Asile: système Eurodac de comparaison des empreintes digitales des démandeurs des pays tiers ou apartrides; demandes de comparaison avec les données d'Eurodac. Refonte

2008/0242(COD) - 12/06/2013 - Texte adopté du Parlement après reconsultation

Le Parlement européen a adopté par 502 voix pour, 126 contre et 56 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil relatif à la création du système "EURODAC" pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° […/…] (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale présentée dans l'un des États membres par un ressortissant de pays tiers ou un apatride) et pour les demandes de comparaison avec les données d'EURODAC présentées par les services répressifs des États membres et Europol à des fins répressives, et modifiant le règlement (UE) n° 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte).

Le Parlement a arrêté sa position en première lecture suivant la procédure législative ordinaire. Les amendements adoptés en plénière sont le résultat d'un compromis négocié entre le Parlement européen et le Conseil. Ils modifient la proposition comme suit :

Objet d'EURODAC : EURODAC doit contribuer à déterminer l'État membre qui, en vertu du règlement (UE) n° …/… de Dublin, sera responsable de l'examen d'une demande de protection internationale introduite dans un État membre par un ressortissant de pays tiers ou un apatride. Le règlement définit également les conditions dans lesquelles les autorités désignées des États membres et Europol pourront demander la comparaison de données dactyloscopiques avec celles conservées dans le système central **à des fins répressives**.

Autorités désignées des États membres à des fins répressives : les États membres devront désigner les autorités qui seront autorisées à demander des comparaisons avec les données d'EURODAC. Ces autorités sont celles qui sont chargées de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière. **Elles ne comprennent pas les agences ou les unités exclusivement responsables du renseignement en matière de sécurité intérieure**.

Autorités des États membres chargées de la vérification à des fins répressives : les États membres devront désigner une **autorité nationale unique** ou une unité de cette autorité qui exerce les fonctions d' autorité **chargée de la vérification**. L'autorité chargée de la vérification est une autorité de l'État membre chargée de la prévention ou de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière. Celle-ci devra agir en toute indépendance quand elle exécutera ses tâches. Cette autorité ne recevra aucune instruction concernant le résultat de ses vérifications. Afin de refléter leur structure organisationnelle et administrative, les États membres pourront désigner **plus d'une autorité chargée de la vérification**, conformément à leurs exigences constitutionnelles ou légales.

L'autorité chargée de la vérification devra veiller à ce que les conditions requises pour demander la comparaison d'empreintes digitales avec les données d'EURODAC sont remplies. **Seul le personnel dûment habilité** de l'autorité chargée de la vérification sera autorisé à recevoir et transmettre une demande d'accès à EURODAC.

Tâches dévolues à Europol : Europol devra désigner en tant qu'autorité chargée de la vérification **une unité spécialisée composée d'agents** dûment habilités, qui, par rapport à l'autorité désignée, agit en toute indépendance et ne reçoit de l'autorité désignée aucune instruction concernant le résultat de ses vérifications. L'unité veille à ce que les conditions requises pour demander la comparaison d'empreintes digitales avec les données d'EURODAC soient remplies. Cette autorité sera chargée de collecter, conserver, traiter, analyser et échanger des informations afin de soutenir et renforcer l'action des États membres en matière de prévention ou de détection des infractions terroristes ou d'autres infractions pénales graves, ou des enquêtes en la matière, qui relèvent du mandat d'Europol.

Collecte, transmission et comparaison des empreintes digitales : chaque État membre devra relever sans tarder l'empreinte digitale de tous les doigts de chaque demandeur d'une protection internationale âgé de 14 ans au moins et la transmettre au système central dès que possible et au plus tard 72 heures suivant l'introduction de la demande de protection internationale. En cas de difficultés techniques graves, les États membres pourront prolonger le délai de 72 heures, d'une durée maximale de 48 heures afin d' exécuter leur plan national de maintenance.

Effacement anticipé des données : les données concernant une personne qui a acquis la nationalité d'un État membre, quel qu'il soit, devront être effacées du système central dès que l'État membre d'origine apprend que la personne concernée a acquis ladite nationalité. Le système central devra informer, **dès que possible et au plus tard après 72 heures**, de cette information, les autorités compétentes.

Conservation des données : les données dactyloscopiques d'un ressortissant de pays tiers ou à un apatride devront être conservées dans le système central pendant **18 mois** à compter de la date à laquelle ses empreintes digitales ont été relevées. Passé ce délai, le système central devra effacer automatiquement ces données.

Comparaison des données dactyloscopiques : en vue de vérifier si un ressortissant de pays tiers séjournant illégalement sur son territoire n'a pas auparavant introduit une demande de protection internationale dans un autre État membre, un État membre pourra transmettre au système central les données dactyloscopiques relatives aux empreintes digitales qu'il peut avoir relevées sur un tel ressortissant de pays tiers ou apatride, âgé de 14 ans au moins, ainsi que le numéro de référence attribué par cet État membre. Une fois les résultats de la comparaison des données dactyloscopiques transmis à l' État membre d'origine, **le système central ne devra conserver un enregistrement de la recherche** qu' aux seules fins prévues au règlement. **Les États membres ou le système central ne pourront conserver aucun autre enregistrement de la recherche à d'autres fins**.

Marquage des données : l'État membre d'origine ayant accordé une protection internationale à un demandeur d'une protection internationale dont les données ont été précédemment enregistrées dans le système central devra marquer les données pertinentes. Ce marquage devra être conservé dans le système central et **le système central devra informer tous les États membres d'origine du marquage par un autre État membre d'origine, de données ayant généré un résultat positif**.

