PARLEMENT EUROPÉEN

2004 *2009*

Commission des libertés civiles, de la justice et des affaires intérieures

PROVISOIRE
2005/0202(CNS)

6.3.2006

*

PROJET DE RAPPORT

sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale
(COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteur: Martine Roure

Légende des signes utilisés

*	Procédure de consultation *majorité des suffrages exprimés*
**I	Procédure de coopération (première lecture) *majorité des suffrages exprimés*
**II	Procédure de coopération (deuxième lecture) *majorité des suffrages exprimés pour approuver la position commune* *majorité des membres qui composent le Parlement pour rejeter ou amender la position commune*
***	Avis conforme *majorité des membres qui composent le Parlement sauf dans les cas visés aux art. 105, 107, 161 et 300 du traité CE et à l'art. 7 du traité UE*
***I	Procédure de codécision (première lecture) *majorité des suffrages exprimés*
***II	Procédure de codécision (deuxième lecture) *majorité des suffrages exprimés pour approuver la position commune* *majorité des membres qui composent le Parlement pour rejeter ou amender la position commune*
***III	Procédure de codécision (troisième lecture) *majorité des suffrages exprimés pour approuver le projet commun*

(La procédure indiquée est fondée sur la base juridique proposée par la Commission.)

Amendements à un texte législatif

Dans les amendements du Parlement, le marquage est indiqué en ***gras et italique***. Le marquage en *italique maigre* est une indication à l'intention des services techniques qui concerne des éléments du texte législatif pour lesquels une correction est proposée en vue de l'élaboration du texte final (par exemple éléments manifestement erronés ou manquants dans une version linguistique). Ces suggestions de correction sont subordonnées à l'accord des services techniques concernés.

SOMMAIRE

Page

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN.....5

EXPOSE DES MOTIFS 37

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale
(COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))

(Procédure de consultation)

Le Parlement européen,

– vu la proposition de la Commission (COM(2005)0475)[1],

– vu l'article 34, paragraphe 2, point b), du traité UE,

– vu l'article 39, paragraphe 1, du traité UE, conformément auquel il a été consulté par le Conseil (C6-0436/2005),

– vu le protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne, conformément auquel il a été consulté par le Conseil,

– vu l'avis de la commission des affaires juridiques sur la base juridique proposée,

– vu les articles 93 et 51 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A6-0000/2006),

1. approuve la proposition telle qu'amendée;

2. invite la Commission à modifier en conséquence sa proposition, conformément à l'article 250, paragraphe 2, du traité CE;

3. invite le Conseil, s'il entend s'écarter du texte approuvé par le Parlement, à en informer celui-ci;

4. demande au Conseil de le consulter à nouveau, s'il entend modifier de manière substantielle la proposition;

5. charge son Président de transmettre la position du Parlement au Conseil et à la Commission.

Texte proposé par la Commission	Amendements du Parlement

[1] JO C ..., du 1.3.2006, p. ...

Amendement 1
Visa 1

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

Justification

Il est nécessaire de préciser la base légale. L'article 30 paragraphe 1, point b) fait ainsi spécifiquement référence à l'échange de données et à la protection des données dans le cadre de la coopération policière. L'article 31, paragraphe 1, point c) vise l'amélioration de la coopération judiciaire, y compris " la compatibilité des règles applicables dans les États membres". Par ailleurs, ces deux articles constituent une base juridique permettant que le champ d'application ne se limite pas aux données échangées entres les autorités compétentes des États membres mais couvre également les situations internes.

Amendement 2
Visa 2 bis (nouveau)

	vu l'avis du contrôleur européen de protection des données,

Justification

Il est indispensable de prendre en compte l'avis du contrôleur européen de protection des données dans la rédaction de cette décision-cadre.

Amendement 3
Considérant 9

(9) La garantie d'un niveau de protection élevé des données à caractère personnel des ***citoyens européens*** exige des dispositions communes pour déterminer la légalité et la qualité des données traitées par les autorités compétentes d'autres États membres.	(9) La garantie d'un niveau de protection élevé des données à caractère personnel des ***personnes qui résident dans l'Union européenne*** exige des dispositions communes pour déterminer la légalité et la qualité des données traitées par les autorités compétentes d'autres États membres. ***Elle exige également que les données à caractère personnel soient collectées et traitées à des fins spécifiques et légitimes. Le traitement ultérieur de ces données ne peut aller à l'encontre de ladite finalité, y compris dans le cadre des échanges croissants d'informations entre***

	les autorités policières et judiciaires et en rapport avec la proposition sur l'interopérabilité des bases de données.

Justification

Toutes les personnes doivent bénéficier de la protection des données et non seulement les citoyens européens. La finalité pour laquelle les données ont été collectées doit également être respectée dans le cadre des échanges entre autorités policières et judiciaires.

Amendement 4
Considérant 12

(12) Lorsque des données à caractère personnel sont transférées d'un État membre de l'Union européenne vers des pays tiers ou des instances internationales, ces données devraient***, en principe,*** bénéficier d'un niveau adéquat de protection.	(12) Lorsque des données à caractère personnel sont transférées d'un État membre de l'Union européenne vers des pays tiers ou des instances internationales, ces données devraient bénéficier d'un niveau adéquat de protection. ***La présente décision-cadre devrait garantir que les données à caractère personnel transmises par des pays tiers répondent au moins aux normes internationales concernant le respect des droits de l'homme.***

Justification

L'échange des données avec les pays tiers doit respecter deux principes fondamentaux: assurer que les données ne peuvent être transférées que vers des pays tiers qui garantissent un niveau approprié de protection des données, et que les données reçues de la part de pays tiers respectent les droits fondamentaux.

Amendement 5
Considérant 15

(15) Il est bon de fixer des règles communes en matière de confidentialité et de sécurité du traitement, de responsabilité et de sanctions pour utilisation illicite par les autorités compétentes, ainsi que de voies de recours offertes à la personne concernée. En outre, il est nécessaire que les États membres prévoient des sanctions pénales pour les infractions particulièrement graves et intentionnelles aux dispositions relatives à la protection	(15) Il est bon de fixer des règles communes en matière de confidentialité et de sécurité du traitement, de responsabilité et de sanctions pour utilisation illicite par les autorités compétentes ***et par les parties privées qui traitent des données à caractère personnel au nom des autorités compétentes ou dans le cadre d'une fonction publique***, ainsi que de voies de recours offertes à la personne concernée. En outre, il est nécessaire que les États

des données.	membres prévoient des sanctions pénales pour les infractions particulièrement graves et intentionnelles aux dispositions relatives à la protection des données.

Justification

Il est important de préciser que lorsque les données sont gérées par des parties privées, notamment dans le cadre de partenariats publics-privés, celles-ci sont soumises au minimum aux mêmes conditions de sécurité des données que celles prévues pour les autorités compétentes publiques.

