N° 48

SÉNAT

SESSION ORDINAIRE DE 2014-2015

Enregistré à la Présidence du Sénat le 22 octobre 2014

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* **États-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***,*

PRÉSENTÉ

au nom de M. Manuel VALLS,

Premier ministre

Par M. Laurent FABIUS,

ministre des affaires étrangères et du développement international

(Envoyé à la commission des affaires étrangères, de la défense et des forces armées, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs

I. - Le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique ont conclu un accord, sous forme d'échange de lettres, 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.

II. - Cet accord s'inscrit dans le double cadre des dispositions prises par les autorités américaines pour renforcer la lutte contre la criminalité et le terrorisme et la coopération judiciaire, technique et opérationnelle conduite entre la France et les États-Unis d'Amérique.

Précisément :

a) Le Gouvernement fédéral des États-Unis a mis en place en 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. Pratiquement, les ressortissants des pays inclus dans le programme ne sont pas assujettis à l'obligation de visa pour un séjour de moins de trois mois.

À ce jour, trente-six pays participent à ce programme, dont vingt-trois États membres de l'Union européenne (Allemagne, Autriche, Belgique, République tchèque, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Portugal, Slovaquie, Slovénie, Suède et Royaume-Uni). La France y participe depuis 1990.

b) À la suite des attentats du 11 septembre 2001, les autorités américaines ont significativement renforcé les conditions d'appartenance ou de maintien au programme. En particulier, la loi américaine du 3 août 2007 oblige les pays bénéficiaires à développer des échanges d'informations avec les États-Unis, plus particulièrement dans le domaine de la prévention et de la répression du terrorisme et de la criminalité grave.

Dans ce contexte, les États-Unis ont souhaité entamer une négociation en matière de coopération policière avec chacun des États membres de l'Union européenne, bénéficiaire du programme d'exemption de visa. À cette fin, ils ont proposé un accord s'inspirant très largement du traité de Prüm[1] du 27 mai 2005, tel qu'il a été partiellement incorporé dans les 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*[2] » et n° 2008/616/JAI « *concernant la mise en œuvre de la décision 2008/615/JAI*[3] ».

III. - C'est en 2008 que les États-Unis ont souhaité entrer en négociation avec la France. Une première proposition d'accord a été présentée en juillet 2009. La négociation a finalement été conclue au printemps 2012 et sanctionnée par un échange de lettres signées respectivement le 3 mai 2012 par le ministre français de l'intérieur et le 11 mai par la secrétaire d'État américaine, chargée de la sécurité du territoire.

Au total, les négociations de l'accord ont ainsi duré deux ans et demi, en raison notamment de la mise au point des dispositions relatives à la protection des données personnelles. La France est, en effet, dotée d'une législation stricte dans ce domaine, allant au-delà des dispositions en vigueur au niveau européen.

À noter à cet égard qu'un considérant de l'accord rappelle également les obligations que la France tire de la Charte des droits fondamentaux de l'Union européenne, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et de 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 du protocole additionnel du 8 novembre 2001.

IV. - L'accord conclu entre le gouvernement français et le Gouvernement des États-Unis d'Amérique vise à permettre une consultation mutuelle et automatisée des fichiers d'analyses ADN et des systèmes d'identification dactyloscopique, selon un système de

---

[1] Traité entre le Royaume de Belgique, la République Fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale.

[2] in JOUE L 201 du 6.08.2008, p. 1 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:FR:PDF)

[3] in JOUE L 201 du 6.08.2008, p. 12 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:FR:PDF)

concordance/sans concordance ou « *hit/no hit* » (dans ce cas, seule l'existence d'une concordance entre les données de l'État demandeur et les données de l'État requis permet l'accès ultérieur aux données personnelles qui sont stockées dans les bases de données de l'État requis).

Précisément, l'accord comporte seize articles.

L'**article 1er** définit les différents termes de l'accord : « profil ADN », « données dactyloscopiques », « données indexées », « données à caractère personnel » et « traitement des données à caractère personnel ».

À noter que les définitions des données indexées relatives aux profils ADN et aux empreintes dactyloscopiques ne doivent pas permettre l'identification directe des individus qu'elles concernent. La définition du « traitement des données à caractère personnel » s'inspire largement de celle qui figure à l'article 24, paragraphe 1, de la décision du Conseil n° 2008/615/JAI précitée.

L'**article 2** définit l'objectif et le champ d'application de l'accord :

- l'objectif de l'accord vise à renforcer la coopération dans le cadre de la justice pénale, principalement par l'échange d'informations relatives aux empreintes génétiques et dactyloscopiques, en vue de prévenir, d'enquêter, de détecter et de poursuivre les infractions liées à la criminalité grave et en particulier au terrorisme ;

- le champ d'application couvre les infractions punies d'une peine privative de liberté égale ou supérieure à trois ans. Ainsi défini, ce champ correspond à la définition de crime grave visée à l'article 2, paragraphe 2, de la décision-cadre n° 2002/584/JAI du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres.

