, les États membres destinataires en sont informés sans délai. Les États membres concernés sont tenus de rectifier ou de supprimer les données. En outre, les données à caractère personnel transmises sont corrigées si elles se révèlent inexactes. Si l'autorité destinataire a des raisons de penser que des données transmises sont inexactes ou devraient être effacées, elle en informe sans délai l'autorité qui les a transmises.
2. Les données dont l'exactitude est contestée par la personne concernée et dont l'exactitude ou la non-exactitude ne peut être déterminée doivent, conformément au droit national des États membres, être marquées à la demande de la personne concernée. Un marquage peut être levé conformément au droit national et uniquement avec le consentement de la personne concernée ou sur décision du tribunal compétent ou de l'autorité indépendante compétente en matière de protection des données.
3. Les données à caractère personnel transmises sont effacées lorsqu'elles n'auraient pas dû être transmises ou reçues. Les données légalement transmises et reçues sont effacées:
 - a) si elles ne sont pas ou plus nécessaires au regard des finalités pour lesquelles elles ont été transmises. Si des données à caractère personnel ont été transmises sans qu'il y ait eu de demande, l'autorité destinataire examine immédiatement si elles sont nécessaires au regard des finalités pour lesquelles elles ont été transmises;
 - b) à l'expiration de la période maximale de conservation des données prévue par le droit national de l'État membre ayant transmis les données, lorsque l'autorité ayant transmis les données a informé l'autorité destinataire de cette période maximale au moment de la transmission.

Lorsqu'il y a des raisons de penser qu'un effacement porterait atteinte aux intérêts de la personne concernée, les données sont verrouillées au lieu d'être effacées, conformément au droit national. Des données verrouillées ne peuvent être utilisées ou transmises qu'aux fins qui ont empêché leur effacement.

Article 29

Mesures techniques et organisationnelles visant à garantir la protection et la sécurité des données

1. L'autorité destinataire et l'autorité qui transmet les données veillent à assurer une protection efficace des données à caractère personnel contre toute destruction fortuite ou non autorisée, perte fortuite, accès non autorisé, altération fortuite ou non autorisée et divulgation non autorisée.
2. Les mesures d'exécution visées à l'article 33 règlent les modalités techniques de la procédure de consultation automatisée et garantissent que:
 - a) des mesures répondant aux techniques les plus récentes sont prises pour assurer la protection et la sécurité des données, et notamment leur confidentialité et leur intégrité;
 - b) lors de l'utilisation de réseaux généralement accessibles, il est fait usage de procédures d'encryptage et d'authentification reconnues par les autorités compétentes à cet égard, et
 - c) l'admissibilité des consultations effectuées conformément à l'article 30, paragraphes 2, 4 et 5, peut être vérifiée.

Article 30

Documentation et journalisation; dispositions particulières relatives à la transmission automatisée et non automatisée

1. Chaque État membre garantit que toute transmission et toute réception non automatisée de données à caractère personnel sont documentées par l'autorité gestionnaire du fichier et par l'autorité effectuant la consultation, afin de vérifier l'admissibilité de la transmission. La documentation comprend les indications suivantes:
 - a) le motif de la transmission;
 - b) les données transmises;
 - c) la date de la transmission, et
 - d) la dénomination ou le code de référence de l'autorité effectuant la consultation et de l'autorité gestionnaire du fichier.
2. Les dispositions suivantes s'appliquent à la consultation automatisée de données effectuée sur la base des articles 3, 9 et 12 et à la comparaison automatisée effectuée en vertu de l'article 4:
 - a) seuls les fonctionnaires des points de contact nationaux particulièrement habilités à cet effet peuvent procéder à la consultation ou à la comparaison automatisées. Sur demande, la liste des fonctionnaires habilités à effectuer des consultations ou des comparaisons automatisées est mise à la disposition des autorités de surveillance visées au paragraphe 5, ainsi que des autres États membres;
 - b) chaque État membre veille à ce que l'autorité gestionnaire du fichier et l'autorité effectuant la consultation notent

toute transmission et toute réception de données dans un registre de journalisation, en précisant si une concordance a été obtenue ou non. La journalisation comprend les informations suivantes:

- i) les données transmises,
- ii) la date et l'heure précises de la transmission, et
- iii) la dénomination ou le code de référence de l'autorité effectuant la consultation et de l'autorité gestionnaire du fichier.

