AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur la proposition de la Commission de règlement du Parlement européen et du Conseil concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur («IMI»)

(2012/C 48/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires à la libre circulation de ces données [2],

vu la demande d'avis formulée par la Commission conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 29 août 2011, la Commission a adopté une proposition de règlement («la proposition» ou «la proposition de règlement») du Parlement européen et du Conseil concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur («IMI») [3]. La proposition a été envoyée au CEPD pour consultation le même jour.

2. Avant l'adoption de la proposition, le CEPD a eu la possibilité de présenter des observations informelles sur la proposition et, auparavant, sur la communication de la Commission «Améliorer la gouvernance du marché unique en intensifiant la coopération administrative: Une stratégie pour étendre et développer le système d'information du marché intérieur ("IMI")» («La communication sur la stratégie relative à l'IMI») [4] qui a précédé la proposition. Bon nombre de ces observations ont été prises en compte dans la proposition et, en conséquence, les garanties de protection des données dans la proposition ont été renforcées.

3. Le CEPD se félicite que la Commission l'ait formellement consulté et qu'une référence à cet avis soit incluse dans les considérants de la proposition.

1.2. Objectifs et champ d'application de la proposition

4. L'IMI est un outil informatique qui permet aux autorités compétentes des États membres de s'échanger des informations aux fins de la mise en œuvre de la législation relative au marché intérieur. L'IMI permet aux autorités nationales, régionales et locales des États membres de l'UE de communiquer rapidement et aisément avec leurs homologues dans d'autres pays européens. Cela implique également le traitement de données pertinentes à caractère personnel, y compris de données sensibles.

5. L'IMI a initialement été conçu en tant qu'outil de communication pour l'échange bilatéral d'informations dans le cadre de la directive sur les qualifications professionnelles [5] et à la directive sur les services [6]. L'IMI aide les utilisateurs à identifier la bonne autorité à contacter dans un autre pays et à communiquer avec elle à l'aide de séries de questions et réponses standard prétraduites [7].

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] COM(2011) 522 final.
[4] COM(2011) 75.
[5] Directive 2005/36/CE du Parlement européen et du Conseil du 7 septembre 2005 relative à la reconnaissance des qualifications professionnelles (JO L 255 du 30.9.2005, p. 22).
[6] Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).
[7] À titre d'illustration, une question typique contenant des données sensibles serait par exemple: «Le document joint justifie-t-il légalement l'absence de suspension ou d'interdiction de poursuite des activités professionnelles pertinentes pour faute professionnelle ou infraction grave en ce qui concerne (le professionnel migrant)?».

6. L'IMI est toutefois conçu comme un système horizontal flexible pouvant servir de soutien à plusieurs domaines de la législation relative au marché intérieur et il est envisagé de l'étendre progressivement à l'avenir à d'autres domaines législatifs.

7. Il est également prévu d'étendre les fonctionnalités de l'IMI. Outre l'échange bilatéral d'informations, d'autres fonctionnalités sont également prévues ou mises en œuvre, telles que «les procédures de notification, les mécanismes d'alerte, les modalités d'assistance mutuelle et la résolution des problèmes» ([8]) ainsi que l'établissement d'«un répertoire d'informations auquel les participants de l'IMI pourront ultérieurement se référer» ([9]). Un grand nombre, mais pas l'ensemble, de ces fonctionnalités peuvent également inclure le traitement des données à caractère personnel.

8. La proposition vise à fournir une base juridique claire et un cadre complet de protection des données pour l'IMI.

1.3. **Contexte de la proposition: une approche graduelle pour établir un cadre complet de protection des données pour l'IMI**

9. Au printemps 2007, la Commission a demandé l'avis du groupe de travail «Article 29» sur la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après dénommé «le groupe de l'article 29») sur les implications de l'IMI qui concernent la protection des données. Le 20 septembre 2007, le groupe de l'article 29 a rendu son avis ([10]). Cet avis recommandait à la Commission de fournir une base juridique plus claire et des garanties spécifiques concernant la protection des données dans le cadre de l'IMI. Le CEPD a participé activement aux travaux du sous-groupe chargé de l'IMI et a soutenu les conclusions du groupe de l'article 29.

10. Ensuite, le CEPD a continué à fournir à la Commission des orientations supplémentaires quant à la façon de garantir, progressivement, un cadre plus complet de protection des données pour l'IMI ([11]). Dans le cadre de cette coopération, et depuis qu'il a rendu son avis sur la mise en œuvre de l'IMI ([12]), le 22 février 2008, le CEPD a toujours fait valoir la nécessité d'un nouvel instrument juridique adopté selon la procédure législative ordinaire, afin d'établir un cadre plus complet de protection des données pour l'IMI et garantir la sécurité juridique. La proposition pour un tel instrument juridique est à présent avancée ([13]).

([8]) Voir le considérant 10.

([9]) Voir l'article 13, paragraphe 2.

([10]) Avis 7/2007 sur les questions de protection des données relatives au système d'information sur le marché intérieur (IMI) du groupe de travail «Article 29» sur la protection des données (IMI), WP140. Disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_fr.pdf

([11]) Les documents clés concernant cette coopération sont disponibles sur le site web IMI de la Commission, à l'adresse http://ec.europa.eu/internal_market/imi-net/data_protection_fr.html ainsi que sur le site web du CEPD à l'adresse http://www.edps.europa.eu

([12]) Avis du CEPD concernant la décision 2008/49/CE de la Commission du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du système d'information du marché intérieur (IMI) (JO C 270 du 25.10.2008, p. 1).

([13]) Le groupe de travail «Article 29» prévoit également de présenter des observations sur la proposition. Le CEPD a suivi ces développements au sein du sous-groupe pertinent du groupe de travail «Article 29» et a formulé des observations.

2. **ANALYSE DE LA PROPOSITION**

2.1. **Opinion générale du CEPD sur la proposition et sur les défis majeurs pour la réglementation de l'IMI**

11. Le CEPD a une opinion globalement positive sur l'IMI. Il soutient l'objectif poursuivi par la Commission dans l'établissement d'un système électronique pour l'échange d'informations et la réglementation de ses aspects qui concernent la protection des données. Ce système rationalisé permettra non seulement d'améliorer l'efficacité de la coopération mais aussi de veiller au respect constant des lois applicables à la protection des données. Il peut également le faire grâce à un cadre clair fixant les informations qui peuvent être échangées, par qui et dans quelles conditions.

12. Le CEPD se réjouit également du fait que la Commission a proposé un instrument juridique horizontal pour l'IMI sous la forme d'un règlement du Conseil et du Parlement. Il se félicite que la proposition souligne de façon globale les questions les plus pertinentes en matière de protection des données de l'IMI. Ses observations doivent être lues dans ce contexte positif.

