COMMISSION EUROPÉENNE

Bruxelles, le 22.4.2010
COM(2010)170 final

RAPPORT DE LA COMMISSION

sur la situation en matière de protection des données dans le Système d'information du marché intérieur

RAPPORT DE LA COMMISSION

sur la situation en matière de protection des données dans le Système d'information du marché intérieur

1. SYNTHESE

La Commission est satisfaite de la façon dont les droits et libertés de l'individu concernant les données à caractère personnel (ci-après la «protection des données») sont garantis dans le Système d'information du marché intérieur (IMI). L'IMI est un système internet d'échange d'informations, sûr et multilingue, qui aide les États membres à accomplir leurs tâches de coopération administrative. La Commission est également satisfaite de l'application de la recommandation sur des lignes directrices en matière de protection des données pour l'IMI.

Les États membres n'ont signalé aucun problème de protection des données. Cela justifie l'approche progressive convenue avec le Contrôleur européen de la protection des données et consistant à établir le cadre juridique de l'IMI en fonction de l'évolution technique et de l'extension du système à d'autres domaines de la législation sur le marché intérieur.

En 2010, la Commission étudiera la possibilité d'étendre l'IMI à d'autres domaines du marché intérieur et acquerra une plus grande expérience de l'utilisation pratique du système dans le domaines des services. Au premier trimestre de 2011, elle publiera un document de travail du personnel de la Commission sur le fonctionnement et le développement du système IMI en 2010, qui couvrira aussi la protection des données.

2. OBJET DU PRESENT RAPPORT

Dans le présent rapport, qui était annoncé dans la recommandation de la Commission sur des lignes directrices en matière de protection des données pour le Système d'information du marché intérieur[1] (ci-après la «recommandation»), sont examinées l'application de la recommandation par les États membres et par la Commission et la situation en matière de protection des données dans l'IMI. Le rapport traite aussi de questions nouvelles qui n'étaient pas abordées dans la recommandation, notamment de la couverture de la nouvelle directive «services».

En établissant le rapport, la Commission a tenu compte des réactions des États membres obtenues par une consultation *ad hoc* lancée en novembre 2009[2] et par des

---

1 C(2009) 2041final. JO L 100 du 18.4.2009, p. 12.

2 Dix-sept États membres ont pris part à la consultation en répondant aux questions suivantes:
- Avez-vous pris contact avec l'autorité nationale chargée de la protection des données? A-t-elle émis un avis sur l'application des lignes directrices au niveau national?
- Avez-vous établi une déclaration de confidentialité générale pour tous les utilisateurs de l'IMI ou des dispositions sont-elles prises au niveau local par les autorités compétentes (AC)?

contacts réguliers avec les coordonnateurs IMI et les représentants des États membres aux réunions de l'IMAC-IMI (comité IMI marché intérieur).

3. DEVELOPPEMENT DE L'IMI EN 2009

L'année 2009 a été une année cruciale pour le développement de l'IMI. L'utilisation de l'IMI pour la législation concernant les qualifications professionnelles a été étendue à vingt nouvelles professions et la plupart des ressources ont été consacrées à l'extension du système pour couvrir la directive «services»[3].

Des coordonnateurs IMI nationaux ont participé au projet pilote d'échange d'informations sur la directive «services» (sur la base de cas réels et fictifs) et aux stages de formation qui ont eu lieu à Bruxelles[4]. La Commission a produit une nouvelle version du logiciel (1.7) pour permettre aux autorités compétentes de s'enregistrer. À la fin de l'année, elle a également produit une version 2.0 intermédiaire qui comprenait une application informatique distincte pour le mécanisme d'alerte[5]. Ce nouveau logiciel est devenu pleinement opérationnel au cours du premier trimestre de 2010.

Grâce aux efforts conjugués de la Commission et des États membres, 4 508 autorités compétentes s'étaient enregistrées dans l'IMI à la fin de janvier 2010 et 3 698 d'entre elles avaient accès au nouveau domaine Services, une augmentation sensible de ce nombre étant encore prévue au cours des prochains mois. Le nombre moyen de connexions d'utilisateurs différents par jour est passé de 40 en janvier 2009 à 180 en décembre.