L'autorité qui effectue la consultation journalise également le motif de la consultation ou de la transmission ainsi que la référence de l'agent qui a réalisé la consultation et celle de l'agent qui a ordonné la consultation ou la transmission.

3. Sur demande des autorités compétentes en matière de protection des données de l'État membre concerné, l'autorité réalisant la journalisation leur transmet sans délai les données journalisées, au plus tard dans les quatre semaines qui suivent la réception de la demande. Les données journalisées ne peuvent être utilisées qu'aux fins suivantes:

- a) contrôler la protection des données;
- b) assurer la sécurité des données.

4. Les données journalisées sont protégées par des dispositions appropriées contre toute utilisation inadéquate et toute autre forme d'abus et sont conservées pendant deux ans. Au terme de la période de conservation, les données journalisées sont immédiatement effacées.

5. Le contrôle légal de la transmission ou de la réception de données à caractère personnel incombe aux autorités indépendantes compétentes en matière de protection des données ou, le cas échéant, aux autorités judiciaires respectives des États membres. Dans le respect du droit national, toute personne peut demander à ces autorités de contrôler la licéité du traitement de données la concernant. Indépendamment de telles demandes, ces autorités ainsi que les autorités chargées de la journalisation effectuent des contrôles aléatoires pour contrôler la licéité des transmissions, à l'aide des dossiers pour lesquels les consultations ont eu lieu.

Les résultats de ces contrôles sont conservés pendant dix-mois en vue d'une inspection des autorités indépendantes compétentes en matière de protection des données. À l'expiration de cette période, ils sont immédiatement effacés. Chaque autorité compétente en matière de protection des données peut être invitée par l'autorité indépendante chargée de la protection des données d'un autre État membre à exercer ses compétences conformément au droit national. Les autorités indépendantes compétentes en matière de protection des données des États membres font preuve de la coopération nécessaire pour effectuer leurs inspections, notamment en échangeant les informations pertinentes.

Article 31

Droits des personnes concernées d'être informées et indemnisées

1. Sur demande de la personne concernée en vertu du droit national et sans que cela entraîne de dépenses excessives, la personne concernée est, une fois son identité prouvée, informée, dans le respect du droit national, en des termes compréhensibles et sans retard déraisonnable, sur les données traitées la concernant et sur leur origine, sur les destinataires ou catégories de destinataires, sur la finalité du traitement ainsi que, lorsque le droit national le requiert, sur la base juridique justifiant le traitement. En outre, la personne concernée a le droit de faire corriger les données inexactes ou de faire supprimer les données traitées illicitement. Les États membres veillent également à ce que la personne concernée puisse, en cas de violation de ses droits en matière de protection des données, saisir effectivement un tribunal indépendant et impartial, établi par la loi, au sens de l'article 6, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme, ou une autorité indépendante de contrôle au sens de l'article 28 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ⁽¹⁾, et à ce qu'elle ait la possibilité de demander, par la voie judiciaire, une indemnisation ou toute autre forme de réparation. Le droit national de l'État membre dans lequel elle fait valoir ses droits régit la procédure détaillée de la mise en œuvre de ces droits ainsi que les motifs permettant de limiter le droit d'accès.

2. Si une autorité d'un État membre a transmis des données à caractère personnel en application de la présente décision, l'autorité destinataire de l'autre État membre ne peut pas invoquer l'inexactitude des données transmises pour se décharger de la responsabilité qui lui incombe conformément à son droit national à l'égard de la personne lésée. Si l'autorité destinataire doit verser des dommages et intérêts en raison de l'utilisation de données indûment transférées, l'autorité qui a transmis lesdites données en rembourse intégralement le montant à l'autorité destinataire.

Article 32

Informations demandées par les États membres

L'État membre destinataire informe, sur demande, l'État membre qui a transmis des données du traitement effectué sur les données transmises et du résultat obtenu.

