RÉPUBLIQUE FRANÇAISE

Ministère des affaires étrangères et du développement international

PROJET DE LOI

autorisant l'approbation de l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des Etats-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de lutter contre la criminalité grave et le terrorisme

NOR : MAEJ1417807L/Bleue-1

ÉTUDE D'IMPACT

I. - Problématique et objectifs de l'accord

I.1- Coopération actuelle

Depuis les attentats du 11 septembre 2001, la sécurité intérieure est devenue une priorité absolue du gouvernement américain. Relèvent ainsi de cette priorité la lutte contre le terrorisme, la sécurisation des frontières, la gestion de crise et la cybercriminalité.

Dans ce contexte, la coopération opérationnelle avec les services américains est soutenue. Elle est en constante augmentation, en particulier avec le *Department of Homeland Security* (DHS) et avec les agences fédérales qui dépendent du ministère de la justice. Entretenue avant tout avec le *Federal Bureau of Investigation* (FBI) et la *Drug Enforcement Administration* (DEA), la coopération avec les États-Unis dans le domaine de la lutte contre la criminalité organisée ou grave est efficace, principalement en matière de lutte contre le trafic de stupéfiants et la pédopornographie. Dans le domaine de la lutte contre la drogue par exemple, la coopération se traduit par des échanges, réguliers et confiants, de renseignements opérationnels et stratégiques entre l'office central pour la répression du trafic illicite des stupéfiants de la Direction centrale de la police judiciaire (DCPJ) et la DEA. Elle est également active au travers d'échanges d'informations via le système Europol.

Les filières et réseaux sont désormais multinationaux et les individus concernés sont particulièrement mobiles, menant des opérations ou des actions tant sur le continent européen qu'américain. Ces organisations recourent également à des hommes "supports", qu'elles prennent soin de régulièrement déplacer dans des pays ou continents différents, afin de garantir leur discrétion et d'éviter l'établissement de rapprochements policiers ou judiciaires qui dévoileraient leurs structures et organisations.

Cette mobilité au sein des mouvements extrémistes violents et des groupes criminels organisés constitue également une forme d'adaptation de leur part aux nouvelles méthodes et techniques d'investigations mises en œuvre par les services d'enquête, qu'ils peuvent ainsi parvenir à contourner.

Dès lors, les outils internationaux sont devenus indispensables en matière de lutte contre la criminalité grave et transfrontalière ainsi que contre le terrorisme et le renforcement de la coopération transatlantique est, plus particulièrement, une nécessité. A titre d'exemple, c'est un renseignement américain qui a permis en juin 2012 la saisie de 113 kg de cocaïne dans le port du Havre.

Or seules les données dactyloscopiques et génétiques permettent désormais d'établir de façon certaine l'identité des personnes et de procéder à des identifications lors de l'utilisation par un même individu d'états civils différents. Il est donc essentiel que toutes les vérifications et recherches utiles puissent être faites par les services répressifs et notamment la consultation des fichiers existants, dans le respect des libertés et des droits fondamentaux.

Les actions de coopération opérationnelle sont difficilement quantifiables, par nature et en raison des différents canaux de coopération (relations directes entre services ; actions menées avec les services américains présents en France ; actions du service de sécurité intérieure de l'ambassade de France aux États-Unis).

En 2013, une centaine de commissions rogatoires internationales ont été traitées en collaboration entre le magistrat de liaison et l'attaché de sécurité intérieure de l'ambassade de France aux Etats-Unis. La coopération opérationnelle est également en constante augmentation avec les partenaires fédéraux et locaux.

Vingt actions de coopération techniques (missions d'experts, missions d'études, échanges de bonnes pratiques, etc.) ont enfin été menées en 2013 par la police et la gendarmerie nationales en matière de lutte contre la criminalité organisée et la pédopornographie et douze ont déjà été organisées au 1er juillet 2014.

I.2- Objectif de l'accord

a) L'accord vise avant tout à renforcer la coopération entre la France et les États-Unis en vue de prévenir, d'enquêter, de détecter et de poursuivre les infractions relatives à la criminalité grave (énumérées en annexe à l'accord), au terrorisme et autres faits passibles d'une peine privative de liberté égale ou supérieure à trois ans, en échangeant des informations sur les profils génétiques et les empreintes dactyloscopiques, ainsi que par la transmission spontanée d'informations à titre préventif.

