COMMISSION EUROPÉENNE

Bruxelles, le 25.1.2012
COM(2012) 12 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

{SEC(2012) 75 final}

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

1. INTRODUCTION

1.1. Contexte

La décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008[1] (ci-après «la décision-cadre») relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale institue un cadre législatif général pour la protection des données en ce qui concerne la coopération policière et judiciaire en matière pénale. Elle est entrée en vigueur le 19 janvier 2009[2].

Cette décision-cadre était nécessaire car il n'existait pas alors d'instrument général au niveau européen couvrant le traitement des données dans le domaine de la coopération policière et judiciaire en matière pénale[3]. L'article 3 de la directive 95/46/CE relative à la protection des données à caractère personnel et à la libre circulation de celles-ci dispose que la directive ne s'applique pas «au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues [au titre VI] du traité sur l'Union européenne, [ni], en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État […] et les activités de l'État relatives à des domaines du droit pénal».

La décision-cadre a pour but d'assurer à l'échelle de l'UE un niveau élevé de protection des libertés et droits fondamentaux des personnes physiques lors du traitement de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale. Elle vise parallèlement à garantir un niveau élevé de sécurité publique[4]. Elle n'empêche pas les États membres de prévoir des garanties plus rigoureuses afin de protéger les données à caractère personnel collectées ou traitées au niveau national[5].

Le champ d'application[6] de la décision-cadre est limité au traitement à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, des données à caractère personnel qui:

---

1 JO L 350 du 30.12.2008, p. 60.
2 Article 30.
3 Cinquième considérant 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, JO L 281 du 23.11.1995, p. 31.
4 Article 1er.
5 Article 1er, paragraphe 5.
6 Article 1er, paragraphe 2.

- sont ou ont été transmises ou mises à disposition entre les États membres;

- sont ou ont été transmises à des autorités ou des systèmes d'information créés sur la base du titre VI du traité sur l'Union européenne («Coopération policière et judiciaire en matière pénale») ou mises à leur disposition par des États membres; ou

- sont ou ont été transmises aux autorités compétentes des États membres, ou mises à leur disposition, par des autorités ou des systèmes d'information créés sur la base du traité sur l'Union européenne ou du traité instituant la Communauté européenne.

Les données à caractère personnel qui ont été transférées d'un État membre à un autre peuvent également être transférées à des États tiers ou à des instances internationales, pour autant que certaines conditions soient remplies[7].

La décision-cadre s'applique pleinement au Royaume-Uni et à l'Irlande car elle constitue un développement de l'acquis de Schengen. Le Royaume-Uni et l'Irlande sont parties à la décision-cadre, conformément à l'article 5 du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne, annexé au traité sur l'Union européenne et au traité instituant la Communauté européenne, ainsi qu'aux décisions 2000/365/CE et 2002/192/CE du Conseil.

En ce qui concerne l'Islande, la Norvège, la Suisse et le Liechtenstein, la décision-cadre constitue un développement de l'acquis de Schengen au sens de l'accord et des protocoles conclus soit par le Conseil de l'Union européenne soit par l'Union européenne avec l'Islande et la Norvège, la Confédération suisse et le Liechtenstein, et des décisions 1999/437/CE, 2008/149/JAI et 2008/262/JAI du Conseil.

1.2. Teneur de la décision-cadre 2008/977/JAI

Le **champ d'application** de la décision-cadre n'inclut pas le traitement national des données à caractère personnel par les autorités judiciaires ou policières compétentes dans les États membres (article 1er, paragraphe 2).

D'une manière générale, les instruments législatifs sectoriels concernant la coopération policière et judiciaire en matière pénale qui contiennent des dispositions relatives à la protection des données à caractère personnel et ont été adoptés **avant** l'entrée en vigueur de la décision-cadre prévalent sur cette dernière (article 28). Les instruments réputés constituer «un ensemble complet et cohérent de règles» en matière de protection des données ne sont pas affectés par la décision-cadre (considérant 39). D'autres mesures sectorielles comportant des dispositions en matière de protection des données dont le champ d'application est plus limité ne s'appliquent en lieu et place de la décision-cadre que si ces dispositions sont plus restrictives que cette dernière. Dans le cas contraire, c'est la décision-cadre qui s'applique (considérant 40).

La décision-cadre définit les objectifs de la protection des données dans le cadre des activités policières et judiciaires. Elle établit les règles concernant la licéité du traitement des données à caractère personnel afin de garantir que toute information susceptible d'être échangée fasse l'objet d'un traitement licite et conforme aux principes fondamentaux relatifs à la qualité des données.