13. Toutefois, le CEPD met aussi en garde contre les risques liés à l'établissement d'un système électronique unique centralisé pour de multiples domaines de coopération administrative. Ces risques comprennent, en particulier, le fait que davantage de données soient échangées d'une façon plus large qu'il n'est strictement indispensable aux fins d'une coopération efficace, et que des informations restent plus longtemps que nécessaire dans le système électronique, y compris des données pouvant être obsolètes et inexactes. La sécurité d'un système d'information accessible dans 27 États membres est également une question délicate, le système n'offrant que le niveau de sécurité de son maillon le plus faible dans le réseau.

Défis majeurs

14. En ce qui concerne le cadre légal pour l'IMI à établir dans la proposition de règlement, le CEPD attire l'attention sur deux défis majeurs:

— la nécessité d'assurer la cohérence du cadre légal tout en respectant la diversité, et

— la nécessité de trouver un équilibre entre flexibilité et sécurité juridique.

15. Ces défis majeurs servent de points de référence important et déterminent, pour une large part, l'approche adoptée par le CEPD dans le présent avis.

Cohérence du cadre légal tout en respectant la diversité

16. Premièrement, l'IMI est un système qui est utilisé dans les 27 États membres. Au stade actuel de l'harmonisation des législations européennes, il existe des différences considérables entre les procédures administratives nationales ainsi qu'entre les lois concernant la protection des données. L'IMI doit être conçu de façon telle que les utilisateurs dans les 27 États membres soient capables de satisfaire à

leurs législations nationales, y compris les lois nationales concernant la protection des données, lors de l'échange des données à caractère personnel par l'intermédiaire de l'IMI. Dans le même temps, les personnes concernées doivent également être rassurées quant au fait que leurs données seront constamment protégées, indépendamment d'un transfert de données par l'intermédiaire de l'IMI vers un autre État membre. La cohérence, tout en respectant la diversité, constitue un défi majeur pour la création de l'infrastructure tant technique que juridique pour l'IMI. Il convient d'éviter une trop grande complexité et une fragmentation. Les opérations de traitement des données dans l'IMI doivent être transparentes et les responsabilités de la prise des décisions concernant la conception du système, sa maintenance journalière et son utilisation, de même que sa surveillance, doivent être clairement établies.

Équilibre entre flexibilité et sécurité juridique

17. Ensuite, contrairement à certains autres systèmes d'information à grande échelle, tels que le système d'information Schengen, le système d'information sur les visas, le système d'information douanier, ou Eurodac, qui sont tous axés sur la coopération dans des domaines spécifiques et clairement définis, l'IMI est un outil horizontal pour l'échange d'informations et peut servir à faciliter l'échange d'informations dans de nombreux domaines politiques différents. Il est également prévu que le champ d'application de l'IMI s'étendra progressivement à d'autres domaines politiques et que ses fonctionnalités pourraient également changer pour inclure des types de coopération administrative non spécifiés à ce jour. Ces éléments distinctifs de l'IMI rendent plus difficile une définition claire des fonctionnalités du système et des échanges d'information pouvant avoir lieu dans le système. Il est dès lors également plus difficile de définir les garanties appropriées de protection des données.

18. Le CEPD reconnaît qu'il existe un besoin de flexibilité et prend note du souhait de la Commission de permettre au règlement de résister «à l'épreuve du temps». Toutefois, cela ne doit pas conduire à un manque de clarté ou de certitude juridique en ce qui concerne les fonctionnalités du système et les garanties de protection des données qui doivent être mises en œuvre. Pour ce motif, la proposition doit, dans la mesure du possible, être plus spécifique et ne pas se contenter de réitérer les principaux principes de la protection des données exposés dans la directive 95/46/CE et dans le règlement (CE) n° 45/2001 ([14]).

2.2. **Champ d'application et développement prévu de l'IMI (articles 3 et 4)**

2.2.1. *Introduction*

19. Le CEPD salue la définition claire offerte par la proposition du champ d'application actuel de l'IMI, avec une énumération à l'annexe I des actes pertinents de l'Union sur la base desquels les informations peuvent être échangées. Cela inclut la coopération dans le cadre de l'application de dispositions spécifiques de la directive sur les qualifications professionnelles, de la directive sur les services et de la directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers ([15]).

20. Une extension du champ d'application de l'IMI étant attendue, les objectifs potentiels de l'extension sont repris à l'annexe II. Les éléments de l'annexe II peuvent être déplacés vers l'annexe I par l'intermédiaire d'un acte délégué à adopter par la Commission à la suite d'une analyse d'impact ([16]).

21. Le CEPD est favorable à cette façon de procéder, qui permet i) de délimiter clairement le champ de l'IMI et ii) d'assurer la transparence, tout en iii) offrant une certaine souplesse au cas où l'IMI serait utilisé à l'avenir pour d'autres échanges d'informations. Cette approche garantit également qu'aucun échange d'informations ne puisse avoir lieu via l'IMI en l'absence i) d'une base juridique appropriée, inscrite dans un acte législatif spécifique relatif au marché intérieur qui permet ou prescrit un échange d'informations ([17]), et ii) d'une mention de cette base juridique dans l'annexe I au règlement.

22. Cela étant dit, des incertitudes demeurent en ce qui concerne le champ de l'IMI, au regard des domaines politiques auxquels l'IMI peut être étendu et au regard des fonctionnalités qui sont ou peuvent être incluses dans l'IMI.

23. Premièrement, il n'est pas exclu que le champ de l'IMI puisse être étendu au-delà des domaines politiques énumérés à l'annexe I et à l'annexe II. Une telle extension peut se produire si l'utilisation de l'IMI est prévue pour certains échanges d'informations non dans un acte délégué de la Commission mais dans un acte adopté par le Parlement et le Conseil dans un cas où cela n'a pas été prévu à l'annexe II ([18]).

([14]) Voir également, à cet égard, nos observations à la section 2.2 concernant l'extension prévue de l'IMI

([15]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

([16]) Le projet de règlement ne fait pas lui-même référence à une analyse d'impact. Toutefois, la page 7 de l'exposé des motifs de la proposition explique que la Commission sera habilitée, «à la suite d'une évaluation de la faisabilité technique, du rapport coût-efficacité, de la convivialité et de l'incidence globale sur le système, de même que, le cas échéant, des résultats d'une phase de test éventuelle», à déplacer des éléments de l'annexe II vers l'annexe I, en adoptant un acte délégué.

([17]) À l'exception de SOLVIT [voir l'annexe II, paragraphe I, point 1)], où seules des «normes juridiques non contraignantes», une recommandation de la Commission, sont disponibles. Du point de vue de la protection des données, selon le CEPD, dans le cas spécifique de SOLVIT, la base juridique du traitement peut être le «consentement» des personnes concernées.

