PARLEMENT EUROPÉEN

DIRECTION GÉNÉRALE DES POLITIQUES INTERNES

DÉPARTEMENT THÉMATIQUE C

DROITS DES CITOYENS ET AFFAIRES CONSTITUTIONNELLES

Affaires constitutionnelles

Liberté, sécurité et justice

Égalité des genres

Affaires juridiques et parlementaires

Pétitions

Les programmes de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE

ETUDE

FR DE, EN

2013

EUROPEAN PARLIAMENT

DIRECTION GÉNÉRALE DES POLITIQUES INTERNES

DÉPARTEMENT THÉMATIQUE C:

DROITS DES CITOYENS ET AFFAIRES CONSTITUTIONNELLES

LIBERTÉS CIVILES, JUSTICE ET AFFAIRES INTÉRIEURES

Les programmes de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE

NOTE

Contenu

Dans la foulée des récentes révélations concernant le programme PRISM, cette note analyse les effets des programmes de surveillance des États-Unis sur les droits des citoyens européens. Elle se penche sur la portée de la surveillance que les États-Unis peuvent exercer en vertu de l'amendement de 2008 de la loi FISA, ainsi que sur les pratiques des autorités américaines dans ce contexte, qui ont d'importantes conséquences sur la souveraineté de l'UE sur les données qu'elle produit et sur la protection des droits des citoyens européens.

Ce document a été demandé par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.

AUTEURS

M. Caspar BOWDEN (chercheur indépendant pour la protection de la vie privée)

Introduction par le professeur Didier BIGO
(King's College, Londres, Royaume-Uni /
Directeur du Centre d'études sur les conflits – liberté et sécurité (CCLS), Paris, France).

Révision: Dr Amandine SCHERRER
(Centre d'études sur les conflits, liberté et sécurité – CCLS, Paris, France)

Assistance bibliographique: Wendy Grossman

ADMINISTRATEUR RESPONSABLE

M. Alessandro DAVOLI
Département thématique "Droits des citoyens et affaires constitutionnelles"
Parlement européen
B-1047 Bruxelles
E-mail: alessandro.davoli@europarl.europa.eu

VERSIONS LINGUISTIQUES

Original: EN
Traduction: DE, FR

À PROPOS DE L'ÉDITEUR

Pour contacter le département thématique ou vous abonner à sa lettre d'information mensuelle, veuillez écrire à l'adresse suivante: poldep-citizens@europarl.europa.eu

Manuscrit achevé en septembre 2013.

Ce document est disponible sur Internet à l'adresse suivante:
http://www.europarl.europa.eu/studies

CLAUSE DE NON-RESPONSABILITÉ

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

ACLU	Union américaine pour les libertés civiles (*American Civil Liberties Union*)
AUMF	Autorisation d'utiliser la force militaire (*Authorization to Use Military Force*)
CIA	Agence centrale de renseignements (*Central Intelligence Agency*)
CNIL	Commission nationale de l'informatique et des libertés
DPA	Autorité chargée de la protection des données
CEPD	Contrôleur européen de la protection des données
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
FAA	Loi de 2008 modifiant la loi sur la surveillance à l'étranger
FBI	Bureau fédéral d'enquête (*Federal Bureau of Investigation*)
FIVE EYES	Partage de renseignements entre le Royaume-Uni, les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA
FISA	Loi de 1978 sur la surveillance à l'étranger (*Foreign Intelligence Surveillance Act*)
FISC	Cour de supervision de la surveillance à l'étranger *(Foreign Intelligence Surveillance Court*)
FISCR	Cour de révision des décisions sur la surveillance à l'étranger (*Foreign Intelligence Surveillance Court of Review*)
NSA	Agence nationale de sécurité (*National Security Agency*)
PAA	Loi de 2007 sur la protection des États-Unis (*Protect America Act*)
SHA	Accord UE-États-Unis de 2000 sur la sphère de sécurité (*Safe Harbour Agreement*)

TIA Connaissance complète de l'information (*Total Information Awareness*)

WP29 Groupe de travail "article 29" sur la protection des données

SYNTHÈSE

Cette note vise à fournir à la commission LIBE des informations générales et contextuelles sur les activités PRISM/FISA/NSA et les programmes américains de surveillance, ainsi que sur leurs effets exacts sur les droits fondamentaux des citoyens de l'UE, y compris en ce qui concerne la protection de leurs données personnelles et de leur vie privée.

