PATRIOT Act et FREEDOM Act

Enjeux, *cloud computing* et accès aux données

Résumé

A l'ère du numérique, la plupart des projets des entreprises et des administrations sont tournés vers les technologies avancées et l'informatique en général. La place occupée par les Américains dans le domaine n'est plus à prouver et ces derniers ont parfaitement conscience de leur position de force.

Le *PATRIOT Act* adopté en 2001 a permis aux Etats-Unis de s'arroger des droits importants, tout particulièrement en ce qui concerne l'accès aux données. Par cet acte, ils ont pu accéder aux données relatives aux citoyens américains mais pas seulement puisque les Européens sont également concernés. Le champ d'application large du *PATRIOT Act* a conduit à ce que la quasi-totalité des personnes physiques mais également des entreprises et administrations soient concernées par son application. Les moyens utilisés pour collecter leurs données étaient en effet nombreux, variés et l'accès à ces informations était relativement aisé pour certaines agences gouvernementales américaines.

Pleinement conscient des enjeux posés par le *PATRIOT Act*, notamment dans le cadre du *cloud computing*, le Cabinet d'Avocats Mathias a rédigé ce Livre Blanc afin de préciser la portée de cet acte législatif américain et ses effets sur les personnes et entreprises européennes.

Abstract

The digital age has increased the number of business and administration projects dealing with IT and advanced technologies. The United States dominance in this field is indisputable and Americans are well aware of their advantage. Since the PATRIOT Act was passed, the United States Government was able to get easy access to personal data all over the world. Its wide scope of application leads to the fact that almost each natural and legal person is somehow concerned by these laws and regulations. Moreover, the means used to collect data are diversified and numerous.

Because we are fully aware of the various issues stemming from the PATRIOT Act, especially regarding cloud computing, we, at Cabinet Mathias, wrote this Whitepaper in order to point out the far-reaching implications of this US law, as well as to stress its legal effects on European citizens and companies.

I - Qu'est-ce que le *PATRIOT Act* ?

Le « Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept an Obstruct terrorism *Act »* ou son acronyme « *USA PATRIOT Act »* est l'acte législatif controversé adopté par le Congrès des Etats-Unis le 26 octobre 2001. Le *PATRIOT Act* est donc apparu dans un contexte bien particulier et avait pour objectif d'apporter une réponse aux attaques terroristes subies par la superpuissance américaine. Nous le verrons, les droits que se sont arrogés les Américains leur ont bien souvent permis de collecter des données de personnes physiques et morales qui semblaient ne pas être liées à des actes de terrorisme.

Le *PATRIOT Act* en réponse à « *l'Axe du mal*[1] »

A la suite des attaques terroristes du 11 septembre 2001, les Etats-Unis sont sous le choc. La peur américaine est à son paroxysme et a sans nul doute contribué au fait que le Congrès renforce les pouvoirs du gouvernement fédéral et de certaines autorités d'investigation en matière de lutte contre le terrorisme.

La communauté internationale était également sous le choc. Le Conseil de sécurité des Nations Unies a lui-même appelé à « *redoubler d'efforts pour prévenir et éliminer les actes terroristes* » et s'est déclaré prêt à « *prendre toutes les mesures nécessaires pour répondre aux attaques terroristes du 11 septembre 2001 et pour combattre le terrorisme sous toutes ses formes*[2] ».

Dans sa résolution du 12 septembre 2001, le Conseil de sécurité appelle tous les Etats à « *travailler ensemble pour traduire en justice les auteurs, organisateurs et commanditaires de ces attaques terroristes et souligne que ceux qui portent la responsabilité d'aider, soutenir et héberger les auteurs, organisateurs et commanditaires de ces actes devront rendre des comptes* ».

Le Conseil reconnaît également aux Etats-Unis un droit de « *légitime défense* », tel que le définit l'article 51 de la Charte des Nations Unies, c'est-à-dire les autorisant à recourir à la force[3]. Dès lors, l'adoption d'actes législatifs en réponse à ces actes terroristes n'était pas étonnant.

Le Code des Etats-Unis, dans son titre 22, chap.38, paragraphe 2656f(d) donne la définition suivante du terrorisme :
«*The term "terrorism", means premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents* ».
Ce même article définit également les termes de groupes terroristes, de terrorisme international ou bien encore de « *sanctuaire terroriste* ».

[1] Discours sur l'état de l'Union du 29 décembre 2002 de Georges W. Bush.

[2] Résolution des Nations Unies 1368 adoptée le 12 septembre 2001

[3] L'article 51 stipule qu' « *aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense […] dans le cas où un membre des Nations unies est l'objet d'une agression armée* ».

On notera par ailleurs que même si le *PATRIOT Act* a été adopté en 2001, celui-ci a longtemps fait débat que ce soit aux Etats-Unis ou au-delà des frontières américaines.

Le *PATRIOT Act* : une loi d'exception ?

Le *PATRIOT Act* s'inscrivait initialement dans un régime d'exception. Il est cependant devenu, au fil du temps, un principe. La loi qui devait s'appliquer pendant dans une période déterminée (quelques semaines) s'est en effet installée durablement dans le paysage législatif américain, tout particulièrement pour certaines de ses dispositions. Le *PATRIOT Act* a donc été prorogé à plusieurs reprises, notamment grâce à l'adoption du ***PATRIOT Act Improvement and Reauthorization Act*** en mars 2006.