([18]) Cela peut se produire à l'initiative de la Commission, mais il n'est pas exclu que l'idée d'utiliser l'IMI dans un domaine politique spécifique puisse surgir ultérieurement dans le processus législatif et puisse être proposée par le Parlement ou le Conseil. Cela s'est déjà produit dans le passé en ce qui concerne la directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers. Une plus grande clarté serait nécessaire pour un tel cas en ce qui concerne la «procédure» d'extension qui semble ne s'être concentrée que sur le cas d'une extension via les actes délégués (voir les dispositions sur l'analyse d'impact, actes délégués, mise à jour de l'annexe I).

24. Ensuite, alors que l'extension du champ à de nouveaux domaines politiques peut, dans certains cas, ne requérir que peu ou pas de changement dans les fonctionnalités existantes du système ([19]), d'autres extensions peuvent nécessiter des fonctionnalités nouvelles et différentes, ou d'importantes modifications à apporter aux fonctionnalités existantes:

— bien que la proposition fasse référence à plusieurs fonctionnalités existantes ou prévues, ces références sont souvent trop peu claires ou trop peu détaillées. Cela s'applique, à divers degrés, aux références aux mécanismes d'alerte, aux acteurs externes, aux répertoires d'informations, aux modalités d'assistance mutuelle et à la résolution des problèmes ([20]). À titre d'illustration, le terme «alerte», qui fait référence à une fonctionnalité majeure existante n'est mentionné qu'une seule fois, au considérant 10;

— aux termes de la proposition de règlement, il est possible d'adopter de nouveaux types de fonctionnalités qui ne sont pas du tout mentionnés dans la proposition;

— l'IMI a jusqu'à présent été décrit comme un outil informatique pour l'échange d'informations: en d'autres termes, un outil de communication (voir, par exemple, l'article 3 de la proposition). Certaines des fonctionnalités visées dans la proposition, y compris la fonction de «répertoire d'informations», cependant, semblent dépasser ce cadre. L'élargissement proposé des délais de conservation des données à une période de cinq ans suggère également un rapprochement d'une «base de données». Ces développements modifieraient de façon fondamentale le caractère de l'IMI ([21]).

2.2.2. *Recommandations*

25. Pour pallier ces incertitudes, le CEPD recommande une double approche. Il propose, premièrement, que les fonctionnalités qui sont déjà prévisibles soient clarifiées et traitées de façon plus spécifique et, deuxièmement, que des garanties procédurales adéquates soient appliquées pour s'assurer que la protection des données sera également soigneusement prise en considération durant le futur développement de l'IMI.

Clarification des fonctionnalités déjà disponibles ou prévisibles (par exemple, des échanges bilatéraux, des mécanismes d'alertes, des répertoires, la résolution des problèmes et des acteurs externes)

26. Le CEPD recommande que le règlement soit plus spécifique en ce qui concerne les fonctionnalités lorsqu'elles sont déjà connues, comme dans le cas des échanges d'informations visés aux annexes I et II.

27. Par exemple, des mesures plus spécifiques et plus claires pourraient être prévues pour l'intégration de SOLVIT ([22]) dans l'IMI (dispositions relatives aux «acteurs externes» et à la «résolution de problèmes») et pour les répertoires de professionnels et de prestataires de services (dispositions relatives aux «répertoires»).

28. Des éclaircissements supplémentaires devraient également être apportés en ce qui concerne les «alertes» qui sont déjà en usage aux termes de la directive sur les services et pourraient l'être aussi à d'autres domaines politiques. Plus particulièrement, l'«alerte», en tant que fonctionnalité, devrait être clairement définie à l'article 5 (ainsi que d'autres fonctionnalités, telles que les échanges bilatéraux d'informations et les répertoires). Les droits d'accès et les délais de conservation pour les alertes doivent également être clarifiés ([23]).

Garanties procédurales (analyse de l'impact de la protection des données et consultation des autorités chargées de la protection des données)

29. Si l'objectif est de s'assurer que le règlement résiste «à l'épreuve du temps» en termes de fonctionnalités supplémentaires pouvant s'avérer nécessaires à plus long terme et, dès lors, de permettre des fonctionnalités supplémentaires non encore définies dans le règlement, cette approche doit s'accompagner des garanties procédurales adéquates afin de veiller à ce que des dispositions appropriées seront établies pour mettre en œuvre les garanties nécessaires de protection des données avant le déploiement de la nouvelle fonctionnalité. Il en va de même pour les élargissements à de nouveaux domaines politiques lorsqu'il en résulte un impact sur la protection des données.

30. Le CEPD recommande un mécanisme clair qui veille à ce que, avant chaque extension de fonctionnalités ou avant des élargissements à de nouveaux domaines politiques, les préoccupations relatives à la protection des données soient soigneusement évaluées et, si nécessaires, à ce que des garanties ou mesures techniques supplémentaires soient mises en œuvre dans l'architecture de l'IMI. En particulier:

— l'analyse d'impact visée à la page 7 de l'exposé des motifs doit être spécifiquement requise dans le règlement proprement dit et doit également inclure une analyse d'impact de la protection des données devant spécifiquement traiter des modifications dans l'architecture de l'IMI qui, le cas échéant, sont nécessaires pour veiller à ce qu'elle contienne toujours les garanties adéquates de protection des données couvrant également les nouveaux domaines politiques et/ou fonctionnalités;

— le règlement doit spécifiquement prévoir que la consultation du CEPD et des autorités nationales de protection des données est requise avant chaque élargissement de l'IMI. Cette consultation peut avoir lieu au moyen du mécanisme prévu à l'article 20 pour la surveillance coordonnée.

([19]) Par exemple, les échanges bilatéraux d'informations dans le cadre de la directive relative aux qualifications professionnelles et la directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers suivent essentiellement la même structure et peuvent être intégrés à l'aide de fonctionnalités similaires sous réserve de garanties similaires en matière de protection des données.

([20]) Voir les considérants 2, 10, 12, 13, 15 et les articles 5, point b), 5, point i), 10, paragraphe 7, et 13, paragraphe 2.

([21]) Il convient de noter par ailleurs que s'il existe une intention de faire en sorte que l'IMI remplace/complète les systèmes existants de traitement et d'archivage des dossiers et/ou d'utiliser l'IMI comme base de données, cette intention doit être exprimée plus clairement à l'article 3.

([22]) Voir l'annexe II, paragraphe I, point 1).

([23]) Voir les sections 2.4 et 2.5.5 ci-dessous.

31. Ces garanties procédurales (analyse d'impact de la protection des données et consultation) doivent s'appliquer à l'élargissement tant via un acte délégué de la Commission (déplacement d'un élément de l'annexe II vers l'annexe I) que via un règlement du Parlement et du Conseil incluant un article non repris à l'annexe II.