L'**article 3** définit les conditions de consultation automatisée des empreintes digitales tandis que l'**article 5** définit les conditions de consultation automatisée des profils ADN. A l'instar des dispositions pertinentes des décisions dites Prüm précitées, ces articles prévoient la consultation mutuelle automatisée des banques nationales de données indexées au moyen du système concordance/non concordance. Dans ce cadre, chaque concordance positive entraîne de manière systématique une vérification humaine, réalisée par le point de contact national.

La consultation doit s'inscrire dans le cadre d'une enquête clairement délimitée. Elle doit ainsi avoir lieu en vue de poursuivre des infractions pénales : partant, elle devra toujours s'effectuer dans le cadre d'une

procédure d'enquête ou d'une procédure judiciaire. La consultation ne peut s'opérer qu'au cas par cas et dans le respect du droit national, à l'instar de ce que prévoient les articles 3 et 9 de la décision du Conseil n° 2008/615/JAI précitée.

En vue de ces échanges, les **articles 4 et 6** prévoient que chaque Partie désigne, conformément à son droit interne, un ou plusieurs points de contact en charge de centraliser et de traiter les demandes ou les réponses aux demandes d'échanges de données indexées. Par ailleurs, les dispositions opérationnelles et techniques des procédures décrites aux articles 3 et 5 seront établies dans le cadre d'arrangements administratifs entre autorités compétentes.

L'**article 7** permet à chaque Partie d'effectuer une consultation de son propre fichier ADN à la demande de l'autre Partie, dans l'attente que la législation de chacune des Parties permette l'accès automatisé aux profils ADN détenus par l'autre Partie.

L'**article 8** stipule que, si la comparaison automatisée fait ressortir des concordances entre les données dactyloscopiques ou les profils ADN, l'échange de données à caractère personnel doit intervenir selon les dispositions du droit national et dans le cadre de l'entraide judiciaire.

L'**article 9** porte sur la transmission d'informations en vue de prévenir des infractions terroristes et des crimes graves. Aux termes de cet article, les Parties peuvent échanger des données à caractère personnel, sur demande ou spontanément, en vue de prévenir des infractions liées à la criminalité grave dont les infractions terroristes, lorsque certains faits laissent présumer que des personnes sont susceptibles de commettre ces infractions. Ces données comprennent les noms, prénoms, date et lieu de naissance, ainsi que les circonstances précises qui conduisent à la présomption invoquée.

L'autorité transmettant les données peut, en vertu du droit national, fixer au cas par cas des conditions relatives à leur utilisation par l'autorité destinataire. Cette dernière est liée par ces conditions. Cet échange d'informations se fait par les points de contacts nationaux.

L'**article 10** vise à garantir un niveau suffisant de protection des données à toute personne dont les données sont recueillies.

Il énumère, d'une part, les dispositions générales devant guider l'utilisation de ces données (principes de sécurité liés à la manipulation des données et de confidentialité qui s'y attache ; engagement des Parties à

transmettre et à traiter les données personnelles conformément à leur législation respective) ;

Il précise, d'autre part, les restrictions imposées aux Parties dans l'utilisation des données. En particulier, celles-ci ne doivent être traitées qu'en vue des finalités prévues par l'accord.

Par ailleurs, les données transmises ne peuvent provenir d'un précédent échange avec un État tiers à l'accord sans le consentement préalable de cet État ; de même, les données transmises entre les Parties ne peuvent-elles être envoyées à un État tiers ou à une organisation internationale qu'avec le consentement préalable de la Partie ayant transmis les données.

La correction, le blocage et la suppression des données sont réalisés à la demande expresse de la Partie qui transmet ces données en vue de leur mise à jour ou de la concordance avec la finalité pour laquelle elles ont été transmises.

Chaque Partie doit tenir un registre afin d'assurer la traçabilité des données, de suivre la mise en œuvre correcte des législations respectives et de garantir la sécurité des données. Les données du registre dont l'accès doit être protégé, sont conservées durant deux ans. Une autorité de contrôle doit être désignée dans le cadre d'arrangements administratifs.

Les Parties doivent prendre les dispositions nécessaires pour garantir la sécurité des données. Elles s'assurent des mesures techniques employées en vue de protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle ou la divulgation, l'altération, l'accès ou toute autre forme de traitement non autorisé.

Les dispositions de l'accord ne portent pas atteinte aux obligations définies par leurs législations respectives, visant à informer sur les finalités du traitement, l'identité du responsable, les destinataires, l'existence du droit d'accès et le droit de rectifier, compléter, actualiser ou supprimer les données concernant la personne, les données échangées, et le droit à réparation tant que ces informations ne nuisent pas à la finalité visée par le traitement, aux enquêtes en cours par les autorités compétentes des deux Parties ou aux droits des tiers. En cas de violation des droits d'une personne, celle-ci peut, en application du droit national de chaque Partie, obtenir réparation sans aucune discrimination liée à sa nationalité ou à son pays de résidence.

L'**article 11** précise que l'accord ne peut limiter ou porter atteinte aux relations existantes entre les États-Unis et la France.