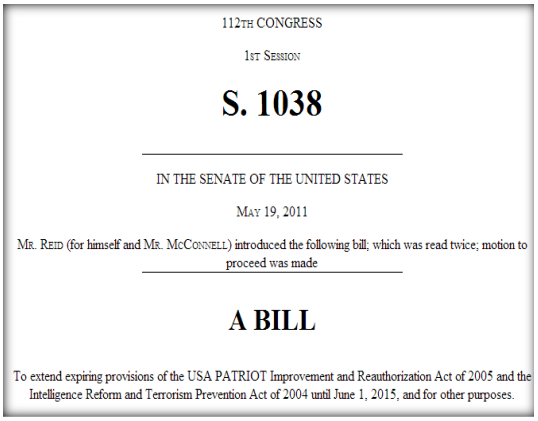
Il convient d'insister sur le fait que certaines des dispositions du texte initial ont acquis un statut permanent. C'est le cas par exemple de la section 218 qui autorise les « *perquisitions secrètes* »[4] via l'application du ***Foreign Intelligence Surveillance Act of 1978***, texte que nous appréhenderons plus loin dans ce Livre Blanc. En ce qui concerne les autres dispositions, celles-ci doivent être votées régulièrement. Ainsi, à la suite du vote de 2006, le *PATRIOT Act* a pu être prolongé *in extremis* en 2011 et le ***Patriot Sunsets Extension Act of 2011*** s'est donc appliqué jusqu'au mois de juin 2015.

[4] Perquisition menée en l'absence de la personne concernée (propriétaire, locataire du logement, local, etc.).

Nous pouvons constater aujourd'hui que le *PATRIOT Act* ne conserve pas vraiment son caractère d'exception.

Le USA FREEDOM Act a été voté le 2 juin 2015 (*Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act*).

Le Congrès s'est ainsi prononcé en faveur d'une nouvelle prolongation du PATRIOT Act qui avait expiré le jour précédent, sous une forme différente pour certaines de ses dispositions (superficielle selon certaines associations) et ce, jusqu'en 2017. Nous y reviendrons dans ce Livre Blanc.



112TH CONGRESS

1ST SESSION

S. 1038

IN THE SENATE OF THE UNITED STATES

MAY 19, 2011

MR. REID (for himself and MR. MCCONNELL) introduced the following bill; which was read twice; motion to proceed was made

A BILL

To extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and the Intelligence Reform and Terrorism Prevention Act of 2004 until June 1, 2015, and for other purposes.

Un champ d'application très large

Le *PATRIOT Act* a conduit à la modification de nombreuses lois fédérales, telles que **l'*Immigration and Nationality Act*, *l'Eletronic Communications Privacy Act of 1986*** ou bien encore le ***Foreign Intelligence Surveillance Act of***

1978. Ce ne sont pas moins d'une quinzaine de lois fédérales qui ont été modifiées par le PATRIOT Act.

L'une des implications les plus remarquables de ce texte de plus d'une centaine de pages consiste en l'élargissement du droit, pour certaines autorités d'investigation américaines telles que le FBI (*Federal Bureau of Investigation*) ou la NSA (*National Security Agency*), d'exiger la communication de données détenues par les entreprises ou leurs prestataires. La question de l'accès aux données est ainsi l'une des implications centrales de ce texte de loi et c'est d'ailleurs cette problématique qui fait plus précisément l'objet de ce Livre Blanc.

Précisons que le *PATRIOT Act* touche à des domaines variés et permet l'utilisation de mesures spécifiques telles que les « *perquisitions secrètes* » par exemple. On ne s'étonnera donc pas que ces dernières aient conduit à des débats pour le moins houleux de l'autre côté de l'Atlantique.

Ce fut par exemple le cas avec une affaire résolue en 2007 à la suite d'un arrêt rendu par un juge fédéral. La décision a conduit à déclarer inconstitutionnelles deux dispositions du *PATRIOT Act* concernant les recherches et la collecte de renseignements par le biais de perquisitions.

Le juge fédéral avait alors fait savoir que le *Foreign Intelligence Security Act* tel qu'il a été amendé permettait au gouvernement d'effectuer certaines opérations de surveillance et recherches ciblant les Américains sans satisfaire au « *critère de la probabilité* »[5].

En l'espèce, l'avocat Brandon Mayfield avait été arrêté à tort pour sa participation supposée aux attentats de Madrid en 2004. L'avocat de Portland affirmait dans son recours contre le gouvernement fédéral que sa maison et son bureau avaient été secrètement fouillés par le FBI. Le FBI aurait ainsi recherché les dossiers de ses clients, effectué secrètement des copies de ses fichiers stockés sur ses ordinateurs professionnels et personnels mais aussi mis sur écoute sa ligne téléphonique tout en mettant sa maison sous surveillance.

"*The Supreme Court has cautioned*
The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation.
For private dissent, no less than open public discourse, is essential to our free society".

Mayfield vs United States of America, 26 September 2007

[5] CNN.com, *Federal Judge rules 2 Patriot Act provisions unconstitutional*, http://edition.cnn.com/2007/US/law/09/26/patriot.act/

Ce cas d'espèce montre bien le genre de mesures qui ont pu être autorisées à la suite de l'adoption du *PATRIOT Act*. Bien entendu, les données en ligne sont tout particulièrement visées par cet acte législatif américain, ce qui impacte bien évidemment le c*loud computing*.

Les sections 215 et 505 du *PATRIOT Act* sont celles qui précisent les données et les supports susceptibles d'être exigés :

- La section 505 du titre V du *PATRIOT Act* intitulée « ***Removing Obstacles to Investigating Terrorism*** » conduit à faciliter l'émission des *National Security Letters* (NSL) prévues dans *l'Electronic Communications Privacy Act*. Ainsi, le gouvernement peut émettre des NSL « *dès lors qu'une enquête pertinente est autorisée afin de se protéger contre tout terrorisme international ou toute activité clandestine de renseignement* ». Cette même section 505 du *PATRIOT Act* a également conduit à amender la section 2709(b) du titre 18 du Code des Etats-Unis relatif **au frais de téléphone et aux documents de transactions**. La disposition conduit alors à ce que « **le *nom, l'adresse, la durée du service, les données de facturation*** *puissent être communiqués dans le cadre d'une enquête* ». On peut par ailleurs souligner qu'il est désormais possible pour les bureaux locaux du FBI[6] d'user directement des NSL et qu'il ne leur est donc plus nécessaire de passer automatiquement par l'autorité centrale.