32. Enfin, le CEPD recommande que le règlement clarifie si le champ d'application des actes délégués que la Commission sera habilitée à adopter conformément à l'article 23 inclura toute autre question en plus du déplacement d'éléments de l'annexe II vers l'annexe I. Si c'est possible, la Commission doit être habilitée, dans le règlement, à adopter des actes d'exécution ou délégués spécifiques afin de définir davantage toute fonctionnalité supplémentaire du système ou traiter de toute préoccupation relative à la protection des données qui pourrait se présenter à l'avenir.

2.3. **Rôles, compétences et responsabilités (articles 7 à 9)**

33. Le CEPD relève avec satisfaction qu'un chapitre complet (chapitre II) a été consacré à la clarification des fonctions et des responsabilités des différents acteurs impliqués dans l'IMI. Les dispositions pourraient encore être renforcées comme suit.

34. L'article 9 décrit les responsabilités qui résultent du rôle de la Commission en tant que responsable du traitement. Le CEPD recommande en outre l'inclusion d'une disposition supplémentaire faisant référence au rôle de la Commission consistant à veiller à ce que le système soit conçu en appliquant les principes de «respect de la vie privée dès la conception» ainsi qu'à son rôle de coordination en ce qui concerne les questions de protection des données.

35. Le CEPD se réjouit de constater que les tâches des coordinateurs IMI reprises à l'article 7 incluent à présent spécifiquement les tâches de coordination relatives à la protection des données, y compris le fait d'agir en qualité d'interlocuteur de la Commission. Il recommande de préciser davantage que ces tâches de coordination incluent également des contacts avec les autorités nationales chargées de la protection des données.

2.4. **Droits d'accès (article 10)**

36. L'article 10 prévoit des garanties en ce qui concerne les droits d'accès. Le CEPD se réjouit du fait qu'à la suite de ses observations, ces dispositions aient été significativement renforcées.

37. Compte tenu de la nature horizontale et extensible de l'IMI, il est important de veiller à ce que le système garantisse l'application de «murailles de Chine» qui confinent les informations traitées dans un domaine politique à ce seul domaine politique: les utilisateurs IMI ne doivent i) avoir accès aux informations que selon le principe du «besoin d'en connaître» et ii) ces informations doivent être restreintes à un seul domaine politique.

38. S'il est inévitable qu'un utilisateur IMI soit autorisé à accéder à des informations pour plusieurs domaines politiques (tel pourrait être le cas, par exemple, dans certains bureaux gouvernementaux locaux), le système ne devrait à tout le moins pas permettre la combinaison d'informations provenant de différents domaines politiques. Des exceptions doivent, si nécessaires, être exposées dans un cadre législatif d'exécution ou un acte de l'Union, en respectant strictement le principe de la limitation des finalités.

39. Ces principes sont à présent énoncés dans le texte du règlement mais pourraient être encore renforcés et précisés.

40. En ce qui concerne les droits d'accès par la Commission, le CEPD se réjouit du fait que l'article 9, paragraphes 2 et 4, et l'article 10, paragraphe 6, de la proposition, considérés conjointement, spécifient que la Commission n'aura pas accès aux données à caractère personnel échangées entre les États membres sauf dans les cas où la Commission est désignée en tant que participante à une procédure de coopération administrative.

41. Les droits d'accès par des acteurs externes et le droit d'accès aux alertes doivent également être spécifiés davantage ([24]). En ce qui concerne les alertes, le CEPD recommande que le règlement dispose que les alertes ne doivent pas, par défaut, être envoyées à toutes les autorités compétentes pertinentes de tous les États membres, mais uniquement à celles concernées selon le principe du «besoin d'en connaître». Cela n'exclut pas l'envoi d'alertes à tous les États membres dans certains cas spécifiques ou dans certains domaines politiques spécifiques, s'ils sont tous concernés. De même, une analyse au cas par cas est nécessaire pour décider si la Commission doit avoir accès aux alertes.

2.5. **Conservation des données à caractère personnel (articles 13 et 14)**

2.5.1. *Introduction*

42. L'article 13 de la proposition étend le délai de conservation des données dans l'IMI du délai de six mois actuellement en vigueur (à compter de la clôture du dossier) à un délai de cinq ans, les données étant «verrouillées» après dix-huit mois. Durant la période de «verrouillage», les données ne sont accessibles que selon une procédure d'extraction spécifique, qui ne peut être engagée qu'à la demande de la personne concernée ou «à la seule fin de prouver l'existence d'un échange d'informations via l'IMI».

43. En fait, les données sont donc conservées dans l'IMI durant trois périodes distinctes:

— du téléchargement à la clôture du dossier;

— de la clôture du dossier et pendant une période de 18 mois ([25]);

— à partir de l'expiration du délai de 18 mois, sous une forme verrouillée, et pendant une nouvelle période de trois ans et six mois (en d'autres termes, jusqu'à l'expiration d'un délai de cinq ans à compter de la clôture du dossier).

([24]) Voir également la section 2.2.2.

([25]) L'article 13, paragraphe 1, suggère que 18 mois constituent un délai «maximum»; dès lors, un délai plus court peut également être établi. Cela n'aurait toutefois pas d'incidence sur la durée totale de la conservation qui, en tout état de cause, aurait une durée de cinq ans à compter de la clôture du dossier.

44. En dehors de ces règles générales, l'article 13, paragraphe 2, permet la conservation des données dans un «répertoire d'informations» aussi longtemps qu'il est nécessaire à cette fin, soit moyennant le consentement de la personne concernée, soit lorsqu'«un acte de l'Union l'impose». En outre, l'article 14 prévoit un mécanisme de verrouillage similaire pour la conservation des données à caractère personnel des utilisateurs IMI, pendant cinq ans, à compter de la date à laquelle ils cessent d'être des utilisateurs IMI.

45. Il n'y pas d'autres dispositions spécifiques. Dès lors, les règles générales sont vraisemblablement supposées s'appliquer non seulement aux échanges bilatéraux mais aussi aux alertes, à la résolution des problèmes [comme dans SOLVIT ([26])] et à toutes les autres fonctionnalités impliquant le traitement de données à caractère personnel.

46. Le CEPD formule plusieurs préoccupations concernant les délais de conservation, à la lumière de l'article 6, paragraphe 1, point e), de la directive 95/46/CE et de l'article 4, paragraphe 1, point e), du règlement (CE) n° 45/2001, qui prescrivent tous deux que des données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées.

2.5.2. *Du téléchargement à la clôture du dossier: la nécessité d'une clôture opportune du dossier*

47. En ce qui concerne la première période, du téléchargement à la clôture du dossier, le CEPD est préoccupé par le risque que certains dossiers ne puissent jamais être clôturés, ou ne soient clôturés qu'après un délai exagérément long. Il peut en résulter une conservation plus longue que nécessaire, voire illimitée, de certaines données à caractère personnel.