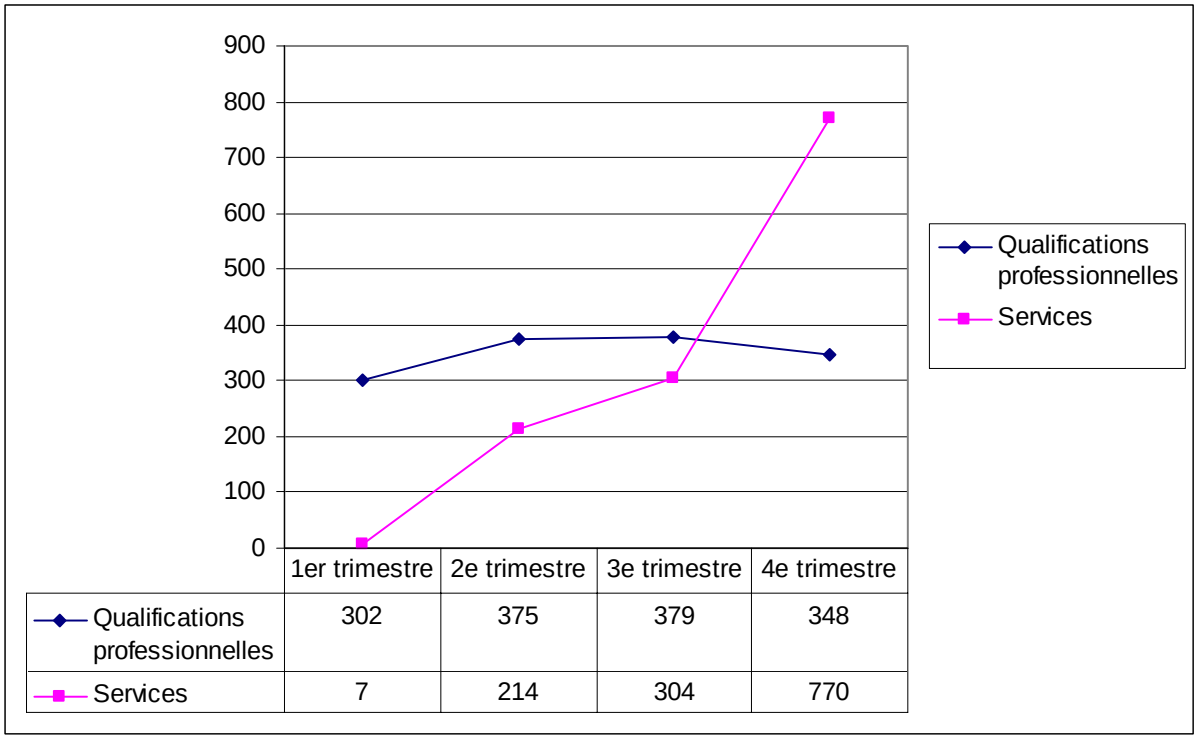
- Les AC ont-elles rencontré des problèmes relatifs à la protection des données pour envoyer une demande ou y répondre dans l'IMI?
- Les AC ont-elles signalé des problèmes pour traiter les questions sur les casiers judiciaires?
- Les AC ont-elles reçu des demandes d'accès, de suppression ou de rectification de la part de personnes concernées?
- Les AC connaissent-elles la procédure de suppression anticipée des données à caractère personnel dans le système? Utilisent-elles cette possibilité?
- Avez-vous intégré la protection des données dans les séances de formation à l'IMI?

3 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).

4 En 2009, la Commission a organisé pour les coordonnateurs, à Bruxelles, trois stages de formation d'un jour qui ont réuni quelque 60 participants chacun. Au cours de la même période, les États membres ont organisé plus de 100 séances de formation au total pour les autorités compétentes aux niveaux local, régional et national.

5 Voir l'article 32 de la directive «services».

Nombre total de demandes envoyées, par trimestre et par domaine législatif, en 2009



	1er trimestre	2e trimestre	3e trimestre	4e trimestre
Qualifications professionnelles	302	375	379	348
Services	7	214	304	770

Dans le domaine des qualifications professionnelles, le système a gagné en maturité et son incontestable succès est une illustration du potentiel de l'IMI en tant qu'outil de coopération administrative dans l'UE. En moyenne, 350 demandes ont été envoyées par trimestre. Plus de 90 % des demandes envoyées en 2009 concernant les qualifications professionnelles provenaient des 15 États qui étaient membres de l'UE avant 2004, ce qui indique le sens de migration de la main-d'œuvre. La Pologne et la Roumanie étaient les destinataires de 32 % des demandes.

