Accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol)

2005/0232(CNS) - 07/06/2007 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté le rapport de la Baronne Sarah **LUDFORD** (ALDE, UK) modifiant, dans la cadre de la procédure de consultation, la proposition de décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins d'enquête en la matière.

Le texte adopté convient que la possibilité donnée à Europol et aux autorités nationales d'avoir accès au VIS ne peut que contribuer de manière positive à la sécurité intérieure et à la lutte contre le terrorisme. L'exigence d'un strict respect des règles relatives à la protection des données à caractère personnel et de conditions d'accès définies est toutefois soulignée.

Les principaux amendements proposés par Parlement sont les suivants :

- chaque État membre devra garantir dans son droit national un niveau de protection des données correspondant au moins à celui résultant de la convention du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ainsi que, pour les États membres qui l'ont ratifié, du protocole additionnel du 8 novembre 2001 ; il sera également tenu compte de la recommandation n° R (87) 15 du Comité des ministres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police du 17 septembre 1987 ;

- les députés proposent que chaque État membre désigne précisément les autorités ainsi que les points d'accès centraux par lesquels l'accès au VIS s'effectue. Chaque État membre tiendra une liste des autorités désignées ainsi que des points d'accès centraux et en informera la Commission. Les demandes d'accès au VIS devront être adressées aux points d'accès centraux par les unités opérationnelles des autorités désignées. Seul le personnel dûment habilité des unités opérationnelles, ainsi que du ou des points d'accès centraux, seront autorisés à avoir accès au VIS ;

- les données à caractère personnel obtenues du VIS doivent être traitées uniquement aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière. Ainsi, le traitement des données VIS ne devrait avoir lieu qu'au cas par cas, toute consultation devant être justifiée par une réelle plus-value dans les enquêtes. La décision définit une série de conditions à réunir afin d'avoir accès aux données, soumises à un contrôle préalable de l'autorité nationale réceptrice de la demande (sauf en cas d'urgence, où le contrôle s'effectue a posteriori) ;

- sauf en cas d'urgence exceptionnelle et sous certaines conditions, les données à caractère personnel obtenues du VIS ne doivent pas être transférées à des pays tiers ou à des organisations internationales ou mises à leur disposition ;

- avant d'être autorisé à traiter des données stockées dans le VIS, le personnel des autorités ayant un droit d'accès doit recevoir une formation appropriée sur les règles en matière de sécurité et de protection des données et être informé des infractions et des sanctions pénales éventuelles en la matière ;

- chaque État membre doit adopter les mesures de sécurité nécessaires en ce qui concerne les données devant être extraites du VIS puis stockées, notamment pour: i) assurer la protection physique des données, notamment en élaborant des plans d'urgence pour la protection des infrastructures critiques; ii) refuser l'accès des personnes non autorisées aux installations nationales dans lesquelles l'État membre stocke des données ; iii) empêcher toute lecture, copie, modification ou tout effacement non autorisés de supports de données ; iv) empêcher l'inspection, la modification ou l'effacement non autorisés de données à caractère personnel stockées ; v) empêcher le traitement non autorisé de données du VIS ; vi) garantir que les personnes autorisées à accéder au VIS n'aient accès qu'aux données pour lesquelles elles ont une autorisation d'accès et uniquement grâce à des identités d'utilisateur individuelles et uniques ainsi qu'à des modes d'accès confidentiels; vii) garantir que toutes les autorités ayant un droit d'accès au VIS créent des profils décrivant les tâches et responsabilités qui incombent aux personnes habilitées à accéder aux données ; viii) garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel peuvent être transmises par des installations de transmission de données ; ix) garantir qu'il puisse être vérifié et constaté quelles données ont été extraites du VIS, à quel moment, par qui et à quelle fin; x) empêcher que des données à caractère personnel puissent être lues et copiées de façon non autorisée lors de leur transmission à partir du VIS ; xi) contrôler l'efficacité des mesures de sécurité et prendre les mesures d'organisation en matière de contrôle interne ;

- toute personne ou tout État membre ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions de la décision a le droit d'obtenir réparation de l'État membre responsable du dommage subi. Cet État est exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait dommageable ne lui est pas imputable;

- les données extraites du VIS peuvent être conservées dans les fichiers nationaux uniquement lorsque cela est nécessaire dans un cas particulier, et pendant une durée n'excédant pas celle nécessaire dans le cas concerné;

- toute personne a le droit de faire rectifier des données la concernant qui sont inexactes dans les faits ou de faire effacer des données la concernant qui sont stockées illégalement. La personne concernée est informée du suivi donné à l'exercice de son droit de rectification et d'effacement dans les meilleurs délais, et en tout cas au plus tard trois mois après la date à laquelle elle a demandé la rectification ou l'effacement, ou plus tôt si la législation nationale prévoit un délai plus court. Dans chaque État membre, toute personne a le droit de former un recours ou de déposer une plainte devant les autorités ou les juridictions compétentes de l'État membre qui lui a refusé le droit d'accès ou le droit de rectification ou d'effacement des données ;

- chaque État membre et Europol doit veiller à ce que toutes les opérations de traitement des données résultant de la consultation du VIS en vertu de la décision soient enregistrées afin de pouvoir contrôler l'admissibilité de la consultation et la licéité du traitement des données, d'assurer un autocontrôle et le bon fonctionnement du système, ainsi que l'intégrité et la sécurité des données.

Il est enfin rappelé que la présente décision constitue un développement des dispositions de l'acquis de Schengen auxquelles l'Irlande et le Royaume-Uni ne participe pas. Toutefois, conformément à la décision-cadre 2006/960/JAI, les informations contenues dans le VIS peuvent être communiquées au Royaume-Uni et à l'Irlande par les autorités compétentes des États membres dont les autorités désignées ont accès au VIS en vertu de la présente décision et les informations tenues dans les registres nationaux relatifs aux visas du Royaume-Uni et de l'Irlande peuvent être transmises aux services répressifs compétents des autres États membres.