---

[7] Article 13.

Elle définit par ailleurs les droits des personnes concernées par les données, de manière à garantir la protection des données à caractère personnel sans compromettre la finalité d'une enquête pénale. Pour ce faire, il est nécessaire que les personnes concernées soient informées et aient accès à leurs données à caractère personnel.

Les autorités de contrôle nationales, qui agissent en toute indépendance dans l'exercice des fonctions qui leur sont confiées, sont chargées de conseiller, et de surveiller l'application des mesures nationales de transposition de la décision-cadre.

1.3. L'obligation de la Commission de présenter un rapport sur la mise en œuvre

Conformément à l'article 29, paragraphe 1, de la décision-cadre, les États membres doivent prendre des mesures pour se conformer à la décision en question avant le 27 novembre 2010.

En vertu de l'article 29, paragraphe 2, ils doivent transmettre au secrétariat général du Conseil et à la Commission le texte des dispositions transposant dans leur droit national les obligations qui leur incombent, ainsi que les informations relatives aux autorités de contrôle visées à l'article 25 de la décision-cadre.

La Commission est tenue de préparer un rapport à l'aide des informations communiquées par les États membres. Le Conseil doit, avant le 27 novembre 2011, examiner dans quelle mesure les États membres se sont conformés à cette décision-cadre.

1.4. Sources d'information sur lesquelles se fonde le présent rapport

À la date du **9 novembre 2011**, 26 États membres sur 27, ainsi que le Liechtenstein, la Norvège, l'Islande et la Suisse, avaient envoyé à la Commission les informations relatives à la mise en œuvre de la décision-cadre.

Sur ces **26** États membres, **14** ont indiqué que leur législation en vigueur mettait en œuvre la décision-cadre (la Belgique, la République tchèque, le Danemark, l'Allemagne, l'Estonie, l'Irlande, la Hongrie, la Lettonie, la Lituanie, le Luxembourg, l'Autriche, la Slovaquie, la Suède et le Royaume-Uni). L'Allemagne, l'Irlande, l'Estonie et la Suède ont déclaré qu'elles examinaient encore la nécessité d'adopter d'autres mesures de mise en œuvre.

On peut considérer que **9** États membres ont partiellement mis en œuvre la décision-cadre puisqu'ils affirment devoir encore adopter les textes mettant en œuvre cette dernière.

Quatre États membres ont soit omis de répondre à la demande d'informations de la Commission (la Roumanie), soit indiqué qu'ils n'avaient pas mis en œuvre la décision-cadre (la Grèce, l'Italie[8], Chypre).

---

[8] L'**Italie** a informé la Commission que les instruments spécifiques de mise en œuvre n'avaient pas encore été officiellement adoptés. Elle renvoie au Code relatif à la protection des données à caractère personnel, au Code de procédure pénale ainsi qu'à d'autres actes contenant des dispositions applicables au traitement de données dans ces domaines. D'autres États membres retiennent une approche différente et indiquent que les règles en vigueur en matière de protection des données s'appliquent également au traitement des données à caractère personnel par la police et la justice au niveau national, de même que dans le cadre du traitement transfrontière de données par la police et la justice dans les affaires pénales. Ils ont en outre informé la Commission que des mesures de mise en œuvre supplémentaires étaient actuellement en cours d'élaboration.

La teneur des informations fournies par les États membres en réponse au questionnaire de la Commission varie, en particulier en ce qui concerne leur degré de précision. Le tableau 1 donne un aperçu des réponses fournies: il reflète l'évaluation par les États membres de l'état de la mise en œuvre de la décision-cadre.

2. MISE EN ŒUVRE DE LA DÉCISION-CADRE

2.1. Décision-cadre fondée sur l'article 34, paragraphe 2, point b), du traité sur l'Union européenne

La décision-cadre est fondée sur le traité sur l'Union européenne (TUE), et notamment sur son article 30, son article 31, paragraphe 1, point e), et son article 34, paragraphe 2, point b).

L'instrument juridique dont les décisions-cadres sont le plus proche est la directive, puisqu'elles lient les États membres quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. Les décisions-cadres n'ont toutefois pas d'effet direct[9].

