N° 3443

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 27 janvier 2016

# RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES SUR LE 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**

PAR M. Philippe BAUMEL
DÉPUTÉ

ET

## ANNEXE : TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES

Voir les numéros :

*Sénat :* **48**, **386**, **387** et T.A. **110** (2014-2015).

*Assemblée nationale* : **2852**

**SOMMAIRE**

___

**Pages**

**INTRODUCTION** ..... 5

**I. RENFORCER LA COOPÉRATION OPÉRATIONNELLE TOUT EN ASSURANT LA PROTECTION DES DONNÉES** ..... 7

A. LA COOPÉRATION POLICIÈRE ET JUDICIAIRE FRANCO-AMÉRICAINE ..... 7

1. Les voies de la coopération en matière de prévention et répression de la criminalité grave et du terrorisme ..... 7

2. Une coopération judiciaire et opérationnelle dense ..... 9

B. UN CADRE DE PROTECTION DES DONNÉES DIFFÉRENT ..... 10

1. Des standards élevés en révision au sein de l'Union européenne ..... 10

2. Une législation et une organisation américaine plus faibles en cours toutefois d'amélioration ..... 13

3. L'encadrement des échanges avec les États-Unis en matière de prévention et répression de la criminalité grave et du terrorisme ..... 13

**II. UN ACCORD POUR LUTTER CONTRE LA CRIMINALITÉ GRAVE ET LE TERRORISME** ..... 17

A. AUTORISER ET FACILITER LA CONSULTATION ET L'ÉCHANGE D'INFORMATION ..... 17

1. Les dispositions générales de l'accord ..... 17

2. La consultation des fichiers ..... 18

3. L'échange spontané ..... 20

B. DES DISPOSITIONS BIEN ENCADRÉES ..... 20

1. Une procédure de consultation en deux étapes ..... 20

2. Des consultations dans un cadre déterminé, réalisées au cas par cas et dans le respect du droit national ..... 21

3. Des dispositions détaillées relatives à la protection des données personnelles (article 10) ..... 22

C. LES DISPOSITIONS D'APPLICATION ..... 24
1. Le suivi de l'application et de l'adéquation de l'accord ..... 24
2. Une application effective qui restera limitée à court terme ..... 25
3. Délais d'entrée en vigueur et de mise en application ..... 25

**CONCLUSION** ..... 29

**EXAMEN EN COMMISSION** ..... 31

**ANNEXES** ..... 33

**ANNEXE N° 1 : LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR** ..... 33

**ANNEXE N° 2 : COMPARATIF ENTRE L'ACCORD ET LES DÉCISIONS « PRÜM »** ..... 35

**ANNEXE - TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES** ..... 39

# INTRODUCTION

Le présent projet de loi, adopté par le Sénat au cours de sa Séance du 4 juin 2015, a pour objet de ratifier un accord conclu sous forme d'échanges de lettres entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique et relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et lutter contre la criminalité grave et le terrorisme. Négociées à partir de 2008 à la demande des États-Unis, les lettres constituant l'accord ont été signées le 3 mai 2012 par le ministre français de l'intérieur et le 11 mai 2012 par la secrétaire d'État américaine, chargée de la sécurité du territoire.

La coopération judiciaire et opérationnelle est très intense avec les États-Unis. Il existe d'abord une coopération ancienne d'entraide en matière pénale fondée sur les accords relatifs à l'extradition du 23 avril 1996 et à l'entraide judiciaire du 10 décembre 1998. La coopération opérationnelle est quant à elle d'excellente qualité et d'une grande efficacité aux dires des services. Elle s'exerce de manière régulière et fructueuse notamment avec le ministère de la sécurité intérieure américain et les agences fédérales qui dépendent du ministère de la justice comme le Federal Bureau of Investigation (FBI) et la Drug Enforcement Administration (DEA), particulièrement dans les domaines du trafic de stupéfiants, du blanchiment et de la cybercriminalité.

Toutefois, outre le canal de l'Organisation internationale de police criminelle (Interpol), cette coopération opérationnelle n'est pas institutionnalisée au travers d'un service centralisé côté américain, en raison d'une multiplicité d'acteurs fédéraux appartenant à différents ministères. Étonnamment, aucun accord de coopération policière ne lie la France et les États-Unis. L'accord soumis a précisément pour objet d'encadrer la coopération opérationnelle en instituant des procédures de consultation des données dactyloscopiques et génétiques, d'échanges consécutifs d'informations nominatives et d'échanges spontanés en matière de prévention des actes de terrorisme et de crimes graves.

À la suite des attentats du 11 septembre 2001, les États-Unis ont souhaité renforcer la sécurité de leur territoire et l'arsenal préventif et répressif de lutte contre le terrorisme. Ils ont alors relevé les exigences liées au maintien de leur programme d'exemption de visa, dont bénéficie la France, et ont notamment posé comme contrepartie l'accroissement des échanges d'informations. Une vingtaine d'autres États membres de l'Union européenne ont signé un accord de même nature que celui qui nous est aujourd'hui soumis à ratification, y compris d'ailleurs des pays qui n'appartiennent pas au programme d'exemption de visa.

C'est en 2008 que les États-Unis ont engagé une négociation avec la France qui s'est avérée assez ardue, notamment au regard des garanties en matière

de protection des données que le gouvernement français estimait indispensables de voir figurer dans l'accord, exigence forte qui ne fut pas celle, ou à des degrés moindres, de nos partenaires européens. Il convient en effet de souligner que les États-Unis ne présentent pas un niveau jugé suffisant de protection des données personnelles. Or, il est ici question de données d'une sensibilité particulières puisqu'il s'agit notamment des données dactyloscopiques et génétiques.

L'accord qui a finalement été signé est assez remarquable de ce point de vue. Sans être aussi prescriptif que l'accord dont il s'inspire et qui lie les États de l'Union européenne, à savoir le traité de Prüm, il comporte des garanties fortes, prévoit de manière précise et stricte les principes essentiels de la protection des données et la manière d'assurer leur respect, toutes choses qui contrastent avec les clauses souvent lapidaires qui figurent dans les accords signés par la France avec des États étrangers. Un registre des données est même prévu pour pouvoir contrôler la pertinence des échanges d'informations réalisés. Dans ces conditions, l'accord répond à l'exigence d'équilibre qui a été mise en exergue au cours de l'année 2015 sous le double mouvement de la gestion de la menace terroriste et du débat sur les limites aux atteintes à la vie privée, suscité notamment par des décisions de justice marquantes comme l'invalidation de l'accord dit « Safe Harbour » de transfert de données avec les États-Unis.

Il ne fait aucun doute que l'efficacité de la coopération opérationnelle est un élément fondamental face à la criminalité transnationale, menace mobile et fluctuante, ainsi que pour la prévention et la répression du terrorisme, comme l'ont démontré les récentes enquêtes ayant permis de déjouer des attentats ou qui ont suivi les attentats commis. Cette coopération permet de gagner du temps dans les enquêtes et de sauver des vies humaines. Avec les États-Unis, l'établissement d'un cadre et d'une organisation définis pour procéder aux échanges, qui permette la consultation de fichiers d'empreintes et le transfert spontané d'informations, permettra de simplifier et fluidifier les conditions de la coopération.

Un point est particulièrement important à la lumière de ces expériences récentes : seules les empreintes permettent souvent d'assurer l'identification des individus et la capacité à tracer leur parcours. L'accord ayant principalement pour objet d'autoriser la consultation des fichiers d'empreintes, il répond donc pleinement à un besoin aigu de nos services de police. Les échanges afférents à des empreintes sont aujourd'hui très limités avec les États-Unis et l'accord permettra en la matière de générer un réflexe plus qu'utile, encore une fois dans des conditions très encadrées en matière de protection des personnes.