À noter en particulier que la possibilité qu'un échange d'informations puisse constituer une preuve conduisant aux États-Unis à une condamnation à la peine capitale est exclue, conformément à l'accord d'entraide judiciaire signé par la France et les États-Unis le 10 décembre 1998 et dont l'article 6 permet le refus de 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 ».

L'**article 12** définit les conditions de consultations mutuelles et la procédure d'évaluation de la mise en œuvre de l'accord. En cas d'interprétation différente du texte entre les Parties, celles-ci se consultent en vue de résoudre leurs divergences.

L'**article 13** stipule que chaque Partie supporte le coût afférent à la mise en œuvre de l'accord par ses services.

Conformément à l'**article 14**, l'accord peut être suspendu par l'une des Parties en cas de manquement substantiel aux obligations de l'accord par l'autre Partie. L'accord peut par ailleurs être dénoncé avec un préavis écrit de trois mois.

Aux termes de l'**article 15**, l'accord peut être amendé à tout moment par un accord écrit entre les Parties.

L'**article 16** précise les conditions d'entrée en vigueur de l'accord. L'entrée en vigueur des articles 5 et 6 relatifs à la consultation des données ADN est subordonnée à la conclusion des arrangements qui doivent préciser les modalités techniques permettant la mise en œuvre de cette consultation.

Telles sont les principales observations qu'appelle l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-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. Cet accord permettra d'échanger des données à caractère personnel, il comporte donc des dispositions de nature législative et doit être soumis au Parlement en vertu de l'article 53 de la Constitution.

PROJET DE LOI

Le Premier ministre,

Sur le rapport des affaires étrangères et du développement international,

Vu l'article 39 de la Constitution,

Décrète :

Le présent 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 États-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, délibéré en Conseil des ministres après avis du Conseil d'État, sera présenté au Sénat par le ministre des affaires étrangères et du développement international, qui sera chargé d'en exposer les motifs et d'en soutenir la discussion.

Article unique

Est autorisée l'approbation de l'accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-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 (ensemble une annexe), signées à Paris le 3 mai 2012 et à Washington le 11 mai 2012, et dont le texte est annexé à la présente loi.

Fait à Paris, le 22 octobre 2014

Signé : MANUEL VALLS

Par le Premier ministre :

Le ministre des affaires étrangères et du développement international,

Signé : LAURENT FABIUS

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./.

A C C O R D

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 (ensemble une annexe),

signées à Paris le 3 mai 2012

et à Washington le 11 mai 2012

Le ministre de l'intérieur
de l'outre-mer,
des collectivités territoriales
et de l'immigration

Paris, le 3 mai 2012.

Chère Madame le Ministre,

J'ai l'honneur, d'ordre de mon Gouvernement, de vous proposer les dispositions contenues dans l'annexe de la présente lettre. Je vous serais obligé de me faire savoir si les termes de cette annexe recueillent l'agrément de votre Gouvernement.

Dans ce cas, la présente lettre et son annexe ainsi que votre réponse constitueront l'accord entre nos deux Gouvernements 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, accord qui entrera en vigueur après la notification par chacun de nos deux Gouvernements à l'autre de l'accomplissement des procédures internes requises par sa législation, conformément à l'article 16.

Je vous prie d'agréer, Madame le Ministre, l'expression de mes respectueux hommages.

Claude Guéant

Madame Janet Napolitano
Secrétaire d'Etat
aux Affaires intérieures
Washington Etats-Unis

Dear Secretary Napolitano,

Acting on the instructions of the French Government, I have the honour of putting forward for your approval the provisions contained in the document enclosed with this letter. I would be much obliged if you would let me know whether the terms of this document are acceptable to the Government of the United States.

If such is the case, the present letter and the document that accompanies it, together with your reply, will constitute the agreement between our two governnents on enhancing cooperation in criminal investigations with a view to preventing and combating terrorism and serious crime. The said agreement will enter into force after each of our governments has notified the other that it has completed the necessary measures required by its domestic law, in accordance with Article 16.

Please accept the renewed assurances of my highest consideration,

Claude Guéant

Ms Janet Napolitano
Secretary of Howeland Security
Washington D.C.
United States of America

Département de la Sécurité intérieure
des Etats-Unis d'Amérique

11 mai 2012.

Monsieur le Ministre,

J'ai l'honneur d'accuser réception de votre lettre, en date du 3 mai 2012, accompagnée de sa pièce jointe.

J'ai également l'honneur de vous informer que la proposition contenue dans votre lettre recueille l'agrément du Gouvernement des Etats-Unis d'Amérique et de confirmer que votre lettre et sa pièce jointe ainsi que la présente lettre constituent un accord entre nos gouvernements sur le renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de combattre le terrorisme et la grande criminalité. Conformément à l'article 16 de la pièce jointe susmentionnée, cet accord entrera en vigueur, hormis les articles 5 et 6 de cette même pièce jointe, le premier jour du deuxième mois suivant la date de réception de la dernière note diplomatique entre les Parties indiquant que chacune d'elles a accompli les procédures internes requises pour l'entrée en vigueur de l'accord.

Je saisis cette occasion pour vous renouveler les assurances de ma plus haute considération.