48. Le CEPD comprend que la Commission a réalisé des progrès, au niveau pratique, pour réduire l'arriéré dans l'IMI et qu'un système est en place pour les échanges bilatéraux afin de surveiller la clôture opportune des dossiers et rappeler périodiquement ceux qui traînent. En outre, une nouvelle modification apportée aux fonctionnalités du système, à la suite d'une approche de «respect de la vie privée dès la conception» permet, en appuyant sur un seul bouton, d'accepter une réponse ainsi que de clôturer, en même temps, le dossier. Précédemment, deux étapes distinctes étaient nécessaires, ce qui peut expliquer certains des dossiers dormants restés dans le système.

49. Le CEPD salue ces efforts réalisés au niveau pratique. Toutefois, il recommande que le texte du règlement lui-même prévoie des garanties selon lesquelles les dossiers seront clôturés en temps opportun et les dossiers dormants (dossiers sans activité récente) seront supprimés de la base de données.

([26]) Voir l'annexe II, paragraphe I, point 1).

2.5.3. *De la clôture du dossier et pendant une période de 18 mois: l'extension du délai de six mois se justifie-t-il?*

50. Le CEPD invite à reconsidérer s'il existe une justification adéquate pour l'extension du délai actuel de six mois à 18 mois après la clôture d'un dossier et, si elle existe, à reconsidérer si cette justification s'applique aux seuls échanges d'informations bilatéraux ou à d'autres types de fonctionnalités également. L'IMI existe à présent depuis plusieurs années et il convient de tirer avantage de l'expérience pratique accumulée à cet égard.

51. Si l'IMI demeure un outil d'échange d'informations (par opposition à un système de traitement des dossiers, à une base de données ou à un système d'archivage), et à condition en outre que les autorités compétentes disposent de moyens permettant d'extraire du système les informations qu'elles ont reçues [soit par voie électronique, soit sur support papier, mais en tout état de cause d'une façon leur permettant d'utiliser les informations extraites en tant qu'éléments de preuve ([27])], il ne semble pas absolument nécessaire de conserver les données dans l'IMI après la clôture du dossier.

52. Dans les échanges d'informations bilatéraux, la nécessité éventuelle de demander de plus amples informations même lorsqu'une réponse a été acceptée, et donc, lorsqu'un dossier a été clôturé, peut éventuellement justifier un délai de conservation (raisonnablement court) après la clôture d'un dossier. Le délai actuel de six semaines semble de prime abord suffisamment généreux à cet effet.

2.5.4. *De 18 mois à cinq ans: données «verrouillées»*

53. Le CEPD considère que la Commission n'a pas non plus fourni de justification suffisante de la nécessité et de la proportionnalité de la conservation de «données verrouillées» pendant une période allant jusqu'à cinq ans.

54. L'exposé des motifs, à la page 8, fait référence à l'arrêt rendu par la Cour de justice dans l'affaire *Rijkeboer* ([28]). Le CEPD recommande que la Commission reconsidère les implications de cette affaire pour la conservation des données dans l'IMI. Selon lui, l'affaire *Rijkeboer* ne requiert pas une configuration de l'IMI pour une conservation des données pendant cinq ans après la clôture des dossiers.

55. Le CEPD ne considère pas la référence à l'arrêt *Rijkeboer* ou aux droits des personnes concernées d'avoir accès à leurs données comme une justification suffisante et adéquate pour la conservation des données dans l'IMI pendant cinq ans après la clôture des dossiers. La simple conservation des «données du registre» (définies de façon stricte pour exclure tout contenu, notamment, toute annexe ou donnée sensible) peut être une option moins intrusive qui mérite une plus grande attention. Toutefois, le CEPD n'est pas convaincu, à ce stade, que même cette mesure soit nécessaire ou proportionnée.

([27]) Nous savons que des efforts ont été consentis afin d'offrir cette garantie au niveau pratique.

([28]) C-553/07 *Rijkeboer* [2009] Rec. p. I-3889.

56. En outre, l'absence de clarté concernant la personne pouvant accéder aux «données verrouillées» et à quelles fins est également problématique. La simple référence à une utilisation «à la seule fin de prouver l'existence d'un échange d'informations» (comme à l'article 13, paragraphe 3) n'est pas suffisante. Si la disposition concernant le «verrouillage» est retenue, il convient en tout état de cause de mieux spécifier qui peut demander une preuve de l'échange d'informations et dans quel contexte. Outre la personne concernée, d'autres seraient-elles habilitées à demander l'accès? Le cas échéant, celles-ci seraient-elles uniquement les autorités compétentes, et à la seule fin de prouver qu'un échange particulier d'informations avec un contenu particulier a eu lieu (au cas où cet échange serait contesté par les autorités compétentes qui ont envoyé ou reçu le message)? D'autres utilisations éventuelles «à la seule fin de prouver l'existence d'un échange d'informations» sont-elles prévues ([29])?

2.5.5. *Alertes*

57. Le CEPD recommande d'établir une distinction plus claire entre les alertes et les répertoires d'informations. Utiliser une alerte en tant qu'outil de communication pour alerter les autorités compétentes sur un méfait ou un soupçon particulier est une chose, et conserver cette alerte dans une base de données ou pour une période prolongée, voire indéfinie, en est une autre. La conservation d'informations relatives aux alertes susciterait des préoccupations supplémentaires et nécessiterait des règles spécifiques ainsi que des garanties supplémentaires de protection des données.

58. Par conséquent, le CEPD recommande que le règlement dispose, en tant que règle par défaut, que i) sauf spécification contraire dans la législation verticale, et sous réserve des garanties supplémentaires adéquates, un délai de conservation de six mois doit s'appliquer aux alertes et, élément important, que ii) ce délai doit être comptabilisé à partir de l'envoi de l'alerte.

59. À titre subsidiaire, le CEPD recommande que des garanties détaillées, en ce qui concerne les alertes, soient spécifiquement exposées dans la proposition de règlement. Le CEPD est disposé à apporter son assistance à la Commission et aux législateurs par un autre avis à cet égard, au cas où cette seconde approche serait suivie.

2.6. **Catégories particulières de données (article 15)**

60. Le CEPD salue la distinction établie entre les données à caractère personnel visées à l'article 8, paragraphe 1, de la directive 95/46/CE, d'une part, et les données à caractère personnel visées à l'article 8, paragraphe 5, d'autre part. Il se réjouit également que le règlement spécifie clairement que le traitement des catégories particulières de données est uniquement autorisé sur la base d'un motif spécifique mentionné à l'article 8 de la directive 95/46/CE.

61. À cet égard, le CEPD considère que l'IMI traitera un volume important de données sensibles relevant de l'article 8, paragraphe 2, de la directive 95/46/CE. En effet, depuis le tout début, lorsqu'il a d'abord été déployé pour soutenir la coopération administrative aux termes des directives sur les services et les qualifications professionnelles, l'IMI a été conçu pour traiter de telles données, notamment les données relatives aux registres des infractions pénales et administratives pouvant avoir une incidence sur le droit des professionnels ou des prestataires de services d'exécuter des travaux/services dans un autre État membre.