Avant que n'éclate le scandale PRISM, les médias européens avaient sous-estimé cette réalité, ne semblant pas conscients du fait que les activités de surveillance des Américains sont principalement orientées sur le reste du monde et non sur les citoyens des États-Unis. Cette note affirme que la portée de la surveillance menée par les États-Unis dans le cadre de la FAA (Loi de 2008 modifiant la loi de 1978 sur la surveillance à l'étranger) a des implications considérables sur la souveraineté de l'UE sur ses propres données et sur la protection des droits de ses citoyens.

La première partie présente un **historique des programmes de surveillance américains**, montrant que les autorités américaines ont systématiquement méprisé le droit fondamental au respect de la vie privée des citoyens des autres pays que les États-Unis. L'analyse de plusieurs programmes de surveillance (ECHELON, PRISM) et de la législation nationale des États-Unis (FISA, "Patriot act" et FAA) révèle de manière claire que les activités de surveillance des autorités américaines ne tiennent aucun compte des droits des citoyens et des résidents des autres pays. Par sa portée pratiquement sans limites la FAA crée un pouvoir de surveillance des masses qui vise de manière sélective les données des citoyens des pays tiers vivant en dehors du territoire américain, y compris les données de l'informatique en nuage, qui échappent à la réglementation de l'UE sur la protection des données.

La deuxième partie présente **une vue d'ensemble des principaux vides et des principales lacunes et controverses juridiques de ces programmes, ainsi que leurs diverses conséquences sur les droits des citoyens des États-Unis et de l'UE.** Cette partie présente les dispositions juridiques régissant les programmes de surveillance des États-Unis ainsi que les incertitudes concernant leur application, par exemple:

- les importantes restrictions du 4^{e} amendement de la Constitution des États-Unis pour les citoyens américains

- les pouvoirs spéciaux sur les communications et les données personnelles des citoyens d'autres pays que les États-Unis

- l'absence de tout droit à la vie privée identifiable pour les citoyens des autres pays que les États-Unis dans les termes de la loi FISA

La deuxième partie démontre par ailleurs que le recours à l'informatique en nuage, déjà répandu et en pleine croissance, fragilise la protection des données des citoyens de l'UE, et qu'un examen de certains des mécanismes existants et proposés mis en place pour protéger les droits des citoyens de l'UE après l'exportation de leurs données révèle que ces mécanismes permettent en réalité de contourner cette protection.

Enfin, **certaines possibilités stratégiques pour le Parlement européen** sont présentées, et des recommandations correspondantes sont formulées pour améliorer la réglementation de l'UE et mettre en place des mesures efficaces de protection des droits des citoyens de l'UE.

INTRODUCTION

Contexte

La présente note a pour objet de fournir à la commission LIBE des informations générales et contextuelles sur les activités PRISM/FISA/NSA et les programmes américains de surveillance, ainsi que sur leurs effets sur les droits fondamentaux des citoyens de l'UE, y compris en ce qui concerne la protection des données personnelles et de la vie privée.

Le 5 juin 2013, le *Washington Post* et le *Guardian* ont publié un décret secret adopté au titre de l'article 215 du "Patriot act" obligeant l'opérateur téléphonique Verizon à transmettre régulièrement à la NSA des détails sur toutes les communications téléphoniques passées à l'intérieur comme à l'extérieur des États-Unis. Le 6 juin, ces deux quotidiens ont révélé l'existence d'un programme de la NSA baptisé PRISM permettant à l'agence d'accéder aux données des grandes entreprises américaines travaillant dans le domaine de l'internet. À la fin de la journée, James Clapper (directeur de la NSA) a officiellement reconnu l'existence du programme PRISM et le fait qu'il s'appuie sur des pouvoirs conférés par l'article 702 de la FAA (article 1881a de la FISA). Le 9 juin, Edward Snowden a volontairement révélé son identité, et un entretien filmé dans lequel il s'exprime a été rendu public.

Dans la résolution du Parlement européen du 4 juillet 2013 sur le programme de surveillance de la NSA, les députés ont fait part de sérieuses préoccupations concernant PRISM et les autres programmes de surveillance, ont fermement condamné l'espionnage de représentants officiels de l'UE, et ont invité les autorités américaines à fournir sans délai des informations complètes sur ces allégations. Des demandes d'enquête de la Commission[1], du groupe de travail "article 29"[2] et de plusieurs membres du Parlement européen ont également été envoyées.

