N° 678

SÉNAT

SESSION EXTRAORDINAIRE DE 2011-2012

Enregistré à la Présidence du Sénat le 18 juillet 2012

PROPOSITION DE RÉSOLUTION EUROPÉENNE

PRÉSENTÉE EN APPLICATION DE L'ARTICLE 73 *QUINQUIES* DU RÈGLEMENT,

sur la proposition de règlement du Parlement européen et du Conseil relative à la modification du **système** *«* **EURODAC** *» pour les demandes de* **comparaison** *avec les* **données d'« EURODAC »** *présentées par les* **services répressifs** *des* **États membres** *et* **Europol** *(E 7388), dont la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale s'est saisie.*

PRÉSENTÉE

Par M. Jean-Yves LECONTE,

Sénateur

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

En décembre 2008, la Commission européenne a présenté une proposition de refonte du règlement (CE) n° 2725/2000 relatif à la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

En septembre 2009, la Commission a modifié sa proposition afin de prendre en compte les remarques qui avait été faites par le Parlement et le Conseil. **En particulier, à la demande du Conseil, cette nouvelle proposition prévoyait une possibilité d'accès des services répressifs ainsi que d'Europol au fichier Eurodac**. Cette proposition étant devenue caduque avec l'adoption du traité sur le fonctionnement de l'Union européenne, la Commission a déposé le 11 octobre 2011 un nouveau texte ne comportant pas les dispositions relatives à l'accès des services répressifs, ceci afin de faciliter la négociation et l'adoption rapide des dispositions relatives à l'agence opérationnelle des systèmes d'information qui devait gérer Eurodac dès décembre 2012.

Toutefois, en mai dernier, à la demande des États membres, la commission a de nouveau modifié sa proposition en réintégrant les dispositions relatives à l'accès des services répressifs des États membres et d'Europol.

Cette nouvelle proposition faisant partie du Paquet « Asile » que la présidence Chypriote souhaite voir aboutir avant la fin de l'année, certains États membres se sont abstenus de manifester leur position afin de conserver une marge de manœuvre dans la négociation sur l'ensemble des textes.

Notre commission des lois s'est donc saisie de ce texte en vertu de l'alinéa 2 de l'article 73 *quinquies* du Règlement du Sénat pour établir une proposition de résolution ainsi qu'un rapport sur cette proposition.

En quoi consiste le traitement de données personnelles Eurodac ?

Eurodac[1] est un traitement de données personnelles communautaire utilisé depuis le 15 janvier 2003 et comprenant un système automatisé de reconnaissance d'empreintes digitales. La finalité de ce traitement est de déterminer l'État membre qui, en vertu de la convention de Dublin, est responsable de l'examen d'une demande d'asile déposée dans un des États de l'Union.

Le système Eurodac vise ainsi à prélever les empreintes digitales de trois catégories d'étrangers : les demandeurs d'asile (catégorie 1) ; les étrangers interpellés lors du franchissement irrégulier d'une frontière extérieure (catégorie 2) ; les étrangers se trouvant illégalement sur le territoire d'un État membre (catégorie 3 ; dans ce dernier cas les empreintes ne sont pas conservées après la comparaison).

En France, lorsqu'une personne demande l'asile dans une zone d'attente ou à la préfecture, ses empreintes sont ainsi comparées par le biais d'une borne Eurodac avec celles contenues dans le fichier, afin de déterminer si un autre État membre n'est pas responsable du traitement de la demande en vertu de Dublin II.

En 2010, la France a transmis près de 36 000 empreintes pour la catégorie 1, ce qui en fait le premier contributeur européen à Eurodac (16,7 % du total). Elle a réadmis 984 personnes sur son territoire et a transféré 883 autres personnes dans un autre État-membre, ce qui est peu élevé[2] et témoigne **du mauvais fonctionnement global du système de réadmission Dublin II**[3].

Pourquoi ouvrir l'accès aux services répressifs ?

La demande d'accéder pour des besoins d'enquête judiciaire au fichier Eurodac a émergé après les attentats de Madrid en 2004.