Relativement à ces chiffres, il est important de signaler que 56 % des demandes ont reçu une réponse en une semaine.

Délai nécessaire pour traiter une demande au titre de la directive sur les qualifications professionnelles en 2009

	Demandes acceptées	**% cumulé**	**Réponses apportées**	**% cumulé**
En 3 jours	**741**	**57,0 %**	**518**	**43,0 %**
En 1 semaine	**216**	**73,7 %**	**167**	**56,8 %**
En 2 semaines	**166**	**86,5 %**	**170**	**71,0 %**
En 4 semaines	**120**	**95,7 %**	**164**	**84,6 %**
En 8 semaines	**35**	**98,4 %**	**106**	**93,4 %**

En plus de 8 semaines	**21**	**100,0 %**	**80**	**100,0 %**
Total:	**1 299**		**1 205**	

(* La différence entre demandes acceptées et réponses apportées est due au fait que des demandes ont été retirées ou étaient encore traitées à la fin de décembre 2009.)

4. AMELIORER LA PROTECTION DES DONNEES DANS L'IMI, UNE APPROCHE PROGRESSIVE

L'IMI suit l'approche dite de «respect de la vie privée dès la conception» selon laquelle l'exigence de protection des données est prise en compte dès le début dans les systèmes contenant des informations. Des considérations relatives à la protection des données sont également associées à l'utilisation quotidienne du système et sont intégrées dans le matériel de formation, approche qui va au-delà de la protection formelle ou théorique. Cela semble être payant car aucun État membre n'a signalé d'incident lié la protection des données dans l'IMI et aucune plainte n'a émané de personnes concernées.

Depuis deux ans, la Commission a engagé un dialogue avec les autorités chargées de la protection des données et avec le Contrôleur européen de la protection des données (CEPD). Le principe directeur de l'approche progressive est que, comme le système garantit un niveau élevé de protection technique et procédurale des données et que la Commission s'est clairement engagée à continuer à l'améliorer, le cadre juridique de l'IMI doit s'adapter à l'évolution technique et à l'extension du système à d'autres domaines de la législation sur le marché intérieur.

Compte tenu de l'expérience limitée de l'utilisation du système, l'approche progressive a permis à la Commission de lever toutes les inquiétudes dont le CEPD a fait part dans un avis du 12 décembre 2007 et d'adopter trois textes législatifs qui traitent de questions relatives à la protection des données dans l'IMI:

a) la décision 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)[6];

b) la recommandation de la Commission du 26 mars 2009 sur des lignes directrices en matière de protection des données pour le Système d'information du marché intérieur (IMI)[7];

c) la décision de la Commission du 2 octobre 2009 établissant les modalités pratiques des échanges d'informations par voie électronique entre les États membres prévus au chapitre VI de la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur[8].

6 C(2007) 6306, JO L 13 du 16.1.2008, p. 18.
7 C(2009) 2041, JO L 100 du 18.4.2009, p. 12.
8 C(2009) 7493, JO L 263 du 7.10.2009, p. 32.

La partie 6 du présent rapport sera consacrée aux autres questions ainsi qu'à la teneur et à l'opportunité de mesures futures, y compris l'adoption éventuelle d'un instrument juridique.

5. MISE EN ŒUVRE DE LA RECOMMANDATION DE LA COMMISSION

5.1. Améliorations apportées par les États membres

5.1.1. Contacts avec les autorités chargées de la protection des données

La recommandation encourageait «*les coordonnateurs IMI nationaux à prendre contact avec leurs autorités nationales chargées de la protection des données afin d'établir le meilleur moyen de mettre en œuvre ces lignes directrices conformément au droit national*». Dans leurs rapports à la Commission, la plupart des États membres ont déclaré avoir consulté leurs autorités nationales chargées de la protection des données. Ces consultations ont donné aux utilisateurs de l'IMI la confirmation que les données à caractère personnel peuvent être échangées par l'intermédiaire de l'IMI en conformité avec la législation sur la protection des données et, en même temps, elles ont permis aux autorités nationales de régulation d'établir des relations de travail avec des représentants des administrations publiques qui accordent une grande importance à la protection des données et se sont engagés à faire de ce projet réellement européen une réussite.