Les points de contact nationaux peuvent accéder mutuellement aux bases de données dactyloscopiques et génétiques pour une consultation automatisée, au cas par cas (interrogation de type : concordance/pas de concordance). Des arrangements administratifs ultérieurs fixeront les modalités techniques de ces consultations. Pour la France, les fichiers interrogés sont le fichier national automatisé des empreintes génétiques pour les profils ADN – FNAEG (article 706-54 du code de procédure pénale), et le fichier automatisé des empreintes digitales – FAED (décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur).

Le FAED a une finalité judiciaire, sous réserve de l'exception introduite par le législateur au 4ème alinéa de l'article 78-3 du code de procédure pénale relatif à la procédure de vérification d'identité. Le FAED, dont le fonctionnement automatisé a démarré en 1991, permet « en vue de faciliter la recherche et l'identification des auteurs de crimes et délits et de faciliter la poursuite l'instruction et le jugement des affaires criminelle et délictuelles » (article 1 décret n°87-249 du 8/4/1987, modifié le 7/2/2001) l'enregistrement et le traitement automatisé des empreintes papillaires relevées sur « des personnes à l'encontre desquelles il existe des indices graves ou concordant rendant vraisemblable qu'elles aient pu participer, comme auteur ou comme complice, à la commission d'un crime ou d'un délit, ou des personnes mises en cause dont l'identification certaine s'avère nécessaire », et des traces papillaires relevées dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire, d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte ou de l'exécution d'un ordre de recherche délivré par l'autorité judiciaire (article 3 décret n°87-249 du 8/4/1987, modifié le 7/2/2001). Cela exclut donc *de facto*, tout traitement automatisé ou toute signalisation papillaire dans un cadre administratif.

L'objectif du FNAEG, qui a également une finalité judiciaire, est d'effectuer des rapprochements entre les empreintes génétiques prélevées sur des individus suspects ou condamnés ou sur des scènes d'infractions, et les profils déjà enregistrés dans la base de données. Il diffère notamment du fichier précédent en raison de la liste des infractions susceptibles de donner lieu à l'enregistrement de données dans le fichier. En effet, ces infractions exclusivement de nature criminelle ou délictuelle sont limitativement énumérées à l'article 706-55 du code de procédure pénale. Ainsi les délits routiers, de même que l'escroquerie simple (article 313-1 du code pénal) ne constituent pas des infractions susceptibles de donner lieu à enregistrement dans le FNAEG.

Au 31 août 2014, le FAED est une base de données dans laquelle les empreintes digitales et palmaires de 5 031 723 individus et 233 300 traces papillaires non identifiées sont enregistrées. Le FNAEG, à la même date, compte 2 655 381 profils génétiques individus et 237 217 profils traces non identifiées.

En France, ces consultations sont réalisées par la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire.

Le point de contact national de l'État requérant est informé par voie automatisée de l'absence de concordance ou des données indexées pour lesquelles une concordance a été constatée.

Les motifs de consultation renvoient à la législation nationale de l'État à l'origine de l'interrogation. Les consultations de données dactyloscopiques s'opèrent donc dans le respect de la législation nationale de l'État à l'origine de l'interrogation. La consultation automatisée de profils ADN n'est par ailleurs permise que lorsque chaque législation nationale l'autorise et selon le principe de réciprocité.

Les dispositions de l'accord limitent les droits de consultation aux fins de prévention et de détection des infractions entrant dans son champ d'application ainsi qu'aux enquêtes en la matière.

Lorsque la consultation d'empreintes digitales ou de profils ADN aboutit à une concordance, la seule information, dont l'accord prévoit la transmission sans renvoi à la législation nationale et de manière automatique, est celle relative à la présence de l'empreinte dactyloscopique ou génétique. A ce stade, cette information ne constitue pas une donnée à caractère personnel, car elle n'est pas encore reliée aux coordonnées enregistrées dans la base de l'État requis. La seule information qui parvient alors à l'État à l'origine de l'interrogation est la confirmation que l'empreinte de l'individu figure dans la base de données interrogée par la transmission des « données indexées » qui sont constituées d'un numéro associé à la donnée biométrique, mais qui ne permettent pas l'identification directe de la personne concernée : celle-ci n'est en aucun cas automatique et n'intervient que lors d'une seconde étape.