Bien cordialement,

[signature]

Janet Napolitano

M. Claude Guéant
Ministre de l'Intérieur

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

Le Gouvernement de la République française et le Gouvernement des Etats-Unis d'Amérique (ci-après dénommés « les Parties ») ;

Motivés par la volonté de coopérer en tant que partenaires pour prévenir et combattre plus efficacement la criminalité grave, et notamment le terrorisme ;

Reconnaissant que le partage des informations est un élément constitutif essentiel dans la lutte contre la criminalité grave, et notamment le terrorisme ;

Reconnaissant l'importance de combattre la criminalité grave, et notamment le terrorisme, tout en respectant les droits et libertés fondamentaux, notamment ceux de la vie privée ;

Ayant à l'esprit les engagements de la France énoncés par l'article 16 et le titre V relatifs aux accords internationaux du Traité sur le fonctionnement de l'Union européenne ; l'article 8, paragraphe 2 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, les articles 7 et 8 de la Charte des droits fondamentaux du 18 décembre 2000, le niveau de protection prévu pour le traitement des données à caractère personnel dans la convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel du 8 novembre 2001 ;

Considérant l'étroite coopération mutuelle qui profite aux services répressifs respectifs des deux Parties et les retombées bénéfiques de cette relation en termes de sécurité accrue de nos citoyens ;

Reconnaissant la coopération de longue date entre les services répressifs respectifs des deux Parties conjuguée à la coopération formelle en vertu des traités d'entraide judiciaire et d'extradition entre la République française et les Etats-Unis d'Amérique ayant intégré des garanties en vue d'assurer l'utilisation appropriée et la protection des données à caractère personnel, dont l'efficacité et l'adéquation ont été démontrées ;

Tenant compte de la mise en œuvre réussie des accords transatlantiques récents de coopération policière et judiciaire, en particulier les accords Etats-Unis d'Amérique-Europol, l'accord Etats-Unis d'Amérique-Eurojust et l'accord entre les Etats-Unis d'Amérique et l'Union européenne portant sur l'entraide judiciaire et l'extradition et les 54 traités entre les Etats-Unis d'Amérique et les Etats membres de l'Union européenne qui appliquent ces accords ;

S'inspirant du traité relatif au renforcement de la coopération transfrontalière, en particulier dans la lutte contre le terrorisme, la criminalité transfrontalière et l'immigration clandestine, signé à Prüm le 27 mai 2005, et de la décision du Conseil de l'Union européenne y afférente du 23 juin 2008 (2008/615/JA1) ;

Considérant l'accord entre l'Union européenne et les Etats-Unis d'Amérique en matière d'entraide judiciaire en date du 25 juin 2003, et notamment son article 9 ; le traité entre la République française et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale du 10 décembre 1998 et l'instrument tel que prévu par l'alinéa 2 de l'article 3 de l'accord d'entraide judiciaire entre l'Union européenne et les Etats-Unis d'Amérique signé le 25 juin 2003 et l'Instrument relatif à la mise en œuvre du traité entre la République française et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale du 10 décembre 1998, signé le 30 septembre 2004 ;

Reconnaissant les efforts menés par l'Union européenne et les Etats-Unis d'Amérique en vue d'aboutir à un accord relatif à la protection des données à caractère personnel lors de leur transfert ou de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de poursuivre leurs auteurs dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale.

Cherchant à améliorer et encourager la coopération entre les Parties dans un esprit de partenariat ;

Sont convenus de ce qui suit :

Article 1er

Définitions

Aux fins du présent Accord :

1. Le « profil ADN » se définit par un code alphanumérique qui représente un ensemble de caractéristiques d'identification de la partie non codante d'un échantillon d'ADN humain analysé, c'est-à-dire la structure moléculaire particulière issue de divers segments d'ADN (loci) ;

2. Les « données dactyloscopiques » sont les images d'empreintes digitales, les images d'empreintes digitales latentes les images d'empreintes palmaires, les images d'empreintes palmaires latentes ainsi que les modèles de ces images (points caractéristiques codés ou minuties) lorsqu'elles sont stockées et traitées dans une base de données automatisée ;

3. Les « données indexées » comprennent, d'une part, le profil ADN issu de la partie non codante de l'ADN et une référence attachée (données de référence ADN), d'autre part, les données dactyloscopiques et une référence attachée (données indexées des empreintes digitales). Les données indexées ne doivent pas contenir des informations permettant l'identification directe de la personne concernée ;

4. Les « données à caractère personnel » comprennent toute information permettant l'identification directe ou indirecte d'une personne ;

5. Le « traitement des données à caractère personnel » concerne toute opération ou ensemble d'opérations réalisées à partir de données à caractère personnel, par des moyens automatisés ou non, tels que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou l'altération, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou la mise à disposition, l'alignement ou la combinaison, le blocage, l'effacement ou la destruction de ces données.