5.1.2. Déclarations de confidentialité

Sur une suggestion du CEPD, la recommandation encourageait aussi les coordonnateurs IMI à discuter du contenu des déclarations de confidentialité avec les autorités locales chargées de la protection des données. Il était impossible que la recommandation fût très précise sur ce point car, même si la directive sur la protection des données prévoyait une harmonisation totale, les États membres conservent une marge de manœuvre dans l'application de certaines dispositions. Les rapports des États membres confirment que les pratiques relatives au contenu et au format des déclarations de confidentialité diffèrent au niveau national. Une petite majorité d'États membres a estimé qu'il appartient à chaque autorité compétente de décider, conformément à la législation locale, quels sont le format et le contenu appropriés des informations à fournir aux individus. Dans certains États membres, en revanche, sont proposés des modèles adaptables pour l'ensemble du pays[9].

5.1.3. Sensibilisation et formation

L'un des résultats les plus importants de la recommandation est qu'elle a davantage sensibilisé les acteurs et utilisateurs de l'IMI à la protection des données dont les principes généraux leur sont désormais familiers, et qu'elle a suggéré des solutions pratiques pour garantir un niveau élevé de protection des données dans l'IMI. Grâce à

---

9 Un bon exemple de modèle national établi avec le soutien technique de l'autorité nationale chargée de la protection des données est fourni par la déclaration de confidentialité (*cláusula de privacidad*) proposée par l'équipe IMI espagnole: http://www.mpt.es/documentacion/sistema_IMI/documentos/protec_datos/ClausulaIMI_ES/documentes/Clausula_IMI.pdf

la recommandation, des références aux lignes directrices en matière de protection des données ont aussi été intégrées dans le matériel de formation à l'IMI élaboré à l'adresse des autorités compétentes.

5.2. Améliorations apportées par la Commission

5.2.1. Plan de sécurité de l'IMI

La sécurité et la confidentialité des données sont régies par la décision de la Commission du 16 août 2006 relative à la sécurité des systèmes d'information utilisés par les services de la Commission[10]. Cette décision a été actualisée par des modalités d'application adoptées en 2009 ainsi que par des lignes directrices et des normes récentes qui sont largement équivalentes à des normes internationales. Les mesures de sécurité dans l'IMI ont été revues et actualisées en conséquence et un plan de sécurité global a été établi en 2009 et sera réexaminé en 2010.

5.2.2. Améliorations techniques

Lorsqu'un échange d'informations porte sur des données sensibles, un message s'affiche désormais à l'écran pour rappeler que les informations sont sensibles et que le gestionnaire du dossier ne doit les demander que si elles sont absolument nécessaires et en rapport direct avec l'exercice de l'activité professionnelle ou la prestation d'un service donné. Des considérations relatives à la protection des données ont été aussi pleinement prises en compte dans la conception et la mise en œuvre du nouveau mécanisme d'alerte (voir point 5.2.3.2 ci-dessous).

Le site internet de l'IMI a aussi été perfectionné pour que les utilisateurs puissent y trouver les documents pertinents de façon plus intuitive. La partie consacrée à la protection des données[11] a été actualisée à l'aide de tous les textes juridiques qui s'y rapportent, de la correspondance avec le CEPD et des questions types proposées par le système. Par souci de transparence et sur proposition du CEPD, les questions concernant les données sensibles ont été recensées.

5.2.3. Nouveau domaine législatif de la directive «services»

5.2.3.1. Utilisation de l'IMI aux fins de la directive «services»

La directive «services» ne fait pas expressément référence à l'IMI (mais uniquement et plus généralement à un système électronique d'échange d'informations). Il était donc nécessaire d'établir formellement que l'IMI serait utilisé à cette fin. Cela a été fait par une décision[12] que la Commission a adoptée conformément à la procédure prévue dans la directive «services» (ci-après la décision «comitologie»).