Compte tenu des délais de rédaction des arrangements administratifs à conclure et des délais techniques nécessaires à l'ouverture d'accès distants, accès qui ne sera ouvert dans un premier temps, compte tenu de la législation américaine, que pour les fichiers d'empreintes dactyloscopiques, il serait hautement souhaitable que la procédure de ratification s'achève très rapidement et que la phase de mise en œuvre puisse s'engager.

# I. RENFORCER LA COOPÉRATION OPÉRATIONNELLE TOUT EN ASSURANT LA PROTECTION DES DONNÉES

Les autorités des États partenaires dans la lutte contre la criminalité transnationale et le terrorisme ont un besoin accru de traiter et d'échanger des données à des fins préventive et répressive. Dans ce contexte, des règles claires et cohérentes en matière de protection des données sont indispensables si l'on veut améliorer la coopération. Cette nécessité de trouver le bon équilibre vaut au sein de l'Union européenne, mais plus encore pour la coopération avec les autorités américaines compte tenu des volumes d'échanges d'information potentiels et *a contrario* des lacunes en matière de protection des données outre-Atlantique.

## A. LA COOPÉRATION POLICIÈRE ET JUDICIAIRE FRANCO-AMÉRICAINE

En l'absence d'accord de coopération policière avec les États-Unis, les demandes d'informations s'effectuent aujourd'hui par le biais d'Interpol ou des mécanismes d'entraide judiciaire qui sont régis par un accord bilatéral.

### 1. Les voies de la coopération en matière de prévention et répression de la criminalité grave et du terrorisme

Au plan juridique, la coopération repose sur les deux traités suivants :

– le traité bilatéral d'entraide judiciaire en matière pénale, signé le 10 décembre 1998 et entré en vigueur le 1er décembre 2001 ;

– et le traité d'extradition, signé le 23 avril 1996 et entré en vigueur le 1er février 2002.

Pour mémoire, Europol, l'Office européen de police, opérationnel depuis 1999, dont la mission est de faciliter l'échange de renseignements entre polices nationales des États membres de l'Union européenne dans la prévention du terrorisme et de la criminalité grave est monté en puissance. Europol et les États-Unis ont signé un accord stratégique le 6 décembre 2001, qui est entrée en vigueur le lendemain. Puis, un accord complémentaire a été signé le 20/12/2002 pour l'échange de données à caractère personnel. Ce dernier est entré en vigueur le 21/12/2002.

La coopération est très soutenue, dans tous les domaines de la criminalité organisée transnationale et dans la lutte contre le terrorisme. Outre le canal Interpol qui permet des échanges nombreux et réciproques, cette coopération n'est toutefois pas institutionnalisée au travers d'un service centralisé. La difficulté repose notamment sur la multiplicité des acteurs fédéraux appartenant à différents ministères (Department of Homeland Security - DHS / Department of Justice - DOJ / Department of Defence - DOD) tous chargés, selon leur juridiction, de l'application de la loi.

Les commissions rogatoires internationales françaises (CRI), et leur équivalent américain, les Mutual Legal Assistance Treaty request (MLAT), sont traitées par nos ministères de la Justice respectifs, au travers de leurs bureaux d'entraide pénale internationale (BEPI). Le Federal Bureau of Investigation (FBI), principale agence fédérale dépendant du DOJ est donc l'acteur majeur des échanges opérationnels entre nos deux pays.

En ce qui concerne Interpol, le bureau central national (BCN) américain est placé sous la juridiction du ministère de la Justice américain (DOJ). Il est géré en partenariat avec le DHS. Le BCN France, dépendant de la division des relations internationales (DRI) de la Direction centrale de la police judiciaire (DCPJ), est donc son partenaire naturel.

Le ministère de la Justice américain, département puissant financièrement, dispose de nombreuses agences fédérales d'application de la loi, telles que le FBI, mais aussi les US Marshals Service (USMS), la Drug Enforcement Administration (DEA), ou encore le Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

À Paris, hormis la DEA qui bénéficie d'un accord de coopération opérationnelle spécifique avec l'office central de répression contre le trafic illicite de stupéfiants (OCRTIS) de la DCPJ, ces agences fédérales, représentées par le bureau du FBI présent à l'ambassade américaine, respectent fidèlement les canaux de coopération.

Le FBI développe de nombreuses connexions directes avec les services de la police et de la gendarmerie français. La majorité des MLAT sont gérés par leur bureau dans un travail classique de liaison sur la base d'échanges directs de service à service, notamment en matière de contre-terrorisme, de criminalité organisée ou de cybercriminalité.

À Washington, notre Service de Sécurité Intérieure (SSI) participe également à ces échanges, en liaison avec notre magistrat de liaison ou en liaison directe avec nos services français.

Le ministère de la sécurité intérieure américain (DHS) dispose également de nombreuses agences fédérales, telles que l'Immigration & Customs Enforcement (ICE), le Customs & Border Protection (CBP), ou encore le US Secret Service (USSS).

L'ICE, agence principalement représentée à Paris, et représentant le DHS dans son ensemble, ne gère que peu de MLAT. Toutefois, à l'instar du FBI, cette agence développe de nombreux contacts directs avec des services de police et de gendarmerie français sur la base d'échanges opérationnels au cas par cas. Les échanges sont de qualité, notamment en matière d'immigration, mais aussi dans la lutte contre la criminalité organisée comme le trafic de biens culturels, la lutte contre la pédopornographie ou la cybercriminalité.

### 2. Une coopération judiciaire et opérationnelle dense

Les relations en matière d'entraide entre la France et les États-Unis sont importantes. Ainsi, depuis 2007, 700 demandes d'entraide ont été échangées entre la France et les États-Unis (85 en matière de terrorisme), dont 475 ont été adressées par les autorités françaises aux États-Unis (48 en matière de terrorisme) et 225 par les autorités américaines à la France (37 en matière de terrorisme). La présence d'un magistrat de liaison français à Washington et d'un magistrat de liaison américain à Paris, ainsi que l'organisation entre les autorités centrales de consultations bilatérales générales et spécifiques à la lutte contre le terrorisme contribuent au renforcement de la coopération entre nos deux États.

Il est difficile de chiffrer avec exactitude le volume d'échanges opérationnels entre nos deux pays. Le rapport d'activité 2014 du service de sécurité intérieure français fait état de 140 demandes de renseignement émanant des services français (police et gendarmerie) transmises à la partie américaine, ainsi que 310 demandes de vérifications opérationnelles, qui ont trouvé leur prolongement dans l'exécution de 6 commissions rogatoires internationales.

Au titre de l'année 2014, 197 Messages SIENA (messagerie Europol) ont été envoyés par la France vers les USA et nous en avons reçu 412. Dans le cadre d'Interpol, en 2013, 1234 messages ont été envoyés par le bureau central national (BCN) France et 1412 ont été reçus du BCN américain. Ces chiffres étaient respectivement, en 2015, d'après la direction centrale de la police judiciaire du ministère de l'Intérieur, pour ce qui est de la messagerie Europol, de 315 et 536 et via Interpol de 607 et 807.

À la suite des attentats du 13 novembre, les États-Unis nous ont apporté un certain nombre d'informations via la consultation du TFTP par Europol (15 réponses en relation avec le TFTP sur 103 messages reçus des agences américaines). Par ailleurs, comme d'autres partenaires, les États-Unis ont fait l'objet d'interrogations via le canal Interpol pour des recherches sur la base d'empreintes digitales ou génétiques.

Par ailleurs, la coopération entre la France et les États-Unis dans le domaine du renseignement a toujours été d'une très grande qualité, basée sur une confiance mutuelle.

Les fichiers d'empreintes qui existent dans les deux pays constituent une base précieuse pour l'identification des criminels, donc la prévention et la répression des crimes.

