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) - 26/06/2013 - Acte final

OBJECTIF : fondre en un règlement unique :

- le règlement sur la création du système «EURODAC» pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement de Dublin et pour les demandes de comparaison avec les données EURODAC présentées par les services répressifs des États membres et Europol à des fins répressives, et
- la modification du 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.

ACTE LÉGISLATIF : Règlement (UE) N° 603/2013 du Parlement européen et du Conseil relatif à la création d'EURODAC pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n° 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'EURODAC présentées par les autorités répressives 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).

CONTENU : le Parlement européen et le Conseil ont adopté un règlement destiné à refondre le règlement «EURODAC».

Il s'agit du dernier texte adopté dans le cadre de la révision de l'acquis communautaire en matière d'asile et de la mise en place d'un régime d'asile européen commun.

Les principaux points abordés par cette révision peuvent se résumer comme suit :

Objet d'EURODAC : comme auparavant, EURODAC contribuera à déterminer l'État membre qui, en vertu du règlement (UE) n° 604/2013 (règlement 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**.

Architecture du système : le règlement rappelle les grands composants du système qui constitue le système EURODAC actuel, soit :

- une base de données dactyloscopiques centrale et informatisée (ou "système central") comprenant: i) une unité centrale; ii) un plan et un système de maintien des activités;

- une infrastructure de communication entre le système central et les États membres, qui fournit un réseau virtuel crypté affecté aux données d'EURODAC ;
- un point d'accès national unique au système par État membre.

La gestion opérationnelle d'EURODAC reviendra à l'Agence. Le système devra être fonctionnel 24h/24 et 7j/7.

Autorités désignées des États membres à des fins répressives : en matière de lutte contre les infractions terroristes et les autres infractions pénales graves, il est essentiel que les autorités répressives disposent des informations les plus complètes et les plus récentes pour pouvoir exécuter leurs tâches. Á cette fin, les autorités désignées des États membres et Europol auront accès aux données d'EURODAC à des fins de comparaison et sous réserve des conditions strictes énoncées au règlement.

Les États membres devront dès lors 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**.

Ces autorités n'auront accès à EURODAC que dans des cas bien définis, et lorsqu'il existe de bonnes raisons de croire que l'auteur d'une infraction terroriste ou d'une autre infraction pénale grave a demandé une protection internationale. En tout état de cause, EURODAC ne pourrait être interrogé que si l'intérêt supérieur de la sécurité publique le commande et que si l'acte commis par le criminel ou le terroriste est si répréhensible qu'il justifie des recherches dans une base de données où sont enregistrées des personnes ayant un casier judiciaire vierge.

Les États membres devront également désigner une **autorité nationale unique** qui exercera la fonction d' autorité **chargée de la vérification**. Ces autorités devront agir en toute indépendance des autorités désignées et 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 également 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. Cette autorité sera chargée de collecter, conserver, traiter, analyser et échanger des informations afin de contribuer à la prévention ou à la détection des infractions terroristes ou d'autres infractions pénales graves.

Collecte, transmission et comparaison des empreintes digitales : chaque État membre sera chargée de relever 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 (ce délai pouvant être prolongé dans certains cas). Le dispositif prévoit la procédure à suivre pour transmettre et analyser les informations transmises au système central.

Type de données relevées et durée de leur conservation : seules seront enregistrées dans le système central les données énumérées au règlement dont en particulier : i) les données dactyloscopiques (empreintes digitales) ; ii) l'État membre d'origine, lieu et date de la demande de protection internationale; iii) la date à laquelle les empreintes ont été relevées, …

Ces données seront conservées en principe **10 ans**. Passé ce délai, elles seront automatiquement effacées.

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.

Comparaison des données dactyloscopiques en cas de franchissement irrégulier des frontières extérieures de l'UE : chaque État membre devra relever l'empreinte digitale de tous les doigts des ressortissants de pays tiers âgés de 14 ans au moins, qui, **à l'occasion du franchissement irrégulier** de sa frontière terrestre, maritime ou aérienne en provenance d'un pays tiers, a été interpellé par les autorités de contrôle compétentes. 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. Une fois les résultats de la comparaison des données 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.

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.

Conditions d'accès à EURODAC par les autorités désignées : il est précisé que la comparaison des données EURODAC 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.

Qualité des données transmises : il est également précisé que les États membres devront veiller à transmettre des données dactyloscopiques d'une qualité appropriée aux fins d'une comparaison par le système central. 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.

La numérisation des empreintes digitales et leur transmission devra s'effectuer dans le format fixé à l'annexe I du règlement. Dans la mesure où cela est nécessaire au bon fonctionnement du système central, l'Agence devra fixer les exigences techniques pour la transmission du format pour les données par les États membres au système central et inversement.

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.

Des dispositions sont également prévues pour assurer une protection adéquate des données et permettre de les rectifier ou de les effacer si elles sont erronées.

Sont également prévues des dispositions pour assurer la sécurité des données avant et pendant leur transmission au système central.

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.

Sanctions : les États membres devront prendre les mesures nécessaires pour que tout traitement des données saisies dans le système central non conforme à l'objet d'EURODAC soit passible de sanctions, y compris administratives et/ou pénales effectives, proportionnées et dissuasives.

Rôle de l'Agence : une série de dispositions ont été introduites pour mettre en conformité le règlement (UE) n° 1077/2011 instituant l'Agence, avec le présent règlement EURODAC révisé.

Rapport, suivi et évaluation : le 20 juillet 2018 au plus tard, et ensuite tous les 4 ans, la Commission devra rédiger un rapport global d'évaluation d'EURODAC qui examinera 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. La Commission devra transmettre cette évaluation au Parlement européen et au Conseil.

Dispositions territoriales : le Danemark, le Royaume-Uni et l'Irlande ne participent au présent règlement ni à son application, conformément aux dispositions pertinentes des traités. Le Royaume-Uni peut toutefois décider de s'y associer dans un délai de 6 mois, à compter de son entrée en vigueur.

ENTRÉE EN VIGUEUR : 19.07.2013.

APPLICABILITÉ : le présent règlement est applicable à partir du 20.07.2015.

Le règlement (CE) n° 2725/2000 et le règlement (CE) n° 407/2002 sont abrogés avec effet au 20.07.2015.