- La section 215 renvoie à la section 501 du *Foreign and Intelligence Act of 1978* qu'elle a amendée. Il est précisé que « *le directeur du FBI ou une personne désignée par le directeur (dont le rang ne doit pas être inférieur à celui de responsable spécial adjoint) peut, par le biais d'une ordonnance, exiger la production de toute chose tangible (y compris **les livres, des dossiers, des papiers, des documents et tout autre élément**) dans le cadre d'une enquête contre le terrorisme ou l'espionnage international* ».

On notera que les **données et les fichiers informatiques sont implicitement inclus**, notamment dans le cadre du ***cloud computing***. Le USA FREEDOM Act a modifié cette section, nous aurons l'occasion d'y revenir à la fin de ce Livre Blanc.

[6] Article 18 du Code des Etats-Unis, § 2709(d)

Le contexte actuel dans lequel évoluent les entreprises et les administrations conduit à ce que toutes les personnes physiques et morales puissent se voir concerner par les mesures du *PATRIOT Act*. Les affaires récentes concernant la NSA tendent par ailleurs à démontrer que le secteur privé tout comme le secteur public sont concernés par son application. L'objectif de ce Livre Blanc est donc de permettre une meilleure appréhension des questions liées à l'accès aux données à caractère personnel, notamment à celles des Européens.

II – L'accès aux données mises en ligne facilité par le *Patriot Act*

Tout d'abord, et contrairement à ce qui est souvent rapporté, le *PATRIOT Act* n'est pas l'acte législatif qui a mis en place les outils principaux permettant l'accès à ces données. Les *FISA Orders* et les *National Security Letters* existaient déjà avant l'adoption du *PATRIOT Act* en 2001. A vrai dire, le texte a surtout conduit au renforcement des mesures existantes, notamment par le biais des *gag Orders*.

Les *FISA Orders*

Comme cela a déjà été précisé, les *FISA Orders* ne sont pas une nouveauté du *PATRIOT Act*. Ils ont en effet été mis en place par le *Foreign Intelligence Security Act* (FISA Act) de 1978. Cet acte est donc celui qui a rendu possible l'obtention de *FISA Orders* par le FBI, même si celui-ci doit tout d'abord solliciter la *Foreign Intelligence Surveillance Court.* Une fois le recours à ce moyen autorisé, il pourra émettre des *FISA Orders* afin d'obtenir des documents commerciaux de la part de tiers dans le cadre des besoins de services de renseignement et d'enquêtes sur le terrorisme international.

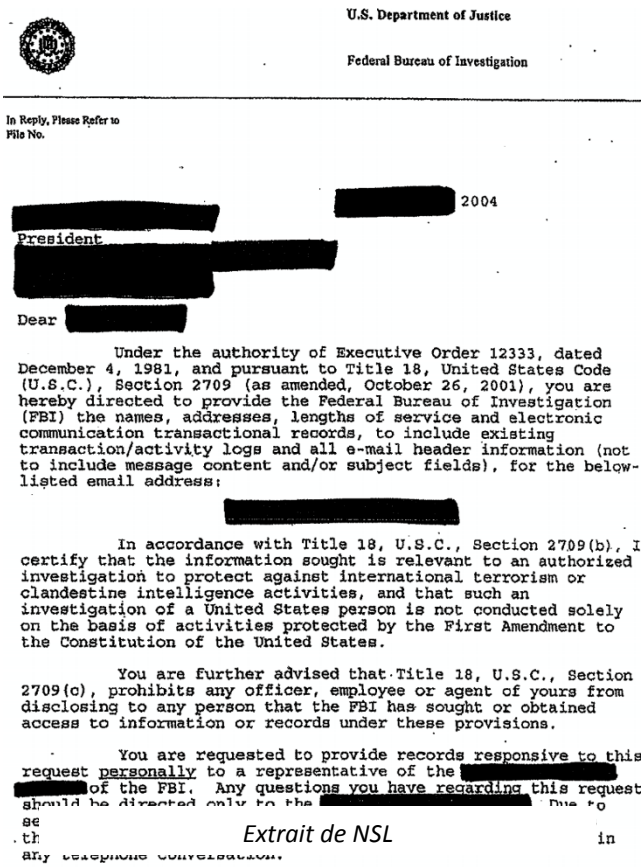
Le *PATRIOT Act* a simplement conduit à une modification des modalités d'émissions des *FISA Orders*. Par exemple, la section 215 du *PATRIOT Act* (*Enhanced Surveillance Procedure*) a permis l'élargissement du champs de recherche à tout élément tangible. L'intérêt des *FISA Orders* est de permettre à certaines agences gouvernementales d'obtenir une ordonnance enjoignant à un tiers la communication de tout élément important dans le cadre d'une enquête liée au terrorisme ou aux activités clandestines de renseignement. Bien entendu, une procédure particulière doit être suivie afin que l'agence concernée puisse obtenir cet acte. Celle-ci doit ainsi préciser que les éléments recherchés s'inscrivent précisément dans le cadre du terrorisme et ces derniers doivent être validés préalablement par la *FISA Court*.

Il existe toutefois une exception à cette procédure. Il n'est en effet pas toujours nécessaire d'avoir l'autorisation de la Cour pour recourir aux *FISA Orders*. Il sera ainsi possible pour le Président de demander une interception de données en autorisant

le Procureur général des Etats-Unis (équivalent du Ministre de la Justice) à recourir à ce moyen pour une période d'un an dans le cadre d'enquêtes sur les activités étrangères[7]. Le cas de guerre constitue également une autre exception : il sera ainsi possible pour le Président de recourir à une surveillance sans mandat au début d'une guerre. Cependant, cette surveillance ne pourra pas excéder plus de quinze jours après la déclaration de guerre par le Congrès[8].