Les services répressifs des États membres ont alors estimé qu'avoir accès aux données d'Eurodac serait utile, en particulier dans le cadre de la lutte contre le terrorisme, **du fait de l'ampleur de la base biométrique**

---

[1] Les données contenues dans Eurodac sont : État membre d'origine, lieu et date de la demande d'asile ; empreintes digitales; sexe ; numéro de référence attribué par l'État membre d'origine ; date à laquelle les empreintes ont été relevées ; date à laquelle les données ont été transmises à l'unité centrale ; date à laquelle les données ont été introduites dans la base de données centrale ; renseignements sur les destinataires des données transmises et date des transmissions.

[2] En effet le taux de réponses positives serait d'environ 15%.

[3] En témoigne également l'impossibilité de renvoyer des personnes en Grèce depuis l'arrêt CEDH MSS c/Grèce et Belgique du 21 janvier 2011.

qui serait ainsi mise à leur disposition. En prévoyant une durée de consultation possible des données de deux ans, ce serait en effet environ 600 000 personnes dont les données deviendraient accessibles aux services répressifs.

Un tel accès permettrait ainsi de comparer une empreinte digitale directe (et, avec les évolutions technologiques prévisibles, une empreinte latente, c'est-à-dire une trace) retrouvée par exemple sur le lieu d'un attentat, avec les empreintes contenues dans la base, ou de comparer une empreinte déjà enregistrée dans un fichier national, en France le fichier national des empreintes digitales (FNAED), avec les empreintes d'Eurodac.

S'il s'avère que les empreintes proposées correspondent à une empreinte contenue dans Eurodac, les services répressifs pourraient, par exemple, parvenir à retracer le cheminement de l'individu suspect entre les différents pays de l'Union.

Selon la direction générale de la police nationale, entendue par votre rapporteur, il s'agirait d'utiliser cette nouvelle possibilité dans les cas les plus graves, comme une attaque terroriste, comme dernier recours si la consultation des fichiers judiciaires n'a pas permis de progresser dans l'enquête. La consultation d'Eurodac dans ce cadre serait donc probablement, selon elle, peu fréquente.

Toutefois, il convient de noter que la proposition de la Commission prévoit que l'accès est ouvert non seulement dans le cadre de la lutte contre le terrorisme mais aussi dans les enquêtes relatives à certains faits évoqués dans les infractions pénales graves visées dans la décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen[1], ce qui représente un champ beaucoup plus large que le seul terrorisme.

Selon quelle procédure technique la consultation aurait-elle lieu ?

La proposition de la Commission n'est pas d'une totale précision en ce qui concerne la nature de l'accès qui serait ouvert aux services répressifs. Deux possibilités sont envisageables :

- Après un simple résultat positif à l'issue d'une recherche (« hit »), avec indication du pays de première demande, les demandes d'informations supplémentaires relèveraient alors d'instruments existants, comme la décision-cadre 2006/960/JAI relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États, la coopération dans le cadre du traité de Prüm et l'entraide judiciaire ;

[1] *2002/584/JAI.*

- La deuxième possibilité est que la demande de données sur le demandeur d'asile soit intégrée au processus, l'État membre requérant pouvant solliciter directement, de l'État membre d'origine, des informations sur le demandeur d'asile auquel appartient l'empreinte digitale, au lieu de devoir utiliser les instruments existants pour faire cette demande ;

- Quant à l'accès d'Europol, il aurait lieu selon des modalités qui semblent encore mal définies et qui suscitent des interrogations (cf. ci-dessous).

Ce qui pose problème dans la possibilité d'un tel accès

1- La préservation de la finalité originelle du fichier

La première difficulté manifeste est que la finalité du fichier Eurodac est essentiellement de déterminer quel est l'État compétent pour traiter une demande d'asile. **La proposition de la commission modifie profondément cette finalité en faisant d'Eurodac un fichier de recherche**, ce qui pose d'emblée un problème de principe, proche de celui soulevé par le Sénat à l'occasion de l'examen de la proposition de loi sur la protection de l'identité. À cet égard, le fait que le système de réadmission Dublin II fonctionne plutôt mal alors qu'il constitue la justification de ce fichier ne doit pas amener à chercher des utilisations supplémentaires de la base Eurodac.