Cette décision «comitologie» établit les modalités pratiques de l'échange d'informations du domaine des services dans l'IMI. Elle contribue au maintien du

---

10 C(2006) 3602.

11 http://ec.europa.eu/internal_market/imi-net/data_protection_fr.html

12 Décision de la Commission du 2 octobre 2009 établissant les modalités pratiques des échanges d'informations par voie électronique entre les États membres prévus au chapitre VI de la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur.

niveau élevé de protection des données du système et confère plus de transparence et de précision aux règles générales découlant de la décision 2008/49/CE et aux lignes directrices en matière de protection des données contenues dans la recommandation. Elle laisse la possibilité de décider ultérieurement, compte tenu de l'expérience de l'utilisation du système, d'instaurer si nécessaire des garanties supplémentaires en matière de protection des données[13].

5.2.3.2. Conception du mécanisme d'alerte respectant la protection des données

Le mécanisme d'alerte est un mécanisme d'avertissement, instauré en vertu de l'article 29, paragraphe 3, et de l'article 32 de la directive «services», qui complète le système RAPEX pour les produits. Il permet de prévenir le risque, pour les destinataires, résultant de services.

Le mécanisme d'alerte permet aux États membres de s'acquitter de l'obligation juridique d'échange d'informations et il est donc parfaitement légal du point de vue de la protection des données. Toutefois, la Commission est consciente des implications, en termes de protection des données, d'un tel système. Elle a donc apporté le plus grand soin à sa conception, en s'assurant que celle-ci respecte la protection des données, et elle enjoint aux États membres, qui sont responsables de la protection des données lorsqu'ils envoient ou reçoivent des alertes, de veiller à appliquer les règles correctement.

Le mécanisme d'alerte contient un bon nombre de garanties en matière de protection des données qui sont des caractéristiques générales du système IMI, ainsi que certaines garanties spécifiques destinées à fournir les assurances suivantes:

a) **L'accès aux données est limité à des autorités compétentes et utilisateurs spécifiques**

Conformément à l'approche globale dans l'IMI, l'accès aux informations en application du mécanisme d'alerte est strictement limité selon le principe du besoin d'en connaître. Les autorités compétentes et les utilisateurs de l'IMI n'ont donc accès aux alertes que si les États membres leur ont accordé un accès, non pas à l'IMI en général mais à l'application spécifique aux alertes. Par défaut, les autorités compétentes et les utilisateurs de l'IMI ne peuvent pas envoyer ou recevoir d'alerte. Cette fonction doit être activée séparément.

b) **Aucune alerte inutile n'est lancée**

Aucune alerte ne peut être envoyée sans qu'on ait rempli une liste de contrôle pour vérifier que les critères sont respectés, par exemple, qu'il existe des circonstances ou des faits graves et précis relatifs à une activité de service et susceptibles de causer un préjudice grave. Si l'autorité d'origine ne vérifie pas tous les critères pertinents, le système ne l'autorise pas à poursuivre le lancement d'alerte.

En outre, l'alerte n'est pas envoyée directement à d'autres États membres mais elle est d'abord soumise à un coordonnateur d'alertes dans le premier État membre. Ce

[13] Voir le chapitre 13, sous-partie «Travaux en cours», point d), de la recommandation.

coordonnateur d'alertes doit, à son tour, estimer s'il faut diffuser ou pas l'alerte à d'autres États membres.

c) **Les alertes ne sont pas diffusées à plus de destinataires que nécessaire pour satisfaire aux exigences d'information prévues par la législation**

En cas d'envoi d'alerte à d'autres États membres, il faut que l'autorité ayant lancé l'alerte et le coordonnateur d'alertes déterminent quels États membres doivent recevoir l'alerte. Si l'État membre où un service est fourni veut envoyer une alerte, seuls la recevront, par défaut, l'État membre d'établissement du prestataire de service et la Commission. Cette configuration par défaut garantit que l'ajout d'autres États membres à la liste des destinataires fera l'objet d'une décision au cas par cas selon le principe du besoin d'en connaître.