62. En outre, un volume important de données sensibles aux termes de l'article 8, paragraphe 1 (essentiellement des données liées à la santé), seront également susceptibles d'êtres traitées dans l'IMI lorsqu'il s'élargira de façon à inclure un module pour SOLVIT ([30]). Enfin, il n'est pas exclu que des données sensibles supplémentaires puissent être collectées par l'intermédiaire de l'IMI à l'avenir, sur une base ad hoc ou systématique.

2.7. **Sécurité (article 16 et considérant 16)**

63. Le CEPD se réjouit de constater que l'article 16 fait spécifiquement référence à l'obligation de la Commission de se conformer à ses propres règles internes adoptées sur la base de l'article 22 du règlement (CE) n° 45/2001 ainsi que d'adopter et d'actualiser un plan de sécurité pour l'IMI.

64. Afin de renforcer davantage ces dispositions, le CEPD recommande que le règlement exige une évaluation des risques et un examen du plan de sécurité avant chaque élargissement de l'IMI à un nouveau domaine politique ou avant l'ajout d'une nouvelle fonctionnalité exerçant un impact sur les données à caractère personnel ([31]).

65. En outre, le CEPD note également que l'article 16 et le considérant 16 font uniquement référence aux obligations de la Commission et au rôle de surveillance du CEPD. Cette référence peut être trompeuse. S'il est vrai que la Commission est l'opérateur du système et, en tant que tel, est responsable d'une part prédominante du maintien de la sécurité dans l'IMI, les autorités compétentes ont également des obligations qui, à leur tour, font l'objet d'une surveillance de la part des autorités nationales chargées de la protection des données. Dès lors, l'article 16 et le considérant 16 doivent également faire référence aux obligations en matière de sécurité applicables au reste des acteurs IMI conformément à la directive 95/46/CE et aux pouvoirs de surveillance des autorités nationales chargées de la protection des données.

2.8. **Information des personnes concernées et transparence (article 17)**

2.8.1. *Informations fournies dans les États membres*

66. En ce qui concerne l'article 17, paragraphe 1, le CEPD recommande des dispositions plus spécifiques dans le règlement afin de veiller à ce que les personnes concernées soient pleinement informées du traitement de leurs données dans l'IMI. Étant donné que l'IMI est utilisé par de multiples autorités compétentes, y compris de nombreux bureaux gouvernementaux locaux ne disposant pas de ressources suffisantes, il est fortement recommandé que l'obligation de notification soit coordonnée au niveau national.

([29]) Bien que la conservation des données à caractère personnel pose comparativement moins de risques pour la protection de la vie privée, le CEPD considère néanmoins que la conservation des données à caractère personnel des utilisateurs de l'IMI pendant une période de cinq ans, une fois qu'ils n'ont plus accès à l'IMI, n'a pas été suffisamment justifiée non plus.

([30]) Voir l'annexe II, paragraphe I, point 1).

([31]) Voir également la section 12 sur les recommandations concernant les audits.

2.8.2. *Informations fournies par la Commission*

67. L'article 17, paragraphe 2, point a), requiert que la Commission mette à disposition un avis sur le respect de la vie privée concernant ses propres activités de traitement des données, aux termes des articles 10 et 11 du règlement (CE) n° 45/2001. En outre, l'article 17, paragraphe 2, point b), requiert que la Commission mette également à disposition des informations sur «les aspects des procédures de coopération administrative dans l'IMI visées à l'article 12 relatives à la protection des données». Enfin, l'article 17, paragraphe 2, point c), requiert que la Commission mette à disposition des informations sur «les exceptions ou limitations aux droits des personnes concernées, visées à l'article 19».

68. Le CEPD se réjouit de constater que ces dispositions contribuent à la transparence des opérations de traitement des données dans l'IMI. Ainsi qu'il est noté dans la section 2.1 ci-dessus, dans le cas d'un système informatique utilisé dans 27 États membres différents, il est capital de garantir la cohérence en ce qui concerne le fonctionnement du système, les garanties de protection des données appliquées et les informations qui sont fournies aux personnes concernées ([32]).

69. Cela étant dit, les dispositions de l'article 17, paragraphe 2, doivent être encore renforcées. La Commission, en tant qu'opérateur du système, est la mieux placée pour jouer un rôle proactif en fournissant un premier «niveau» de notification de protection des données et d'autres informations pertinentes aux personnes concernées sur son site web multilingue, ainsi que «pour le compte» des autorités compétentes, c'est-à-dire couvrant les informations requises aux termes de l'article 10 ou 11 de la directive 95/46/CE. Il serait alors souvent suffisant que les avis fournis par les autorités compétentes dans les États membres fassent simplement référence à l'avis fourni par la Commission, en ne la complétant que dans la mesure du nécessaire pour satisfaire à toute information supplémentaire spécifique, requise aux termes de la législation nationale.

70. En outre, l'article 17, paragraphe 2, point b), doit préciser que les informations fournies par la Commission couvriront de manière exhaustive tous les domaines politiques, toutes les procédures de coopération administrative et toutes les fonctionnalités dans l'IMI et incluront également de façon spécifique les catégories de données qui peuvent être traitées. Cela doit également inclure la publication des ensembles de questions utilisées dans la coopération bilatérale sur le site web de l'IMI telle qu'elle a lieu actuellement, dans la pratique.

2.9. **Droits d'accès, de rectification et d'effacement (article 18)**

71. Le CEPD souhaiterait faire à nouveau référence, ainsi qu'il est noté dans la section 2.1 ci-dessus, au fait qu'il est capital de garantir la cohérence en ce qui concerne le fonctionnement du système et des garanties de protection des données appliquées. Pour ce motif, le CEPD souhaiterait spécifier davantage les dispositions sur les droits d'accès, de rectification et d'effacement.

72. L'article 18 doit spécifier à qui les personnes concernées doivent adresser une demande d'accès. Cela doit être clair en ce qui concerne l'accès aux données durant les différentes périodes:

— avant la clôture du dossier,

— après la clôture du dossier mais avant l'expiration du délai de conservation de 18 mois,

— et enfin, pendant la période durant laquelle les données sont «verrouillées».

73. Le règlement doit également requérir des autorités compétentes qu'elles coopèrent en ce qui concerne les demandes d'accès dans la mesure du nécessaire. La rectification et l'effacement doivent être réalisés «dès que possible mais dans un délai maximum de 60 jours» plutôt que «dans les 60 jours». Il devrait également être fait référence à la possibilité de créer un module de protection des données et développer des solutions du respect de la vie privée dès la conception pour la coopération entre les autorités en ce qui concerne les droits d'accès, ainsi que «l'autonomisation des personnes concernées», par exemple en leur donnant un accès direct à leur données, le cas échéant et lorsque c'est réalisable.