La transmission de données complémentaires s'effectue en vertu du droit national de l'État requis, y compris les dispositions relatives à l'entraide judiciaire. Les données pouvant être transmises comprennent les noms, prénoms, date et lieu de naissance, ainsi qu'un exposé des circonstances à l'origine des soupçons d'infractions de l'intéressé (2ème paragraphe de l'article 9).

L'État requis peut soumettre l'utilisation des données transmises à certaines conditions. A cet égard, l'article 8 du présent accord dispose très clairement qu'en cas de concordance de données dactyloscopiques ou de profils génétiques, toute transmission s'opère en vertu de la législation nationale de l'État requis. Cette clause permet donc à la France de refuser la transmission de données complémentaires si leur utilisation contrevient à la législation nationale, en particulier dans les procédures pénales pour lesquelles la peine de mort est encourue, conformément à l'article 66-1 de la Constitution du 4 octobre 1958.

Dans le cadre de la coopération policière, l'envoi de la requête par le canal d'Interpol à partir de la plateforme de la section centrale de coopération opérationnelle de police (SCCOPOL), rattachée à la direction centrale de la police judiciaire, permettra de bénéficier de la présence sur place de la mission « justice » du bureau de l'entraide pénale internationale (BEPI). Ce bureau appartient à la direction des affaires criminelles et des grâces du ministère de la Justice, mission avec laquelle la SCCOPOL travaille quotidiennement en matière d'échanges d'informations de nature ou à vocation judiciaire (mandats d'arrêt et commissions rogatoires internationales).

Jusqu'à ce que les deux législations nationales permettent les consultations génétiques automatisées, chaque État peut effectuer, à la demande de l'autre, une consultation de son propre fichier. En effet, l'organisation fédérale américaine attribue à chaque Etat fédéré la gestion de son propre fichier génétique. Le laboratoire du FBI centralise, notamment, les profils génétiques des personnes concernées par certaines infractions fédérales, celles du district de Columbia (siège du laboratoire), ou encore certains profils de ressortissants étrangers condamnés par des juridictions fédérales.

Le futur système prévu par l'accord permettra une interrogation directe des bases de données de chaque Etat, contenues dans le "National DNA Index System" (NDIS), qui centralisait - en mars 2013 - environ 12 millions de données. Toutefois, dans l'attente d'un tel système intégré entre la France et les Etats-Unis et en application du présent accord, l'interrogation doit demeurer possible par les canaux actuels (Interpol).

Par ailleurs, dans le domaine du terrorisme et de la criminalité organisée, l'accord prévoit aussi la possibilité, en application de la législation nationale de chaque État, d'échanges d'informations d'initiative (dont des données à caractère personnel), pour prévenir la commission d'infractions. S'agissant plus particulièrement de la prévention des actes de terrorisme, l'unité de coordination de la lutte anti-terroriste (UCLAT), rattachée à la direction générale de la police nationale, est le point de contact dans les relations bilatérales avec les États-Unis. L'UCLAT sera donc le point de contact pour la transmission d'informations.

b) Le présent accord s'inscrit par ailleurs dans un contexte où le gouvernement fédéral des États-Unis a mis en place dès 1986 un programme d'exemption de visa (« *Visa Waiver Program* ») pour les pays développés dans le but de faciliter le tourisme et les voyages d'affaires sur son territoire, pour des séjours n'excédant pas trois mois.

Après les attaques terroristes de septembre 2001, les conditions de maintien du programme d'exemption de visa impliquent désormais que les pays bénéficiaires développent des échanges d'informations avec les États-Unis, plus particulièrement pour la prévention et la lutte contre la criminalité grave et le terrorisme.

Les États-Unis ont dès lors proposé la conclusion d'accords de coopération en matière de prévention et de répression de la criminalité organisée et du terrorisme aux États membres de l'UE bénéficiaires du *Visa Waiver Program* (à ce jour, seuls la Bulgarie, la Roumanie, la Pologne, la Croatie et Chypre n'en font pas partie) et désireux de le conserver.

c) Enfin, le présent accord s'inspire largement :

- d'une part, du Traité relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, signé le 27 mai 2005 par la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche (dit « traité de Prüm ») ;

- d'autre part, des décisions du Conseil de l'Union européenne du 23 juin 2008 n° 2008/615/JAI « *relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière*[1] » et n° 2008/616/JAI « *concernant la mise en œuvre de la décision 2008/615/JAI*[2] ». Ces deux actes ont eu pour objet de faire entrer les dispositions principales du traité de Prüm dans le cadre juridique de l'Union européenne.