En outre, lorsque l'alerte est diffusée à d'autres États membres, elle n'est pas envoyée à toutes les autorités compétentes dans les États membres destinataires mais seulement à une boîte de réception des alertes (généralement au coordonnateur d'alertes national). C'est le destinataire qui décidera quelles autorités compétentes de son État membre sont concernées et doivent être alertées.

d) **La Commission, lorsqu'elle reçoit des alertes comme prévu par la directive «services», n'a pas accès aux données à caractère personnel**

La directive «services» prévoit que toutes les alertes soient envoyées à la Commission mais celle-ci, à la différence des États membres, n'a pas besoin d'accès aux données à caractère personnel. La Commission reçoit donc des alertes sans données à caractère personnel.

e) **Si, malgré les précautions, une alerte injustifiée est envoyée, il est possible de la rappeler rapidement ou de corriger ou supprimer des données incorrectes**

Le système IMI permet à une autorité compétente qui a envoyé une alerte injustifiée de la rappeler immédiatement, en la rendant invisible pour tous les utilisateurs de l'IMI. Si l'alerte était justifiée mais qu'il est nécessaire de rectifier certaines informations, l'autorité compétente ayant lancé l'alerte peut le faire à tout moment. De plus, le système IMI permet aux autorités compétentes qui ont reçu l'alerte d'indiquer que certaines des informations qui y sont fournies sont incorrectes.

f) **Les alertes sont clôturées dès qu'il n'y a plus de risque, les données deviennent immédiatement invisibles pour tous les utilisateurs et les données à caractère personnel sont supprimées six mois après la clôture de l'alerte**

Une fois disparu le risque qui a motivé l'alerte, celle-ci doit être clôturée. Le système IMI permet donc à l'État membre d'établissement de clôturer l'alerte et un message électronique de rappel est envoyé aux autorités responsables. Une fois clôturée, l'alerte devient invisible. Six mois au plus tard après la clôture, toutes les données à caractère personnel sont automatiquement supprimées et retirées du système.

6. QUESTIONS A APPROFONDIR

Même si la plupart des États membres ont une opinion favorable de la protection des données dans l'IMI, quelques-uns d'entre eux ont soulevé des questions qui sont étudiées dans cette partie du rapport.

6.1. Règles applicables à la sécurité et à la confidentialité des données

Le traitement des données à caractère personnel dans l'IMI implique un traitement conjoint (par la Commission et les États membres), un contrôle conjoint (par les différents utilisateurs et acteurs) et une supervision conjointe (par les autorités nationales chargées de la protection des données et le CEPD). Dans une situation aussi complexe, il n'est pas toujours aisé de répartir les responsabilités.

Les autorités danoises et allemandes chargées de la protection des données ont estimé que, comme les autorités compétentes situées sur leur territoire doivent satisfaire à certaines exigences nationales (p. ex. mécanisme d'authentification plus forte, comme indiqué au point suivant), elles doivent insister pour que l'IMI satisfasse aussi à ces exigences nationales ou bien cesser d'utiliser le système. Les autorités compétentes ont transmis ces demandes à la Commission qui est responsable de la sécurité du système.

La Commission estime que l'IMI est un système sûr et qu'un réseau réellement européen comme l'IMI ne pourrait tout bonnement pas fonctionner si chaque État membre exigeait le respect de ses normes nationales de sécurité. La directive sur la protection des données, adoptée il y a presque vingt ans, poursuivait le double objectif, d'une part, de protéger le droit fondamental à la protection des données et, d'autre part, de garantir la libre circulation des données à caractère personnel entre les États membres et entre ces derniers et les institutions de l'UE[14].

Sur cette base, la Commission maintient que, vu le niveau élevé des garanties offertes en matière de protection des données dans le système IMI et le principe de coopération loyale énoncé à l'article 4, paragraphe 3, du traité sur l'Union européenne, les autorités nationales chargées de la protection des données ne doivent pas opposer d'obstacle à l'utilisation du système par les autorités nationales compétentes.

6.2. Vers une authentification plus forte dans l'IMI

Le système d'authentification de l'IMI est une version avancée de l'authentification à un seul facteur car il combine un nom d'utilisateur et un mot de passe avec un numéro d'identification personnel (NIP). Il est demandé à l'utilisateur, lorsqu'il tente d'accéder au système, de saisir une combinaison de caractères choisis de façon aléatoire dans le code NIP.

---

[14] Ce principe est clairement énoncé à l'article 1er, paragraphe 2, de la directive sur la protection des données ainsi qu'à l'article 1er, paragraphe 1, et au considérant 13 du règlement sur la protection des données: «Il s'agit par là de garantir tant le respect effectif des règles de protection des libertés et droits fondamentaux des personnes que la libre circulation des données à caractère personnel entre les États membres et les institutions et organes communautaires ou entre les institutions et organes communautaires, dans l'exercice de leurs compétences respectives».