D'après les informations transmises à votre Rapporteur, le FAED compte 5 532 000 fiches personnes et le FNAEG plus de 3 200 000 profils (traces et individus). En ce qui concerne les fichiers américains, le ministère de l'Intérieur ne dispose pas des éléments de réponse. D'après l'Ambassade des États-Unis à Paris, le Gouvernement américain compterait plus de 100 millions d'empreintes digitales dans les registres du Département de la sécurité intérieure (DHS IDENT),

et plus de 70 millions dans les bases de données du FBI. Les données génétiques n'étant pas centralisées, le nombre n'est pas connu.

Pour autant, à ce jour, les échanges en matière de données génétiques ou dactyloscopiques sont très restreints et s'élèvent à seulement quelques dizaines de demandes par an.

## B. UN CADRE DE PROTECTION DES DONNÉES DIFFÉRENT

La législation française en matière de protection des données est régie par loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés, qui a été modifiée à plusieurs reprises depuis son adoption. Elle est aussi régie par le droit européen, pour l'élaboration et l'actualisation duquel la Commission nationale informatique et libertés (CNIL) prend une part active. Enfin, elle est soumise aux décisions des juridictions européennes.

Le transfert de données vers des États tiers n'appartenant pas à l'Union européenne est régi par les articles 68, 69 et 70 de la loi du 6 janvier 1978 modifiée. 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.

### 1. Des standards élevés en révision au sein de l'Union européenne

Depuis le traité de Lisbonne, la protection des données à caractère personnel est un droit fondamental au regard de la législation de l'UE, reconnu par le traité sur le fonctionnement de l'Union européenne et la Charte des droits fondamentaux de l'UE.

La Commission a proposé une réforme de la législation relative à la protection des données en 2012, afin d'actualiser et moderniser les règles contenues dans la directive de 1995 sur la protection des données et dans la décision-cadre de 2008 relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Le « paquet protection des données » est composé d'un règlement et d'une directive ayant respectivement pour objet :

– de réviser les règles de protection des données établies par la directive 95/46 en matières civiles et commerciales ainsi que les règles applicables à certains traitements du secteur public ;

– de réviser la décision-cadre 2008/977, dont le champ était toutefois limité aux échanges de données entre États membres ou État membres et États tiers à l'Union dans le cadre de la prévention, de la détection ou de la poursuite des infractions pénales, et d'harmoniser les règles de protection des données

applicables aux fichiers nationaux dans ce domaine, qui sont actuellement soumis aux seules législations des États membres.

Lors d'une réunion extraordinaire qui s'est tenue le 17 décembre 2015, la commission Libertés civiles, justice et affaires intérieures du Parlement européen a exprimé sa position sur les textes ayant fait l'objet d'un accord dans le cadre des négociations en trilogue entre le Conseil, le Parlement européen et la Commission. Le 18 décembre 2015, le Comité des représentants permanents (Coreper) a approuvé ces textes de compromis. Le règlement et la directive devraient entrer en vigueur au printemps 2016 et seraient applicables dès le printemps 2018.

Parallèlement, la Cour de justice de l'Union européenne a démontré ces deux dernières années son rôle de gardienne des exigences en matière de protection des données personnelles et de la vie privée.

Par deux arrêts du 8 avril 2014 dans les affaires « Digital Rights Ireland» et « Seitlinger », la Cour de Justice de l'Union européenne (Grande Chambre) a déclaré invalide la directive 2006/24/CE du 15 mars 2006 relative à la conservation des données de connexion dans le cadre des communications électroniques. Elle a considéré que cette directive portait une atteinte disproportionnée aux droits prévus par les articles 7 (respect de la vie privée) et 8 (protection des données à caractère personnel) de la Charte des droits fondamentaux de l'Union européenne [(1)] .

L'invalidation de la directive n'a pas pour effet direct ou automatique de rendre caduques les législations nationales assurant sa transposition en droit interne. Les États membres gardent en effet la possibilité d'imposer aux opérateurs une obligation de conservation des données de connexion sur la base de la directive 2002/58 dite « vie privée et communication électronique », ainsi que l'article 13 de la directive 95/46 relative à la protection des données personnelles. Dans une majorité d'États membres, comme en France, la législation nationale relative à la conservation des données de connexion est demeurée en vigueur, parfois amendée dans le sens d'un renforcement des garanties procédurales.

Il convient de mentionner également la question préjudicielle « Tele2 Sverige », posée à la CJUE le 4 mai 2015. Il est question de savoir si une obligation générale de conservation des données, relative à toute personne et à tous les moyens de communication électronique, est compatible avec la directive

---

*(1) Était principalement en cause l'obligation faite aux opérateurs économiques de collecter, conserver et rendre disponibles pendant un temps déterminé un nombre considérable de données à caractère personnel recueillies lors des communications individuelles dans l'ensemble de l'Union, ce afin de lutter contre des activités criminelles graves. La Cour a jugé que, tant l'obligation de conservation des données à caractère personnel que l'accès des autorités nationales à ces données ou leur traitement constituent une ingérence flagrante dans les droits fondamentaux des individus. En effet, «* la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données ».

2002/58 « vie privée et communications électroniques », en particulier son article 15, au regard de la Charte des droits fondamentaux de l'UE. En l'espèce, la législation suédoise en cause prévoit un délai de conservation des données pendant 6 mois. L'arrêt dans cette affaire ne devrait pas être rendu avant le second semestre de l'année 2016. Il permettra de disposer d'une analyse exhaustive et utile des conséquences de l'arrêt de la CJUE du 8 avril 2014.

Par ailleurs, dans son arrêt rendu le 6 octobre dernier, dans l'affaire C-362/M14, Maximilian Schrems / Data Protection Commissioner, sur une question préjudicielle de la juridiction suprême irlandaise, la CJUE a invalidé rétroactivement la décision de la Commission européenne (dite « Safe harbor ») permettant le transfert de données personnelles de l'Union européenne vers les États-Unis, dans le contexte du fonctionnement des programmes de surveillance américains, révélé par Edward Snowden durant l'été 2013.

Le « Safe Harbor » est une décision d'adéquation « sectorielle » de l'UE (du 26/07/2000), adoptée dans le cadre de la Directive 95/46 (qui organise le régime juridique de protection des données de l'Union européenne). Il constitue depuis 2001, dans le domaine civil et commercial, le cadre juridique qui permet le transfert de données de l'Union européenne aux entreprises américaines respectant un certain niveau de protection des données du fait de leur adhésion à certains principes. La liste de ces entreprises est publiée, et en principe mise à jour par le Département du Commerce américain (FTC).

Dans une communication publiée le 29 novembre 2013, la Commission européenne en a fait une évaluation assez critique, assortie de 13 recommandations visant à renforcer le dispositif existant. Soutenue par les experts représentants les États membres en janvier 2014, la Commission a entamé des discussions avec les États-Unis. Parmi les demandes européennes majeures, figurent la restriction des dérogations au Safe Harbor en matière de sécurité nationale et l'introduction des voies de recours juridictionnelles sur le territoire américain pour les résidents européens.

Cette invalidation rétroactive rend nécessaire de trouver un accord entre Américains et Européens sur la protection des données personnelles, notamment sous l'angle du droit de recours judiciaire accordé aux citoyens européens. Le G 29 (groupe des CNIL européennes) a donc vivement encouragé les institutions européennes et les gouvernements à trouver une solution juridique et technique d'ici le 31 janvier 2016. Durant cette période, les entreprises peuvent recourir aux règles contraignantes d'entreprise (Binding Corporate rules) et aux clauses contractuelles types, mais il n'est pas certain que ces outils soient juridiquement sûrs au regard des exigences de l'arrêt Schrems. L'annulation de cet arrêt crée un vide juridique aux conséquences économiques importantes qui restent encore à évaluer pour les entreprises françaises devant transférer des données personnelles aux États-Unis.

### 2. Une législation et une organisation américaine plus faibles en cours toutefois d'amélioration

Aux États-Unis, le dispositif de la protection des données à caractère personnel est différent du système européen en général et français en particulier, 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. L'autorité concernée dépend du secteur d'activité, et du texte qui s'applique (au niveau fédéral ou des États). La FTC (Federal Trade Commission), agence fédérale indépendante, est toutefois assez largement compétente.