Amendement 6
Considérant 20

(20) La présente décision-cadre ne porte pas préjudice aux dispositions spécifiques prévues en matière de protection des données par les instruments juridiques pertinents relatifs au traitement et à la protection des données à caractère personnel par Europol, Eurojust et le système d'information des douanes.	(20) La présente décision-cadre ne porte pas préjudice aux dispositions spécifiques prévues en matière de protection des données par les instruments juridiques pertinents relatifs au traitement et à la protection des données à caractère personnel par Europol, Eurojust et le système d'information des douanes. ***Toutefois, à long terme, les principes de protection des données applicables à Europol, Eurojust et au système d'information des douanes devront être pleinement compatibles avec la présente décision-cadre afin d'améliorer la cohérence et l'efficacité du cadre juridique relatif à la protection des données.***

Justification

La proposition prévoit l'exclusion de son champ d'application d'Europol, d'Eurojust et du système d'information des douanes car ceux-ci ont leurs propres systèmes de protection des données personnelles. Étant donné que la mise en place d'un espace européen de liberté, de sécurité et de justice engendre un échange accru de données personnelles entre les autorités compétentes, y compris avec Europol et Eurojust, il serait incohérent de les exclure. Il faut donc prévoir à terme une convergence entre les principes de protection des données de la présente décision-cadre et les principes d'Europol, d'Eurojust et du système d'information des douanes.

Amendement 7
Considérant 22

(22) Il est bon que la présente décision-cadre s'applique aux données à caractère personnel traitées dans le cadre du système d'information Schengen de deuxième génération et à l'échange d'informations supplémentaires qui y est lié conformément à la décision JAI/2006 …. sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération.	(22) Il est bon que la présente décision-cadre s'applique aux données à caractère personnel traitées dans le cadre du système d'information Schengen de deuxième génération et à l'échange d'informations supplémentaires qui y est lié conformément à la décision JAI/2006 …. sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération ***et dans le cadre du système d'information sur les visas conformément à la Décision JAI/2006/... sur l'accès en consultation au système d'information sur les visas VIS par les autorités compétentes des États membres et par l'Office européen de police Europol.***

Justification

Il convient d'ajouter une référence au VIS afin que la présente décision-cadre s'applique également à l'accès au système d'information sur les visas par les services répressifs.

Amendement 8
Article 3, paragraphe 2 bis (nouveau)

	2 bis. La présente décision-cadre n'est pas d'application si une législation spécifique, au sens du titre VI du Traité sur l'Union européenne, dispose clairement que les données à caractère personnel ne doivent être traitées, consultées ou transmises que sur la base de conditions ou de restrictions plus spécifiques.

Justification

La présente décision-cadre ne doit pas interdire une législation plus spécifique régissant notamment le traitement des données.

Amendement 9
Article 4, paragraphe 1, point d)

d) exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables sont prises pour que les données inexactes ou	d) exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables sont prises pour que les données inexactes ou

incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. ***Les*** États membres peuvent prévoir un traitement des données selon divers degrés d'exactitude et de fiabilité, auquel cas ils doivent prévoir que les données sont classées selon leur degré d'exactitude et de fiabilité, et notamment que les données fondées sur des faits soient distinguées des données fondées sur des opinions ou appréciations personnelles;	incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées. ***Cependant, les*** États membres peuvent prévoir un traitement des données selon divers degrés d'exactitude et de fiabilité, auquel cas ils doivent prévoir que les données sont classées selon leur degré d'exactitude et de fiabilité, et notamment que les données fondées sur des faits soient distinguées des données fondées sur des opinions ou appréciations personnelles; ***les États membres font en sorte que la qualité des données à caractère personnel soit vérifiée régulièrement. Dans la mesure du possible, les décisions de justice et les décisions d'arrêt des poursuites doivent être indiquées et les données fondées sur des opinions ou des appréciations personnelles doivent être vérifiées à la source et leur degré d'exactitude ou de fiabilité doit être précisé. Sans préjudice de la procédure pénale nationale, les États membres font en sorte que les données à caractère personnel soient «annotées» à la demande de la personne concernée si leur exactitude est niée par celle-ci et si leur exactitude ou inexactitude ne peut être vérifiée. Cette «annotation» n'est effacée qu'avec le consentement de la personne concernée ou sur le fondement d'une décision de la juridiction compétente ou de l'autorité de contrôle compétente;***

Justification

Ce paragraphe est déplacé de l'article 9, paragraphe 6. En effet, ces dispositions doivent être déplacées du Chapitre III vers le Chapitre II afin qu'elles s'appliquent à tous les traitements de données réalisés par les services répressifs et non seulement aux données échangées entre les États membres.

Amendement 10
Article 4, paragraphe 4

4. Les États membres prévoient que le	***supprimé***

traitement des données à caractère personnel n'est nécessaire que si

– il y a de bonnes raisons de croire, à la lumière de faits établis, que les données à caractère personnel concernées rendraient possible, faciliteraient ou accéléreraient la prévention et la détection des infractions pénales, et les enquêtes et poursuites en la matière,

– il n'existe pas d'autre moyen qui affecte moins la personne concernée et

– le traitement des données n'est pas disproportionné par rapport à l'infraction en cause.

Justification

Cette formulation ne respecte pas les critères établis par la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 8 de la Convention européenne des droits de l'homme. La jurisprudence prévoit qu'il n'est possible d'imposer des restrictions au droit à la vie privée que si cela est nécessaire dans une société démocratique et non si cela faciliterait ou accélèrerait le travail des autorités policières ou judiciaires. Il convient donc de remplacer les dispositions prévues. Le critère de nécessité et de proportionnalité des données sera reformulé dans l'article 5.

Amendement 11
Article 4, paragraphe 4 bis (nouveau)

4 bis. Les États membres tiennent compte des différentes catégories de données et des diverses finalités pour lesquelles elles sont collectées en vue d'établir des conditions appropriées pour la collecte, les limites de temps, le traitement ultérieur et le transfert des données à caractère personnel concernées. Les données à caractère personnel des non-suspects ne sont traitées que pour la finalité pour laquelle elles ont été collectées, dans une période de temps définie, et avec des limitations adéquates quant à l'accès et au transfert.

Justification

La distinction entre les différents types de données prévue au paragraphe 3 est très utile. Il

convient de la renforcer en accordant une attention particulière aux données des non-suspects qui doivent être assorties de mesures de protection spécifiques pour les conditions de collecte des données, la durée de conservation et les modalités d'accès des autorités.

Amendement 12
Article 4 bis, paragraphe 1 (nouveau)

Article 4 bis

Traitement ultérieur des données à caractère personnel

1. Les États membres font en sorte que, conformément à la présente décision-cadre, en particulier à ses articles 4, 5 et 6, les données à caractère personnel ne fassent l'objet d'un traitement ultérieur que

a) pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition, ou

b) si cela est strictement nécessaire, dans un cas spécifique, à des fins de prévention, d'enquête, de détection ou de poursuites judiciaires relatives à des infractions pénales,

c) à des fins de prévention de menaces contre la sécurité publique ou une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations.

Justification

Il convient de limiter le traitement ultérieur des données et de l'inscrire dans le Chapitre II afin qu'il s'applique à tous les traitements de données réalisés par les services répressifs et non uniquement aux données échangées avec d'autres États membres. Tout traitement ultérieur doit respecter le principe de finalité pour lequel les données ont été récoltées et doit être envisagé au cas par cas.

Amendement 13
Article 4 bis, paragraphe 2 (nouveau)

2. Les données à caractère personnel

	concernées font l'objet d'un traitement ultérieur pour les finalités visées au paragraphe 1, point c), uniquement avec le consentement préalable de l'autorité qui a transmis les données personnelles ou les a mises à disposition, et les États membres peuvent, sous réserve de garanties juridiques appropriées, adopter des mesures législatives autorisant ledit traitement ultérieur.

Justification

Voir justification de l'amendement précédent.