Le problème de la surveillance internationale de masse et de la démocratie[3]

Les révélations d'Edward Snowden sur le programme PRISM montrent que la cybersurveillance de masse à l'échelle internationale donne lieu à des violations systématiques des droits fondamentaux. Celles-ci nous conduisent à nous interroger sur les proportions prises par la surveillance internationale de masse et sur les implications de celle-ci pour nos démocraties.

> "*La nature même de notre gouvernement, et l'instinct de notre société ouverte basée sur la Constitution et la Déclarations des droits, interdisent automatiquement la création d'organisations de renseignement du type de celles qui se sont développées dans les États policiers.*" (Allen Dulles, 1963)[4]

[1] Commissaire européenne – Reding, Viviane (2013), lettre au procureur général des États-Unis, Réf. Ares (2013)1935546 - 10/06/2013, Bruxelles, 10 juin 2013
[2] Groupe de travail "article 29", lettre du président à Mme Reding concernant le programme PRISM, 13 août 2013
[3] Préface du professeur Didier Bigo
[4] Dulles, Allen Welsh (1963), *The Craft of Intelligence*, New York: Harper&Row, p. 257.

"*Cela fait des années qu'ont lieu des activités d'espionnage, de surveillance et ainsi de suite; je ne juge pas cet état de fait, c'est la nature de notre société.*"

(Eric Schmidt, président exécutif de Google, 2013)

Cinquante ans séparent ces deux citations. Leurs réponses sont différentes, mais elles concernent la même question centrale: dans quelle mesure les sociétés démocratiques peuvent-elles préserver leur nature si leurs activités de renseignement comprennent une surveillance de masse des populations? Pour Eric Schmidt et la plupart des médias dans le monde, la nature de la société a changé: les technologies de télécommunications, y compris les téléphones mobiles, l'internet, les satellites et de manière plus générale toutes les données susceptibles d'être numérisées et intégrées dans des plates-formes informatiques, ont ouvert la voie à la collecte de quantités de données sans précédent ainsi qu'à leur conservation, leur organisation et leur consultation. Si les technologies existent, elles doivent être utilisées: "il est impossible de nager contre le courant". Dès lors, personne ne devrait être surpris de découvrir que les programmes des services de renseignement peuvent utiliser ces techniques à leur plein potentiel et dans le plus grand secret. L'idée est que si tous les pays disposant de ces capacités techniques les utilisent, alors nous devons en faire autant. Ne pas le faire serait naïf, voire pire: nous risquerions de compromettre la sécurité nationale d'un pays en laissant un autre pays profiter des possibilités résultant de ces technologies.

Sommes-nous toutefois contraints de vivre avec cet espionnage élargi à la surveillance de masse des populations, et de l'accepter comme s'il s'agissait d'une réalité irréversible? Heureusement, les régimes totalitaires ont plus ou moins disparu avant que ces capacités ne soient pleinement opérationnelles. Dans les régimes démocratiques actuels, lorsque ces technologies sont utilisées, des limites leur sont volontairement imposées, et elles sont principalement utilisées pour la collaboration dans la lutte contre le terrorisme, et afin de prévenir les attentats. Le point de vue des services de renseignement à travers le monde est que ces technologies ne mettent pas en danger les libertés civiles: elles représentent au contraire le meilleur moyen de protéger les citoyens contre le terrorisme international. Les services de renseignement repèrent les comportements suspects et l'échange des informations s'opère au niveau international. En principe, seuls les "vrais suspects" font l'objet d'une surveillance. De ce point de vue, loin d'être une source d'embarras, les révélations concernant les programmes comme PRISM pourraient être considérées comme la preuve d'une saine collaboration, qui devra encore être renforcée pour lutter contre les nombreuses formes de violence.

En réponse à ce concert de bonnes intentions mis en musique par les principales autorités des diverses agences de renseignement et de lutte contre le terrorisme nord-américaines, britanniques, françaises, et même par l'UE, il semble urgent et essentiel d'examiner la prétendue "nouvelle nature" de nos sociétés. Les conséquences des transformations technologiques dans les sociétés démocratiques, la manière d'utiliser ces technologies comme ressources à la fois pour l'échange d'informations et pour affronter la concurrence dans le domaine de l'information (cette dernière étant un élément essentiel à l'ère de la mondialisation), les droits des différents gouvernements de traiter ces informations: voilà les questions centrales.

