

Groupe de travail du Conseil sur l'e-justice et l'interconnexion des registres d'insolvabilité

Bruxelles, le 15 juillet 2009.

Giovanni BUTTARELLI

Contrôleur européen adjoint de la protection des données

Points de l'intervention

I. Introduction

La protection des données ne doit plus être considérée de façon traditionnelle, comme la protection de la vie privée, mais comme une nouvelle forme d'ingénierie de l'utilisation des données à caractère personnel. A cet égard, je vois d'un bon œil le développement d'initiatives d'e-justice, qui rendront la justice plus transparente et plus accessible.

Les initiatives d'e-justice seront fondées en grande partie sur le traitement et l'échange de données à caractère personnel entre des acteurs implantés dans divers États membres. Le respect de la protection des données est non seulement une obligation légale, mais également un élément essentiel pour le succès des systèmes envisagés, par exemple la garantie de la qualité des échanges de données. Le respect de la vie privée et la protection des données sont, essentiellement, des «facteurs-clés de réussite». Il est dès lors logique d'y investir le plus tôt possible et je suis ravi à cet égard que le CEPD ait été informé des évolutions pertinentes par la Commission - qui a également présenté un exposé pratique à mes collaborateurs. Je suis par ailleurs très heureux d'être invité à contribuer à ce stade précoce au débat sur le façonnement concret de l'e-justice.

Je commencerai par présenter au groupe de travail les grandes lignes de l'avis du CEPD sur l'e-justice et aborderai ensuite quelques considérations sur la question spécifique

de l'interconnexion des registres d'insolvabilité. Ces deux sujets ont à nouveau été abordés récemment dans l'avis du CEPD sur le programme de Stockholm, adopté par le CEPD vendredi dernier.

Dans ce dernier avis, le CEPD a réitéré son soutien total à l'ambitieux projet d'e-justice et a demandé qu'il soit explicitement mentionné dans le programme de Stockholm, étant donné qu'il s'agit d'un pas en avant significatif vers un espace européen de justice qui permettra aux citoyens d'accéder plus facilement à la justice. L'e-justice et la protection des données ne sont pas le moins du monde incompatibles. Il conviendrait au contraire de considérer la protection des données comme une alliée nécessaire et comme une abondante source d'inspiration sur la façon de mener à bien les initiatives d'e-justice. Dans le cadre de cet avis positif, le CEPD a souligné quelques points que je vais présenter brièvement.

II. Observations importantes sur les initiatives d'e-justice

Nécessité d'un cadre uniforme et global pour l'UE en matière de protection des données. En guise d'entrée en matière plus générale, j'aimerais évoquer la nécessité de veiller à ce que le cadre juridique pour la protection des données à caractère personnel couvre uniformément et de façon satisfaisante toutes les activités de l'UE, indépendamment du pilier concerné. Il est regrettable que les initiatives d'e-justice soient soumises aux différentes dispositions sur la protection des données provenant soit de la directive 95/46, soit de la décision-cadre 2008/977 (en particulier son article premier, paragraphe 2, point a), en fonction des limites, parfois floues, entre les piliers. À cet égard, j'aimerais attirer votre attention sur le fait que la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale peut s'appliquer dans certains cas aux initiatives d'e-justice.

Attribution des responsabilités dans des systèmes à plusieurs niveaux. De nombreux outils d'e-justice auront pour caractéristique commune le fait que les informations et les données à caractère personnel seront échangées et gérées par différents acteurs, aux échelons national et de l'UE, qui sont soumis à des obligations en matière de protection des données et à des autorités de contrôle établies sur la base de la directive 95/46/CE ou du règlement 45/2001. À cet égard, comme le CEPD l'a déjà précisé dans son avis sur le

système d'information du marché intérieur (IMI), il est essentiel de veiller à ce que les responsabilités concernant le respect des règles en matière de protection des données soient assumées efficacement et de façon homogène, en déterminant clairement les contrôleurs des activités de traitement et la répartition des responsabilités entre eux.