Amendement 14
Article 5, paragraphe 1

Les États membres font en sorte que les données à caractère personnel ***ne*** puissent être traitées par les autorités compétentes ***qu'***en vertu d'une loi établissant que ce traitement est nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée et aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière.	***1.*** Les États membres font en sorte que les données à caractère personnel puissent être traitées par les autorités compétentes ***uniquement:***
	a) en vertu d'une loi établissant que ce traitement est nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée et aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière;
	b) avec le consentement explicite de la personne concernée, à condition que le traitement soit effectué dans l'intérêt de cette dernière; ou
	c) si le traitement est nécessaire pour le respect d'une obligation juridique à laquelle le contrôleur est soumis,
	d) si le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée.

Justification

Il convient d'ajouter à l'article 5 les principes de proportionnalité et de nécessité des données. Le traitement des données à caractère personnel ne doit être considéré comme nécessaire que lorsque les autorités compétentes peuvent clairement en démontrer le besoin, et à condition qu'il ne soit pas possible de recourir à des mesures plus respectueuses de la vie privée.

Amendement 15
Article 5, paragraphe 1 bis (nouveau)

1 bis. Les États membres font en sorte que les données à caractère personnel ne soient traitées que si:

- les autorités compétentes peuvent prouver, sur base de faits établis, que le traitement des données personnelles concernées est réellement nécessaire à des fins de prévention, d'enquête, de détection ou de poursuites judiciaires relatives à des infractions pénales,

- il n'existe pas d'autre moyen ayant un impact moindre pour la personne concernée et

- le traitement des données n'est pas disproportionné par rapport à l'infraction en cause.

Justification

Il convient d'introduire les principes de finalité et de proportionnalité comme critères pour établir la licéité du traitement des données.

Amendement 16
Article 6, paragraphe 2, tiret 1

– le traitement est prévu par un texte de loi et absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, ***et*** d'enquêtes et de poursuites en la matière, ou si la personne concernée a expressément consenti au traitement, et	– le traitement est prévu par un texte de loi et absolument nécessaire pour l'accomplissement des tâches légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ***et qu'il est limité à une enquête particulière***, ou si la personne concernée a expressément consenti au traitement, ***à condition que le traitement soit réalisé dans l'intérêt de la personne concernée, et que le refus de consentement n'entraîne pas de***

conséquences négatives pour cette personne; et

Justification

Le traitement des données sensibles fondé sur le consentement explicite de la personne concernée ne devrait être autorisé que dans la mesure où le traitement est réalisé dans l'intérêt de celle-ci. Par ailleurs, le refus de consentir ne devrait pas avoir d'effets négatifs pour la personne concernée.

Amendement 17
Article 6, paragraphe 2 bis (nouveau)

2 bis. Les États membres appliquent des exigences techniques et organisationnelles spécifiques pour le traitement des données à caractère sensible.

Justification

Les États membres doivent mettre en place des mesures techniques spécifiques pour assurer la sécurité des données à caractère sensible.

Amendement 18
Article 6, paragraphe 2 ter (nouveau)

2 ter. Les États membres mettent en place des garanties supplémentaires spécifiques pour les données biométriques et les profils ADN, en vue de garantir que:

- les données biométriques et les profils ADN ne sont utilisés que sur la base de normes techniques bien établies et interopérables,

- le niveau d'exactitude des données biométriques et des profils ADN est soigneusement pris en considération et peut être aisément contesté par la personne concernée,

- le respect de la dignité et de l'intégrité de la personne est pleinement garanti.

Justification

Il est nécessaire de mettre en place des normes supplémentaires de protection pour les données biométriques et les profils ADN. En effet, ces données sont particulièrement sensibles mais sont parfois utilisées dans le domaine de la coopération policière et judiciaire.

Amendement 19
Article 7, paragraphe 1

1. Les États membres font en sorte que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées***, sauf disposition contraire du droit national.*** Les données à caractère personnel des personnes visées à l'article 4, paragraphe 3, dernier tiret, sont conservées dans la limite de la durée strictement nécessaire à la réalisation de la finalité pour laquelle elles sont collectées.	1. Les États membres font en sorte que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées ***ou traitées ultérieurement, conformément à l'article 4, paragraphe 1, point e) et à l'article 4 bis.*** Les données à caractère personnel des personnes visées à l'article 4, paragraphe 3, dernier tiret, sont conservées dans la limite de la durée strictement nécessaire à la réalisation de la finalité pour laquelle elles sont collectées.

Justification

Il faut supprimer la possibilité de dérogation générale aux garanties prévues à la seule condition que le droit national en dispose autrement. Cela mettrait en péril l'harmonisation des critères de protection des données et est incompatible avec le droit à la protection des données.

Amendement 20
Article 7, paragraphe 2

2. Ils mettent en place les mesures procédurales et techniques appropriées garantissant que les durées de conservation des données à caractère personnel sont respectées. Le respect de ces durées de conservation est régulièrement contrôlé.	2. Ils mettent en place les mesures procédurales et techniques appropriées garantissant que les durées de conservation des données à caractère personnel sont respectées. ***Lesdites mesures incluent l'effacement régulier et automatique des données à caractère personnel à l'issue d'une période de temps donnée.*** Le respect de ces durées de conservation est régulièrement contrôlé.

Justification

Les mesures garantissant la durée de conservation doivent prévoir un effacement automatique après une période définie.

Amendement 21
Article 8

Les États membres font en sorte que les données à caractère personnel ne soient transmises aux autorités compétentes des autres États membres, ou mises à leur disposition, que si cela est nécessaire pour l'accomplissement des tâches légitimes de l'autorité transmettrice ou réceptrice aux fins de prévention et de détection ***des infractions pénales***, et d'enquêtes et de poursuites en la matière.	Les États membres font en sorte que les données à caractère personnel ***collectées et traitées par les autorités compétentes*** ne soient transmises aux autorités compétentes des autres États membres, ou mises à leur disposition, que si cela est nécessaire pour l'accomplissement des tâches légitimes de l'autorité transmettrice ou réceptrice aux fins de prévention et de détection ***d'infractions pénales spécifiques***, et d'enquêtes et de poursuites en la matière.

Justification

Seules les données récoltées par les autorités compétentes peuvent être transmises aux autorités compétentes. Cela permet de limiter l'accès et la transmission de données retenues par des parties privées.

Amendement 22
Article 9, paragraphe 6

6. Sans préjudice de la procédure pénale nationale, les États membres font en sorte que les données à caractère personnel soient «annotées» à la demande de la personne concernée si leur exactitude est niée par celle-ci et si leur exactitude ou inexactitude ne peut être vérifiée. Cette «annotation» n'est effacée qu'avec le consentement de la personne concernée ou sur le fondement d'une décision de la juridiction compétente ou de l'autorité de contrôle compétente.	***supprimé***

Justification

Ces dispositions doivent être déplacées du Chapitre III vers le Chapitre II afin qu'elles

s'appliquent à tous les traitements de données réalisés par les services répressifs et non seulement aux données échangées entre les États membres.

Amendement 23
Article 9, paragraphe 7, troisième tiret

– si ces données ne sont pas ou plus nécessaires pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition.	– ***et, dans tous les cas,*** si ces données ne sont pas ou plus nécessaires pour la finalité spécifique pour laquelle elles ont été transmises ou mises à disposition.

Justification

Les données doivent systématiquement être effacées si elles ne sont plus nécessaires pour la finalité pour laquelle elles ont été transmises ou mises à disposition.