Les *National Security Letters*

Les *National Security Letters* (NSL) constituent l'un des autres mécanismes de référence pour l'accès aux données. Ces NSL existaient avant l'adoption du *PATRIOT Act*.



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

[redacted] 2004

President

[redacted]

Dear [redacted]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, lengths of service and electronic communication transactional records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields), for the below-listed email address:

[redacted]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the [redacted] of the FBI. Any questions you have regarding this request should be directed only to the [redacted]. Due to se
th in
any telephone conversation.

Extrait de NSL

Leur émission était en effet déjà possible par le biais de quatre lois fédérales. Parmi elles, il est possible de citer le ***Financial Privacy Act*****,** le ***National Security Act*** et le plus important en ce qui concerne notre sujet de l'accès aux données électroniques, l'ECPA (***Electronic Communications Privacy Act***). Ce dernier est d'autant plus important qu'il s'intéresse tout particulièrement aux fournisseurs de services mobiles et de communication électronique, dont les fournisseurs d'accès à internet.

Ces NSL consistent en une sorte d'injonction administrative dont la délivrance a été facilitée par la section 505 du *PATRIOT Act*. Cette disposition autorise en effet le gouvernement à délivrer des NSL dès lors qu'il s'agit de la protection « *contre le terrorisme international ou les activités de surveillance clandestines* ».

Le changement apporté par le *PATRIOT Act* consiste en l'augmentation du nombre de cas où une NSL peut être délivrée. Antérieurement, la demande de divulgation de renseignements via les NSL devait être accompagnée de preuve de faits précis. A la suite de son entrée en vigueur, la charge de la preuve est devenue moins lourde, il suffisait d'établir la pertinence des données faisant l'objet de la demande par rapport à une enquête en cours.

Par ailleurs, les cinquante-six agences du FBI ont obtenu la faculté de délivrer des NSL[9]. Ainsi, le siège du FBI n'est plus le seul à décider de leurs émissions, ce qui permet aux différentes agences d'émettre

[7] Article 50 du Code des Etats-Unis, § 1801
[8] Article 50 du Code des Etats-Unis, § 1811
[9] Article 18 du Code des Etats-Unis, §2709

elles-mêmes ces injonctions sans avoir à demander l'aval du siège.

Malgré tout, il faut souligner que la délivrance de tels actes envers les citoyens américains est limitée. Ces derniers ne peuvent en effet faire l'objet d'une enquête conduite « *uniquement sur la base d'activités protégées par le premier amendement de la Constitution des Etats-Unis* ».

Enfin, il est possible de noter qu'à la différence des *FISA Orders*, les NSL ne nécessitent aucune décision juridictionnelle préalable afin de pouvoir être délivrées.

Les *gag Orders*

S'il est un changement opéré par le *PATRIOT Act* qui fait l'objet de larges débats Outre-Atlantique, c'est bien la question des « *gag Orders* » ou « *ordonnance de bâillonnement* ». Cette ordonnance consiste à cacher aux personnes directement concernées par les NSL ou *FISA Orders* que des recherches ont été faites les concernant.

A titre d'exemple, un prestataire de *cloud* devra dissimuler à ses clients qu'il a dû transmettre des données les concernant, sous peine de poursuites pénales non négligeables (amende et emprisonnement).

En ce qui concerne les *FISA Orders*, le *USA Patriot Improvement and Reauthorization Act of 2005* a permis de réduire quelque peu la portée des *gag Orders.* La personne réceptrice d'une telle ordonnance a en effet obtenu le droit de contester la décision un an après son émission.

C'est également ce même acte qui a permis de réduire la portée de ces ordonnances pour les NSL. La section 216 du *PATRIOT Act* permet donc de limiter la confidentialité normalement exigée en permettant aux fournisseurs de services mobiles ou de communication électronique de faire savoir que le FBI a cherché ou obtenu l'accès à certaines informations, sauf si le FBI en a décidé autrement.

La section 115 de l'*USA Patriot Improvement and Reauthorization Act* permet, pour la personne concernée par la confidentialité, de demander une révision par la Cour de cette obligation de garder le secret.

Le tableau suivant permet de récapituler les différences entre les NSL et les *FISA Orders* et les moyens d'action de ces différents mécanismes.

Caractéristiques	***FISA Orders***	***National Security Letters* (NSL)**
Objectifs	Accès aux données « ***justifié par les intérêts nationaux autre que l'application du droit pénal*** ».	Idem.
Base légale	Le ***Foreign Intelligence Surveillance Act*** a été inséré au Titre 50 du Code des Etats-Unis intitulé « *War and National Defence* ».	5 lois sont relatives aux NSL : - *The Right to Financial Privacy Act*; - *National Security Act* ; - *The Fair Credit Reporting Act*; - *The Electronic Communications Privacy Act*; - *PATRIOT Act*.
Particularités	**La section 215 du *PATRIOT Act*** facilitant l'émission des *FISA Orders* s'est vue prolongée à plusieurs reprises (actuellement jusqu'en 2015).	Des **amendements** relatifs aux NSL sont souvent réalisés.
Procédure	**En principe,** le *FISA Order* doit tout d'abord être **approuvé par la *Foreign Intelligence Surveillance Court*. Toutefois,** l'approbation de la Cour n'est pas nécessaire si le but est la surveillance d'une puissance étrangère (durée d'un an).	**Aucun contrôle juridictionnel n'est requis**. Les NSL peuvent être délivrées par le gouvernement ainsi que par les 56 agences du FBI.
Types de données accessibles	Champ d'application large. Se rapporte aux **informations substantielles**.	**Champ d'application strict**. Se rapporte à des informations non-substantielles.
***gag Orders* (ordonnance de bâillonnement)**	En principe, un ***gag Order*** accompagne le *FISA Order*.	Généralement, **pas de *gag Order*.**
Utilisation	Faible	Importante

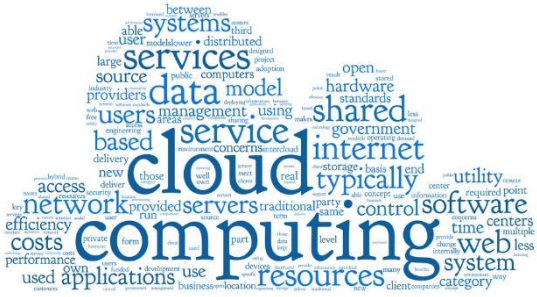
Nous verrons ensuite de quelle manière les Etats-Unis sont parvenus à mettre en place un mécanisme juridique leur permettant un accès simple aux données des différents utilisateurs du *cloud computing*.