Depuis 2013, le débat a porté en priorité aux États-Unis sur le programme de collecte de masse des métadonnées téléphoniques des citoyens américains, mis en œuvre par la NSA. La section 215 du Patriot Act, qui servait de base à ce programme, a expiré le 1er juin. Le Congrès a ainsi adopté, le 2 juin 2015, le USA Freedom Act, qui met fin à ce programme tel qu'il existait jusque-là : la loi prévoit, après une période de transition de six mois, le transfert du stockage des métadonnées aux opérateurs de téléphonie. Il encadre par ailleurs davantage l'accès de la NSA à ces métadonnées, sous le contrôle accru de la Cour de surveillance du renseignement étranger (FISA Court). Cette législation sera valide jusqu'au 15 décembre 2019.

La question s'est également posée de l'extension aux ressortissants de pays tiers de certaines garanties dont bénéficient les citoyens américains et les résidents aux États-Unis en matière de protection de leurs données personnelles, en vertu du Privacy Act de 1974. Le Congrès s'en est saisi, et un projet de loi, le « Judicial Redress Act », a été introduit à la Chambre des représentants et au Sénat respectivement en mars et juin 2015.

Ce projet de loi accorde des voies de recours devant les juridictions américaines, sous certaines conditions, pour les ressortissants de pays tiers ne résidant pas aux États-Unis, en cas de violations de leurs droits en matière de protection des données personnelles par les autorités de police américaines. Le texte été adopté le 20 octobre 2015 par la Chambre des représentants. La date relative à l'adoption par le Sénat n'est pas encore fixée, mais le département d'État assure tout mettre en œuvre pour inciter le Sénat à adopter rapidement le texte, qui s'inscrit dans la lignée des annonces faites par le Président Obama en janvier 2014 pour rétablir la confiance sur la scène internationale.

### 3. L'encadrement des échanges avec les États-Unis en matière de prévention et répression de la criminalité grave et du terrorisme

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 États-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.

Deux accords ont été conclus entre les États-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.

La question du transfert et de l'exploitation de données personnelles de ressortissants de l'Union européenne vers un pays tiers et entre autres les États-Unis à des fins de prévention, détection et de lutte contre le terrorisme et les formes graves de criminalité ne pourront vraiment faire l'objet d'une analyse consolidée qu'une fois que la Cour apportera des précisions dans l'arrêt qu'elle doit rendre dans l'affaire C-203/15 (Tele2Sverige) et de l'avis de compatibilité avec les Traités qu'elle rendra sur le projet d'accord PNR entre l'Union européenne et le Canada (affaire1/15).

Car, parallèlement, le Conseil a adopté un mandat permettant à la Commission de négocier un accord de protection des données avec les États-Unis. Cet accord vise à protéger le transfert entre l'UE et les États-Unis de données à caractère personnel transférées entre les autorités des États membres de l'Union et les autorités des États-Unis pour les besoins de la prévention, de l'enquête, de la détection ou de la poursuite des infractions de nature criminelle et notamment les infractions terroristes (« EU-US data protection, "Umbrella Agreement" »).

Les négociations avec les États-Unis sont assez abouties, un accord ayant été trouvé après quatre années de négociations et paraphé le 8 septembre 2015 en marge de la réunion Justice et Affaires intérieures des hauts fonctionnaires Union européenne – États-Unis d'Amérique.

L'accord prévoit notamment des règles harmonisées au regard de la qualité et de l'intégrité des données transférées. Conformément à la loi dite « Informatique et libertés » applicable en droit français, les données doivent être exactes, adéquates, complètes et la durée de conservation de ces données doit notamment prendre en considération leur finalité et leur nature. Un droit d'accès aux données et de rectification de celles-ci est également garanti aux personnes concernées et les autorités compétentes de chaque État doivent garantir la sécurité des données qui leur sont transférées. L'accord instaure également un mécanisme

de notification des failles de sécurité à l'autorité compétente et, éventuellement, à la personne concernée.

Enfin, l'accord introduit également la possibilité pour les Européens de saisir une juridiction américaine d'un litige entrant dans le champ de l'accord et, vice versa, un citoyen des États-Unis pourra saisir les juridictions d'un État membre de l'Union européenne dans le même contexte. Non seulement la saisine d'une juridiction américaine sera donc possible, mais la loi américaine s'appliquera également au litige, en l'occurrence, le US Privacy Act de 1974. Cela n'est aujourd'hui pas possible, parmi les non Américains, seuls les résidents permanents disposent de voies de recours.

Toutefois, la Commission tout comme le Conseil, ont clairement indiqué que l'adoption par le Congrès américain du « judicial redress act » restait une condition non négociable pour que cet « accord parapluie » soit signé. Par ailleurs, le Parlement européen, qui doit autoriser l'accord pour qu'il puisse être mis en œuvre, a indiqué à l'automne dernier, qu'il souhaitait avant de se prononcer, vérifier si les garanties de cet accord n'étaient pas en deçà de celles prévues par la directive protection des données. Les députés européens ont saisi leur service juridique en ce sens et ont demandé à la Commission européenne d'effectuer également cette analyse. Ce dossier n'a pas été réinscrit à ce stade à l'ordre du jour au Parlement européen.

En effet, deux failles semblent problématiques. D'une part, les citoyens non Européens mais résidant en Europe dont les données auront été transmises par les autorités répressives européennes à leurs homologues américains, n'auront toujours pas le droit à un recours auprès du juge américain (conformément à l'article 19 seuls les "citoyens des parties" sont concernés). D'autre part, certaines pratiques de traitement et de conservation des données ne constitueraient pas un motif de recours.

Il n'en demeure pas moins que, sous réserve de sa légalité, la conclusion d'un tel accord parapluie constituerait une avancée incontestable dans la protection des données des Européens et rendrait possible une coopération accrue à des fins de répression des crimes graves et en particulier du terrorisme dans de bonnes conditions. Les accords passés entre les États-Unis et plusieurs pays européens sont considérés comme lacunaires sur le plan de la protection des données et de la vie privée et les autorités de protection des données soutenaient la démarche d'un accord parapluie pour élever le standard.

## II. UN ACCORD POUR LUTTER CONTRE LA CRIMINALITÉ GRAVE ET LE TERRORISME

L'accord soumis à ratification s'inspire largement de l'accord Prüm, conclu entre la France, la Belgique, l'Allemagne, l'Espagne, les Pays-Bas et l'Autriche et des décisions européennes qui l'ont en partie intégré dans le droit de l'Union de 2008 (décisions 2008/615 JAI et 2008/616 JAI), ce qui lui vaut son surnom de « Prüm Atlantique ». Une annexe au présent rapport dresse la comparaison entre les deux accords.

### A. AUTORISER ET FACILITER LA CONSULTATION ET L'ÉCHANGE D'INFORMATION

#### 1. Les dispositions générales de l'accord

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 ».

L'**article 2** définit l'objectif et le champ d'application de l'accord. Les finalités de cet accord sont la prévention et lutte contre la criminalité grave (« serious crime »), en particulier le terrorisme (article 2). Les crimes et délits sont énumérés en annexe de l'accord, sans que cette liste soit limitative.

Plus précisément, 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 crimes et délits énumérés en annexe ainsi que toutes 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. Elle est donc plus stricte que pour l'application de l'accord Prüm (infractions punies d'une peine privative de liberté égale ou supérieure à un an), qui a été retenue dans les accords signés par nos partenaires européens avec les États-Unis. Il s'agit ainsi d'une spécificité de l'accord signé avec la France d'avoir limité les consultations à des crimes d'une particulière gravité.