Conformément à l'article 10 du protocole sur les dispositions transitoires relatives aux actes adoptés sur la base des titres V et VI du traité sur l'Union européenne avant l'entrée en vigueur du traité de Lisbonne (protocole n° 36), annexé aux traités, les attributions de la Commission en vertu de l'article 258 du TFUE ne sont pas applicables (et celles de la Cour de justice de l'Union européenne demeurent limitées) en ce qui concerne les actes adoptés au titre de «l'ancien troisième pilier» pendant une période transitoire de cinq ans à compter de l'entrée en vigueur du traité de Lisbonne (c'est-à-dire jusqu'au 1er décembre 2014).

La mise en œuvre de quatre dispositions essentielles de la décision-cadre est exposée plus en détail ci-après sur la base des informations fournies par les États membres en réponse à la demande de la Commission du 9 décembre 2010.

2.1.1. Champ d'application des mesures nationales de mise en œuvre

La décision-cadre s'applique au seul traitement des données à caractère personnel transmises ou mises à disposition entre les États membres (article 1er, paragraphe 2). Le traitement des données à caractère personnel par la police et la justice dans le cadre d'affaires pénales au niveau national ne relève pas de cette décision-cadre.

Le tableau 2 joint en annexe offre un aperçu des mesures de mise en œuvre adoptées par les États membres. La plupart des États membres ont mentionné la législation générale en matière de protection des données comme étant l'une des mesures de mise en œuvre de la décision-cadre et ont renvoyé en outre aux dispositions législatives sectorielles applicables aux services de police, de justice, des douanes et des impôts. Certains États membres ont décidé de ne pas adopter d'instruments législatifs, mais de mettre en œuvre la décision-cadre au moyen de circulaires administratives (l'Allemagne et le Royaume-Uni, par exemple).

---

9 Voir l'arrêt rendu le 16.5.2005 dans l'affaire C-105/03, Pupino, points 34, 43 à 45, 47 et 61, dans lequel la Cour de justice de l'Union européenne a considéré que les juridictions nationales étaient tenues, lorsqu'elles interprétaient la législation nationale, de s'efforcer de parvenir à une interprétation également conforme aux décisions-cadres.

La plupart des États membres ont indiqué que les **données à caractère personnel traitées par les services de police et de justice tant au niveau national que dans un contexte transfrontière[10] étaient soumises à leur législation générale en matière de protection des données dont l'application est souvent concomitante de celle des textes régissant la procédure pénale et les données policières[11].** Treize États membres (la Belgique, la République tchèque, l'Allemagne, l'Estonie, l'Italie, le Luxembourg, la Hongrie, Malte, les Pays-Bas, la Slovénie, la Slovaquie, la Finlande et la Suède) ont renvoyé à leur code de procédure pénale ou à des législations similaires. Sept États membres (la République tchèque, l'Allemagne, la Hongrie, les Pays-Bas, la Slovénie, la Finlande, et la Suède) ont fait part de l'existence d'une loi spéciale sur les données policières[12]. Trois États membres (la Bulgarie, le Portugal et la Lituanie) ont ajouté avoir également adopté une législation spéciale pour mettre en œuvre certaines dispositions de la décision-cadre qui n'étaient pas couvertes par leur législation générale et concernent uniquement le traitement transfrontière de données à caractère personnel[13].

Trois États membres ont considéré que le champ d'application limité de la décision-cadre constituait un problème. L'Italie et les Pays-Bas ont évoqué la difficulté d'établir, dans la pratique, une distinction entre le traitement transfrontière des données conformément à la décision-cadre 2008/977 et le traitement de celles-ci au niveau national, ainsi que la difficulté en découlant pour les autorités répressives nationales de s'adapter à des règles de traitement différentes applicables aux mêmes données à caractère personnel; De manière générale, la Pologne a relevé les lacunes de la décision-cadre et a, notamment, exprimé son soutien à l'objectif poursuivi par la Commission d'instituer un cadre global et d'étendre les règles générales en matière de protection des données au domaine de la coopération policière et judiciaire en matière pénale[14].

2.1.2. Information des personnes concernées par les données (article 16, considérants 26 et 27)

Conformément à la décision-cadre, les États membres doivent veiller à ce que les autorités nationales compétentes informent les personnes concernées que leurs données sont traitées ou ont été transmises à un autre État membre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales. C'est dans le cadre de la législation nationale qu'il convient de fixer la forme et la teneur de cette information, ainsi que la méthode à appliquer à cette fin et les exceptions en la matière (telles que la non-information ou la communication de certaines informations uniquement). Ceci peut se faire sous une forme générale, par l'adoption d'un acte législatif ou la publication de la liste des opérations de traitement. Lorsque des données sont transférées à un autre État membre, chacun des États membres en question peut demander à l'autre de ne pas informer la personne concernée par les données.