CHAPITRE 7

DISPOSITIONS DE MISE EN ŒUVRE ET DISPOSITIONS FINALES

Article 33

Mesures d'exécution

Le Conseil, statuant à la majorité qualifiée et après consultation du Parlement européen, arrête les mesures nécessaires pour mettre en œuvre la présente décision au niveau de l'Union.

(1) JO L 281 du 23.11.1995, p. 31. Directive modifiée par le règlement (CE) n° 1882/2003 (JO L 284 du 31.10.2003, p. 1).

Article 34

Frais

Chaque État membre assume les frais opérationnels engagés par ses propres autorités dans le cadre de l'application de la présente décision. Dans des cas particuliers, les États membres concernés peuvent convenir d'autres modalités.

Article 35

Rapport avec d'autres instruments

1. À l'égard des États membres concernés, les dispositions pertinentes de la présente décision s'appliquent en lieu et place des dispositions correspondantes qui figurent dans le traité de Prüm. Les autres dispositions du traité de Prüm restent d'application entre les parties contractantes du traité de Prüm.

2. Sans préjudice des engagements qui leur incombent en vertu d'autres actes adoptés en application du titre VI du traité:

- a) les États membres peuvent continuer d'appliquer les accords bilatéraux ou multilatéraux ou les conventions de coopération transfrontalière qui sont en vigueur à la date de l'adoption de la présente décision, pour autant que ces accords ou conventions ne soient pas incompatibles avec les objectifs de la présente décision;
- b) après l'entrée en vigueur de la présente décision, les États membres peuvent conclure des accords bilatéraux ou multilatéraux ou des conventions de coopération transfrontalière, ou leur donner effet, pour autant que ces accords ou conventions prévoient d'étendre les objectifs de la présente décision.

3. Les accords et conventions visés aux paragraphes 1 et 2 ne peuvent porter préjudice aux relations avec des États membres qui n'y sont pas parties.

4. Les États membres informent le Conseil et la Commission, dans les quatre semaines qui suivent la prise d'effet de la présente décision, des accords ou conventions existants visés au paragraphe 2, point a), qu'ils souhaitent continuer d'appliquer.

5. Les États membres informent également le Conseil et la Commission de tout nouvel accord ou convention au sens du paragraphe 2, point b), dans les trois mois qui suivent leur signature ou, s'il s'agit d'instruments signés avant l'adoption de la présente décision, dans les trois mois qui suivent leur entrée en vigueur.

6. Aucune disposition de la présente décision ne porte atteinte aux accords ou conventions bilatéraux ou multilatéraux conclus entre des États membres et des États tiers.

7. La présente décision ne porte pas préjudice aux accords existants en matière d'assistance judiciaire ou de reconnaissance mutuelle des décisions de justice.

*Article 36***Mise en œuvre et déclarations**

1. Les États membres prennent les mesures nécessaires pour se conformer aux dispositions de la présente décision dans l'année qui suit sa prise d'effet, à l'exception du chapitre 2, pour lesquelles les mesures nécessaires seront prises dans les trois ans qui suivent la prise d'effet de la présente décision et de la décision du Conseil relative à la mise en œuvre de la présente décision.

2. Les États membres indiquent au secrétariat général du Conseil et à la Commission qu'ils ont mis en œuvre les obligations qui leur incombent en vertu de la présente décision et transmettent les déclarations prévues par la présente décision. Ce faisant, chaque État membre peut notifier qu'il appliquera immédiatement la présente décision dans le cadre de ses relations avec les États membres qui ont procédé à la même notification.

3. Les déclarations faites conformément au paragraphe 2 peuvent être modifiées à tout moment par une déclaration adressée au secrétariat général du Conseil, qui transmet aux États membres et à la Commission toutes les déclarations qu'il reçoit.

4. Sur la base de ces éléments et d'autres informations fournies par les États membres sur demande, la Commission soumet au Conseil, au plus tard le 28 juillet 2012, un rapport sur la mise en œuvre de la présente décision, assorti des propositions qu'elle juge appropriées en vue d'un développement futur.

*Article 37***Application**

La présente décision prend effet le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Luxembourg, le 23 juin 2008.

Par le Conseil

Le président

I. JARC