2.10. **Contrôle (article 20)**

74. Ces dernières années, le modèle de «surveillance coordonnée» a été élaboré. Ce modèle de surveillance, tel qu'il est à présent opérationnel dans Eurodac et dans certaines parties du système d'information douanier, a également été adopté pour le système d'information sur les visas (VIS) et le système d'information Schengen de deuxième génération (SIS-II).

75. Ce modèle a trois niveaux:

— la surveillance au niveau national est assurée par les autorités nationales de protection des données;

— la surveillance au niveau de l'UE est assurée par le CEPD;

— la coordination est assurée au moyen de réunions régulières et autres activités coordonnées soutenues par le CEPD en qualité de secrétariat de ce mécanisme de coordination.

76. Ce modèle s'est avéré efficace et a produit d'excellents résultats. Son utilisation devrait être envisagée à l'avenir pour d'autres systèmes d'information.

77. Le CEPD salue le fait que l'article 20 de la proposition prévoie spécifiquement une surveillance coordonnée entre les autorités nationales de protection des données et le CEPD selon — d'une manière générale — le modèle établi dans les règlements VIS et SIS II ([33]).

([32]) Cette approche visant à garantir la cohérence doit, bien sûr, prendre dûment en considération toutes divergences nationales lorsque cela s'avère nécessaire et justifié.

([33]) Voir le règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28.12.2006, p. 4) et le règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (JO L 218 du 13.8.2008, p. 60).

78. Le CEPD souhaiterait un renforcement des dispositions relatives à la surveillance coordonnée sur certains points et soutiendrait, à cet effet, des dispositions similaires à celles qui sont en place par exemple dans le contexte du système d'information sur les visas (articles 41 à 43 du règlement VIS), Schengen II (articles 44 à 46 du règlement SIS II) et envisagées pour Eurodac ([34]). Plus particulièrement, il serait utile que le règlement:

— à l'article 20, paragraphes 1 et 2, fixe et répartisse plus clairement les tâches de surveillance respectives des autorités nationales de protection des données et du CEPD ([35]);

— à l'article 20, paragraphe 3, spécifie que les autorités nationales de protection des données et le CEPD, agissant chacun dans les limites de leurs compétences respectives, «coopèrent activement» et «assurent une surveillance coordonnée du système IMI» (au lieu de faire simplement référence à la surveillance coordonnée sans mentionner de coopération active) ([36]); et

— spécifie, de façon plus détaillée, ce que la coopération peut inclure, par exemple, en exigeant que les autorités nationales de protection des données et le CEPD, «agissant chacun dans les limites de leurs compétences respectives, échangent les informations utiles, s'assistent mutuellement pour mener les audits et inspections, examinent les difficultés d'interprétation ou d'application du règlement IMI, étudient les problèmes pouvant se poser lors de l'exercice du contrôle indépendant ou dans l'exercice des droits de la personne concernée, formulent des propositions harmonisées en vue de trouver des solutions communes aux éventuels problèmes et assurent, si nécessaire, la sensibilisation aux droits en matière de protection des données» ([37]).

79. Cela étant dit, le CEPD est conscient de la taille actuellement réduite, de la nature différente des données traitées ainsi que de la nature évolutive de l'IMI. Dès lors, il reconnaît qu'en ce qui concerne la fréquence des réunions et des audits, une plus grande souplesse serait peut-être souhaitable. En bref, le CEPD recommande que le règlement fournisse les règles minimales nécessaires pour garantir une coopération efficace mais sans créer de charges administratives inutiles.

80. L'article 20, paragraphe 3, de la proposition ne requiert pas de réunions régulières mais dispose simplement que le CEPD peut «le cas échéant, inviter les autorités de contrôle nationales à le rencontrer […]». Le CEPD se réjouit du fait que ces dispositions laissent aux parties concernées la liberté de décider de la fréquence et des modalités des réunions, ainsi que d'autres détails de procédure concernant leur coopération. Ces points peuvent être convenus dans les règles des procédures, déjà mentionnées dans la proposition.

81. En ce qui concerne des audits réguliers, il pourrait également être plus efficace de laisser les autorités de coopération déterminer, dans leurs règles de procédures, quand et à quelle fréquence ces audits doivent être tenus. Cela peut dépendre de plusieurs facteurs et varier également au fil du temps. Dès lors, le CEPD soutient l'approche de la Commission qui permet une plus grande souplesse également à cet égard.

2.11. **Utilisation nationale de l'IMI**

82. Le CEPD salue le fait que la proposition prévoie une base juridique claire pour l'utilisation nationale de l'IMI et que cette utilisation soit assujettie à plusieurs conditions, dont le fait que l'autorité nationale de protection des données doit être consultée et que cette utilisation doit être en conformité avec la législation nationale.

2.12. **Échange d'informations avec les pays tiers (article 22)**

83. Le CEPD salue les exigences fixées à l'article 22, paragraphe 1, pour les échanges d'information, ainsi que le fait que l'article 22, paragraphe 3, garantisse la transparence de l'élargissement par une publication au Journal officiel d'une liste actualisée des pays tiers concernés utilisant l'IMI (article 22, paragraphe 3).

84. Le CEPD recommande en outre que la Commission restreigne la référence faite aux dérogations en vertu de l'article 26 de la directive 95/46/CE pour n'y inclure que l'article 26, paragraphe 2. En d'autres termes, les autorités compétentes ou les acteurs externes d'un pays tiers qui n'offre pas la protection adéquate ne doivent pas pouvoir bénéficier d'un accès direct à l'IMI sauf si des clauses contractuelles appropriées sont en place. Ces clauses doivent être négociées au niveau de l'UE.

85. Le CEPD souligne que d'autres dérogations, telles que le fait que «le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice», ne doivent pas servir à justifier des transferts de données vers des pays tiers ayant un accès direct à l'IMI ([38]).

2.13. **Obligation de rendre compte (article 26)**

86. Dans le droit fil du renforcement escompté des modalités pour une plus grande obligation de rendre compte durant l'examen du cadre de protection des données de l'UE ([39]), le CEPD recommande que le règlement établisse un cadre clair pour des mécanismes de contrôle interne adéquats, qui garantisse la conformité à la protection des données et fournisse des éléments de preuve à cet égard, contenant au moins les éléments notés ci-dessus.

([34]) Règlement du Conseil (CE) n° 2725/2000 du 11 décembre 2000 concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin (JO L 316 du 15.12.2000, p. 1), qui fait actuellement l'objet d'un réexamen. Dans ce contexte, des dispositions similaires sont envisagées comme dans les règlements VIS et SIS II.

([35]) Voir, par exemple, les articles 41 et 42 du règlement VIS.

([36]) Voir, par exemple, l'article 43, paragraphe 1, du règlement VIS.

([37]) Voir, par exemple, l'article 43, paragraphe 2, du règlement VIS.