Article 2

Objectif et champ d'application

1. L'objectif du présent Accord est de renforcer, dans le cadre de la justice pénale, la coopération entre les Etats-Unis d'Amérique et la France en vue de prévenir, enquêter, détecter et poursuivre les infractions relatives à la criminalité grave, et en particulier au terrorisme, principalement par des échanges d'informations concernant les profils ADN et les données dactyloscopiques.

2. Le champ d'application du présent Accord couvre les infractions énoncées à l'annexe de cet Accord et les autres faits passibles d'une peine privative de liberté égale ou supérieure à trois ans.

Article 3

Consultation automatisée des données dactyloscopiques

1. Aux fins énoncées à l'article 2, les Parties autorisent les points de contact nationaux de l'autre Partie, visés à l'article 4, à accéder à leurs traitements automatisés d'identification dactyloscopique, sur la base d'une interrogation « concordance/pas de concordance ».

2. Les droits de consultation prévus par le présent Accord sont exclusivement utilisés aux fins de prévention et de détection des crimes graves et des enquêtes relatives à ceux-ci, et uniquement si des circonstances particulières et fondées en droit concernant une personne déterminée conduisent à rechercher si cette dernière commettra ou a commis un crime grave. Les consultations ne peuvent s'opérer qu'au cas par cas et dans le respect de la législation nationale de la Partie requérante.

3. L'établissement définitif d'une concordance entre une donnée dactyloscopique et une donnée indexée détenue par la Partie gestionnaire du fichier doit être réalisé par le point de contact national de la Partie requérante, par la transmission, par voie automatisée, des données indexées nécessaires à l'établissement d'une concordance claire. Si aucune concordance ne peut être constatée, ce résultat est communiqué de manière automatisée.

Article 4

Points de contact nationaux et arrangements de mise en œuvre

1. En vue de la mise en œuvre des dispositions de l'article 2 du présent Accord, chaque Partie désigne, au sein des services en charge des missions mentionnées à l'article 2, un ou plusieurs points de contact nationaux pour la demande ou la transmission de données telles que prévues à l'article 3 du présent Accord. Les compétences du ou des points de contact nationaux sont régies par la législation nationale de cet Etat.

2. Les modalités techniques permettant de mettre en œuvre la procédure de consultation visée à l'article 3 seront définies dans le cadre d'arrangements administratifs ultérieurs.

Article 5

Consultation automatisée des profils ADN

1. Aux fins énoncées à l'article 2, si la législation nationale de chacune des Parties l'autorise et sur la base de la réciprocité,

les Parties autorisent les points de contact nationaux de l'autre partie (visés à l'article 6) à accéder aux profils ADN contenus dans leurs traitements automatisés pour procéder à des comparaisons sur la base d'une interrogation « concordance/pas de concordance ».

2. Les droits de consultation prévus par le présent Accord sont exclusivement utilisés aux fins de prévention, de détection des crimes graves et des enquêtes relatives à ceux-ci et uniquement si des circonstances particulières et fondées en droit concernant une personne déterminée conduisent à rechercher si cette dernière commettra ou a commis un crime grave. Les consultations ne peuvent s'opérer qu'au cas par cas et dans le respect de la législation nationale de la Partie requérante.

3. Si, dans le cadre d'une consultation automatisée, une concordance est établie entre un profil ADN transmis et un profil ADN enregistré dans le fichier de la Partie requise, le point de contact national de la Partie requérante est informé par voie automatisée des données indexées pour lesquelles une concordance a été constatée. Si aucune concordance ne peut être constatée, communication en est faite de manière automatisée.

Article 6

Points de contact nationaux et arrangements de mise en œuvre

1. En vue de la mise en œuvre des dispositions de l'article 2 du présent Accord, chaque Partie désigne, au sein des services en charge des missions mentionnées à l'article 2, un ou plusieurs points de contact nationaux pour la demande ou la transmission de données telles que prévues à l'article 5 du présent Accord. Les compétences du ou des points de contact nationaux sont régies par la législation nationale de chacune des Parties.

2. Les modalités techniques permettant de mettre en œuvre la procédure de consultation visée à l'article 5 seront définies dans le cadre d'arrangements administratifs ultérieurs.

Article 7

Autres moyens de consultation des fichiers ADN

Jusqu'à ce que les législations des deux Parties permettent des consultations de profils ADN telles que décrites dans l'article 5, chaque Partie peut, à la demande de l'autre Partie, conformément à la législation et dans le respect des contraintes techniques de la Partie requise, effectuer une consultation de son propre fichier ADN.

Article 8

Transmission de données à caractère personnel complémentaires et d'autres données suite à une concordance

1. En cas de constatation de concordance de données dactyloscopiques ou de profils ADN dans le cadre de la procédure prévue aux articles 3 et 5, la transmission de données à caractère personnel complémentaires disponibles et de toute autre donnée relative aux données indexées s'opère en vertu de la législation nationale de la Partie requise, y compris, le cas échéant et sans préjudice du paragraphe 3 de l'article 9, les dispositions relatives à l'entraide judiciaire.

2. Ces données peuvent porter sur les noms, prénoms, date et lieu de naissance de la personne pour laquelle la constatation de concordance a eu lieu ainsi qu'un exposé des circonstances ayant justifié la collecte et l'enregistrement des données par la Partie requise.