Votre Rapporteur s'est interrogé sur la manière dont les accords équivalents signés entre les États-Unis et nos partenaires européens étaient dans les faits appliqués. Les États-membres n'ayant pas fait de publicité des accords

signés avec les États-Unis, il est difficile d'obtenir des informations et les autorités américaines respectent le principe de confidentialité dans le cadre d'accords bilatéraux signés avec leurs partenaires.

Néanmoins, l'Ambassade des États-Unis a donné plusieurs exemples de transmissions de données biométriques d'individus en fuite à des pays qui avaient déjà eu affaire à eux lors d'enquêtes criminelles :

- le FBI a fourni des données biométriques à un pays européen signataire relatives à une personne recherchée aux États-Unis pour fraude électronique et blanchiment d'argent. Le pays partenaire a établi une correspondance à partir de sa base de données avec un individu qui avait été arrêté pour l'utilisation de documents falsifiés ;

- le FBI a fourni des données biométriques à un pays européen signataire relatives à une personne recherchée aux États-Unis pour possession de cocaïne avec intention de la distribuer. Le pays partenaire a établi une correspondance à partir de sa base de données avec un individu qui avait été arrêté pour vol de véhicule ;

- le FBI a fourni des données biométriques à un pays européen signataire de l'Accord PCSC relatives à une personne recherchée aux États-Unis pour homicide. Le pays partenaire a établi une correspondance à partir de sa base de données avec un individu qui avait été arrêté dans le pays partenaire pour vol de véhicule ;

- le FBI a fourni des données biométriques à un pays européen signataire relatives à une personne recherchée aux États-Unis pour fraude bancaire, complot en vue de commettre une fraude bancaire et vol d'identité aggravé. Le pays partenaire a établi une correspondance à partir de sa base de données avec un individu qui avait été arrêté pour vol de véhicule.

Cette liste permet de comprendre pourquoi l'accord signé avec la France ne se limite pas à certains crimes d'une extrême gravité mais pose le principe d'une peine minimale de 3 ans qui permet d'inclure le vol.

### 2. La consultation des fichiers

L'accord tend à permettre une consultation mutuelle et automatisée des fichiers d'analyses ADN et des systèmes d'identification dactyloscopique, selon un système de concordance/sans concordance (« hit/no hit »). 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.

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 FNAEG ET LE FAED**

Le décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales (FAED) géré par le ministère de l'Intérieur a fait l'objet d'une modification par le décret n° 2015-1580 du 2 décembre 2015 lequel avait pour objet de :
- préciser les finalités pour lesquelles le traitement automatisé de traces et empreintes digitales et palmaires est autorisé,
- limiter aux seuls crimes et délits le champ infractionnel dans le cadre duquel il est possible de recourir au traitement,
- préciser les données pouvant être enregistrées suivant le cadre juridique du recueil ainsi que les conditions d'accès des différents services aux données,
- garantir un droit effectif à l'effacement des données personnelles des personnes ayant bénéficié d'un acquittement, d'une relaxe, d'un classement sans suite ou d'un non-lieu avant la fin des vingt-cinq ans correspondant à la durée de conservation maximale des données,
- de moduler les durées de conservation des traces et empreintes au regard de la gravité de l'infraction et de la qualité de la personne, selon notamment qu'elle est majeure ou mineure,
- de permettre, en application des articles 6 et 9 de la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, le recueil et l'exploitation des empreintes digitales aux fins d'identification de personnes décédées ou en cas de découverte de personnes disparues en dehors de toutes procédure pénale.

Les dispositions réglementaires relatives au fichier national des empreintes génétiques (FNAEG) font actuellement l'objet d'un projet de modification. Le projet de décret actuellement en cours d'examen devant la CNIL a pour objet :

- de prendre en compte les dispositions de l'article 19 de la loi du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle, qui élargit le champ de la collecte de données au sein du FNAEG en permettant l'enregistrement des profils génétiques de toutes les personnes déclarées coupables de l'une des infractions visées à l'article 706-55 du code de procédure pénale.

- de tirer les conséquences de la décision du Conseil Constitutionnel du 16 septembre 2010 et, par coordination, de modifier certaines dispositions relatives au service central de préservation des prélèvements biologiques.

Dans cette décision, le Conseil Constitutionnel a considéré que la durée de conservation des données collectées au FNAEG devait être réglementairement proportionnée en tenant compte de l'objet de ce fichier, de la nature ou de la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des mineurs.

- de prendre en compte les dispositions de l'article 16-11 du code civil introduites par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure en vue de permettre l'identification de cadavre anonyme ou la découverte de personnes disparues en dehors de toute procédure pénale ;

- de modifier, dans le prolongement de la décision de la Cour européenne des droits de l'Homme « M. K. c. FRANCE » du 18 avril 2013 sur le Fichier Automatisé des Empreintes Digitales (FAED), les règles d'effacement des données relatives aux personnes mises en cause enregistrées dans le FNAEG.

Dans cette décision, la CEDH a souligné le manque de clarté du champ infractionnel du FAED ne permettant pas de le limiter aux seuls crimes et délits ainsi que les faiblesses des droits d'effacement ouverts au bénéfice des personnes concernées par le traitement.
- et d'ajouter les personnes habilitées à réaliser les analyses des empreintes génétiques, à la liste des personnes susceptibles d'être habilitées à accéder au FNAEG.

*Source : ministère des Affaires étrangères et du développement international*

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. En France, ces consultations seront réalisées par

la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire pour les dossiers de grande criminalité. Pour les États-Unis, il s'agira du FBI et du Département de la Sécurité Intérieure (DHS), seules agences qui seront habilitées à interroger les bases de données françaises. L'intérêt de cet accord est ainsi de structurer la procédure côté américain avec un point de contact identifié qui travaille dans le cadre d'une procédure établie.

Les dispositions opérationnelles et techniques des procédures décrites aux articles 3 et 5 seront établies dans le cadre d'arrangements administratifs entre autorités compétentes.

### 3. L'échange spontané

Afin de lutter contre la criminalité grave et le terrorisme, chaque partie, sur sa propre initiative, peut transmettre les données complètes d'identification d'un individu, lorsqu'il y a raison de croire que l'intéressé a commis ou va commettre des actes terroristes/criminels graves, ou a participé/va participer à leur préparation (**article 9**). Les données transmises sont les suivantes :

– nom, prénoms, alias, sexe, date et lieu de naissance,

– un exposé des circonstances qui motivent la transmission.

Il s'agit du même type d'information pour la décision 2008/615/JAI et l'accord franco-américain.

Cet échange d'informations se fait par les points de contacts nationaux. 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.

L'introduction d'un cadre pour procéder à la transmission d'informations à titre préventif apporte une plus-value réelle. Pour la police judiciaire, le renseignement criminel est devenu un pilier de la stratégie opérationnelle policière et l'échange à des fins de prévention s'insère dans cette évolution essentielle.

## B. DES DISPOSITIONS BIEN ENCADRÉES

### 1. Une procédure de consultation en deux étapes

À l'instar des dispositions pertinentes des décisions dites Prüm précitées, l'accord prévoit 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.

Le mécanisme défini dans l'accord franco-américain n'implique pas une transmission automatique des données personnelles. A la différence du cadre juridique défini décision 2008/615/JAI qui postule un échange entre États membres, c'est-à-dire entre pays ayant un droit national offrant un haut niveau de protection des données, l'accord franco-américain encadre fortement les conditions d'envoi des données.

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, 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.

C'est dans un deuxième temps que l'État requis transfère des informations complémentaires, sur demande et selon sa législation. Les arrangements administratifs prévus par l'accord ne portent pas sur cette deuxième phase qui s'inscrit dans les procédures existantes. 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).

### 2. Des consultations dans un cadre déterminé, réalisées au cas par cas et dans le respect du droit 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. Les motifs de consultation renvoient à la législation nationale de l'État à l'origine de l'interrogation.

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, y compris de l'entraide judiciaire. Cela impliquera par exemple l'impossibilité de transmettre des données pour une infraction non visée par l'article 706-55 du Code de procédure pénale.