Les données des bénéficiaires d'une protection internationale qui sont conservées dans le système central et qui sont marquées devront rester disponibles pour comparaison **pendant 3 ans** après la date à laquelle la protection internationale a été accordée à la personne concernée. Passé ce délai, le système central devra verrouiller automatiquement la transmission de ces données pour comparaison à des fins répressives, jusqu'à leur effacement définitif.

Conditions d'accès à EURODAC par les autorités désignées : les autorités désignées ne pourront présenter une demande électronique motivée de comparaison de données dactyloscopiques avec les données conservées dans le système central, que dans les limites de leurs compétences et que si la comparaison avec les bases nationales de données dactyloscopiques, les systèmes automatisés nationaux

d'identification par empreintes digitales d'autres États membres et, si possible, le système d'information sur les visas n'a donné **aucun résultat positif** en plus d'autres conditions cumulatives.

Il est également précisé que la comparaison ne pourra intervenir que s'il existe **des motifs raisonnables de penser que la comparaison contribuera de manière significative à la prévention ou à la détection de l'une des infractions pénales** ou aux enquêtes en la matière.

Des modalités équivalentes sont prévues pour conditionner l'accès d'EURODAC à Europol.

Procédure de comparaison à des fins répressives en cas d'urgence exceptionnelle : des dispositions nouvelles ont été introduites pour prévoir une transmission **en urgence** en vue de prévenir un danger imminent lié à une infraction terroriste ou à toute autre infraction pénale grave.

Lorsque l'identification définitive révèle que le résultat de la comparaison reçu du système central ne correspond pas aux données dactyloscopiques envoyées pour comparaison, les États membres devront effacer immédiatement le résultat de la comparaison.

Qualité des données transmises : dans un considérant, il est précisé que les États membres devront veiller à transmettre des données dactyloscopiques d'une qualité appropriée aux fins d'une comparaison par le système informatisé de reconnaissance des empreintes digitales. Toutes les autorités ayant un droit d'accès à EURODAC devraient investir dans une formation appropriée ainsi que dans l'équipement technologique nécessaire.

L'impossibilité temporaire ou permanente de recueillir et/ou de transmettre des données dactyloscopiques, soit pour des raisons telles qu'une qualité insuffisante des données pour effectuer une comparaison appropriée, des problèmes techniques ou des motifs de protection de la santé, soit du fait que la personne concernée est mise dans l'impossibilité ou dans l'incapacité de fournir des empreintes digitales en raison de circonstances hors de son contrôle, ne devrait pas avoir d'incidence négative sur l'examen de la demande de protection internationale que cette personne a introduite, ni sur la décision en l'espèce.

Protection des données à caractère personnel à des fins répressives : les États membres devront veiller à ce que les dispositions qu'ils ont adoptées pour mettre en œuvre la décision-cadre 2008/977/JAI s' appliquent aussi au traitement par les autorités nationales, de données à caractère personnel aux fins répressives. Les autorités compétentes de contrôle devront notamment contrôler la licéité du traitement de données à caractère personnel effectué par les États membres. Le Contrôleur européen de la protection des données devra également jouer un rôle dans ce cadre.

Incidents de sécurité : les États membres devront informer l'Agence européenne, des incidents de sécurité détectés dans leurs systèmes. De même, l'Agence devra informer les États membres, Europol et le Contrôleur européen de la protection des données en cas d'incidents de sécurité.

Interdiction de transfert à des pays tiers : les données à caractère personnel obtenues par un État membre ou EUROPOL et traitées par la suite dans des bases de données nationales ne pourront être communiquées à un pays tiers ni à aucune organisation internationale ou entité de droit privé établie ou non dans l'Union, ni mises à leur disposition. Les données à caractère personnel qui ont leur origine dans un État membre et sont communiquées entre États membres à la suite d'un résultat positif obtenu aux fins répressives, ne pourront être transmises à des pays tiers s'il existe un risque grave qu'en raison d'un tel transfert, la personne concernée puisse être soumise à la torture ou à un autre traitement inhumain et dégradant, à un châtiment ou à toute autre violation de ses droits fondamentaux.

Audit : les États membres devront veiller à ce qu'un organisme indépendant réalise chaque année un audit du traitement des données à caractère personnel aux fins répressives, y compris une analyse d'un échantillon des demandes électroniques motivées.

Rapports et évaluation : tous les 4 ans, la Commission devra rédiger un rapport global d'évaluation d' EURODAC qui examine les résultats obtenus par rapport aux objectifs fixés, ainsi que l'impact sur les droits fondamentaux, y compris la question de savoir si l'accès à des fins répressives a conduit à des discriminations indirectes à l'encontre des personnes relevant du règlement, et qui détermine si les principes de base restent valables, en tire toutes les conséquences pour les opérations futures et formule toute recommandation utile. La Commission devra transmettre cette évaluation au Parlement européen et au Conseil.

Sur la base des rapports annuels des États membres et d'Europol et outre le rapport global d'évaluation, la Commission devra compiler un rapport annuel sur l'accès des autorités répressives à EURODAC et transmettre ce rapport au Parlement européen, au Conseil et au Contrôleur européen de la protection des données.

Autres dispositions: des dispositions ont enfin été prévues en matière de :

- mise en place d'un plan de maintien des activités tenant compte des besoins en entretien et des temps d'arrêt imprévus du système ;
- relevé de statistiques trimestrielles ;
- prise en compte de l'intérêt supérieur de l'enfant lors de l'application du règlement ;
- réalisation d'une brochure à destination des personnes dont les empreintes sont relevées afin de leur communiquer des informations sur leurs droits.