III – Un accès aux données hors les frontières américaines

Le droit américain prévoit une compétence extrêmement large en ce qui concerne les personnes dont les données sont susceptibles de faire l'objet d'une demande de communication, ce qui lui permet de viser des citoyens non-américains.

Le *FISA Act* vise directement les étrangers

Un amendement du ***Foreign Intelligence Security Act*** en 2008 concernait tout particulièrement la question de l'accès aux données des non-citoyens des Etats-Unis et a repris les mesures du ***Protect America Act*** (qui a expiré la même année) sur le sujet en y ajoutant un nouveau Titre VII.



Ainsi, la **section 702 du *FISA Act*** se retrouve désormais à l'article 1881 du Code des Etats-Unis et s'intitule : "*Procedures for targeting certain persons outside the United States other than United States persons*", soit les procédures à l'encontre de certaines personnes à l'extérieur des Etats-Unis, autres que les citoyens américains.

Cet article relatif à l'acquisition de données dispose ainsi que « (a) *le procureur général et le directeur du renseignement national peuvent autoriser conjointement, pour une période allant jusqu'à un an à compter de la date d'effet de l'autorisation, le ciblage de personnes qui se trouvent en dehors du territoire des Etats-Unis afin d'obtenir des informations de renseignement étranger* ».

La deuxième partie de cet article démontre que ce sont bien les citoyens non américains qui sont concernés par cette norme : « *(b) limitations : Une acquisition [de données] autorisée en vertu du paragraphe (a)*

(1) Ne peut cibler intentionnellement toute personne se trouvant aux Etats-Unis au moment de l'acquisition

(2) Ne peut cibler intentionnellement une personne qui se trouve hors des Etats-Unis si le but d'une telle acquisition est de cibler un particulier qui réside aux Etats-Unis

(3) Ne peut pas cibler intentionnellement un citoyen américain que l'on croit raisonnablement résident en dehors des Etats-Unis

(4) Ne peut obtenir intentionnellement une communication lorsque l'expéditeur et tous les destinataires sont connus comme étant situés aux Etats Unis au moment de l'acquisition et

(5) *Il faut que celle-ci soit menée d'une manière compatible avec le quatrième amendement de la Constitution des Etats-Unis* ».

Il n'est donc pas étonnant que l'un des domaines les plus concernés soit le *cloud*

computing, les entreprises et administrations occidentales actuelles en étant désormais presque toutes utilisatrices.

Le *cloud computing* particulièrement concerné

D'après l'ENISA (*European Union Agency for Network and information Security*), « *le cloud computing est un modèle de service à la demande pour la ressource informatique, souvent basé sur la virtualisation et une distribution des technologies informatiques. L'architecture du cloud computing se compose :*

- *de ressources hautement abstraites ;*
- *d'une scalabilité et d'une flexibilité quasi instantanée ;*
- *d'un approvisionnement quasi instantané ;*
- *de ressources partagées (de matériel, base de données, mémoire…) ;*
- *de « service à la demande », avec habituellement un système de facturation du type « pay as you go » ;*
- *d'une gestion de programme.*[10] ».

JORF n°0129 du 6 juin 2010 page 10453 texte n°42 :

En France, on parle aussi de « l'informatique en nuage » dont une simple définition officielle a été publiée au Journal Officiel[1]. Il s'agit donc d'un « *mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* ».

La question posée par le *PATRIOT Act* est donc l'accès aux données des différents utilisateurs, notamment celles des Européens. En ce qui concerne notre sujet, il est intéressant de consulter les règles de confidentialité de Google pour les utilisateurs de Gmail.

La société Google fait ainsi savoir qu'elle peut être amenée à partager les données pour des besoins juridiques : « *Nous ne partagerons des données personnelles avec des entreprises, des organisations ou des personnes tierces que si nous pensons en toute bonne foi que l'accès, l'utilisation, la protection ou la divulgation de ces données est raisonnablement justifiée pour :*

- *se conformer à des obligations légales, réglementaires, judiciaires ou administratives ;*
- *faire appliquer les conditions d'utilisation en vigueur, y compris pour constater d'éventuels manquements à celles-ci ;*

[10] ENISA, Cloud Computing, Benefit, risks and recommendations for information security, December 2012

- *déceler, éviter ou traiter des activités frauduleuses, les atteintes à la sécurité ou tout problème d'ordre technique* ».

Cette même conformité à la loi est mentionnée chez Microsoft et il est alors possible de rappeler les propos du directeur de Microsoft UK en 2011. Celui-ci a avait en effet fait savoir qu'aucune donnée n'était tenue à l'écart du *PATRIOT Act* et que celles-ci pouvaient être transmises aux services de renseignements américains[11]. Quelques mois après, ce fut au tour de Google d'admettre la transmission de données du *cloud* européen aux autorités américaines[12].

Comment les Américains parviennent-ils à obtenir ces données via les services de *cloud computing* ? L'application du critère du « *minimum contact* » est l'une des réponses à cette question.