Les autorités allemandes et danoises chargées de la protection des données ont fait part de leurs inquiétudes concernant le système d'authentification de l'IMI. La Commission estime que le mécanisme actuel d'authentification est approprié, compte tenu de l'état de l'art et du coût de mise en œuvre, mais elle admet qu'une authentification plus forte est souhaitable à plus long terme. Comme les États membres ont instauré différents systèmes d'authentification qui ne sont pas toujours interopérables, la solution privilégiée pour une authentification plus forte dans l'IMI semble être celle d'identités électroniques, gérées au niveau national, qui deviendraient interopérables à l'aide d'un intergiciel.

L'une des options possibles est le projet STORK qui est actuellement réalisé par un consortium auquel certains États membres participent et qui est financé au titre du programme d'appui stratégique en matière de TIC du programme pour l'innovation et la compétitivité. La Commission suivra de près l'avancement du projet au cours des prochains mois qui seront déterminants et conditionneront la décision de l'utiliser ou pas dans l'IMI.

D'autres considérations sur la sécurité des données figurent au point 7.2.

6.3. Conservation des données

La politique en matière de conservation des données dans l'IMI est très stricte[15] et certains acteurs et utilisateurs ont indiqué qu'elle devait être revue. La suppression rapide de données à caractère personnel dans le système n'est pas toujours dans l'intérêt de la personne concernée qui préférerait peut-être que les données la concernant, par exemple s'agissant de procédures judiciaires, fussent conservées plus longtemps dans l'IMI.

Dans un arrêt récent[16], la Cour de justice a déclaré que le droit d'accès à l'information[17] s'applique aux données détenues non seulement dans le présent mais aussi dans le passé. Aussi la Cour estime-t-elle que limiter l'accès aux données en les supprimant peut aller à l'encontre de la législation, à moins qu'il puisse être démontré qu'une conservation plus longue de l'information constituerait une charge excessive pour le responsable du traitement. La Commission estime que conserver des informations à caractère personnel plus longtemps dans l'IMI ne constituerait pas une charge excessive et entend donc réfléchir à une durée de conservation plus longue, éventuellement avec une phase transitoire de blocage des données, au cours de laquelle les données seraient rendues invisibles pour tous les utilisateurs avant d'être définitivement supprimées. Les questions que peut soulever une politique de blocage – par exemple, qui pourrait accéder aux données bloquées et à quelles fins – seront étudiées avec soin.

Cela montre bien qu'il faut prendre tout le temps de la réflexion avant d'arrêter une série de règles soumettant le fonctionnement de l'IMI à un instrument juridique contraignant. Il est essentiel que la Commission et les États membres, tout en

---

15 Il est possible de supprimer rapidement, d'un clic ou deux, des données à caractère personnel et, dans tous les cas, toutes les données à caractère personnel sont automatiquement supprimées six mois après la clôture de la demande d'information.

16 Affaire C-553/07, Rotterdam contre Rijkeboer.

17 Voir l'article 12, point a), de la directive 95/46/CE.

garantissant une protection satisfaisante des données et la participation des autorités responsables au processus, puissent avoir assez d'expérience du système pour ne pas instaurer de règles inefficaces, voire contreproductives, en la matière.

6.4. Utilisation nationale de l'IMI

La transposition de la directive «services» aux Pays-Bas prévoit l'utilisation de l'IMI à des fins nationales, c'est-à-dire l'échange d'informations entre administrations néerlandaises également. La Commission européenne recommande cette approche qui illustre le potentiel d'utilisation interadministrative de l'IMI. Toutefois, l'utilisation nationale de l'IMI par les États membres est soumise à trois conditions:

a) que le traitement de données à caractère personnel et la conservation d'informations sur des serveurs de la Commission soient considérés comme licites en vertu du droit national,

b) que le système soit utilisé en l'état, avec les mêmes questions types et fonctionnalités, et

c) que l'État membre assume la pleine responsabilité de tout problème (de protection des données ou autre) relatif à l'utilisation du système à des fins nationales.