L'**article 11** précise que l'accord ne peut limiter ou porter atteinte aux relations existantes entre les États-Unis et la France. Ainsi, 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 9** relatif à l'échange spontané prévoit quant à lui que 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.

### 3. Des dispositions détaillées relatives à la protection des données personnelles (article 10)

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* ».

L'accord comporte dans son préambule des références à la protection des données. Outre le rappel des engagements de la France au niveau européen et la mention des négociations d'un accord parapluie, le préambule précise que la coopération se fait « *en respectant les droits et libertés fondamentaux, notamment ceux de la vie privée* », avec « *des garanties en vue d'assurer l'utilisation appropriée et la protection des données à caractère personnel* ».

Surtout, l'accord contient un article 10 long et précis relatif à la protection des données à caractère personnel. Cet article reprend la plupart des principes essentiels de protection des données de la législation française, à savoir la finalité, l'utilisation cantonnées à ces seules fins sauf à obtenir l'accord de l'autre partie, la durée de conservation limitée au nécessaire, le respect des droits des personnes concernées et des mesures de sécurité des données. On rappellera utilement que toute utilisation de données dans le cadre d'un procès pénal, nécessitera que son origine, directe ou indirecte, soit légale et donc conforme à l'accord, ce qui donne force aux dispositions de l'article 10.

Les principales garanties apportées par l'article 10 en la matière sont : un système d'authentification ; la mise en place d'une documentation des transmissions et des réceptions des données ; la tenue par chaque Partie d'un registre permettant d'assurer le contrôle effectif du respect des règles ; la possibilité de suspendre l'application et de dénoncer l'accord.

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. Par ailleurs, les dispositions de l'accord ne portent pas atteinte aux obligations définies par les 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.

À cet égard, l'échange de données avec les États tiers ne peut être effectué que si l'autre partie consent à ce transfert. Ainsi, 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.

Une nuance doit être apportée par rapport à l'accord Prüm : l'absence de délai de conservation sous la forme d'une limite temporelle stipulée. Les données sont en effet conservées aussi longtemps qu'il apparaît nécessaire (article 10 a) 2.), si bien qu'au-delà du concept commun entre la décision et l'accord de conservation des données pendant une durée utile, la période maximale de conservation des données prévue par le droit européen n'existe pas dans l'accord franco-américain.

L'article 10.f prévoit que l'accord ne peut faire obstacle au droit de la personne concernée de solliciter la communication d'informations la concernant, ce qui inclut celle relative au transfert de ses données ADN/digitales aux autorités américaines. Toutefois, selon l'article 10.f.2, la mise à disposition de ce droit peut être refusée, conformément à la législation nationale, notamment lorsque la transmission d'informations risque de compromettre les finalités du traitement et les enquêtes ou les poursuites menées par les autorités compétentes aux États-Unis d'Amérique ou par les autorités compétentes en France.

En application de l'article 39 de la loi du 6 janvier 1978, toute personne justifiant de son identité a le droit d'interroger le responsable du traitement en vue d'obtenir des informations relatives aux transferts de ses données. Par dérogation, l'article 41 de la loi du 6 janvier 1978 dispose que pour les traitements tels que le FAED ou le FNAEG, le droit d'accès s'exerce indirectement auprès de la CNIL qui dans ce cas, ne communique pas au requérant le contenu du traitement le concernant. Il lui est seulement notifié qu'il a été procédé aux vérifications. Ce n'est que lorsque la CNIL constate, en accord avec le responsable du traitement, que la communication des données ne remet pas en cause les finalités du traitement qu'il est fait droit à la demande du requérant. En conséquence, le ministère de l'intérieur, responsable des traitements FAED et FNAEG, décidera,

dans le cadre d'une procédure de droit d'accès indirect, si la communication de l'information selon laquelle les données ADN/digitales ont été transférées aux autorités américaines, met en cause la finalité de ces traitements et doit être refusée.

L'accord franco-américain stipule surtout que 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. Dans les faits, ce droit effectif suppose l'adaptation de la législation américaine. À défaut, la Partie française serait fondée à invoquer l'article 14 et d'en suspendre l'application.

Enfin, l'insertion de stipulations relatives à la sécurité des données a pour objectif global et direct de faire satisfaire l'accord aux engagements internationaux de la France en matière de protection des données.

## C. LES DISPOSITIONS D'APPLICATION

### 1. Le suivi de l'application et de l'adéquation de l'accord

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. Y sont mentionnés :

– le motif de la transmission ;

– les informations relatives aux données transmises ;

– la date de transmission ;

– l'ensemble des destinataires.

Ce registre permet, outre la traçabilité des échanges et la sécurité des données, le contrôle effectif des dispositions de l'accord relatives aux consultations automatisées des deux types de fichier, d'une part, et de la législation nationale des Parties relative à la protection des données personnelles, d'autre part. Les données du registre dont l'accès doit être protégé, sont conservées durant deux ans.

Une autorité de contrôle doit par ailleurs être désignée dans le cadre d'arrangements administratifs.

Cette disposition figurant à l'article 10 est extrêmement positive, car il est utile de voir si l'application effective de l'accord permet de renforcer l'efficacité de la coopération et si la transmission de données personnelles était ainsi justifiée.

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. Un an après la mise en œuvre de l'accord, les Parties se consulteront pour dresser un bilan de son application, « en prêtant particulièrement attention à la protection des données à caractère personnel ».Une consultation est expressément prévue en cas d'évolution des négociations de l'accord « parapluie » entre l'Union européenne et les États-Unis.

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. Une défaillance dans l'application de l'article 10 relatif à la protection des données pourrait justifier une telle suspension.

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.

### 2. Une application effective qui restera limitée à court terme

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.

De fait, l'organisation fédérale américaine attribue à chaque État 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. Dans les conditions de la législation américaine actuelle, les accès aux fichiers des États ne sont pas possible et en l'absence de centralisation systématique, l'article 5 ne pourra être mis en œuvre.

### 3. Délais d'entrée en vigueur et de mise en application

L'**article 16** précise les conditions d'entrée en vigueur de l'accord.

L'accord constitue au regard du droit américain un accord de type « *executive agreement* », qui relève du pouvoir exécutif. L'administration américaine a accompli toutes les procédures internes requises avant la signature du texte. La signature du texte constitue l'acte final d'approbation de l'accord, qui ne nécessite donc pas d'autorisation du Congrès américain pour entrer en vigueur. L'accord a simplement été notifié au Congrès pour information après sa signature.

Aucune autre procédure interne n’est requise par le gouvernement fédéral américain pour l’entrée en vigueur de l’accord.

Une fois que la partie française aura achevé ses procédures internes de ratification, il est prévu que la notification par chacune des parties de l’achèvement des procédures nationales internes se fasse par note verbale, ce qui permettra l’entrée en vigueur de l’accord.

L’article 16 énonce : « *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* ».

L’entrée en vigueur des articles 5 et 6 relatifs à la consultation des données est subordonnée à la conclusion des arrangements qui doivent préciser les modalités techniques permettant la mise en œuvre de cette consultation. Le contenu de ces deux arrangements (un pour les données ADN, un pour les données dactyloscopiques) s’inspirera vraisemblablement de l’annexe à la Décision 2008/616/JAI du Conseil de l’UE : format des données, règles de concordance, modalités techniques d’accès distant aux bases de données, choix du réseau de communication, architecture informatique, sécurité des données. Pour information, avec les partenaires européens ayant signé un accord similaire avec les États-Unis, 7 Réseaux virtuels privés (Virtual Private Networks) pour l’échange d’empreintes digitales ont été créés et 22 réseaux temporaires sont opérationnels.

Les développements techniques et fonctionnels à engager nécessiteront des échanges avec les personnels américains idoines afin de définir le format des données et le canal technique à utiliser. Les délais de mise en œuvre seront donc fonction de la situation, notamment si un écart est noté entre les deux architectures techniques.