II. - <u>Conséquences estimées de la mise en œuvre de l'accord</u>

II.1- <u>Conséquences en matière de lutte contre la criminalité</u>

Les échanges de profils génétiques et de données dactyloscopiques qui seront effectués contribueront à renforcer de façon significative la coopération bilatérale avec les États-Unis, à optimiser les échanges entre les deux États et à accélérer le traitement des dossiers visant le démantèlement des réseaux liés à la criminalité grave et au terrorisme.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:FR:PDF
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:FR:PDF

II.2- Conséquences économiques

Compte tenu des éléments précités, l'accord constituera un outil supplémentaire à la disposition des autorités des deux États pour la lutte contre la criminalité transnationale, y compris dans sa dimension économique.

A noter toutefois, par ailleurs, que le risque que la France ne remplisse plus les conditions pour être un État bénéficiaire du *Visa Waiver Program* aurait des conséquences négatives pour les deux États, notamment en matière économique, dès lors que le retour à un régime de visa obligatoire aurait pour effet de compliquer l'accès de nos ressortissants au territoire des États-Unis.

II.3- Conséquences financières

Aucune nouvelle structure administrative ne devrait être créée et, de ce point de vue, aucune charge financière supplémentaire ne sera induite par la mise en œuvre de l'accord (*cf. infra point II.5 sur les conséquences administratives*). Sur le plan technique, la mise en œuvre de l'accord pourrait impliquer des développements en matière de systèmes informatiques et de canaux d'échanges d'informations, qui ne peuvent être chiffrés à ce jour car les choix techniques ne sont pas arrêtés et les flux d'échanges envisagés sont difficiles à estimer.

II.4- Conséquences juridiques

II.4.1- Articulation avec le droit interne et les conventions internationales

Les considérants de l'accord soulignent l'importance de la coopération dans la lutte contre le terrorisme et la criminalité grave, l'importance de l'échange d'informations entre les autorités compétentes, tel que prévu dans le traité et les décisions Prüm de l'Union européenne et la volonté des États de rendre cette coopération plus efficace, tout en respectant les libertés et les droits fondamentaux, notamment le respect de la vie privée.

Une telle coopération s'opère dans le respect des droits fondamentaux qui résultent des exigences constitutionnelles des deux États. Sont notamment visés dans l'accord :

- la Charte des droits fondamentaux de l'Union européenne, dont les articles 7 et 8 garantissent le respect de la vie privée et la protection des données à caractère personnel ;

- la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, selon laquelle toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance (article 8) ;

- la Convention 108 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 le Protocole additionnel du 8 novembre 2001[3], qui fixe les normes minimales destinées à protéger les personnes contre les abus qui pourraient se produire lors de la collecte et du traitement de données à caractère personnel et qui est également destinée à réglementer les flux transfrontaliers des données à caractère personnel.

[3] http://conventions.coe.int/treaty/fr/treaties/html/181.htm

A noter par ailleurs que les accords d'extradition et d'entraide judiciaire conclus respectivement entre la France et les États-Unis les 23 avril 1996 et 10 décembre 1998 rappellent l'ancienneté de la coopération en matière d'extradition et d'entraide judiciaire avec les Etats-Unis. En particulier, la possibilité qu'un échange d'informations puisse constituer une preuve conduisant aux États-Unis à une condamnation à la peine capitale est de fait exclue, l'article 6 de l'accord d'entraide judiciaire précité permettant à chaque partie de refuser l'entraide «*lorsque l'exécution de la demande risque de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels*».

Enfin, les échanges d'empreintes digitales se réaliseront dans le cadre d'un fichier des empreintes digitales (FAED) réformé. En effet, la Cour européenne des droits de l'Homme a jugé que certaines dispositions du décret n°87-249 du 8 avril 1987 relatif au FAED étaient contraires à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, 18/04/2013, n° 19522/09 - Affaire M. K. c/ France). Suite à cet arrêt, la modification en cours du décret du 8 avril 1987 a pour objectif de limiter aux seuls crimes et délits le champ infractionnel dans le cadre duquel il est possible de recourir au FAED et de garantir un droit effectif à l'effacement en cas d'acquittement, de relaxe, d'un classement sans suite ou d'un non-lieu avant la fin des 25 ans correspondant à la durée de conservation maximale des données prévues par le décret.