Il est vrai que ce fichier connaît déjà une utilisation accessoire par rapport à sa finalité essentielle : en effet, les État-membres peuvent comparer les empreintes de personnes appréhendées en situation irrégulière sur le territoire et qui refusent de présenter des documents d'identité ou présentent des faux documents (catégorie 3). Il s'agit d'offrir une chance supplémentaire à la police de pouvoir identifier la personne, **mais, en principe, seulement dans le cadre d'une procédure administrative d'éloignement**[1]. Par ailleurs, les conditions d'utilisation d'Eurodac ne paraissent pas, déjà actuellement, totalement sécurisées.

En France, il est en principe impossible pour les policiers ou les gendarmes d'effectuer directement, pour les besoins d'une enquête, des recherches dans une base de données qui ne regroupe pas des personnes suspectes d'avoir commis un crime ou un délit ou d'être susceptible d'en commettre. En effet, des fichiers spécifiques ont été créés à cette fin, au premier rang desquels le fichier national des empreintes digitales (FNAED) et celui des empreintes génétiques (FNAEG). Quant aux fichiers dont les

[1] *Dans ce cas, les empreintes ne sont pas enregistrées après la comparaison avec celles contenues dans Eurodac.*

finalités sont purement administratives, ils ne sont pas accessibles en principe pour les besoins d'une enquête, sauf dans certains cas sur réquisition judiciaire.

Si l'accès des policiers et des gendarmes à certains fichiers purement administratifs est tout de même prévu par l'acte réglementaire qui en définit le régime, cet accès est directement lié aux tâches que ces agents ont à accomplir pour mettre en œuvre les finalités administratives du fichier.

Ainsi, les services de police ou de gendarmerie utilisent aujourd'hui régulièrement l'application AGDREF de gestion du droit au séjour des étrangers, dans laquelle les demandeurs d'asile sont inscrits, ce que contestent d'ailleurs plusieurs associations. Toutefois, cette consultation a en principe pour seule finalité la mise en œuvre des décisions administratives relatives à ces étrangers.

Il existe toutefois une exception : la loi du 23 janvier 2006 a en effet donné accès aux fichiers administratifs courants[1] aux services de police et de gendarmerie, sans réquisition judiciaire, mais **dans le seul cadre de la lutte contre le terrorisme**. Encore cette possibilité a-t-elle été limitée dans le temps, de sorte que le législateur devra se prononcer avant le 31 décembre 2012 pour la proroger.

La Commission indique par ailleurs avoir consulté le contrôleur européen à la protection des données et le HCR. **Ces deux instances ont donné un avis défavorable**, en considérant que l'accès des services répressifs au fichier constituerait un détournement de la finalité originelle de celui-ci. Or, la Commission n'indique pas pourquoi elle n'a pas suivi ces avis.

En particulier, le contrôleur européen à la protection des données a estimé que l'accès des services répressifs à un fichier qui n'a pas cette finalité ne devrait être possible que « *pour autant que la nécessité de l'ingérence s'appuie sur des éléments clairs et indéniables et que la proportionnalité du traitement soit démontrée* ». Ainsi, selon lui, « *la nécessité de cet accès doit être prouvée par la démonstration de preuves solides d'un lien entre les demandeurs d'asile et/ou les formes graves de criminalité, ce qui n'a pas été fait dans les propositions* »[2].

Le HCR insiste pour sa part sur le risque qui serait encouru par les demandeurs si des informations étaient communiquées à leur pays d'origine, ainsi que sur **la stigmatisation** qui pourrait résulter d'une confusion entre demande d'asile et criminalité.

---

[1] *Fichiers des immatriculations, des permis de conduire, des cartes nationales d'identité, des passeports, des ressortissants étrangers en France, des demandes de visas et de titres de séjour.*

[2] *Avis n°2011/C 101/03.*

La CNIL a indiqué qu'elle n'était, quant à elle, pas favorable à la pratique qui consiste à ajouter peu à peu de nouvelles finalités à des fichiers créés dans un but précis.