La question du « *minimum contact* »

Comme cela a déjà été précisé, le droit américain prévoit une compétence large en ce qui concerne les personnes susceptibles de faire l'objet d'une demande de communication de données. Cela peut être constaté à travers l'interprétation large par les tribunaux américains du critère du « *minimum contact* » (lien suffisant) entre la personne visée et le territoire des Etats-Unis. Dans tous les autres cas, le critère du « *minimum contact* » sera notamment invoqué lorsqu'une personne exerce un contrôle sur les données recherchées. On parle alors du "***Possession, custody or control***". Cette notion de contrôle implique d'analyser le degré de contrôle relatif à la structure d'une personne ou d'un groupe et sa capacité à accéder matériellement aux données visées par les recherches.

Diverses situations peuvent donc être appréhendées en ce qui concerne le transfert de données dans le cadre du c*loud computing*. Ainsi, les juridictions américaines pourront demander la communication de données dès lors, par exemple, qu'un prestataire européen sous-traite le traitement des données à un prestataire américain (la société américaine aurait en effet le contrôle sur les données). Lorsque le sous-traitant est européen et a une filiale américaine, celle-ci pourrait transmettre les données qu'elle a en sa possession. De

[11] ZDNet.com, Microsoft admits Patriot Act can access EU-based cloud Data, 28 juin 2011 http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225

[12] ZDNet.com, Google Admits Patriot Act requests, Handed over European data to U.S. authorities, août 2011 http://www.zdnet.com/blog/igeneration/google-admits-patriot-act-requests-handed-over-european-data-to-u-s-authorities/12191

même, si le prestataire européen est une filiale d'une société américaine, le lien sera immédiatement retenu.

A ce sujet, la Cour fédérale de l'Etat de New-York a rendu le 25 avril 2014, un arrêt relatif à une demande d'annulation partielle d'un mandat de recherche et de saisie formulée par Microsoft. Celui-ci l'obligeait à communiquer le contenu des messages électroniques de l'un de ses clients. La particularité de cette affaire résidait dans le fait que les messages en question étaient stockés sur des serveurs situés en Irlande. La demande a été rejetée par la Cour car le mandat visait Microsoft, société américaine qui contrôle et assure la maintenance des comptes de messagerie visés.

Une affaire similaire concernant Microsoft est d'ailleurs en cours[13]. Cependant, la société américaine s'est montrée réticente à la transmission des données stockées également sur un serveur en Irlande. Microsoft a fait appel et cette affaire est suivie de près par ses concurrents et par les Européens[14]. Le gouvernement allemand aurait ainsi fait savoir à Microsoft qu'il n'aurait plus recours aux sociétés américaines de stockage de données si la décision du juge était confirmée[15].

Dès lors, le stockage à l'étranger de données concernant des citoyens américains ou européens ne fait aucunement obstacle à la communication des données par les prestataires de services de *cloud computing*.

L'application de ce critère est tellement large qu'il n'existe qu'un seul cas où la communication des données aux autorités américaines pourrait être refusée. Il faudrait alors être en présence d'un utilisateur européen du *cloud*, que celui-ci contracte avec un prestataire européen et que ce dernier stocke les données sur le territoire de l'Union Européenne. Il semblerait donc que les juridictions américaines ne pourraient avoir accès aux données, sauf application de l'accord relatif à l'entraide judiciaire conclu entre l'Union européenne et les Etats-Unis d'Amérique, signé le 25 juin 2003.

Les utilisateurs du Cloud peuvent donc facilement faire l'objet d'un *FISA Order* ou d'une NSL et ce, d'autant plus que les grands prestataires sur le marché du *cloud computing* sont américains (Microsoft, IBM ou encore Google). Les données d'une entreprise française ou d'une administration britannique contenues dans le *cloud* peuvent donc tomber sous la compétence des juridictions américaines.

D'une certaine manière, les utilisateurs du *cloud computing* sont dépossédés du

[13] http://blogs.wsj.com/law/2014/08/29/judge-lifts-freeze-on-microsoft-search-warrant

[14] http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant

[15] http://www.forbes.com/sites/emmawoollacott/2014/09/02/microsoft-defies-judge-refuses-to-hand-over-customer-emails

contrôle sur leurs propres données, notamment celles considérées comme des données à caractère personnel. Il n'est donc pas étonnant que le *PATRIOT Act* ait fait l'objet de nombreuses critiques.

IV – Un acte souvent critiqué

Les diverses révélations sur les transferts de données vers les Etats-Unis n'ont pas manqué d'alerter les Européens. Cependant, ces derniers ont mis beaucoup de temps à réagir. Certes, une directive pour la protection des données existe depuis 1995[16] mais celle-ci étant plus ancienne que le *PATRIOT Act*, comment peut-elle protéger efficacement les citoyens Européens ?

L'accès aux données à caractère personnel des Européens reste encore aisé pour les autorités américaines et ce, malgré le fait que les instances européennes aient pris conscience des enjeux liés au *PATRIOT Act*.

Le 6 octobre, la CJUE a toutefois invalidé la décision par laquelle la Commission européenne avait constaté que les États-Unis assurent un niveau de protection suffisant des données à caractère personnel européennes transférées.

La CJUE rappelle en effet que « *l'Union est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux (…). Les décisions de la Commission (…) ne sauraient donc échapper à un tel contrôle.* ».

La Cour reconnaît également que « *le niveau de protection assuré par un pays tiers est susceptible d'évoluer* ». Dès lors, « *il incombe à la Commission (…) de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifiée en fait et en droit.* ». Et la Cour d'ajouter qu'une « *telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard* »[17].

Cependant, il semblerait que seule la mise en place d'un cloud 100% européen puisse empêcher toute collecte de données par les autorités de surveillance des Etats-Unis.