Article 9

Transmission d'informations en vue de prévenir des actes de terrorisme et des crimes graves

1. Afin de prévenir des infractions constituant une menace sérieuse pour l'intérêt public, les Parties peuvent, en application de leur législation nationale, au cas par cas, sans même en avoir reçu la demande, transmettre au point de contact national approprié de l'autre Partie, comme énoncé au paragraphe 5 du présent article, les données à caractère personnel visées au paragraphe 2 du présent article. Dans la mesure où cela est nécessaire, cette transmission pourra s'effectuer au vu de circonstances particulières laissant penser que le personne concernée est susceptible de commettre des infractions terroristes ou liées au terrorisme, ou des infractions en lien avec un groupe ou une association terroriste, ou des infractions liées à la grande criminalité telles qu'elles sont définies par la législation nationale de la partie émettrice.

2. Les données pouvant être transmises comprennent les noms, prénoms, date et lieu de naissance ainsi qu'un exposé des circonstances qui sont à l'origine des soupçons visés au paragraphe 1 du présent article.

3. La Partie émettrice peut, en vertu de sa législation nationale, imposer, au cas par cas, des conditions quant à l'utilisation qui peut être faite de ce type de données par la Partie destinataire. Si la Partie destinataire accepte lesdites données, elle est tenue au respect de toutes ces conditions. La Partie émettrice ne saurait toutefois, en application du présent paragraphe, imposer à la partie destinataire, comme condition à la transmission des données, des restrictions d'ordre générique au cadre légal relatif au traitement de données à caractère personnel de la Partie destinataire.

4. En complément des données à caractère personnel visées au paragraphe 2 du présent article, les Parties peuvent se transmettre mutuellement des données à caractère non personnel en relation avec les infractions visées au paragraphe 1 du présent article.

5. Chaque Partie désigne un ou plusieurs points de contact nationaux, afin d'échanger, comme prévu au présent article, avec le ou les points de contact de l'autre Partie des données à caractère personnel ou autres types de données. Les droits et obligations des points de contacts nationaux sont définis par la législation nationale de leur pays.

Article 10

Protection des données à caractère personnel

a) Règles de principe

1. Les Parties reconnaissent comme essentielles lors de leur traitement le respect de la confidentialité et la protection appropriée des données à caractère personnel transférées dans le cadre du présent Accord.

2. Les Parties transmettent et traitent les données à caractère personnel conformément à leur législation nationale respective et aux objectifs du présent Accord. Elles s'engagent en conséquence à :

– s'assurer que les données à caractère personnel transmises sont adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont communiquées ;
– conserver les données transmises pendant la seule durée d'utilisation nécessaire au regard des finalités définies à l'article 2 du présent Accord ;
– s'assurer que toute erreur constatée dans les données à caractère personnel soit signalée à la Partie destinataire, afin que des mesures rectificatives appropriées soient entreprises par celle-ci.

3. Le présent Accord n'affecte pas les droits existants par ailleurs en vertu de la législation nationale des Parties, qu'il s'agisse de la création de nouveaux droits ou de la limitation de ceux existants.

b) Limitations dans les procédures de traitement

1. Les informations personnelles sont soit transmises dans le cadre du présent Accord uniquement aux fins des investigations ou de l'enquête ayant motivé la demande, soit transmises spontanément en vertu de l'article 9. Les données transmises en vertu du présent Accord doivent être traitées selon les modalités prévues au paragraphe *a* 2 du présent article.

2. Ces données à caractère personnel peuvent aussi, avec le consentement préalable de la Partie émettrice, être utilisées pour traiter des procédures relevant du présent Accord et directement liées aux procédures, investigations ou à l'enquête pour lesquelles elles ont été sollicitées ou transmises.

3. Ce consentement est donné selon les modalités prévues au présent Accord, notamment aux fins relevant du présent Accord.

4. Les dispositions du présent article ne préjugent pas du recours à l'assistance judiciaire mutuelle dans les cas spécifiques où les Parties considéreront qu'elle est la voie appropriée pour obtenir ou transmettre des informations.

5. Les données transmises pour comparaison doivent être effacées immédiatement après que celle-ci a été effectuée ou après avoir reçu la réponse automatisée résultant de la demande en cours, sauf si elles sont nécessaires à la poursuite de l'enquête en cours.

6. Les données transmises en vertu des articles 3 et 5 du présent Accord ne peuvent provenir d'échanges de données préalablement effectués avec des Etats tiers sans le consentement de ces derniers.

7. Les Parties ne peuvent transmettre les données reçues dans le cadre du présent Accord à un Etat tiers ou à une organisation internationale sans le consentement de la Partie émettrice.

c) Rectification, blocage et suppression des données

1. A la demande expresse de la Partie émettrice, la Partie destinataire rectifie, bloque ou efface, si nécessaire, les données reçues en application du présent Accord si elles sont incorrectes ou incomplètes ou si leur collecte ou traitement complémentaire enfreint le présent Accord ou les règles applicables à la Partie émettrice.