Les initiatives d'e-justice doivent être construites autour de normes en matière de protection des données («respect de la vie privée et protection des données dès la conception»). Il est également crucial que les questions de protection des données soient prises en compte au stade le plus précoce possible et soient intégrées dans l'architecture des outils envisagés. Plus spécifiquement, l'architecture du système et la mise en œuvre de mesures de sécurité adéquates sont particulièrement importantes. Grâce à cette approche axée sur «le respect de la vie privée et la protection des données dès la conception», les initiatives d'e-justice permettraient une gestion efficace des données à caractère personnel tout en assurant le respect des principes de protection des données et la sécurité des échanges de données entre les différentes autorités.

Dans ce contexte, j'apprécie que la préférence soit accordée aux architectures décentralisées. Déjà dans son avis sur ECRIS, le CEPD estimait qu'une architecture décentralisée permettait d'éviter une duplication supplémentaire de données à caractère personnel dans une base de données centrale. Toutefois, l'attention accordée au respect de la vie privée et à la protection des données devrait également être une priorité dans le cadre du développement de l'architecture et des fonctionnalités de ces systèmes.

Un contrôle effectif. Des mécanismes de coordination effective doivent être mis en place entre les autorités de protection des données afin d'assurer un contrôle effectif et la bonne qualité de la circulation transfrontalière des données tirées des casiers judiciaires. Ces mécanismes devraient également tenir compte de la compétence de contrôle du CEPD à l'égard de l'infrastructure s-TESTA. Les outils d'e-justice pourraient venir à l'appui de ces mécanismes qui pourraient être développés en coopération étroite avec les autorités de la protection des données.

Interconnexion/interopérabilité et limitation de la finalité. L'interconnexion et l'interopérabilité des systèmes devraient respecter le principe de limitation de la finalité.

Le CEPD recommande que, dans le cadre de l'interconnexion et de l'interopérabilité des systèmes, il soit tenu compte de manière appropriée du principe de limitation de la finalité, selon lequel les données à caractère personnel sont uniquement collectées à des fins précisées et explicites et ne sont pas traitées ensuite d'une façon incompatible avec ces fins. Il

convient d'évaluer en profondeur toute forme d'interaction entre différents systèmes. Il conviendrait de définir les objectifs envisagés de l'interconnexion et de l'interopérabilité des systèmes avant de les mettre en œuvre et ensuite d'évaluer le respect des principes de finalité et d'objectif. Dès lors, en matière d'interopérabilité, il est essentiel de définir au préalable qui peut accéder à ou utiliser des données déterminées, et à quelles fins. Le CEPD souhaite souligner à nouveau que l'interopérabilité devrait respecter le principe de limitation de la finalité.

Dans ce contexte, il conviendrait par exemple de définir la notion d'insolvabilité, actuellement plutôt floue.

Concernant l'interopérabilité des logiciels utilisés par les États membres, tous les États membres ne doivent pas forcément utiliser les mêmes logiciels, même si cette option serait la plus pratique, mais les logiciels doivent offrir une interopérabilité complète sur les plans sémantique, technique et organisationnel.

Questions relatives à la traduction automatique / l'exactitude. L'e-justice implique des échanges d'informations établies au départ dans des langues différentes. Dans ce contexte, la traduction automatique est un instrument utile, susceptible de favoriser la compréhension mutuelle entre les acteurs concernés des États membres, ainsi que des initiatives comme l'élaboration d'un glossaire juridique et sémantique.

Toutefois, la traduction automatique doit être utilisée en prêtant particulièrement attention à la préservation de la qualité des informations échangées, en particulier lorsque ces informations servent à prendre des décisions qui ont des effets juridiques pour les personnes concernées.

Avantages pour les citoyens et les personnes concernées. Dans la même ligne, le CEPD rejoint également l'avis du Conseil selon lequel les citoyens devraient profiter rapidement des avantages des outils d'e-justice. Le CEPD approuve, comme le Conseil, l'idée de développer des systèmes d'authentification afin d'offrir des services différents et différenciés à des utilisateurs différents. Les mécanismes d'authentification contribuent à garantir la proportionnalité et le besoin de connaître et peuvent par ailleurs favoriser les droits des personnes concernées.

À cet égard, le CEPD est particulièrement favorable aux outils promouvant le respect des droits des personnes concernées, comme la possibilité offerte aux citoyens de demander leur casier judiciaire en ligne et dans la langue de leur choix. Cette approche de type «guichet unique», déjà avancée par le CEPD dans d'autres domaines (coordination des systèmes de sécurité sociale, échange des casiers judiciaires) s'inscrit dans la droite ligne de l'idée,

avancée par la Commission européenne dans sa récente communication sur le «programme de Stockholm», de construction d'un espace de liberté, de sécurité et de justice au service des citoyens.