Enfin, il convient de rappeler que **le fichier Eurodac n'est pas, à l'heure actuelle, tenu correctement par les pays-membres et en particulier par la France**. Les services de police et ceux de l'asile ont en effet eux-mêmes indiqué lors de leur audition par votre rapporteur que les données relatives aux demandeurs d'asile n'étaient pas, faute de moyens, mises à jour. Ainsi, les fiches des personnes qui ont obtenu le statut de réfugié ou la protection subsidiaire ne sont pas verrouillées. Les données relatives aux personnes qui ont obtenu la nationalité française ne sont pas non plus effacées. Cette situation rend encore plus nécessaire un usage prudent du fichier et qui soit conforme à sa finalité première.

2- La protection particulière des demandeurs d'asile

La question de la finalité du fichier se double en l'espèce de celle de la nécessaire protection des demandeurs d'asile. En effet, ceux-ci jouissent en droit interne d'une protection particulière, en raison de la vulnérabilité liée à leur situation précaire et à la nécessité absolue d'éviter que des informations les concernant puissent parvenir aux autorités des pays qui sont susceptibles de les avoir persécutés. Ce dernier risque est bien réel, certains pays de l'Union européenne n'ayant pas un système fiable de protection des données et étant même parfois susceptibles de transmettre par accident des informations à des pays tiers.

À l'occasion de son examen de la loi n° 97-396 du 24 avril 1997 portant diverses dispositions relatives à l'immigration, le Conseil Constitutionnel s'est ainsi prononcé sur l'accès des services répressifs au fichier de l'OFPRA, contenant les données relatives aux demandeurs d'asile. Il avait alors censuré la disposition prévoyant cet accès au motif que « *Considérant que la confidentialité des éléments d'information détenus par l'office français de protection des réfugiés et des apatrides relatifs à la personne sollicitant en France la qualité de réfugié est une garantie essentielle du droit d'asile, principe de valeur constitutionnelle qui implique notamment* ***que les demandeurs du statut de réfugié bénéficient d'une protection particulière*** *; qu'il en résulte que seuls les agents habilités à mettre en œuvre le droit d'asile, notamment par l'octroi du statut de réfugié, peuvent avoir accès à ces informations, en particulier aux empreintes digitales des demandeurs du statut de réfugié ; que dès* ***lors la possibilité donnée à des agents des services du ministère de l'intérieur et de la gendarmerie nationale d'accéder aux données du fichier informatisé des empreintes digitales des demandeurs du statut de réfugié***

créé à l'office français de protection des réfugiés et apatrides prive d'une garantie légale l'exigence de valeur constitutionnelle posée par le Préambule de la Constitution de 1946 ».

3- L'insuffisante définition des infractions concernées

La référence à la décision-cadre relative au mandat d'arrêt européen présente l'inconvénient de ne pas définir de manière précise les infractions concernées. Il ne peut certes s'agir que d'infractions punies par le droit pénal des États-membres de 3 ans d'emprisonnement au moins, mais avec un champ très large, incluant par exemple l'aide à l'entrée et au séjour irréguliers.

4- Le manque de précision des dispositions concernant l'accès d'Europol

Les dispositions de la proposition de Règlement prévoyant l'accès d'Europol à Eurodac pour les mêmes finalités que les services répressifs des État-membres sont peu claires. En effet, si la proposition évoque logiquement le cas où « *la comparaison est nécessaire pour l'accomplissement de ses tâches conformément à la décision Europol* », elle précise également qu'Europol pourrait consulter le traitement « **aux fins d'une analyse spécifique ou d'une analyse de portée générale et de type stratégique** ».

Comme l'a souligné la direction générale de la police nationale, la finalité de cette dernière disposition semble peu claire. En tout état de cause, un tel traitement général et stratégique semble impliquer une conservation de certaines données au-delà des seuls besoins d'une enquête judiciaire déterminée, ce qui ne semble pas souhaitable.