Sous réserve de ce qui précède, pour les interrogations du FAED, la connexion pourrait se faire en quelques mois. Quant aux interrogations du FNAEG, cela dépendra de la capacité des États-Unis, notamment sur le plan législatif, à mettre en œuvre l’accord. Dans l’attente, la procédure habituelle et actuelle sera maintenue (transmission via les canaux de la coopération policière d’Europol et d’Interpol).

D’autre part, si des développements techniques devaient être engagés, ces derniers ne devront pas impacter les échéances des travaux de modernisation actuellement en cours sur les deux applications françaises concernées (FAED et FNAEG), qui sont contractualisées et budgétisées. Un décalage dans leur mise en œuvre aurait un impact budgétaire considérable.

## CONCLUSION

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.

Parmi les pays de l'Espace économique européen pratiquant l'exemption de visa, tous disposent d'un accord de cette nature avec les États-Unis ou d'une base alternative autorisant l'échange de données. Plusieurs autres pays qui ne sont pas membres du Programme d'exemption de visa, dont les cinq pays de l'Union européenne entrant dans cette catégorie, ont négocié un tel accord (la Bulgarie, la Croatie, Chypre et la Roumanie l'ont signé, alors que les négociations sont en cours avec la Pologne).

Si la consultation automatisée des fichiers génétiques pour établir la concordance ou non concordance d'une empreinte ne pourra être mise en œuvre dans un avenir proche, la consultation des fichiers d'empreintes digitales ainsi que la possibilité dans la cadre de la prévention de la criminalité grave et du terrorisme de procéder à des échanges spontanés pourront s'avérer d'une très grande utilité au regard de la rapidité et de l'efficacité requises dans les enquêtes. Lorsqu'un message est aujourd'hui envoyé, la réponse arrive après quelques jours ou plusieurs semaines alors que l'accord permettrait immédiatement d'établir l'existence d'une concordance.

S'agissant des données dactyloscopiques, les demandes de transmission demeurent trop faibles au regard de leur pertinence face à des criminels qui usent de plusieurs identités. Le réflexe de consultation, couplée à une procédure bien établie, pourrait avoir un impact substantiel. Soulignons que la France émet 1300 demandes par an environ à ses partenaires « Prüm ». C'est la raison pour laquelle, au-delà des positions du Congrès américain sur la question du maintien du programme d'exemption de visa, tant le gouvernement des États-Unis que le Gouvernement français accordent autant d'importance à cet accord.

La législation américaine devrait être en mesure de répondre aux dernières exigences françaises en matière de recours avant la mise en application de l'accord. Dès lors, compte tenu encore une fois des nombreuses garanties contenues dans l'accord et des mécanismes de suivi institués, qui rendent cet accord singulier comme l'ont confirmé les conseillers de l'Ambassade des États-Unis à Paris, votre Rapporteur ne peut qu'émettre un avis favorable à la ratification de l'accord.

## EXAMEN EN COMMISSION

La commission examine le présent projet de loi au cours de sa séance du mercredi 27 janvier 2016 à 9 heures 45.

Après l'exposé du rapporteur, un débat a lieu.

**M. Jacques Myard.** Je voudrais souligner que cet accord a été bien négocié, notamment parce qu'il l'a été sur la base de la réciprocité. En cela, il diffère de l'accord que nous avons négocié en matière de fraude fiscale, qui était sans doute nécessaire mais qui a maintenant pour effet que des citoyens français travaillant aux États-Unis ne peuvent pas avoir de compte bancaire en France.

Il faudrait donc renégocier cet accord sur le modèle de celui dont nous parlons aujourd'hui. Il doit être appliqué de bonne foi, mais il est fondé sur la réciprocité avec des verrous qui sont la loi nationale.

Ma question est la suivante : compte tenu du caractère fédéral du système politique américain et de la force des Etats fédérés surtout en matière de police et de données, est-ce que la loi fédérale qui va passer permettra de le mettre en œuvre cet accord et d'avoir des échanges réciproques ?

**M. Thierry Mariani.** J'approuve ce texte qui est nécessaire et qui effectivement entraine des obligations réciproques.

Je souhaiterais poser deux questions. La première est, si j'ose dire, neutre : des accords similaires ont été négociés, avez-vous dit, avec les autres États européens. Pourquoi, dans ce cas, ne pas l'avoir négocié entre les États-Unis et l'Union européenne ? Est-ce parce que cela ne rentre pas dans les compétences de l'Union européenne ?

Ma deuxième question, qui rejoint la remarque de Jacques Myard, est la suivante : la structure fédérale des États-Unis ne va-t-elle pas faire obstacle à l'application de cet accord pour certains transferts d'informations ?

**M. Philippe Baumel, rapporteur.** Je partage l'avis de Jacques Myard sur la qualité de cet accord. Concernant la loi fédérale en cours d'examen, la démarche semble assurée car on nous a fait savoir qu'elle être votée par le Sénat américain dans le courant de l'année et elle permettra l'application de l'accord sur la question des recours.

Concernant l'Union européenne, un accord entre cette dernière et les États-Unis est en fait en cours de négociation sur les règles de protection des

données échangées. D’une certaine façon nous l’avons anticipé. Les Etats-Unis ont négocié des accords bilatéraux avec les partenaires du programme d’exemption de visas pour autoriser les échanges et améliorer la coopération opérationnelle entre services. Nous avons besoin d’un accord spécifique entre nos deux pays. L’accord franco-américain comporte des clauses de protection des données avancées et s’il y a un accord global au niveau européen en cours de négociation, sa procédure d’adoption n’est pas achevée.

**M. Thierry Mariani.** Que contiendra de plus l’accord européen ?

**M. Philippe Baumel, rapporteur**. Il renforcera les règles de protection des données personnelles par rapport à beaucoup d’accords bilatéraux, mais son analyse détaillée est en cours.

Suivant l’avis du rapporteur, la commission *adopte* le projet de loi (n° 2852) sans modification.

# ANNEXES

## ANNEXE N° 1 :

## LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR

– Mme Mireille BALLESTRAZZI, directeur central de la police judiciaire, Madame Florence MOURARET, commissaire de police, adjointe au chef du service central d'identité judiciaire (S.C.I.J.) de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire et M. Alexandre PICHON, commissaire divisionnaire ;

– M. Émile GABRIÉ, chef du service régalien et collectivités territoriales de la CNIL et Mme Tiphaine INGLEBERT, Conseillère pour les questions institutionnelles et parlementaires ;

– M. Peter AXELROD, attaché de Justice près l'Ambassade des États-Unis à Paris et M. Timothy FITZGIBBONS, premier Secrétaire aux Affaires politiques de l'Ambassade.