L'Union Européenne a donc tenté de mettre en place des dispositifs afin de protéger ses citoyens. La dernière avancée majeure sur le sujet date d'octobre 2013 avec l'approbation par la Commission des

[16] 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

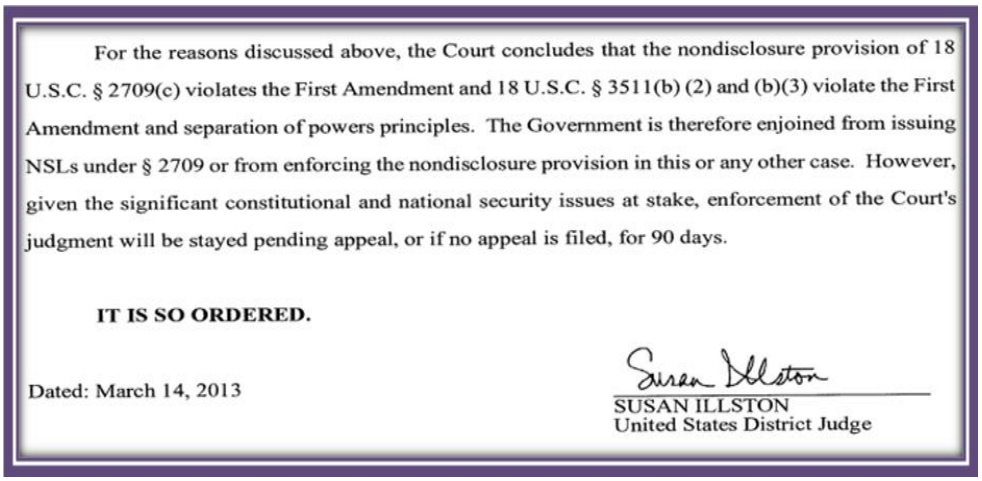
[17] http://www.avocats-mathias.com/donnees-personnelles/invalidation-safe-harbor

libertés civiles, de la justice et des affaires intérieures (LIBE) de deux propositions. La

première consiste en une proposition de règlement sur la protection des données personnelles et la seconde est une proposition de directive en matière de police et de justice (cette dernière concerne tout particulièrement sur le traitement des données biométriques).

D'après la Commission Nationale de l'Informatique et des Libertés[18], la proposition de règlement conduirait à un contrôle des autorités de protection sur les demandes provenant d'autorités de pays tiers pour accéder aux données relatives à des citoyens européens.

Cependant, la question de savoir si le règlement sera suffisant se pose et certains n'hésitent pas à faire savoir que cela s'annonce pour le moins compliqué, notamment car certains points majeurs ne sont pas encore précisés (la question de la compétence des autorités de protection par exemple). Il est donc clair qu'à l'heure actuelle, de nombreuses questions restent en suspens. La pression internationale ne sera sans doute pas suffisante pour conduire les Etats-Unis à une révision du *PATRIOT Act*. Toutefois, des critiques américaines se font de plus en plus importantes.



For the reasons discussed above, the Court concludes that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and 18 U.S.C. § 3511(b) (2) and (b)(3) violate the First Amendment and separation of powers principles. The Government is therefore enjoined from issuing NSLs under § 2709 or from enforcing the nondisclosure provision in this or any other case. However, given the significant constitutional and national security issues at stake, enforcement of the Court's judgment will be stayed pending appeal, or if no appeal is filed, for 90 days.

IT IS SO ORDERED.

Dated: March 14, 2013

SUSAN ILLSTON
United States District Judge

[18] CNIL, *Règlement européen sur la protection des données : une étape décisive franchie par le Parlement européen*, 23/10/2013. http://www.cnil.fr/nc/linstitution/actualite/article/article/reglement-europeen-sur-la-protection-des-donnees-une-etape-decisive-franchie-par-le-parlemen/

Des critiques internes

Aux Etats-Unis également, le *PATRIOT Act* fait toujours débat. L'arrêt Mayfield déjà précité en est un exemple, mais des arrêts rendus récemment par différentes juridictions américaines remettent en cause la constitutionnalité de cet acte législatif.

Ainsi, l'un des arrêts intéressants sur la question a été rendu en mars 2013 et concernait tout particulièrement les NSL. Le Juge du *Northern District of California* a tranché en faveur d'une société de télécommunication en demandant que le FBI cesse d'utiliser les NSL ainsi que les *gag Orders*. D'après le juge, les NSL sont inconstitutionnelles car elles accordent un pouvoir unilatéral au FBI pour « *bâillonner* » les personnes concernées par ces lettres. Dès lors, ce *gag Order* rendrait illégal l'ensemble du processus.

Cependant, l'injonction de la Cour de mettre fin à l'émission de ces NSL est suspendu jusqu'à l'appel[19]. La procédure est encore pendante, la Cour ayant décidé de renvoyer l'affaire du fait de l'adoption du USA freedom Act[20].

Cette affaire n'a pas été la seule aux Etats-Unis à remettre en cause le *PATRIOT Act*. La plupart d'entre elles concernaient le transfert de données mises en ligne mais pas seulement.

Siège de la NSA à Fort Meade (Maryland, USA)

[19] Electronic Frontier Foundation, *EFF Convinces Court to Declare National Security Letters Unconstitutional*, 29/12/2013 https://www.eff.org/deeplinks/2013/12/2013-review-eff-convinces-court-declare-national-secruity-letters-unconstitutional

[20] https://www.eff.org/deeplinks/2015/08/justice-delayed-ninth-circuit-sends-effs-nsl-cases-back-consideration-under-usa

Le tableau suivant permet de mettre en avant les cas principaux relevant l'inconstitutionnalité de l'acte législatif américain.