Par conséquent, au cas où des États membres seraient intéressés par une utilisation nationale de l'IMI, il leur est conseillé de consulter d'abord leurs autorités nationales chargées de la protection des données, puis de prendre contact avec la Commission pour en discuter et s'assurer que cela ne pose aucun problème en rapport avec la législation sur la protection des données.

6.5. Garanties spécifiques, en matière de protection des données, dans une législation communautaire juridiquement contraignante

Dans son avis du 12 décembre 2007 et l'échange de lettres avec la Commission, le CEPD a préconisé, dès lors que le champ d'application de l'IMI s'étend au-delà des directives sur les services et sur les qualifications professionnelles, d'introduire des garanties spécifiques et juridiquement contraignantes en matière de protection des données dans la législation de l'UE. Les autorités allemandes chargées de la protection des données partagent cette opinion.

En 2010, la nouvelle Commission portera un regard neuf sur le fonctionnement du marché unique et sur l'éventualité d'un recours accru à l'IMI pour améliorer l'application de la législation sur le marché intérieur par les États membres. Aussi recherchera-t-elle à quels autres domaines politiques l'IMI pourrait être utile.

Il existe déjà un ensemble solide de mesures en matière de protection des données et le retour d'informations des États membres a été positif. Par conséquent, la Commission estime que, avant d'avancer une proposition législative, il serait plus sage de définir le champ d'application de l'IMI et de tirer les enseignements de l'utilisation pratique du système pour les services. Toute proposition future devra tenir dûment compte de cette évolution afin de garantir une base solide et à l'épreuve du temps pour l'IMI et la protection des données.

Entre-temps, la Commission continuera à améliorer la protection des données dans l'IMI, en étroite coopération avec les États membres et le CEPD, comme exposé ci-dessous.

7. AMELIORATIONS FUTURES

7.1. Améliorations techniques

Une future version du logiciel comprendra des messages automatiques de rappel et des listes des urgences pour l'envoi d'une réponse, de sorte que les demandes ne restent pas ouvertes plus longtemps que nécessaire. Concernant une procédure en ligne de rectification, de blocage ou d'effacement des données, la Commission estime que, comme il n'y a encore eu aucune demande et qu'il est très improbable qu'il y en ait beaucoup à l'avenir, il serait plus approprié d'instaurer une procédure plus légère convenablement documentée avec l'aide du délégué à la protection des données de la Commission et du CEPD.

7.2. Sécurité des données

Conformément aux nouvelles lignes directrices et aux normes récemment adoptées par la Commission, celle-ci procédera à une nouvelle évaluation des risques liés à l'IMI en 2010 et actualisera le plan de sécurité en conséquence, en recensant les parties du système qui doivent être étudiées, les menaces potentielles et les mesures nécessaires en matière d'infrastructure et de logiciel. S'il ressort de l'évaluation des risques qu'il faut prendre des mesures de sécurité supplémentaires, celles-ci seront progressivement intégrées dans de futures versions du logiciel.

Au début de 2011, aura également lieu un audit externe qui sera surtout axé sur les performances et la stabilité du système, mais pourra aussi couvrir des aspects relatifs à la protection des données et à la sécurité.

7.3. Réexamen de la directive sur les qualifications professionnelles

En 2010-2011, il sera procédé à une évaluation de la directive sur les qualifications professionnelles, qui consistera notamment à analyser la coopération administrative et l'utilisation de l'IMI, y compris les problèmes de protection des données.

8. CONCLUSIONS

La Commission est satisfaite de l'application de la recommandation et de la situation concernant la protection des données dans l'IMI. Néanmoins, elle continuera à œuvrer à de nouveaux perfectionnements du système, en particulier à des améliorations techniques et de la sécurité des données.

La Commission entend aussi étudier la possibilité d'étendre l'IMI à d'autres domaines du marché intérieur tout en acquérant une plus grande expérience pratique de l'utilisation du système dans le domaine des services. Toute proposition future de législation européenne tiendra compte de ces évolutions et réflexions afin de fournir une base solide et à l'épreuve du temps pour l'IMI et la protection des données.

Au premier trimestre de 2011, sera publié un document de travail du personnel de la Commission sur le fonctionnement et le développement du système IMI en 2010. Ce rapport couvrira aussi la protection des données.