---

10 Tel était déjà le cas avant l'adoption de la décision-cadre [voir le document de travail des services de la Commission, Analyse d'impact, SEC(2005)1241 du 4.10.2005, point 5.1.2.].

11 Voir tableau 2.

12 Voir tableau 2.

13 Voir les observations des Pays-Bas.

14 Voir également la contribution de la Pologne (ministère de l'intérieur) à la consultation publique organisée par la Commission à la fin de l'année 2010 (mentionnée dans sa réponse au questionnaire): http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/pl_min_pl.pdf.

Il ressort du tableau 3 que les États membres ont **presque tous** déclaré fournir aux personnes concernées **certaines** informations relatives au traitement de leurs données à caractère personnel. La **France** a indiqué qu'elle ne le faisait pas. Le **Danemark** n'accorde pas non plus ce droit, mais a signalé que le responsable du traitement doit tenir un registre et informer le public.

Ce droit d'information fait l'objet de **limitations dans la grande majorité des États membres.** Soit la législation nationale limite son exercice à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, soit elle en exclut l'application aux traitements de données effectués par certains responsables de cette opération (services de police et/ou services judiciaires). Il arrive que des limitations/exemptions soient prévues sans que les activités concernées ne soient précisées. Un nombre important d'États membres signalent que de telles limitations existent pour la police, la police militaire, les juridictions, les douanes et les services des impôts.

Les **Pays-Bas** ont déclaré que l'obligation générale d'informer la personne concernée par les données n'était pas totalement compatible avec la nature du travail de la police et de la justice, mais que certaines dispositions avaient été prises pour répondre suffisamment à l'obligation d'informer la personne concernée au sujet du traitement de données par les autorités policières et judiciaires (en d'autres termes, les lois énoncent les cas et conditions dans lesquels les données sont traitées; le ministère public informe la personne concernée de l'exercice de pouvoirs d'investigation spéciaux, pour autant que l'intérêt de l'enquête le permette). Les Pays-Bas ont également déclaré qu'il n'était pas nécessaire de mettre en œuvre cette disposition car l'article 16, paragraphe 1, se rapporte uniquement au droit national des États membres.

La décision-cadre institue le droit à l'information des personnes concernées par les données mais ne comporte aucune précision quant à la méthode à employer ou à d'éventuelles exceptions en la matière. Même si, aux dires des États membres, le droit à l'information est généralement accordé, sa mise en œuvre varie considérablement.

2.1.3. Droit d'accès des personnes concernées par les données (article 17)

La décision-cadre prévoit qu'une personne concernée par des données a le droit d'obtenir, sans contrainte et sans délais ni frais excessifs, au moins les informations suivantes:

a) la confirmation du responsable du traitement ou de l'autorité de contrôle nationale que des données la concernant ont été ou non transmises ou mises à disposition et des informations sur les destinataires ou catégories de destinataires auxquels les données ont été communiquées, et la communication des données faisant l'objet du traitement; ou

b) la confirmation de l'autorité de contrôle nationale que toutes les vérifications requises ont été effectuées.

Les États membres peuvent adopter des dispositions législatives limitant ce droit d'accès pour éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires; éviter de nuire à la prévention, à la détection, à la recherche et à la poursuite d'infractions pénales ou pour exécuter des sanctions pénales; protéger la sécurité publique; protéger la sûreté de l'État; et protéger la personne concernée par les données ou les droits et libertés d'autrui (article 17, paragraphe 2). Tout refus opposé par le responsable du traitement de fournir ces informations doit être communiqué par écrit (article 17, paragraphe 3).

Les renseignements relatifs au droit d'accès qui ont été fournis par les États membres et sont consignés dans le tableau 4 reflètent la situation existante en matière de communication d'informations aux personnes concernées par les données. Il en ressort que **tous les États membres[15] accordent dans une certaine mesure un droit d'accès aux personnes concernées par les données**. Ce droit est généralement inscrit dans la législation nationale générale en matière de protection des données. De nombreux États membres réglementent également les modalités du droit d'accès dans la législation sectorielle (comme la législation policière).