Amendement 24
Article 9, paragraphe 9 bis (nouveau)

	9 bis. Les États membres font en sorte que la qualité des données personnelles transmises ou mises à disposition par un pays tiers fasse l'objet d'une évaluation spécifique dès leur réception et que leur degré d'exactitude et de fiabilité soit indiqué.

Justification

Il convient de vérifier la qualité des données reçues de pays tiers afin d'indiquer leur fiabilité, y compris en ce qui concerne le respect des droits fondamentaux.

Amendement 25
Article 10, paragraphe 1

1. Les États membres font en sorte que chaque transmission et chaque réception automatisées de données à caractère personnel, en particulier par accès direct automatisé, soient enregistrées dans un journal afin de permettre la vérification ultérieure des motifs justifiant la transmission, des données transmises, du jour et de l'heure de la transmission, des autorités concernées et, dans la mesure où	1. Les États membres font en sorte que chaque ***consultation,*** transmission et réception automatisées de données à caractère personnel, en particulier par accès direct automatisé, soient enregistrées dans un journal afin de permettre la vérification ultérieure des motifs justifiant ***l'accès et*** la transmission, des données transmises ***ou consultées***, du jour et de l'heure de la transmission ***ou de l'accès***,

l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.	des autorités concernées et, dans la mesure où l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.

Justification

Il convient également d'enregistrer dans le journal l'accès aux données afin de s'assurer que tout accès aux données est légitime.

Amendement 26
Article 10, paragraphe 2

2. Les États membres font en sorte qu'une trace documentaire soit conservée de chaque transmission et de chaque réception non automatisées de données à caractère personnel afin de permettre la vérification ultérieure des motifs justifiant la transmission, des données transmises, du jour et de l'heure de la transmission, des autorités concernées et, dans la mesure où l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.	2. Les États membres font en sorte qu'une trace documentaire soit conservée de chaque ***consultation,*** transmission et réception non automatisées de données à caractère personnel afin de permettre la vérification ultérieure des motifs justifiant ***l'accès ou*** la transmission, des données transmises ***ou consultées***, du jour et de l'heure de la transmission ***ou de l'accès***, des autorités concernées et, dans la mesure où l'autorité réceptrice est concernée, des personnes ayant reçu les données et des personnes ayant été à l'origine de leur réception.

Justification

Il convient également d'enregistrer dans le journal l'accès aux données afin de s'assurer que tout accès aux données est légitime.

Amendement 27
Article 10, paragraphe 3

3. L'autorité ayant enregistré dans un journal ces informations ou en ayant conservé une trace documentaire les communique immédiatement à ***l'autorité de contrôle compétente à la demande de cette dernière.*** Ces informations ne sont utilisées que pour contrôler la protection des données et pour garantir le traitement approprié des données ainsi que leur	3. L'autorité ayant enregistré dans un journal ces informations ou en ayant conservé une trace documentaire ***les garde à la disposition de l'autorité de contrôle compétente et*** les communique immédiatement à ***ladite autorité***. Ces informations ne sont utilisées que pour contrôler la protection des données et pour garantir le traitement approprié des

intégrité et leur sécurité.	données ainsi que leur intégrité et leur sécurité.

Justification

Le journal doit être mis à disposition de l'autorité de contrôle compétente sans qu'elle en fasse la demande.

Amendement 28
Article 13, partie introductive

Les États membres font en sorte que les données à caractère personnel ***reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle ci*** ne soient ***ensuite*** transmises à des autorités, autres que leurs autorités compétentes, que dans des cas déterminés et si l'ensemble des conditions suivantes sont réunies:	Les États membres font en sorte que les données à caractère personnel ne soient transmises à des autorités, autres que leurs autorités compétentes, que dans des cas ***particuliers*** déterminés ***et solidement documentés,*** et si l'ensemble des conditions suivantes sont réunies:

Justification

Cet article doit s'appliquer à l'ensemble des données policières et judiciaires, même si elles ne sont pas transmises ou mises à disposition par les autorités compétentes d'un autre État membre.

Amendement 29
Article 13, point b), alinéa 1

est nécessaire pour atteindre la finalité spécifique pour laquelle les données ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;	est nécessaire pour atteindre la finalité spécifique pour laquelle les données ont été ***collectées,*** transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

Justification

La finalité pour laquelle les données ont été collectées doit également être un critère pour la transmission à des autorités autres que les autorités compétentes. Cet article ainsi modifié peut s'appliquer à l'ensemble des données policières et judiciaires, même si elles ne sont pas transmises ou mises à disposition par les autorités compétentes d'un autre État membre.

Amendement 30
Article 13, point c)

c) l'autorité compétente ***de l'***État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les ***transmettre***, ou les ayant mises à la disposition de celle ci, ***a*** donné son consentement préalable à leur transmission ultérieure.	c) ***Lorsque des données à caractère personnel ont été transmises ou mise à disposition par*** l'autorité compétente ***d'un autre*** État membre***, lesdites données ne sont pas ultérieurement transmises aux autorités d'un État membre autres que les autorités compétentes, à moins que l'État membre*** ayant transmis les données concernées à l'autorité compétente qui entend ensuite les ***transférer***, ou les ayant mises à la disposition de celle ci, ***ait*** donné son consentement préalable à leur transmission ultérieure.

Justification

Tout traitement ultérieur des données doit être autorisé par l'autorité qui les a mises à disposition et doit respecter les règles en matière de traitement ultérieur (article 4 bis nouveau).

Amendement 31
Article 14

Sans préjudice des règles nationales de procédure pénale, les États membres font en sorte que les données à caractère personnel ***reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle-ci*** ne soient ensuite transmises à des personnes privées dans un État membre que dans des cas déterminés et si l'ensemble des conditions suivantes sont réunies:	Sans préjudice des règles nationales de procédure pénale, les États membres font en sorte que les données à caractère personnel ne soient ensuite transmises à des personnes privées dans un État membre que dans des cas déterminés et si l'ensemble des conditions suivantes sont réunies:
a) la transmission fait l'objet d'une obligation ou d'une autorisation légale claire;	a) la transmission fait l'objet d'une obligation ou d'une autorisation légale claire;

b) la transmission est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;	b) la transmission est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été ***collectées,*** transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations, et
c) ***l'autorité compétente de l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle ci, a donné son consentement préalable à leur transmission ultérieure à des personnes privées.***	c) ***lorsque des données à caractère personnel ont été transmises ou mise à disposition par l'autorité compétente d'un autre État membre, lesdites données ne sont pas ultérieurement transmises aux autorités d'un État membre autres que les autorités compétentes, à moins que l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transférer, ou les ayant mises à la disposition de celle ci, ait donné son consentement préalable à leur transmission ultérieure.***

Justification

Cet article doit s'appliquer à l'ensemble des données et non seulement celles transmises par un autre État membre. La finalité pour lesquelles les données ont été collectées doit également être respectée. Tout transfert ultérieur à des parties privées doit être autorisé par l'État membre qui a mis à disposition les données.

Amendement 32
Article 14 bis (nouveau)

	Article 14 bis
	Les États membres font en sorte que les autorités compétentes puissent consulter et traiter les données à caractère personnel conservées par des parties privées uniquement au cas par cas, dans des circonstances établies, à des fins définies et sous le contrôle judiciaire des États membres.

Justification

Il convient de réglementer l'accès des autorités compétentes aux données conservées par des parties privées et de le limiter au cas par cas et pour des raisons établies et justifiées. Cet accès doit être autorisé par une décision judiciaire.