III. Commentaires spécifiques concernant l'interconnexion des registres d'insolvabilité

Permettez-moi maintenant de me concentrer sur une question plus spécifique: l'interconnexion des registres d'insolvabilité, qui selon ce que j'ai compris vous intéresse tout particulièrement à ce stade. Permettez-moi tout d'abord de souligner qu'il convient d'analyser au préalable les conséquences pour les personnes de l'interconnexion de registres nationaux avec des données à caractère personnel délicates, comme des registres d'insolvabilité.

Plus grand dénominateur commun. Lorsque l'on recourt à des approches nationales non homogènes, le principe de base est la nécessité de conserver le plus grand dénominateur commun dans tous les aspects du système, et plus particulièrement concernant les aspects de protection des données (éléments traités, finalités de leur publication, information des utilisateurs, limitation des autres utilisations incompatibles, mesures de sécurité). C'est ce même principe que tente de suivre le modèle actuel, en évitant que le portail publie davantage d'informations que ce qui est autorisé par chaque système national.

Répartition des responsabilités. Le portail (et donc la Commission qui le gère) jouera un rôle important et apportera une valeur ajoutée à la facilité de recherche de données (autrement dit, l'ensemble est plus que la simple somme de ses parties). Indépendamment du fait que les données proviennent de registres nationaux, la façon dont un traitement est vraiment conçu influence la répartition des responsabilités juridiques et les conséquences pour les citoyens. Dans le cas des registres d'insolvabilité, une analyse approfondie pourrait contribuer à déterminer les rôles qu'il faut définir et pourrait également montrer la voie pour les évolutions à venir. Dès lors, une évaluation/répartition minutieuse des responsabilités (également du point de vue de la protection des données, p. ex. qui sont les contrôleurs ?) est essentielle (voir système IMI).

Définition/limitation de la finalité. Il convient de définir très précisément les finalités pour lesquelles les données sont disponibles, en tenant compte également des limitations

nationales, en particulier en ce qui concerne le traitement de données de personnes. L'utilisation pour d'autres finalités/usages incompatibles devrait être clairement proscrite - par exemple par un avis sur le site web - et évitée autant que possible par des moyens techniques. Les capacités de recherche du portail doivent refléter ses objets et ne pas faciliter les utilisations à d'autres fins incompatibles.

Réduction des données au minimum. Etant donné que les registres nationaux contiennent des catégories de données très variées, il serait judicieux de créer un ensemble minimum de données qui s'affichera directement sur le portail d'e-justice. Ces données devraient être suffisantes pour identifier les personnes en évitant les «faux positifs», sans dépasser le niveau de détail requis pour la finalité du portail. Pour obtenir des données supplémentaires, les utilisateurs pourraient être redirigés vers les portails nationaux. Cela n'implique pas de modifier, d'altérer ou d'influencer les diverses sources nationales, mais seulement, en recourant au principe de réduction des données au minimum, d'ajouter une couche au niveau du portail e-justice. Cette approche, assortie d'avis adéquats relatifs au respect de la vie privée et à la délimitation des responsabilités, pourrait éliminer certains problèmes potentiels.

Qualité des données. Il est essentiel de déployer les meilleurs efforts pour garantir que les informations fournies soient comprises correctement et avec précision, en particulier dans des contextes autres que ceux d'origine. Il importe par exemple de clarifier avec soin la définition de la notion d'insolvabilité.

Mesures de sécurité. Il convient d'accorder une attention toute particulière à la sécurité du traitement des données, plus particulièrement en ce qui concerne les mesures tendant à éviter autant que possible les utilisations du système non liées à son objet original (p. ex. des recherches en masse pour copier des données). Cet élément peut également être intégré dans la politique d'utilisation du site web.

Sur ce point, je conclurai en soulignant que même si l'interconnexion des registres d'insolvabilité peut être vue comme une sorte de projet pilote, elle pose d'importantes questions en matière de protection des données qui seront également pertinentes dans d'autres initiatives d'e-justice.