# ANNEXE N° 2 :

# COMPARATIF ENTRE L'ACCORD ET LES DÉCISIONS « PRÜM »

| Décision Prüm 2008/615 JAI | Accord France – États-Unis |
|---|---|
| **Finalités**<br>Les finalités sont les suivantes :<br>- la lutte contre le terrorisme ;<br>- la criminalité transfrontière ;<br>- la migration illégale.<br>L'article 35 de la décision, relatif au *« Rapport avec d'autres instruments »* n'envisage la conclusion d'accords bilatéraux postérieurement à son entrée en vigueur qu'entre les États membres (*point b)*, puisqu'elle évoque au point 6 de cet article les accords bilatéraux entre des États-membres et des États-tiers antérieurs à la décision. Elle ne comporte pas de disposition relative à des accords bilatéraux futurs conclus par les États-membres avec des États-tiers. | Les finalités de cet accord sont la prévention et lutte contre la criminalité grave (« *serious crime* »), en particulier le terrorisme (Article 2). Les crimes et délits sont énumérés en annexe de l'accord.<br><br>**Les finalités sont partiellement concordantes.** |
| **Les catégories de données**<br>1) consultation des fichiers d'analyse ADN (Articles 3 et suivants)<br>- consultation de profils ADN issus de la partie non codante de l'ADN<br>- comparaison effectuée à partir des données indexées des fichiers d'analyse ADN<br>- un numéro de référence qui ne permet pas l'identification directe de la personne concernée ;<br>A ce stade de la consultation, aucune donnée d'identification directe de la personne.<br>- **Accès automatique des points de contact nationaux dans le fichier d'analyse ADN (FNAEG)**, consultation automatisée, au cas par cas, dans le respect du droit national de la partie consultante. Lorsqu'une concordance est mise en évidence, le point de contact national dans lequel la consultation est effectuée reçoit automatiquement les données indexées et communique sans délai au point de contact national de l'autre État membre les données indexées pour lesquelles une concordance a été mise en évidence.<br>- Si, dans le cadre d'une enquête ou d'une procédure judiciaire, le profil ADN d'une personne déterminée fait défaut, le pays de l'UE requis peut être tenu d'établir un profil ADN pour cette | 1) consultation des fichiers d'analyse ADN (Article 5)<br>- profils ADN issus de la partie non codante de l'ADN ;<br>-Accès automatique à la base de données nationale (FNAEG) par le point de contact américain, information automatique en cas de concordance ou de non concordance.<br>- En cas de concordance de l'ADN, **une notification automatique au point de contact national américain est adressée avec la référence concordante, en vue de la seconde étape : transmission des données à caractère personnel qui peut être assortie d'une condition liée au respect de la législation française (voir 3. de l'article 9)**[1].<br>Même en cas de non-concordance, il y a également notification automatique.<br><br>**Par conséquent, le mécanisme défini dans l'accord franco-américain n'implique pas une transmission automatique des données personnelles.** |

[1] *Pour prendre un exemple concret, pas d'utilisation possible de ces données dans le cadre d'un procès qui pourrait conduire à l'application de la peine de mort.*

| | |
|---|---|
| personne. | |
| 2) <u>consultation des fichiers d'empreintes digitales</u> (Article 8 et suivants)<br>- données dactyloscopiques<br>- référence<br>Consultation du fichier d'empreintes digitales à l'aide d'une « donnée indexée », le lien entre la donnée dactyloscopique et la donnée indexée est réalisée par le point de contact national. La réponse automatisée donne une réponse univoque. | 2) <u>consultation des fichiers d'empreintes digitales</u> (Article 3)<br>- Processus identique à celui décrit pour le fichier ADN. Consultation directe du FAED sur un mode concordance/non concordance.<br>La même étape préalable à la transmission de données personnelles s'applique dans l'accord franco-américain, tant pour les empreintes digitales que l'ADN.<br>**A la différence du cadre juridique défini décision 2008/615/JAI qui postule un échange entre États membres, c'est-à-dire entre pays ayant un droit national offrant un haut niveau de protection des données, l'accord franco-américain encadre fortement les conditions d'envoi des données.** |
| <u>3) consultation automatisée de données dans les registres d'immatriculation de véhicules</u>. (Article 12) | **Non prévu** |
| 4) <u>Des données à caractère non personnel et à caractère personnel peuvent être transmises en vue de prévenir des infractions pénales et de maintenir l'ordre et la sécurité publique lors de manifestation de grande envergure à dimension transfrontalière</u>. (Article 14) | **Non prévu** |
| 5) <u>Afin de prévenir des infractions terroristes</u> Les États membres peuvent échanger entre eux certaines données à caractère personnel, en l'occurrence le nom, prénom, date et lieu de naissance, et la description des faits desquels dont découle la présomption que les personnes concernées vont commettre des infractions similaires à celles visées par l'accord. (Article 16) | <u>Afin de lutter contre la criminalité grave et le terrorisme, l</u>e même type de disposition est repris dans le projet d'accord ; chaque partie, sur sa propre initiative, peut transmettre les données complètes d'identification d'un individu, lorsqu'il y a raison de croire que l'intéressé a commis ou va commettre des actes terroristes/criminels graves, ou a participé/va participer à leur préparation (article 9). Les données transmises sont les suivantes :<br>- nom, prénoms, alias, sexe, date et lieu de naissance,<br>- un exposé des circonstances qui motivent la transmission.<br>**Il s'agit du même type d'information pour la décision 2008/615/JAI et l'accord franco-américain.** |
| **La durée de conservation des données/mise à jour des données**<br>Un délai maximal est prévu pour la conservation des données dans le droit national de la partie contractante transmettant les données. Ce délai maximum doit être indiqué à l'autorité destinataire au moment de la transmission.<br>Pour le FNAED et le FNAEG, les délais de conservation sont au maximum de 25 ans.<br>Les données légalement transmises et reçues sont effacées si elles ne sont pas ou plus nécessaires au regard des finalités pour lesquelles elles ont été transmises. (article 28) | Absence de délai de conservation sous la forme d'une limite temporelle stipulée. Les données sont conservées aussi longtemps qu'il apparaît nécessaire (article 10 a) 2.).<br>Au-delà du concept commun entre la décision et l'accord de conservation des données pendant une durée utile, la période maximale de conservation des données prévue par le droit européen n'existe pas dans l'accord franco-américain. |
| **Les destinataires des données**<br>Ce sont les points de contact nationaux qui sont | Les points de contact nationaux, sont aussi régis par |

| | |
|---|---|
| régis par leur droit national. (Articles 6, 11 et 15) | leur droit national. (Article 4) |
| **Les échanges avec les pays tiers**<br>L'autorité transmettant des données peut en vertu du droit national fixer les conditions relatives à l'utilisation des données et informations par l'autorité destinataire et cette dernière est liée par ces conditions.<br>Chaque partie contractante s'engage à garantir un niveau de protection des données correspondant au moins à celui résultant de la Convention du Conseil de l'Europe du 28 janvier 1981 relatif 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. (article 34) | L'échange de données avec les États tiers ne peut être effectué que si l'autre partie consent à ce transfert (article 10 b) 7.). |
| **Les droits d'accès et droit de recours**<br>Chaque pays de l'UE doit garantir dans son droit national un niveau de protection des données personnelles traitées conformément à cette décision.<br>Le droit au recours est garanti par l'article 31 de la décision qui ouvre également le droit à réparation.<br>Par ailleurs, le droit d'accès est explicitement assuré par un renvoi aux dispositions du droit national. | L'accord franco-américain stipule que 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.<br>Dans les faits, ce droit effectif suppose l'adaptation de la législation américaine. A défaut, la Partie française serait fondée à invoquer l'article 14 et d'en suspendre l'application. |
| **La sécurité des données**<br>**La décision vise à garantir un niveau approprié de protection des données et respecte le niveau de protection prévu pour le traitement des données à caractère personnel au niveau du droit conventionnel européen[1].** (Article 29)<br>Plusieurs garanties sont offertes :<br>- la documentation de la transmission et de la réception des données ;<br>- la tenue d'un registre de journalisation ;<br>- un mécanisme de traçabilité ;<br>- un système d'authentification. | **L'insertion de stipulations relatives à la sécurité des données a pour objectif global et direct de faire satisfaire l'accord aux engagements internationaux de la France en matière de protection des données.** (Article 10)<br>Les principales garanties apportées par le projet d'accord :<br>- un système d'authentification ;<br>- la mise en place d'une documentation des transmissions et des réceptions des données ;<br>- la tenue par chaque Partie d'un registre permettant d'assurer le contrôle effectif du respect des règles<br>- la possibilité de suspendre l'application et de dénoncer l'accord pour un effet au terme de trois mois |

*Source : ministère des Affaires étrangères et du développement internationale*

[1] *Convention 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 dans son protocole additionnel du 8 novembre 2001, ainsi que les principes énoncés dans la recommandation n° R (87) 15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.*

# ANNEXE

## TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES

### Article unique
*(Non modifié)*

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.

---

NB : Le texte de l’accord figure en annexe au projet de loi (n° 2852)