Amendement 33
Article 14 ter (nouveau)

Article 14 ter

Traitement des données par des parties privées dans le cadre d'une fonction publique

Les États membres prévoient dans leur législation nationale que, lorsque les parties privées collectent et traitent les données dans le cadre d'une fonction publique, elles sont soumises à des obligations au moins équivalentes ou supérieures à celles imposées aux autorités compétentes.

Justification

Lorsque les parties privées récoltent ou traitent les données dans le cadre d'une fonction publique, des mesures supplémentaires à la directive 95/46/CE à laquelle elles sont soumises, et supérieures à celles imposées aux autorités compétentes, doivent leur être imposées.

Amendement 34
Article 15, paragraphe 1

1. Les États membres font en sorte que les données à caractère personnel ***reçues de l'autorité compétente d'un autre État membre ou mises à disposition par celle ci*** ne soient pas transférées ensuite aux autorités compétentes de pays tiers ou à des instances internationales, sauf si ce transfert est conforme à la présente décision cadre et, notamment, si l'ensemble des conditions suivantes sont réunies:	1. Les États membres font en sorte que les données à caractère personnel ne soient pas transférées ensuite aux autorités compétentes de pays tiers ou à des instances internationales, sauf si ce transfert est conforme à la présente décision cadre et, notamment, si l'ensemble des conditions suivantes sont réunies:

Justification

Il convient que cet article s'applique à l'ensemble des données et non seulement à celles transmises par un autre État membre.

Amendement 35
Article 15, paragraphe 1, point b)

b) le transfert est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;	b) le transfert est nécessaire pour atteindre la finalité pour laquelle les données concernées ont été ***collectées ou*** transmises ou mises à disposition, ou à des fins de prévention ou de détection des infractions pénales, ou d'enquêtes ou de poursuites en la matière, ou à des fins de prévention de menaces à l'encontre de la sécurité publique ou d'une personne, sauf lorsque la nécessité de protéger les intérêts ou les droits fondamentaux de la personne concernée l'emporte sur ce type de considérations;

Justification

La finalité pour laquelle les données ont été collectées doit également être respectée.

Amendement 36
Article 15, paragraphe 1, point c)

c) l'autorité compétente d'un autre État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transmettre, ou les ayant mises à la disposition de celle ci a donné son consentement préalable à leur transfert ultérieur;	***supprimé***

Justification

Il convient que cet article s'applique à l'ensemble des données et non seulement à celles transmises par un autre État membre. Le transfert ultérieur est traité dans le nouveau paragraphe 4 bis.

Amendement 37
Article 15, paragraphe 1, alinéa 1 bis (nouveau)

	Lorsque des données à caractère personnel ont été transmises ou mise à disposition par l'autorité compétente d'un autre État membre, lesdites données ne sont pas ultérieurement transmises aux autorités compétentes d'un pays tiers ou à des organismes internationaux, à moins que l'État membre ayant transmis les données concernées à l'autorité compétente qui entend ensuite les transférer, ou les ayant mises à la disposition de celle ci, ait donné son consentement préalable à leur transmission ultérieure.

Justification

Voir justification de l'amendement précédent.

Amendement 38
Article 15, paragraphe 3

3. Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers ou une instance internationale n'assurent pas un niveau de protection adéquat au sens du paragraphe 2.	3. Les États membres et la Commission s'informent mutuellement ***et informent le Parlement européen*** des cas dans lesquels ils estiment qu'un pays tiers ou une instance internationale n'assurent pas un niveau de protection adéquat au sens du paragraphe 2.

Justification

Le Parlement européen doit également être consulté dans l'évaluation du niveau de protection des données assuré par les pays tiers.

Amendement 39
Article 15, paragraphe 4

4. ***Lorsqu'il est établi, conformément à la procédure prévue à l'article 16***, qu'un pays tiers ou une instance internationale n'assure pas un niveau de protection adéquat au sens du paragraphe 2, les États membres	4. ***Lorsque la Commission, après consultation du Conseil et du Parlement européen, établit*** qu'un pays tiers ou une instance internationale n'assure pas un niveau de protection adéquat au sens du

prennent les mesures nécessaires en vue d'empêcher tout transfert de données à caractère personnel vers le pays tiers ou l'instance internationale en cause.	paragraphe 2, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de données à caractère personnel vers le pays tiers ou l'instance internationale en cause.

Justification

Le Parlement européen doit également être consulté dans l'évaluation du niveau de protection des données assuré par les pays tiers.

Amendement 40
Article 15, paragraphe 5

5. ***Il peut être établi, conformément à la procédure prévue à l'article 16***, qu'un pays tiers ou une instance internationale assure un niveau de protection adéquat au sens du paragraphe 2, en raison de sa législation interne ***ou*** de ses engagements internationaux, pour ce qui est de la protection de la vie privée et des libertés et droits fondamentaux des personnes.	5. ***La Commission, après consultation du Conseil et du Parlement européen, peut établir*** qu'un pays tiers ou une instance internationale assure un niveau de protection adéquat au sens du paragraphe 2, en raison de sa législation interne ***et*** de ses engagements internationaux, pour ce qui est de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Justification

Le Parlement européen doit également être consulté dans l'évaluation du niveau de protection des données assuré par les pays tiers.

Amendement 41
Article 15, paragraphe 6

6. À titre exceptionnel, les données à caractère personnel ***reçues de l'autorité compétente d'un autre État membre*** peuvent ***ensuite*** être transférées aux autorités compétentes de pays tiers ou à des instances internationales n'assurant pas un niveau adéquat de protection ou au sein desquelles ce niveau de protection n'est pas assuré, en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un État membre, ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de	6. À titre exceptionnel, ***par dérogation au paragraphe 1, point d),*** les données à caractère personnel peuvent être transférées aux autorités compétentes de pays tiers ou à des instances internationales n'assurant pas un niveau adéquat de protection ou au sein desquelles ce niveau de protection n'est pas assuré, en cas d'absolue nécessité afin de sauvegarder les intérêts essentiels d'un État membre, ou à des fins de prévention de menaces imminentes graves à l'encontre de la sécurité publique ou d'une ou de plusieurs

plusieurs personnes en particulier.	personnes en particulier. ***Dans ce cas, les données à caractère personnel sont traitées par la partie réceptrice uniquement si cela est absolument nécessaire pour la finalité spécifique pour laquelle elles ont été transmises. Ces transferts sont notifiés à l'autorité de contrôle compétente.***

Justification

Les conditions d'applicabilité de l'exception prévue au paragraphe 6, qui permet le transfert de données à des pays tiers n'assurant pas un niveau adéquat de protection des données, doivent être précisées. Cette exception doit permettre de déroger uniquement au critère de "protection adéquate" et non aux autres principes de cette décision-cadre. Le transfert des données en vertu de cette exception doit satisfaire des conditions appropriées et être notifié à l'autorité de supervision compétente.

Amendement 42
Article 16

Article 16	***supprimé***
Comité	
1. Lorsqu'il est fait référence au présent article, la Commission est assistée d'un comité composé de représentants des États membres et présidé par un représentant de la Commission.	
2. Le comité adopte son règlement intérieur, sur proposition du président, sur la base du règlement intérieur type publié au Journal officiel de l'Union européenne.	
3. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 205, paragraphe 2, du traité instituant la Communauté européenne pour l'adoption des décisions que le Conseil est appelé à prendre sur proposition de la Commission. Lors des votes au sein du comité, les voix des représentants des	

États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

4. La Commission arrête les mesures envisagées lorsqu'elles sont conformes à l'avis du comité. Lorsque les mesures envisagées ne sont pas conformes à l'avis du comité, ou en l'absence d'avis, la Commission soumet sans tarder au Conseil une proposition relative aux mesures à prendre et en informe le Parlement européen.