II.4.2- Compétence nationale pour conclure un accord de ce type et articulation avec le droit de l'Union européenne

a/ Il convient de rappeler que, conformément à une jurisprudence constante de la Cour de justice, les Etats membres ne peuvent plus signer et conclure d'engagements internationaux dans des domaines relevant des compétences partagées au plan interne qui ont fait l'objet d'une harmonisation complète au niveau de l'Union (voir, notamment, arrêt du 5 novembre 2002, Commission/Danemark, C-467/98, points 83 et 84, et avis de la Cour de justice 1/03, du 7 février 2006, point 122) ou dans des domaines relevant des compétences partagées au plan interne qui sont couverts en grande partie par des règles communes, c'est-à-dire par des règles de droit dérivé (voir, notamment, avis de la Cour de justice 2/91 du 19 mars 1993, points 25 et 26).

Or, s'il n'est pas contestable que l'espace de liberté de sécurité et de justice relève en grande partie de compétences partagées couvertes par des règles communes, la directive 95/46/CE[1], la directive 2002/58/CE[2] et le [règlement 45/2001[3]], ne s'appliquent pas au traitement des données à caractère personnel mis en œuvre pour l'exercice d'activités dans le domaine pénal (voir article 3, paragraphe 2, de la directive 95/46/CE, article 1er, paragraphe 3, de la directive 2002/58/CE, et article 3, paragraphe 1er, lu à la lumière du quinzième considérant, du règlement 45/2001).

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

[2] Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

[3] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation des données

Par ailleurs, si la décision-cadre 2008/977/JAI[4] porte sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, celle-ci s'applique uniquement aux traitements transfrontières de données échangées entre les autorités des Etats membres ou avec les autorités ou systèmes d'information de l'Union (voir article 1er, paragraphe 2, de la décision-cadre).

En tout état de cause, la décision du Conseil de l'Union européenne du 23 juin 2008 n° 2008/615/JAI «*relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière*», et qui avait pour but d'intégrer, en substance, les dispositions du traité de Prüm dans le cadre juridique de l'Union européenne (cf. 1er considérant), prévoit explicitement qu'après son entrée en vigueur, *«les Etats membres peuvent conclure des accords bilatéraux (…), ou leur donner effet, pour autant que ces accords prévoient d'étendre les objectifs de la présente décision »* (cf. article 35, paragraphe 2, sous b).

C'est ce que le présent accord vise précisément à faire vis-à-vis des Etats-Unis.

La décision précitée prévoit en outre qu'aucune de ses dispositions « *ne porte atteinte aux accords ou conventions bilatéraux ou multilatéraux conclus entre des États membres et des États tiers »* (cf. article 35, paragraphe 6).

b/ Il convient par ailleurs de préciser que, suite aux révélations de l'affaire Prism (du nom du programme américain de la NSA permettant aux services américains de surveiller les communications des citoyens non-Américains transitant par les serveurs internet de Google, Facebook, Yahoo ou Microsoft), la Commission a adopté, en novembre 2013, une communication concernant les échanges de données entre l'Union européenne et les Etats-Unis et présenté des propositions pour rebâtir la confiance vis-à-vis de ces transferts. Ces propositions portent notamment sur l'adoption de la révision du cadre juridique européen en matière de protection des données (champ d'application territorial, règles en matière de transferts internationaux, etc.), ainsi que sur le renforcement de la protection des données dans le cadre de la coopération judiciaire et policière en matière pénales.

c/ Le présent accord s'inscrit dans le contexte de plusieurs négociations en cours en matière de protection des données personnelles.

D'une part, le paquet législatif (proposition de règlement et proposition de directive) de la Commission présenté début 2012 a qui a pour objet de réviser le cadre juridique de la protection des données dans l'UE. Cette réforme majeure doit garantir un haut degré de protection des données personnelles.

[4] Décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

D'autre part, les négociations menées par la Commission, au nom de l'UE, en vue d'un accord avec les Etats-Unis relatif à la protection des données personnelles lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou d'en poursuivre les auteurs. Conformément au mandat de négociation qui lui a été confié par le Conseil (JAI) du 3 décembre 2010, la Commission a pour mission d'atteindre les quatre objectifs suivants : garantir un niveau élevé de protection des libertés, apporter un cadre juridique cohérent et contraignant de normes régissant la protection des données, assurer un degré élevé de protection des données, favoriser la coopération judiciaire et policière.