2. Lorsqu'une Partie est informée que les données reçues de l'autre Partie en vertu du présent Accord ne sont pas exactes, elle doit prendre, afin de se prémunir de leur manque de fiabilité, toute mesure appropriée comme compléter, supprimer ou corriger lesdites données.

d) Tenue d'un registre des données

1. Chaque Partie tient un registre des données transmises à l'autre Partie ou reçues de celle-ci en application du présent Accord. Ce registre est créé aux fins :

– d'assurer le contrôle effectif du respect des règles de protection des données conformément aux législations nationales respectives des Parties ;
– de permettre aux Parties d'user effectivement des droits qui leur sont octroyés aux termes des articles 3 et 5 ;
– d'assurer la sécurité des données.

2. Doivent être inclus dans le registre :

– le motif ayant entraîné la transmission de données ;
– les informations relatives aux données transmises ;
– la date de transmission ;
– l'ensemble des destinataires des données s'il y a lieu de les partager avec d'autres entités.

3. Les informations contenues dans ce registre doivent être protégées par des mesures adéquates contre une utilisation inappropriée et doivent être conservées pendant deux ans.

4. Le contrôle du respect des règles applicables à la transmission ou à la réception de données à caractère personnel relève de la responsabilité des autorités indépendantes en charge de la protection des données ou, le cas échéant, des autorités compétentes en la matière de la Partie concernée. La désignation de la ou des autorités indépendantes compétentes doit figurer dans les arrangements administratifs subséquents.

e) Sécurité des données

1. Les Parties s'assurent que les mesures techniques et les modes d'organisation appropriés sont utilisés pour protéger les données contre la destruction accidentelle ou illégale, la perte accidentelle ou la divulgation non autorisée, l'altération, l'accès ou toute autre forme de traitement non autorisée. Les Parties doivent notamment prendre des mesures afin de garantir que seuls les agents des services répressifs chargés des missions mentionnées à l'article 2 soient autorisés à avoir accès aux données à caractère personnel.

2. Les accords et les arrangements de mise en œuvre qui régissent les procédures de consultation automatisée des fichiers d'empreintes digitales et d'ADN conformément aux articles 3 et 5 doivent prévoir :

– une utilisation appropriée des technologies modernes afin que la protection, la sécurité, la confidentialité et l'intégrité des données soient garanties ;
– des procédures de cryptage et d'autorisation reconnues par les autorités compétentes dès lors que des réseaux publiquement accessibles sont utilisés ;
– un mécanisme de traçabilité permettant de contrôler que seules des consultations autorisées sont menées.

f) Transparence – Transmission d'informations aux personnes concernées par les données – Droit de recours

1. Aucune disposition du présent Accord ne saurait être interprétée comme interférant avec les obligations légales des Parties, telles que prévues par leurs législations respectives, de fournir à la personne concernée des informations sur les finalités du traitement, l'identité de l'autorité de contrôle, les destinataires ou catégories de destinataires, l'existence du droit d'accès, de rectification, d'ajout, de mise à jour ou de suppression des données la concernant, ainsi que toute autre information supplémentaire telle que les bases juridiques relatives à l'opération de traitement, les données échangées et le droit de recours, dans la mesure où ces informations supplémentaires sont nécessaires.

2. La mise à disposition de telles informations peut être refusée conformément à la législation nationale respective des Parties si leur transmission risque de compromettre :

– les finalités du traitement ;
– les enquêtes ou les poursuites menées par les autorités compétentes aux Etats-Unis d'Amérique ou par les autorités compétentes en France ; ou
– les droits et libertés des tierces parties.

3. Les Parties garantissent l'existence de procédures qui permettent à toute personne concernée d'avoir accès à un recours approprié pour violation de ses droits à la protection des données à caractère personnel, indépendamment de la nationalité ou du pays de résidence de l'intéressé.

Article 11

Rapports avec les autres accords internationaux

Aucune disposition du présent Accord ne saurait être interprétée comme limitant ou portant préjudice aux dispositions des autres traités ou accords, aux relations de travail entre services répressifs ou au droit national qui permettent les échanges d'informations entre les Etats-Unis d'Amérique et la France.

Article 12

Consultations et suivi

1. A l'expiration d'un délai d'un an à compter de l'entrée en vigueur du présent Accord et, par la suite, à intervalles réguliers si l'une des Parties ou les deux Parties l'estiment nécessaire, les Parties se consulteront au sujet de sa mise en œuvre, en prêtant particulièrement attention à la protection des données à caractère personnel.

2. Les Parties se consultent également au sujet de toute évolution pertinente qui interviendrait au niveau de l'Union européenne et des Etats-Unis d'Amérique en matière de protection des données à caractère personnel dans le cadre de la coopération policière.

3. En cas de différend sur l'interprétation ou l'application du présent Accord, les Parties se consultent afin d'en faciliter le règlement.

Article 13

Frais

Chaque Partie prend en charge les frais encourus par ses services lors de la mise en œuvre du présent Accord. Dans des cas particuliers, les Parties peuvent convenir de dispositions différentes.