5- Un gain opérationnel limité par rapport aux possibilités dont disposent déjà les services répressifs

Il est peu probable que les services répressifs tirent un bénéfice important d'un accès à Eurodac. À titre de comparaison, lorsque les empreintes des personnes sont prises à des fins d'identification au titre de la catégorie 3 (« personne appréhendée en situation irrégulière sur le territoire »), les réponses positives du fichier semblent rares (moins de 2 %).

En outre, les services répressifs de chaque État-membre ont déjà accès au système d'information sur les visas (VIS) dans le cadre de la lutte contre le terrorisme et contre d'autres infractions graves, ce système

incluant dès l'origine une finalité de préservation de la sécurité intérieure de l'Union. Ils peuvent également, par le biais de la coopération policière, accéder sous certaines conditions aux fichiers biométriques nationaux des autres États-membres.

L'atteinte aux principes de finalité des fichiers et de protection particulière des demandeurs d'asile que constituerait un accès à Eurodac par les services répressifs serait donc sans doute disproportionnée par rapport au gain attendu.

Quelles sont cependant les garanties prévues en cas d'ouverture aux services répressifs ?

- L'accès à Eurodac ne pourra avoir lieu qu'au cas par cas, pour les besoin d'une enquête déterminée. En outre, la consultation ne pourra avoir lieu « *que s'il existe des motifs raisonnables de penser que la comparaison d'une empreinte avec celles contenues dans Eurodac contribuera à la prévention ou à la détection des infractions pénales (…) ou aux enquêtes en la matière* ». Certains États membres souhaitent toutefois la suppression de cette précision qu'ils jugent trop restrictive ;

- L'accès à Eurodac sera subsidiaire : les services demandeurs devront déjà avoir fait des recherches dans les bases de données dactyloscopiques de leur pays ainsi que, par les mécanismes de coopération, dans celles des autres États-membres[1] ;

- Les États-membres devront désigner une « *autorité vérificatrice* » chargée d'examiner la demande formulée par le service opérationnel de police. Cette autorité vérificatrice transmettra la demande de comparaison au point d'accès national si toutes les conditions requises sont remplies. Le point d'accès national interrogera ensuite le système central qui indiquera si l'empreinte proposée correspond à une empreinte du fichier ;

- Toutefois, dans des cas d'urgence exceptionnels, l'autorité chargée de la vérification pourra transmettre des données dactyloscopiques au point d'accès national pour comparaison immédiate dès réception d'une demande et ne vérifier qu'a posteriori si toutes les conditions sont remplies, et notamment s'il s'agit effectivement d'un cas d'urgence exceptionnel ;

- La décision-cadre 2008/977/JAI sur la protection des données en matière de coopération policière, judiciaire et pénale est applicable. Cette décision garantit toutefois un niveau de protection assez peu élevé ;

---

[1] *Dans le cadre de la décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.*

- Les données à caractère personnel qu'un État membre ou Europol obtient d'Eurodac en vertu du présent règlement seront effacées des dossiers nationaux et de ceux d'Europol après un mois, si ces données ne sont pas nécessaires à la poursuite d'une enquête pénale spécifique ;

- Les données recueillies ne pourront être transmises à aucun État-tiers. Une minorité d'États-membres souhaite toutefois que l'interdiction porte seulement sur le transfert de données au pays d'origine du demandeur d'asile. Or, **ce point est crucial puisqu'il ne faut en aucun cas que des données relatives à un demandeur d'asile puissent finalement parvenir à des autorités de son pays d'origine**.

La CNIL considère, sans préjudice de son appréciation négative sur le changement de finalité du fichier, que ces garanties semblent globalement substantielles et sérieuses.

En tout état de cause, quelles que soient ces garanties (et l'on pourrait envisager des garanties supplémentaires telles **qu'un contrôle judiciaire de l'accès aux données** et des efforts particuliers de traçabilité et d'évaluation des consultations), **elles ne peuvent remédier aux difficultés fondamentales que constituent le changement de finalité du fichier et l'atteinte à la protection des demandeurs d'asile qui en résulte**.