Par ailleurs, deux accords ont été conclus entre les Etats-Unis et l'Union européenne en matière de lutte anti-terroriste. Il s'agit d'une part de l'accord entré en vigueur le 1er août 2010 concernant le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (Terrorist Finance Tracking Program) et, d'autre part, de l'accord sur le transfert des données des passagers des compagnies aériennes (PNR), entré en vigueur le 1er juillet 2012.

A noter enfin que l'arrêt rendu le 8 avril dernier par la CJUE (Digital Rights Ireland et Seitlinger, C-293/12 et C-594/12) invalidant la directive 2006/24 relative à la conservation des données par les fournisseurs de services de communications électroniques n'a pas d'incidence sur le présent accord. En effet, ce dernier ne concerne pas la conservation de données de trafic et de localisation afférentes aux communications électroniques, mais l'accès aux données dactyloscopiques (empreintes digitales) et au profil ADN. La directive 2006/24 et cet accord ont donc des objets différents, tant s'agissant des données en cause que des opérations dont elles font l'objet.

II.4.3- Protection des données et sécurité des échanges avec les États-Unis

a) Le transfert de données vers des Etats tiers n'appartenant pas à l'Union européenne est régi par les articles 68, 69 et 70 de la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés. Ces articles transposent les articles 25 et 26 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Les entreprises établies aux Etats-Unis ont la possibilité d'adhérer à un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Ces principes sont rassemblés sous le terme de *Safe Harbor* (« *sphère de sécurité* »). L'adhésion de l'entreprise à ces principes l'autorise à recevoir des données en provenance de l'Union européenne.

Les échanges de données prévus par l'accord relèvent de l'article 69 de la loi du 6 janvier 1978 qui prévoit un régime particulier lorsqu'il s'agit d'échanger des données avec des services de police étrangers notamment aux fins de sauvegarde de l'intérêt public. Pour mémoire, cet article transpose l'article 26 de la directive 95/46 précitée prévoyant une dérogation au principe de transfert des données exclusivement vers des pays assurant un niveau de protection adéquat des données personnelles au motif que « *le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice* ». Il prévoit une procédure par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, lorsque « *le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet* ».

Dans le présent accord, la partie française a négocié des garanties détaillées *infra* afin d'encadrer les échanges de données dans un ensemble de dispositions protectrices des libertés et des droits fondamentaux.

b) Aux États-Unis, le dispositif de la protection des données à caractère personnel est différent du système français car il est organisé par chaque État fédéré et par matière. Il est notamment dépourvu d'une autorité de contrôle nationale indépendante, telle qu'en France avec la Commission nationale informatique et libertés, et il n'existe pas de recours individuel pour des citoyens non-résidents.

Toutefois, dans la lignée des annonces faites à ce sujet par le président Obama en janvier 2014, le ministre de la Justice américain, Eric Holder, s'est engagé le 25 juin dernier, lors de la rencontre ministérielle UE-Etats-Unis dans le domaine « Justice-affaires intérieures », à favoriser l'introduction au Congrès de projets de législation visant à étendre aux Européens certaines des protections prévues par le *Privacy Act* de 1974 en matière de données personnelles, notamment la possibilité de former des recours judiciaires.

c) Afin de répondre aux exigences en matière de protection des données à caractère personnel et de respect de la vie privée protégée par les accords internationaux appliqués par la France, les stipulations de l'accord répondent aux impératifs suivants :

- les données échangées doivent répondre strictement aux finalités de l'accord et doivent être pertinentes, adéquates et non excessives ;

- les garanties relatives à la protection des données doivent être mises en œuvre de manière effective.

Au titre des garanties substantielles négociées pour cet accord figurent :

- la gestion par chaque État d'un registre des données transmises ou reçues afin, notamment, de contrôler le respect des règles de protection desdites données (principe de proportionnalité, adéquation, pertinence et exactitude des données), de vérifier le bien-fondé des demandes et de permettre une traçabilité des échanges ;

- la limitation des transmissions de données reçues en provenance d'un État tiers ou à destination d'un État tiers ou d'une organisation internationale (subordonnée au consentement de l'État concerné ou de l'État émetteur) ;

- la transmission et la conservation des données le temps nécessaire à la procédure pour laquelle elles ont été demandées. Elles peuvent être utilisées également pour d'autres procédures mais seulement avec l'accord de l'État qui les transmet ;

- un mécanisme de contrôle, par une autorité indépendante chargée de la protection des données ou une autorité compétente en la matière ;

- l'existence de procédure permettant à toute personne un droit de recours approprié pour violation de ses droits à la protection des données, indépendamment de la nationalité ou du pays de résidence de l'intéressé ;

- la possibilité de suspendre l'application de l'accord en cas de manquement substantiel aux obligations fixées ;

- la possibilité de dénoncer l'accord pour tout motif, avec préavis de trois mois.