Amendements	*USA PATRIOT Act*[21]
Ier Amendement : « *Le Congrès ne fera aucune loi ayant pour objet l'établissement ou interdise le libre exercice d'une religion, ni ne restreigne la liberté de la parole ou de la presse, ou le droit qu'a le peuple de s'assembler paisiblement et d'adresser des pétitions au gouvernement pour qu'il mette fin aux abus* ».	**Remise en cause de la liberté d'expression** : la large définition de la notion du terrorisme pourrait aller jusqu'à inclure les groupes qui se livrent à une « *désobéissance civile non violente* ». **Remise en cause du droit d'accès aux informations gouvernementales :** une circulaire du département de la justice des Etats-Unis encourage l'Etat Fédéral, les Etats fédérés et les responsables locaux à limiter l'accès au document officiels malgré *le Freedom of Information Act.*
IVème Amendement : « *Le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration, ni sans que le mandat décrive particulièrement le lieu à perquisitionner et les personnes ou les choses à saisir* ».	**Perquisition :** le gouvernement fédéral a pu permettre des recherches et faire saisir les documents et les effets des citoyens américains sans même une cause probable pouvant aider dans l'enquête contre le terrorisme (Mayfield vs United States of America, 2007).
VIème amendement : *« Dans toute poursuite criminelle, l'accusé aura le droit d'être jugé promptement et publiquement par un jury impartial de l'Etat et du district où le crime aura été commis - le district ayant été préalablement délimité par la loi -, d'être instruit de la nature et de la cause de l'accusation, d'être confronté avec les témoins à charge, d'exiger par des moyens légaux la comparution de témoins à décharge, et d'être assisté d'un conseil pour sa défense* ».	**Droit à un procès rapide et public:** le gouvernement peut incarcérer des Américains sans procès dans le cadre de la lutte contre le terrorisme. **Droit à une représentation juridique :** le gouvernement fédéral peut surveiller les conversations entre les avocats et leurs clients dans les établissements pénitentiaires et nier le droit à un avocat pour les accusés de crimes terroristes. **Droit à la liberté:** les Américains peuvent être incarcérés sans inculpation, sans être en mesure de se confronter aux témoins les dénonçant.

[21] Concerned Citizens Against the Patriot Act, Patriot Act vs Constitution, http://www.scn.org/ccapa/pa-vs-const.html et New York, civil liberties Union, "*Eroding Liberty, rights and freedoms we have needlessly lost in the name of national security*", http://www.nyclu.org/pdfs/eroding_liberty.pdf

Il est certain que le *PATRIOT Act* a fait couler beaucoup d'encre et que le débat le concernant est encore loin d'être achevé, comme le prouvent les nombreuses voix qui continuent à s'élever contre lui, que ce soit aux Etats-Unis et en Europe. Le scandale concernant le programme de surveillance PRISM et les révélations sur la *National Security Agency*, notamment en ce qui concerne les écoutes téléphoniques ont conduit les politiques à repenser ses implications.

Différents groupes aux Etats-Unis ont donc pu appeler à une plus grande protection des données à caractère personnel[22]. Parmi eux, des experts mandatés par le Président Barack Obama qui concluaient, dans un rapport rendu public en décembre 2013 sur les méthodes de surveillance de la NSA, « *(…) certaines des autorités qui ont été créées ou développées dans la foulée du 11-Septembre sacrifient indûment les intérêts fondamentaux de libertés individuelles, de vie privée et de gouvernance démocratique* ». Barack Obama s'était alors dit prêt à engager des réformes.

Pour certains, cette réforme semble avoir eu lieu. Le **USA Freedom Act** a en effet été voté en juin par le Congrès, après avoir été introduit par le Sénateur Leahy (également Président de la commission judiciaire du Sénat).

Le Sénateur a tenté de contourner les atténuations apportées à la version adoptée par la Chambre des Représentants. Il regrette en effet que la chambre des Représentants ait opté en faveur d'une version allégée de l'acte, notamment en faisant en sorte que les formulations pour les collectes de données de la part de la NSA soient vagues et très larges. Le Sénateur a ainsi fait savoir qu'il continuera à « *faire pression en faveur de ces réformes importantes* ». Le Sénateur avait toutefois affirmé : « *si la proposition est adoptée, cela représenterait la plus importante réforme des services de surveillance du gouvernement depuis l'adoption du PATRIOT Act, il y a de cela 13 ans* ».

Cela permet en effet notamment de limiter la collecte massive des données téléphoniques[23]. Cela était vivement critiqué compte tenu des intrusions massives dans la vie privée des Américains mais également du fait du manque de preuve concernant son efficacité.

[22] The Hill, *Privacy Groups calls for « strong and resonant » data law* http://thehill.com/policy/technology/214413-privacy-groups-call-for-strong-and-resonant-data-law

[23] Site du Sénateur Patrick Leahy, *The USA Freedom Act, two pager final* http://www.leahy.senate.gov/download/usa-freedom-act-two-pager-final

V – Vers une protection accrue de la vie privée ?

La recherche d'une véritable transparence était à l'origine de cette nouvelle loi intitulée USA FREEDOM Act. Toutefois, le Sénateur Leahy rappelait que « *des réformes supplémentaires allant au-delà du USA Freedom Act seront nécessaires afin de garantir une véritable protection de la vie privée des Américains* ». Au vu des changements superficiels opérés par le USA FREEDOM Act sur le PATRIOT Act, il semble que des réformes supplémentaires soient en effet nécessaires.

La plupart des dispositions du PATRIOT Act restent en vigueur. Le seul changement notable concerne la collecte de masse des données téléphoniques des citoyens américains.

La NSA devra ainsi mettre fin à la collecte de masse de données téléphoniques et s'adressera désormais aux opérateurs qui lui transmettront uniquement et seulement les données nécessaires à leurs investigations. Etant précisé que la durée de conservation des données par ces opérateurs n'a pas été modifiée et sera toujours de 18 mois maximum.

Même si le USA FREEDOM Act est un premier pas, il semble que cette loi ne mérite pas son nom.

Si vous souhaitez de plus amples informations au sujet du PATRIOT Act ou du droit des technologies avancées, n'hésitez pas à nous contacter à l'adresse suivante : contact@avocats-mathias.com

Vous pouvez également suivre l'actualité juridique des technologies avancées sur Twitter : @GaranceMathias ou en vous inscrivant à notre Newsletter trimestrielle (www.avocats-mathias.com/sabonner-newsletter).