Les autres éléments nouveaux apportés par la proposition de Règlement

- La proposition introduit un délai maximal de 72 heures pour la transmission de l'empreinte d'un demandeur d'asile à la base centrale. Cette mesure, destinée à obliger certains pays à accélérer leur procédure de prise des empreintes, ne concerne pas la France qui les transmet immédiatement par le biais des bornes Eurodac ;

- La proposition prévoit une gestion unifiée des traitements de données personnelles communautaires par l'agence opérationnelle des systèmes d'information, ce qui semble de nature à améliorer l'efficacité de cette gestion ;

- **La proposition prévoit par ailleurs le marquage des données relatives aux personnes ayant obtenu une protection dans un État membre**. Jusqu'à présent, ces données étaient « verrouillées » dans le système. Elles n'étaient déverrouillées que si la personne concernée perdait sa protection. Dans le nouveau système, les données seraient marquées comme étant celles d'un demandeur qui a obtenu la protection. Il s'agirait d'éviter qu'une personne puisse faire une demande d'asile dans un État membre alors qu'elle a déjà obtenu la protection d'un autre État membre.

Selon l’analyse d’impact de la première proposition de modification du Règlement Eurodac faite par la Commission, seules 414 personnes (sur plus de un million dont les empreintes ont été relevées entre 2003 et 2007) auraient été dans ce cas, de sorte que l’on peut s’interroger sur la nécessité de ce dispositif ;

- Enfin, la proposition prévoit une modification de la durée de conservation des empreintes de catégorie 2, c’est-à-dire de celles des demandeurs appréhendés lors du franchissement irrégulier d’une frontière extérieure. Cette conservation passerait de deux ans à un an. Cette réforme, qui n’est pas justifiée par la Commission, ne semble pas particulièrement nécessaire.

PROPOSITION DE RÉSOLUTION

① Le Sénat,

② Vu l'article 88-4 de la Constitution,

③ Vu la proposition la proposition de règlement du Parlement européen et du Conseil (E 7388) relative à la refonte d'EURODAC ;

④ Considérant que la France et l'Union européenne se sont dotées d'un cadre juridique garantissant un haut niveau de protection des données personnelles ;

⑤ Considérant que l'utilisation des traitements de données personnelles en conformité avec des principes de finalité et de proportionnalité constitue un élément essentiel de ce cadre juridique et une garantie de l'acceptation sociale de ces traitements ;

⑥ Considérant par ailleurs que le droit d'asile est un principe de valeur constitutionnelle qui implique notamment que les demandeurs du statut de réfugié bénéficient d'une protection particulière ;

⑦ Considérant que toute atteinte à ces principes ne pourrait être fondée que sur une nécessité dûment justifiée ;

⑧ Considérant que le texte ne contient aucun élément étayant la probabilité que des personnes suspectées de terrorisme ou d'autres infractions graves se trouvent parmi les personnes ayant demandé l'asile dans un des pays membres de l'Union européenne ;

⑨ Estime que le fichier Eurodac doit garder sa finalité première qui est de déterminer, conformément au Règlement Dublin II, le pays responsable du traitement d'une demande d'asile ;

⑩ Estime que la circonstance que les garanties encadrant l'introduction de cette nouvelle finalité semblent sérieuses ne permet pas de lever la difficulté essentielle que pose cette nouvelle finalité, d'autant que l'intervention d'un juge n'est prévue à aucun stade de la procédure ;

⑪ Considère en revanche que l'amélioration de la gestion du traitement de données Eurodac, qui n'est actuellement pas satisfaisante, doit constituer une priorité, et approuve par conséquent les améliorations proposées par la Commission dans ce domaine ;

⑫ Considère enfin que l'intérêt d'un « marquage » dans Eurodac des personnes ayant déjà obtenu une protection internationale ainsi que d'un passage de deux à un an de la durée de conservation des données relatives aux personnes dont les empreintes ont été relevées à l'occasion d'un passage irrégulier de frontières n'est pas démontré.