5. Le Conseil peut statuer à la majorité qualifiée sur la proposition, dans un délai de deux mois à compter de sa saisine.

Si, dans ce délai, le Conseil a indiqué, à la majorité qualifiée, qu'il s'oppose à la proposition, la Commission réexamine celle-ci. Elle peut soumettre au Conseil une proposition modifiée, soumettre à nouveau sa proposition ou présenter une proposition législative. Si, à l'expiration de ce délai, le Conseil n'a pas adopté les mesures d'application proposées ou s'il n'a pas indiqué qu'il s'opposait à la proposition de mesures d'application, les mesures d'application proposées sont arrêtées par la Commission.

Justification

La procédure de comitologie ne s'applique pas au troisième pilier.

Amendement 43
Article 18

Les États membres font en sorte que l'autorité compétente de laquelle des données à caractère personnel ont été reçues ou qui les a mises à disposition soit informée ***à sa demande*** du traitement ultérieur de ces données et des résultats obtenus.	Les États membres font en sorte que l'autorité compétente de laquelle des données à caractère personnel ont été reçues ou qui les a mises à disposition soit informée du traitement ultérieur de ces données et des résultats obtenus.

Justification

Les autorités compétentes desquelles les données ont été reçues doivent toujours être informées de tout traitement ultérieur.

Amendement 44
Article 19, paragraphe 1, point c), quatrième tiret bis (nouveau)

- les limites de temps pour la conservation des données

Justification

La personne concernée doit être informée de la durée pour laquelle les données la concernant seront conservées.

Amendement 45
Article 19, paragraphe 2, partie introductive, points a) et b)

2. La fourniture des informations énumérées au paragraphe 1 ***est refusée*** ou limitée uniquement si cela s'avère nécessaire	2. La fourniture des informations énumérées au paragraphe 1 ***n'est pas assurée*** ou ***est*** limitée uniquement si cela s'avère nécessaire
a) pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante,	
b) pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités compétentes de leurs tâches légales,	pour éviter de compromettre des enquêtes, recherches ou procédures en cours, ou de nuire à l'accomplissement par les autorités ***de contrôle et/ou*** compétentes de leurs tâches légales,

Justification

Le traitement satisfaisant des données ne doit pas constituer un critère de refus pour communiquer les informations la concernant à la personne visée. Cela constituerait une dérogation trop large et trop vague aux droits de la personne concernée.

Amendement 46
Article 19, paragraphe 4

4. Les motifs justifiant un refus ou une limitation en application du paragraphe 2 ne sont pas communiqués si leur	4. Les motifs justifiant un refus ou une limitation en application du paragraphe 2 ne sont pas communiqués si leur

communication compromet la finalité du refus. En pareil cas, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales. Si la personne concernée forme un recours auprès de l'autorité de contrôle, cette dernière examine ce recours. Lorsqu'elle examine le recours, l'autorité de contrôle ***fait simplement savoir à la personne concernée si les données ont été traitées correctement et, dans la négative, si toutes les corrections nécessaires ont été apportées.***	communication compromet la finalité du refus. En pareil cas, le responsable du traitement informe la personne concernée qu'elle peut introduire un recours devant l'autorité de contrôle compétente, sans préjudice d'éventuels recours juridictionnels et procédures pénales nationales. Si la personne concernée forme un recours auprès de l'autorité de contrôle, cette dernière examine ce recours. Lorsqu'elle examine le recours, l'autorité de contrôle ***informe la personne concernée de l'issue de son recours.***

Justification

La personne concernée doit être informée de l'issue de son recours dans tous les cas et non uniquement si des corrections ont eu lieu.

Amendement 47
Article 20, paragraphe 1, partie introductive

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée ou ont été obtenues de sa part sans qu'elle ait connaissance ou conscience du fait que des données étaient collectées à son sujet, les États membres font en sorte que le responsable du traitement ou son représentant fournisse gratuitement à la personne concernée, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, ***dans un délai raisonnable après*** la première communication de données, au moins les informations énumérées ci-dessous, sauf si la personne concernée dispose déjà de ces informations ou si la fourniture d'informations s'avère impossible ou impliquerait un effort disproportionné:	1. Lorsque les données n'ont pas été collectées auprès de la personne concernée ou ont été obtenues de sa part sans qu'elle ait connaissance ou conscience du fait que des données étaient collectées à son sujet, les États membres font en sorte que le responsable du traitement ou son représentant fournisse gratuitement à la personne concernée, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, ***au plus tard au moment de*** la première communication de données, au moins les informations énumérées ci-dessous, sauf si la personne concernée dispose déjà de ces informations ou si la fourniture d'informations s'avère impossible ou impliquerait un effort disproportionné:

Justification

La notion de "délai raisonnable" est ouverte à interprétation. Il faut donc préciser que les

informations, lorsque les données n'ont pas été collectées auprès de la personne concernée, sont fournies à cette personne "au plus tard au moment de la première communication de données".

Amendement 48
Article 20, paragraphe 2, partie introductive et point a)

2. Les informations énumérées au paragraphe 1 ne sont pas fournies si cela s'avère nécessaire	Les informations énumérées au paragraphe 1 ne sont pas fournies ***uniquement*** si cela s'avère nécessaire
a) pour permettre au responsable du traitement d'accomplir ses tâches légales de manière satisfaisante,	

Justification

Le traitement satisfaisant des données ne doit pas constituer un critère de refus pour communiquer les informations la concernant à la personne visée. Cela constituerait une dérogation trop large et trop vague aux droits de la personne concernée.

Amendement 49
Article 21, paragraphe 1, point c)

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b)***, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.***	c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b)**.**

Justification

La notification aux tiers de toute rectification doit être systématique.

Amendement 50
Article 21, paragraphe 2, partie introductive et point a)

2. Tout acte auquel la personne concernée peut prétendre conformément au paragraphe 1 est refusé si cela s'avère nécessaire	2. Tout acte auquel la personne concernée peut prétendre conformément au paragraphe 1 est refusé ***uniquement*** si cela s'avère nécessaire
a) pour permettre au responsable du traitement d'accomplir ses tâches légales	

de manière satisfaisante,

Justification

Le traitement satisfaisant des données ne doit pas constituer un critère de refus pour communiquer les informations la concernant à la personne visée. Cela constituerait une dérogation trop large et trop vague aux droits de la personne concernée.

Amendement 51
Article 22 bis (nouveau)

Article 22 bis

Décisions individuelles automatisées

1. Les États membres accordent à toute personne le droit de ne pas être soumise à une décision ou à une action qui produit des effets juridiques à son égard ou bien a pour elle un impact considérable et qui est uniquement fondée sur un traitement automatisé des données visant à évaluer certains aspects personnels la concernant, tels que sa fiabilité, son comportement, etc.

2. Sous réserve des autres articles de la présente décision-cadre, les États membres font en sorte qu'une personne ne puisse faire l'objet d'une décision telle que celle visée au paragraphe 1 que si ladite décision ou action est autorisée par une loi prévoyant également des mesures visant à protéger les intérêts légitimes de la personne concernée, telles que la possibilité d'être aisément informée de la logique mise en œuvre dans le traitement automatisé de ses données et d'exprimer son point de vue, à moins que cela ne soit incompatible avec la finalité pour laquelle les données sont traitées.