De même, les États membres prévoient tous des **dérogations au droit d'accès**. Les motifs les plus fréquemment invoqués pour refuser le droit d'accès sont les suivants:

– la prévention, la recherche, la détection et la poursuite d'infractions pénales;

– la sûreté de l'État, la défense et la sécurité publique;

– les intérêts économiques et financiers d'un État membre et de l'UE (y compris dans les domaines monétaire, budgétaire et fiscal)[16];

– la protection des droits et libertés de la personne concernée par les données ou d'autrui.

En ce qui concerne les **modalités d'accès aux données à caractère personnel**, plusieurs États membres ont explicitement abordé ce sujet, d'autres non. Certains ont indiqué qu'ils accordaient aux personnes concernées le droit d'adresser directement à l'autorité compétente la demande d'accès à leurs données (à savoir l'Autriche, l'Allemagne, la Bulgarie, la Finlande, l'Irlande, la Lettonie, Malte, les Pays-Bas, la Pologne, la Slovaquie, la Suède et le Royaume-Uni), tandis que d'autres n'autorisent qu'un accès «indirect» (la Belgique et la France). Dans ce dernier cas, c'est l'autorité de contrôle nationale qui a accès à toutes les données à caractère personnel relatives à la personne concernée et non cette dernière. En Finlande et en Lituanie, les personnes concernées par les données ont le choix. Au Portugal, l'accès direct constitue la règle générale, mais l'accès indirect est prévu dans les cas où le traitement des données à caractère personnel présente un lien avec la sûreté de l'État, la prévention d'une infraction pénale ou une enquête pénale. La situation est similaire au Luxembourg, où l'accès est généralement accordé directement, mais si l'une des dérogations s'applique, la demande d'accès doit être adressée à l'autorité chargée du contrôle de la protection des données.

La décision-cadre contient des dispositions générales conférant aux personnes concernées le droit de consulter leurs données. Elle ne détaille pas le type d'informations à fournir aux personnes concernées. Elle laisse également aux États membres le soin de décider si ces personnes peuvent exercer ce droit d'accès directement ou si elles doivent le faire par la voie indirecte.

---

15 Il est permis de tirer cette conclusion bien que certains États membres n'aient pas fourni de précisions (voir les détails dans le tableau 3).

16 Cette dérogation n'est pas expressément mentionnée à l'article 17 de la décision-cadre 2008/977. Elle correspond toutefois à une exception énumérée à l'article 13, paragraphe 1, de la directive 95/46/CE.

2.1.4. Autorités de contrôle nationales (article 25)

La décision-cadre 2008/977 reconnaît que la création, dans les États membres, d'autorités de contrôle exerçant leurs fonctions en toute indépendance est «une composante essentielle de la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire entre les États membres» (considérant 33). Elle dispose également que les autorités de contrôle déjà mises en place dans les États membres en vertu de la directive «peuvent aussi» assumer cette responsabilité (considérant 34). L'article 25 de la décision-cadre 2008/977 reproduit une grande partie de la disposition relative aux autorités de contrôle de l'article 28 (paragraphes 1 à 4 et paragraphe 7) de la directive 95/46/CE, qui concerne les pouvoirs attribués à l'autorité ainsi que l'obligation pour celle-ci d'agir en toute indépendance et de respecter le secret professionnel. Chaque autorité doit être investie d'un certain nombre de pouvoirs, incluant des pouvoirs d'investigation (y compris l'accès aux données et la collecte des informations nécessaires), des pouvoirs effectifs d'intervention (comme émettre et publier des avis préalablement à la mise en œuvre des traitements; ordonner le verrouillage, l'effacement ou la destruction de données; interdire temporairement ou définitivement un traitement; adresser un avertissement ou une admonestation au responsable du traitement; saisir les parlements nationaux ou d'autres institutions politiques) et le pouvoir d'ester en justice.

Comme le montre le tableau 5, dans la plupart des cas, les autorités de contrôle nationales chargées de surveiller la mise en œuvre et l'application de la réglementation générale en matière de protection des données ont également pour tâche de surveiller la mise en œuvre et l'application de la décision-cadre 2008/977.

La Suède a indiqué que son conseil national d'inspection des données devait encore être désigné comme l'autorité de contrôle compétente au titre de l'article 25 de la décision-cadre.