Article 14

Suspension et dénonciation de l'Accord

1. En cas de manquement substantiel aux obligations du présent Accord par une Partie, l'autre Partie, après consultation bilatérale, sera admise à en suspendre l'application, avec effet immédiat, moyennant notification écrite.

2. Chaque Partie peut dénoncer le présent Accord moyennant notification écrite par la voie diplomatique.

Ladite dénonciation prend effet au premier jour du mois suivant un délai de trois mois à compter de la date de réception de la notification de dénonciation par l'autre Partie.

En cas de dénonciation, les Parties appliqueront les dispositions du présent Accord aux données obtenues en vertu de celui-ci, à moins qu'elles n'en conviennent autrement.

Article 15

Modifications

1. Les Parties se consultent, à la demande de l'une d'entre elles, en vue de l'adoption de toute modification.

2. Le présent Accord peut être modifié à tout moment par un accord écrit entre les Parties. Les modifications ainsi apportées entrent en vigueur dans les conditions prévues à l'article 16 du présent Accord.

Article 16

Entrée en vigueur

1. A l'exception des articles 5 et 6, le présent Accord entrera en vigueur le premier jour du deuxième mois suivant la date de réception de la dernière des notes diplomatiques attestant l'accomplissement par les Parties des procédures internes requises pour son entrée en vigueur.

2. Les articles 5 et 6 du présent Accord entreront en vigueur après la conclusion du ou des arrangements de mise en œuvre mentionnés à l'article 6 et à la date de la note mettant fin à l'échange de notes diplomatiques entre les Parties attestant que chaque Partie est en mesure d'appliquer, sur une base de réciprocité, les articles 5 et 6. Cet échange de notes interviendra à condition que la législation des deux Parties autorise les comparaisons des profils ADN telles que prévues à l'article 5.

ANNEXE

Les crimes et délits visés dans le cadre du présent Accord sont énumérés ci-après et comprennent également les infractions de conspiration en vue de procéder à leur commission, l'adhésion à un groupe criminel organisé, ou la tentative de commettre ces infractions, lorsqu'elles sont punissables.

1. Infractions contre les personnes : génocide ; torture ; meurtre ; homicide et infractions associées ; traite d'êtres humains ; esclavage et servitude ; viol et autres infractions à caractère sexuel telles que la pornographie infantile et l'agression sexuelle ; agression et/ou coups et blessures avec l'intention de causer des blessures graves ou ayant pour conséquences lesdites blessures ; enlèvement, prise d'otage ; proxénétisme.
2. Crimes contre l'Etat : infractions terroristes (y compris les infractions visées dans les conventions de l'ONU sur le terrorisme, la fourniture d'un support matériel aux terroristes, la fourniture d'un support matériel aux organisations terroristes étrangères ainsi que le fait de recevoir un entraînement militaire d'une organisation terroriste ou de fournir un tel type d'entraînement) ; violations des résolutions de l'ONU relatives au blocage de la propriété et à l'interdiction des transactions avec des personnes enfreignant les règles applicables du trafic d'armes international ; transactions illicites portant sur des substances biologiques, chimiques ou nucléaires ; sabotage ; espionnage (y compris l'espionnage en matière informatique et économique) ; trafic de migrants ; atteintes à l'action de la justice ; faux témoignage ou incitation au faux témoignage ; fausses déclarations ; menaces.
3. Infractions relatives aux armes : délits impliquant des armes à feu, incluant, sans que cette liste ne soit exhaustive, le trafic d'armes ; délits liés à des engins de destruction ou des substances explosives ; port d'arme prohibée avec l'intention d'en faire usage ; utilisation ou possession illicite d'arme biologique, chimique ou nucléaire, ou de toute autre arme de destruction massive ; production, transfert ou possession de dispositifs de dispersion radiologique.
4. Crimes et délits relatifs aux vols et fraudes : cambriolage ; vol ; vol à main armée ; chantage ; vol avec effraction ; corruption ; détournement de fonds ; extorsion ; blanchiment d'argent ; racket ; infractions résultant de fraudes (faux-monnayage, usage de faux, fraude, usage frauduleux et illégal de documents, y compris mais sans s'y limiter de cartes de crédits et de passeports) ; fraude fiscale ; infractions relatives au vol ; contrebande ; trafic de marchandises volées ; falsification de monnaie ou contrefaçon de marchandises.
5. Infractions graves impliquant des substances réglementées : distribution ou trafic de produits stupéfiants, de substances réglementées et psychotropes ainsi que de cannabis ou marijuana ; possession ou possession avec intention de vente, de narcotiques, de substances réglementées et psychotropes, ou de cannabis ou marijuana, à l'exception de la possession de faibles quantités n'étant pas qualifiée d'infraction grave en vertu du droit national.
6. Crime contre la propriété : incendie volontaire, attentats avec substances explosives ; destruction volontaire de biens ; piraterie en haute mer ; crimes et délits environnementaux ; atteintes graves à la confidentialité des données, y compris l'accès illégal aux bases de données ; infractions graves en matière informatique.

TCA 2012-51. – Imprimerie de la direction de l'information légale et administrative

550120510000712