Justification

L'expérience pratique montre que les services répressifs utilisent de plus en plus le traitement automatisé des données qu'il faut donc aborder dans cette décision-cadre. Les décisions fondées uniquement sur le traitement automatisé doivent être soumises à des conditions et à des mesures de protection très strictes lorsqu'elles produisent des effets juridiques à l'égard

de la personne concernée ou lorsqu'elles ont pour elle un impact considérable. Ces décisions ou actions ne doivent être permises que si elles sont expressément prévues par un texte de loi et devraient faire l'objet de mesures appropriées visant à protéger les intérêts de la personne concernée.

Amendement 52
Article 24, paragraphe 1, alinéa 2

Ces mesures doivent assurer, compte tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. ***Les mesures sont réputées nécessaires si l'effort qu'elles supposent n'est pas disproportionné par rapport à l'objectif de protection visé.***	Ces mesures doivent assurer, compte tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Justification

Les mesures techniques et organisationnelles qui assurent la sécurité des données personnelles sont toujours nécessaires et ne doivent pas être liées aux efforts qu'elles engendrent.

Amendement 53
Article 24, paragraphe 2, point j bis) (nouveau)

	j bis) mettre en œuvre des mesures qui permettent systématiquement de contrôler et de faire rapport sur l'efficacité de ces mesures de sécurité (auto-vérification systématique des mesures de sécurité)

Justification

Le traitement automatisé des données doit être systématiquement contrôlé afin d'assurer son efficacité et sa sécurité.

Amendement 54
Article 25, paragraphe 1, partie introductive

1. Les États membres font en sorte que chaque responsable du traitement tienne un registre des traitements ou séries de traitements poursuivant une même finalité	1. Les États membres font en sorte que chaque responsable du traitement tienne un registre ***des accès et*** des traitements ou séries de traitements poursuivant une

ou des finalités liées. Les renseignements devant figurer dans le registre comprennent notamment	même finalité ou des finalités liées. Les renseignements devant figurer dans le registre comprennent notamment

Justification

Le registre doit également enregistrer l'accès aux données.

Amendement 55
Article 26, paragraphe 3

3. ***Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.***	3. ***Lors de l'élaboration de mesures législatives concernant le traitement des données, les autorités de contrôle sont consultées sur les dispositions relatives à la protection des droits et des libertés des personnes.***

Justification

Les autorités de contrôle et non les États membres sont responsables de la protection des droits des personnes lors de l'élaboration de mesures législatives concernant le traitement des données.

Amendement 56
Article 29, paragraphe 2 bis (nouveau)

	2bis. Les États membres font en sorte que les infractions qui sont commises par les parties privées collectant ou traitant des données à caractère personnel dans le cadre d'une fonction publique et qui correspondent à des violations graves des dispositions adoptées en application de la présente décision-cadre, notamment de ses dispositions sur la confidentialité et sur la sécurité des traitements des données, soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

Justification

Lorsque les parties privées collectent et traitent les données dans le cadre d'une fonction publique, elles doivent être soumises à des sanctions pénales pour toute mauvaise utilisation

des données.

Amendement 57
Article 30, paragraphe 4, alinéa 1 bis (nouveau)

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de contrôle de la légalité du traitement des données. Dans toutes les circonstances, la personne concernée est informée de la réalisation d'un contrôle.

Justification

L'autorité de contrôle doit également pouvoir vérifier la légalité du traitement des données et en informer la personne concernée.

Amendement 58
Article 31, paragraphe 2, alinéa 1

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci nomment un représentant commun.	Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente***, conformément aux règles nationales en vigueur applicables à la représentation.*** Lorsqu'un État membre a désigné plusieurs autorités de contrôle, celles-ci nomment un représentant commun.

Justification

La participation du président du groupe établi conformément à l'article 29 de la directive 95/46/CE, aux réunions du nouveau groupe créé par cette décision-cadre permettra de promouvoir la communication et les échanges entre ces deux groupes.

Amendement 59
Article 31, paragraphe 2, alinéa 2 bis (nouveau)

Le président du groupe établi conformément à l'article 29 de la directive 95/46/CE participe aux réunions du groupe ou y est représenté.

Justification

La participation du président du groupe établi conformément à l'article 29 de la directive 95/46/CE, aux réunions du nouveau groupe créé par cette décision-cadre permettra de promouvoir la communication et les échanges entre ces deux groupes.

Amendement 60
Article 31, paragraphe 3

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle des États membres.	3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle des États membres ***et du contrôleur européen de protection des données.***

Justification

Le contrôleur européen de protection des données assurera la cohérence avec les directives relevant du premier pilier.

Amendement 61
Article 34 bis (nouveau)

	Article 34 bis
	Relation avec Europol, Eurojust et le système d'information des douanes
	Au plus tard deux ans après la date mentionnée à l'article 35, paragraphe 1, la Commission soumet des propositions visant à rendre les dispositions relatives à la protection des données applicables à Europol, à Eurojust et au système d'information des douanes et pleinement compatibles avec la présente décision-cadre.

Justification

La proposition prévoit l'exclusion de son champ d'application d'Europol, d'Eurojust et du système d'information des douanes car ceux-ci ont leurs propres systèmes de protection des données personnelles. Étant donné un échange accru des données personnelles, y compris avec Europol et Eurojust, dans la mise en place d'un espace européen de liberté, de sécurité et de justice, il serait incohérent de les exclure. Il faut donc prévoir à terme une convergence entre les principes de protection des données de la présente décision-cadre et Europol, Eurojust et le système d'information des douanes.

EXPOSE DES MOTIFS

1. Introduction

Depuis la création du troisième pilier, le Parlement européen demande des normes de protection des données en matière de coopération judiciaire et policière qui soient comparables aux normes en vigueur dans le droit communautaire. Ces normes devraient par conséquent remplacer les principes actuellement retenus par la Convention 108 et la Recommandation 87 du Conseil de l'Europe. Nous accueillons donc favorablement la proposition de la Commission qui donne suite à la demande parlementaire.

Cet instrument est nécessaire pour deux raisons principales:

- la mise en place d'un espace européen de liberté, de sécurité et de justice engendre l'échange d'un nombre croissant de données, y compris personnelles, dans les domaines couverts par le troisième pilier. Cet échange accru doit se plier aux exigences de l'Union européenne en matière de protection des droits fondamentaux et respecter les articles 7 et 8 de la Charte des droits fondamentaux (respect de la vie privée et protection des données à caractère personnel);

- une meilleure protection des données permettra de renforcer le principe de confiance mutuelle entre les autorités compétentes et contribuera ainsi à un meilleur fonctionnement de la coopération européenne dans les secteurs policier et judiciaire.

La proposition de décision-cadre ([1]) présentée par la Commission revêt une importance particulière eu égard à l'adoption récente de la proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ([2]) . En effet, lors de son adoption, le Parlement européen avait assorti la directive d'une demande explicite concernant la présente décision-cadre:

"...estime que, en ce qui concerne l'accès aux données, la présente directive constitue seulement une première étape nécessaire et demande au Conseil de pratiquer une coopération loyale en vue de l'adoption rapide de garanties appropriées dans le contexte de la décision-cadre sur la protection et le traitement des données au sein de la coopération judiciaire et policière en matière pénale".