([38]) Une approche similaire a été suivie à l'article 22, paragraphe 2, pour la Commission en tant qu'acteur de l'IMI.

([39]) Voir la section 2.2.4 de la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — «Une approche globale de la protection des données à caractère personnel dans l'Union européenne», COM(2010) 609 final. Voir également la section 7 de l'avis du CEPD formulé sur cette communication de la Commission le 14 janvier 2011.

87. Dans ce contexte, le CEPD salue l'exigence visée à l'article 26, paragraphe 2, du règlement selon laquelle la Commission doit faire rapport, tous les trois ans, au CEPD sur les aspects liés à la protection des données, y compris la sécurité. Il serait souhaitable que le règlement précise que le CEPD sera, à son tour, tenu de partager le rapport de la Commission avec les autorités nationales de protection des données, dans le cadre de la surveillance coordonnée visée à l'article 20. Il serait également utile de préciser que le rapport doit discuter, en ce qui concerne chaque domaine politique et chaque fonctionnalité, de la façon dont les principes et préoccupations majeurs en matière de protection des données (par exemple, les informations aux personnes concernées, les droits d'accès, la sécurité) doivent être traités dans la pratique.

88. En outre, le règlement doit préciser que le cadre pour les mécanismes de contrôle interne doit également inclure des évaluations du respect de la vie privée (comprenant également une analyse des risques en matière de sécurité), une politique de protection des données (comprenant un plan de sécurité) adoptée sur la base des résultats de ces évaluations ainsi que des examens et audits périodiques.

2.14. **Respect de la vie privée dès la conception**

89. Le CEPD salue la référence à ce principe au considérant 6 du règlement ([40]). Il recommande qu'au-delà de cette référence, le règlement introduise également des garanties spécifiques de respect de la vie privée dès la conception, telles que:

— un module de protection des données afin de permettre aux personnes concernées d'exercer leurs droits plus efficacement ([41]);

— un isolement clair des différents domaines politiques inclus dans l'IMI («murailles de Chine») ([42]);

— des solutions techniques spécifiques pour limiter les capacités de recherche dans les répertoires, les informations relatives aux alertes et ailleurs, afin de garantir une limitation des finalités;

— des mesures spécifiques afin de garantir la clôture des dossiers ne présentant aucune activité ([43]);

— des garanties procédurales adéquates dans le contexte des développements futurs ([44]).

3. **CONCLUSIONS**

90. Le CEPD a une opinion globalement positive sur l'IMI. Il soutient l'objectif poursuivi par la Commission dans l'établissement d'un système électronique pour l'échange d'informations et la réglementation de ses aspects qui concernent la protection des données. Le CEPD se réjouit également du fait que la Commission a proposé un instrument juridique horizontal pour l'IMI sous la forme d'un règlement du Conseil et du Parlement. Il se félicite que la proposition souligne de façon globale les questions les plus pertinentes en matière de protection des données de l'IMI.

91. En ce qui concerne le cadre légal pour l'IMI à établir dans la proposition de règlement, le CEPD attire l'attention sur deux défis majeurs:

— la nécessité d'assurer la cohérence du cadre légal tout en respectant la diversité, et

— la nécessité de trouver un équilibre entre flexibilité et sécurité juridique.

92. Les fonctionnalités de l'IMI qui sont déjà prévisibles doivent être clarifiées et traitées de façon plus spécifique.

93. Des garanties procédurales adéquates doivent être appliquées pour s'assurer que la protection des données sera soigneusement prise en considération durant le futur développement de l'IMI. Cela inclut une évaluation de l'impact ainsi que la consultation du CEPD et des autorités nationales de protection des données avant chaque élargissement du cadre de l'IMI à un nouveau domaine politique et/ou à de nouvelles fonctionnalités.

94. Les droits d'accès par des acteurs externes et le droit d'accès aux alertes doivent également être spécifiés davantage.

95. En ce qui concerne les délais de conservation:

— le règlement doit prévoir des garanties selon lesquelles les dossiers seront clôturés en temps opportun et les dossiers dormants (dossiers sans activité récente) seront supprimés de la base de données;

— il convient de reconsidérer s'il existe une justification adéquate pour l'extension du délai actuel de six mois à 18 mois après la clôture d'un dossier;

— la Commission n'a pas fourni de justification suffisante de la nécessité et de la proportionnalité de la conservation de «données verrouillées» pendant une période allant jusqu'à cinq ans et, dès lors, cette proposition doit être reconsidérée;

— une distinction plus claire doit être établie entre les alertes et les répertoires d'informations: le règlement doit disposer, en tant que règle par défaut, que i) sauf spécification contraire dans la législation verticale, et sous réserve des garanties supplémentaires adéquates, un délai de conservation de six mois doit s'appliquer aux alertes et, élément important, que ii) ce délai doit être comptabilisé à partir de l'envoi de l'alerte.

96. Le règlement doit requérir une évaluation des risques et un examen du plan de sécurité avant chaque élargissement de l'IMI à un nouveau domaine politique ou avant l'ajout d'une nouvelle fonctionnalité exerçant un impact sur les données à caractère personnel.

97. Les dispositions sur les informations aux personnes concernées et les droits d'accès doivent être renforcées et doivent encourager une approche plus cohérente.

([40]) Idem.
([41]) Voir la section 2.9 ci-dessus.
([42]) Voir la section 2.4 ci-dessus.
([43]) Voir la section 2.5.2 ci-dessus.
([44]) Voir la section 2.2.2 ci-dessus.

98. Le CEPD souhaiterait un renforcement des dispositions relatives à la surveillance coordonnée sur certains points et soutiendrait, à cet effet, des dispositions similaires à celles qui sont en place par exemple dans le contexte du système d'information sur les visas, Schengen II et envisagées pour Eurodac. En ce qui concerne la fréquence des réunions et des audits, le CEPD soutient la proposition dans son approche souple visant à garantir que le règlement fournisse les règles minimales nécessaires pour garantir une coopération efficace sans pour autant créer de charges administratives inutiles.

99. Le règlement doit veiller à ce que les autorités compétentes ou d'autres acteurs externes d'un pays tiers qui n'accorde pas une protection adéquate ne puissent avoir directement accès à l'IMI sauf si des clauses contractuelles appropriées sont en place. Ces clauses doivent être négociées au niveau de l'UE.

100. Le règlement doit établir un cadre clair pour des mécanismes adéquats de contrôle interne, garantissant le respect de la protection des données et fournissant des éléments de preuve à cet égard (y compris une analyse des risques en matière de sécurité), une politique de protection des données (y compris un plan de sécurité) adoptée sur la base des résultats de ces derniers ainsi que des examens et des audits périodiques.

101. Le règlement doit également introduire des garanties spécifiques de respect de la vie privée dès la conception.

Fait à Bruxelles, le 22 novembre 2011.

Giovanni BUTTARELLI

Contrôleur adjoint européen de la protection des données