Certains États membres ont expressément soulevé le problème du contrôle du traitement de données par le pouvoir judiciaire[17]. Le Danemark a indiqué que l'administration des tribunaux était compétente pour contrôler le traitement de données par le pouvoir judiciaire. Quant à l'Autriche, elle a signalé que l'autorité de contrôle de la protection des données n'était pas compétente pour connaître des réclamations déposées pour violation de la réglementation sur la protection des données par le pouvoir judiciaire. Au Luxembourg, le contrôle du traitement des données incombe d'une manière générale à la Commission nationale pour la protection des données. Les traitements effectués dans le cadre d'une disposition de droit interne appliquant une convention internationale sont contrôlés par une autorité composée du procureur général d'État ou de son adjoint et de deux membres de la Commission nationale pour la protection des données proposés par cette dernière et nommés par le ministre.

2.1.5. Autres questions soulevées par les États membres

Sur 26 États membres, 20 – dont 8 n'ont pas même répondu à cette question (Belgique, Danemark, Estonie, Grèce, Hongrie, Luxembourg, Chypre et Autriche) – n'ont signalé aucun problème particulier tenant à la décision-cadre. Ainsi qu'il ressort du tableau 6, 6 États membres ont formulé des commentaires sur des sujets qui les préoccupent, tels que ceux énumérés ci-après:

---

[17] Voir la dernière phrase du considérant 35 de la décision-cadre, qui dispose que les pouvoirs des autorités de contrôle «ne devraient interférer ni avec les règles spécifiques fixées pour la procédure pénale, ni avec l'indépendance du pouvoir judiciaire».

- la Pologne a considéré que la décision-cadre présentait de nombreuses lacunes auxquelles il convenait de remédier et s'est déclarée favorable à une réforme en vue de l'instauration d'un régime global et cohérent de protection des données au niveau de l'Union;

- l'Italie et les Pays-Bas ont évoqué la difficulté d'établir dans la pratique une distinction entre le traitement transfrontière des données conformément à la décision-cadre 2008/977 et le traitement de celles-ci au niveau national, ainsi que la difficulté en découlant pour les services répressifs nationaux de s'adapter à des règles de traitement différentes applicables aux mêmes données à caractère personnel;

- l'Italie, la République tchèque et les Pays-Bas ont désapprouvé les règles relatives aux transferts internationaux prévues dans la décision-cadre. En particulier, l'Italie a déclaré qu'il était nécessaire de prévoir un niveau adéquat et plus uniforme de protection pour les transferts de données vers des pays tiers. Les Pays-Bas ont considéré comme problématique que la décision-cadre ne fixe pas de critères permettant de déterminer le caractère adéquat de la protection assurée par un pays tiers, ce qui donne lieu à une mise en œuvre hétérogène de celle-ci par les États membres. Quant à la République tchèque, elle a jugé «irréaliste» de prévoir dans la décision-cadre des règles relatives aux transferts internationaux;

- la France a évoqué un problème qui lui est propre en ce qui concerne les durées de conservation des données à caractère personnel transférées à un pays tiers ou reçues d'un tel pays dont les exigences à cet égard sont différentes;

- la Slovaquie a souligné la nécessité d'établir une distinction plus marquée entre le traitement de données par la police et par le pouvoir judiciaire (procédures juridictionnelles);

- la République tchèque et les Pays-Bas ont tous deux indiqué qu'il était déroutant pour les autorités répressives de devoir se conformer à de multiples règles relatives à la protection des données existant aux niveaux international (telles celles édictées par le Conseil de l'Europe), européen et national.

3. PERSPECTIVES

Le présent rapport rend compte de l'état d'avancement de la mise en œuvre et du fonctionnement de la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

Les difficultés pratiques rencontrées par un certain nombre d'États membres pour établir la distinction entre règles applicables respectivement au traitement national de données et au traitement transfrontière de celles-ci pourraient être résolues grâce à un corps unique de règles visant le traitement de données tant au niveau national que dans un contexte transfrontière. Il conviendrait de clarifier davantage, au niveau de l'Union, le champ d'application du droit d'information des personnes concernées par les données ainsi que les éventuelles dérogations à ce droit. La définition de critères harmonisés minimaux en ce qui concerne le droit d'accès des personnes concernées par les données pourrait renforcer les droits de ces personnes tout en prévoyant des dérogations pour permettre aux services de police et de justice de remplir convenablement leurs missions.

En vertu de l'article 16 du traité sur le fonctionnement de l'Union européenne, qui consacre le droit à la protection des données à caractère personnel, il est possible à présent d'instituer un cadre global relatif à la protection des données garantissant à la fois un niveau élevé de

protection des données des personnes physiques dans le domaine de la coopération policière et judiciaire en matière pénale, et des échanges plus fluides des données à caractère personnel entre les autorités nationales policières et judiciaires, dans le respect entier du principe de subsidiarité.