Il est précisé explicitement dans l'accord (cf. article 10, litera f) que ses stipulations ne sauraient être interprétées comme interférant avec les obligations légales des États, telles que prévues par leurs législations respectives. Aucune modification de la législation nationale n'est nécessaire pour l'entrée en vigueur de l'accord.

L'accord est conclu pour une durée indéterminée. L'article 12 prévoit toutefois un bilan, un an après sa mise en œuvre, puis autant que de besoin, notamment en ce qui concerne la question de la protection des données.

II.4.4- Autorisation des traitements concernés.

Il n'est pas nécessaire de modifier les décrets qui concernent ces fichiers, dans la mesure où leur consultation pour le compte d'autres États est prévue par :

- le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur[4] (article 9-1) ;

- le décret n° 2009-785 du 23 juin 2009 relatif à l'accès d'organisations internationales et d'États étrangers au fichier national automatisé des empreintes génétiques[5] (article 1er qui insère un article R.53-19-1 au code de procédure pénale).

II.5- Conséquences administratives

La mise en œuvre de l'accord implique la désignation par chaque État d'un ou de plusieurs « points de contacts nationaux ». Elle ne semble pas de nature à engendrer des charges excessives ou substantiellement supérieures à celles résultant de la coopération déjà engagée entre les deux États ou à celle déjà mise en place pour les coopérations avec d'autres partenaires. En effet, et quoique les décisions n'aient pas encore été arrêtées, les points de contact désignés seront vraisemblablement ceux déjà en place dans le cadre des décisions « Prüm». Aucune nouvelle structure administrative ne devrait donc être créée.

Les échanges actuels de données biométriques avec les Etats-Unis sont réalisés dans le cadre des lettres d'entraide internationale via l'OIPC-Interpol et sont très limités. Deux raisons peuvent expliquer ces faibles flux : la faiblesse de la demande nationale actuelle (tant américaine que française) et l'absence d'un outil technique simple pour permettre ces échanges.

Avec la mise en place d'un outil analogue aux décisions « Prüm » de 2008, la possibilité d'un accroissement des échanges avec les Etats-Unis existe, mais ne peut être évalué de façon chiffrée ou précise à ce stade.

Un outil de régulation de ces échanges pourra cependant aisément être basé sur celui prévalant pour les échanges « Prüm », limitant notamment le nombre d'interrogations quotidiennes pour les données dactyloscopiques. Par ailleurs, les interrogations étant réalisées au cas par cas, les flux en termes de données génétiques ne devraient pas occasionner de difficultés.

[4] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006065909
[5] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020788005&dateTexte=&categorieLien=id

III- Historique des négociations

En 2008, les États-Unis ont exprimé le souhait d'entrer en négociation avec la France en vue d'échanger les données génétiques et empreintes digitales, afin de lutter contre la criminalité organisée. Une première proposition de la Partie américaine d'un protocole d'accord est intervenue en juillet 2009.

Conduites pendant presque 3 ans, les négociations, complexes, ont porté sur deux principaux points sensibles pour la France : le cadre d'échange des informations, ainsi que le niveau de protection des données à caractère personnel.

IV- État des signatures et ratifications

Le texte de l'accord a été signé par le ministre français de l'Intérieur le 3 mai 2012 et la secrétaire d'État américaine aux affaires intérieures le 11 mai 2012.

A ce jour, les États-Unis n'ont pas encore achevé leur procédure de ratification. L'accord bilatéral « Prüm transatlantique » signé par les Etats-Unis (dits aux Etats-Unis « Preventing and Combating Serious Crime Agreements-PCSC ») entre dans la catégorie des « executive agreements ». Celui-ci n'a pas besoin d'être ratifié par le Sénat (à la différence des traités) pour entrer en vigueur après leur signature. Le pouvoir exécutif doit toutefois les notifier au Congrès dans un délai de 60 jours suivant la signature de l'accord.

S'agissant d'un accord international comportant des stipulations intervenant dans le champ législatif, son approbation doit faire, côté français, l'objet d'une procédure d'autorisation parlementaire en vertu de l'article 53 de la Constitution./.