2. Relations avec autres propositions (SIS II, VIS, principe de disponibilité)

La proposition de décision-cadre sur la protection des données dans le troisième pilier est liée à plusieurs propositions actuellement à l'examen au Parlement, notamment sur le VIS ([3]), le SIS II ([4]), le principe de disponibilité ([5]) et l'interopérabilité des bases des données européennes dans le domaine JAI ([6]), car celles-ci prévoient des banques de données ou des mesures facilitant l'accès par les autorités compétentes à des données personnelles.

Ainsi les propositions communautaires relatives à VIS et SIS II comportent également une proposition relevant du troisième pilier afin de prévoir l'accès et l'utilisation des données par les autorités policières et judiciaires. Ces propositions devraient désormais faire référence claire aux principes de la présente décision-cadre pour ce qui est de la protection des données personnelles.

C'est pourquoi la présente décision-cadre devrait être adoptée en même temps que la proposition relative au SIS II.

Cette proposition de décision-cadre fait également référence au principe de disponibilité dont l'objet est *"que les informations nécessaires à la lutte contre la criminalité franchissent sans obstacles les frontières intérieures" par un "accès direct en ligne, pour les services répressifs des États membres et pour les agents d'Europol".*

On observe cependant deux obstacles à la disponibilité des données:
"- les écarts entre les niveaux de protection font obstacle à l'échange d'informations confidentielles,
- il n'y a pas de règles communes pour le contrôle de la licéité de l'utilisation des informations obtenues d'un autre État membre et les possibilités de retrouver la source et la finalité des informations sont limitées."

L'adoption de règles communes relatives à la protection des données lorsque celles-ci sont destinées à des fins sécuritaires constitue par conséquent une condition préalable de la mise en place du principe de disponibilité également. Bien évidemment, s'il est essentiel que la présente décision-cadre soit adoptée pour le bon fonctionnement du principe de disponibilité, elle devrait cependant être adoptée sans préjuger des résultats des débats sur ce sujet.

3. Premières orientations du rapporteur

Nous devons assurer la cohérence et l'uniformité des principes de protection des données dans l'Union européenne, y compris entre les premier et troisième piliers. Les principes établis dans la directive 95/46/CE doivent constituer le noyau dur de la législation européenne et fixer les principes généraux de la protection des données.

En tant que rapporteur, je souhaite, dans la mesure du possible, reprendre dans le troisième pilier les principes de protection des données établis par les directives communautaires afin de garantir le même niveau de protection tout en prenant en considération la spécificité du travail policier et judiciaire. Il faut ainsi compléter le dispositif de la directive 95/46/CE en prévoyant des dispositions complémentaires pour ce qui est du ressort de la coopération judiciaire et policière en matière pénale, tout en maintenant la cohérence avec les principes généraux établis par le droit communautaire.

Pour ce faire, il apparaît essentiel que les règles communes de protection des données s'appliquent à l'ensemble des données dans les secteurs policier et judiciaire et ne se limitent pas aux échanges transfrontaliers entre États membres. Je souhaite soutenir un large champ d'application de la décision-cadre afin que les règles européennes soient également appliquées dans le traitement des données à l'intérieur des États membres.

Europol, Eurojust et le système d'information des douanes sont exclus de la proposition de décision-cadre car ils disposent de leurs propres règles de protection des données. Afin d'assurer la cohérence des règles de protection des données, y compris par les agences et organismes créés par l'Union européenne, je souhaite favoriser la convergence des règles spécifiques de ces organes avec la présente décision-cadre.

Je propose donc d'ajouter un nouvel article dans les "dispositions finales" demandant à la Commission de soumettre dans les deux ans une proposition visant à ce que les règles de protection des données soient applicables à Europol, Eurojust et au système d'information des douanes.
La collecte des données doit être limitée à des fins spécifiques et doit respecter les principes de proportionnalité et de nécessité. Ainsi, tout traitement ultérieur des données doit suivre des règles définies, et le transfert ultérieur pour des finalités différentes de celles pour lesquelles les données ont été collectées doit être strictement limité. Je propose de rédiger un nouvel article afin de définir le traitement ultérieur. Par ailleurs, je propose d'inclure à l'article 7 une mesure d'effacement automatique des données personnelles après une période définie.

Les différentes catégories de données (suspects, personnes condamnées, victimes, témoins, etc.) sont traitées différemment et avec des garanties spécifiques. Je propose donc d'ajouter un paragraphe à l'article 4 qui précise que les données liées à des non-suspects doivent être utilisée uniquement pour les fins pour lesquelles elles ont été collectées.

Des garanties supplémentaires doivent être ajoutées à l'article 6 pour l'ADN et les données biométriques afin de garantir la sécurité de la qualité des données et le respect des droits fondamentaux dans l'utilisation de ces données.

Cet instrument nous permet de définir l'accès des autorités compétentes aux données. Nous devons ici définir l'accès aux données conservées par des parties privées comme c'est le cas dans la directive sur la rétention des données. Je propose ainsi d'ajouter un nouvel article après l'article 14 spécifiant que l'accès à ces données sera accordé au cas par cas, pour un objet défini et sous le contrôle judiciaire des États membres.

Pour ce qui est du rôle des parties privées dans la gestion et le traitement des données dans le cadre d'une fonction publique et à des fins de sécurité, je propose de soumettre ces activités à des conditions très strictes, à prévoir par une législation nationale et assorties de sanctions pénales.

Si le transfert de données à des autorités de pays tiers ne peut être complètement exclu dans le cadre de la coopération internationale pour la lutte contre la grande criminalité organisée, il doit cependant être strictement encadré. Premièrement, les données seront transmises à un pays tiers uniquement si celui-ci garantit un niveau adéquat de protection des données. Deuxièmement, la qualité des données reçues d'un pays tiers seront évaluées, y compris au

regard des droits fondamentaux. Ainsi, les données obtenues par la torture ne seront pas exploitées par les autorités européennes.

Nous devons ajouter dans cette décision-cadre la question de l'accès à des décisions automatisées, comme cela est le cas dans d'autres instruments de protection des données. En effet, le nombre croissant de banques de données européennes permet un accès automatisé des autorités à des données collectées par les autorités d'un autre État membre. Or cet accès automatisé ne doit pas mettre en péril les droits fondamentaux. Je propose donc d'insérer un nouvel article précisant qu'une décision ayant un effet sur une personne ne peut pas être prise uniquement sur la base d'un traitement automatisé de données la concernant. En outre, je souhaite clarifier par le biais d'amendements que l'accès et l'utilisation par les autorités de répression compétentes à ces bases de données doivent se faire dans le respect des principes et des dispositions de cette décision-cadre.

---

[1] Proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (SEC(2005)1241) COM(2005)0475-CNS 2005/0202.

[2] Voir le texte adopté par le PE le 14 décembre 2005 (doc. P6_TA-PROV(2005)0512).

[3] Proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (SEC(2004)1628) COM(2005)0835 - COD 2004/0287.

[4] Proposition de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) COM(2005)0236 - COD 2005/0106.
Proposition de règlement du Parlement européen et du Conseil sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) COM(2005)0237 - COD 2005/0010.
Proposition de décision du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) COM(2005)0230 - CNS 2005/0103.

[5] Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité (SEC(2005)1270) COM(2005)0490 - CNS 2005/0207.

[6] Communication de la Commission au Conseil et au Parlement européen sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases COM(2005)0597.