Comme le formulait Allen Dulles un peu plus haut, les justifications des services de renseignement vont dans le sens de l'État policier et sont contradictoires avec la nature même d'une société ouverte évoluant sous l'autorité sereine d'un régime démocratique. Les défenseurs d'une société ouverte pensent que, contrairement à la tendance exposée ici, les technologies ne doivent pas déterminer les actions des hommes, mais bien plutôt être

utilisées de manière raisonnable et sous le contrôle de la loi. L'évolution vers une société totalement contrôlée doit être stoppée. Les dispositions constitutionnelles doivent être appliquées et la présomption d'innocence vaut pour toutes les personnes (pas seulement pour les citoyens d'un certain pays). Si des soupçons existent, ils doivent être clairement liés à certaines formes de criminalité, pas à des comportements ou des modes de vie marginaux. Par conséquent, ce qui est en jeu ici, ce ne sont pas les mécanismes par lesquels les lois et les activités liées à la lutte contre le terrorisme doivent être réglementées au niveau transatlantique, même s'il s'agit d'un sous-chapitre de la question. Ce qui est en cause, ce ne sont même pas les activités d'espionnage auxquelles s'adonnent les divers gouvernements. **Ce qui est en cause, c'est la question de la nature, du niveau et du degré de surveillance qui peuvent être tolérés au sein des démocraties et entre elles.**

Les révélations d'Edward Snowden ont exposé en pleine lumière de nombreuses violations des droits fondamentaux. Celles-ci touchent en premier lieu toutes les personnes dont les données ont été obtenues en interceptant leurs télécommunications, des signaux transmis par câble, ou les données de l'informatique en nuage, dès qu'elles tombent sous le coup de certaines catégories de suspicion ou de certains intérêts liés au renseignement extérieur. Cependant, toutes ces personnes ne bénéficient pas du même degré de protection, surtout si elles ne sont pas citoyennes des États-Unis. **Les citoyens de l'UE sont donc dans une position de fragilité particulière, pris en étau qu'ils sont entre le marteau des services de renseignement américains et l'enclume des grandes compagnies privées qui fournissent ce type de services à l'échelle mondiale et exercent à leur guise leur droit de propriété sur les données échangées.** Il est évident que si les citoyens de l'UE ne bénéficient pas du même niveau de protection que les citoyens des États-Unis à cause des pratiques des services de renseignement américains et du manque de mesures efficaces de protection, ils seront les premières victimes de ces systèmes. La liberté de pensée, d'opinion, d'expression, et la liberté de la presse sont des valeurs cardinales qui doivent être protégées. Tout citoyen de l'UE a le droit d'avoir une vie privée, à savoir une vie qui n'est pas sous la surveillance intégrale d'une quelconque autorité étatique. Il convient de rappeler fermement aux services d'investigation de tous les gouvernements la différence entre les activités publiques et les activités privées, ou entre ce qui constitue un acte illégal et ce qui représente simplement un mode de vie différent. En recueillant d'énormes quantités de données sur les modes de vie des personnes en vue de repérer certaines tendances et de se livrer au profilage politique, ou économique, le programme PRISM semble avoir permis la mise en place d'une collecte de renseignements dont l'échelle et le degré sont sans précédent, qui va bien au-delà de la lutte contre le terrorisme et au-delà des activités d'espionnage des régimes libéraux du passé. Cela pourrait conduire à une forme illégale de connaissance intégrale de l'information, dans le cadre de laquelle les données de millions de personnes seront collectées et traitées par la NSA.

Cette note vise à évaluer cette question du métier du renseignement, et ses limites nécessaires au sein des démocraties et entre elles. Comme nous le verrons, les documents rendus publics par Edward Snowden révèlent que PRISM est un programme d'envergure mondiale qui intercepte les données numériques et viole les droits fondamentaux de vastes groupes de population, et notamment ceux des citoyens de l'UE. Les institutions de l'UE ont donc non seulement le droit mais aussi le devoir d'examiner ce phénomène émergent de cybersurveillance de masse ainsi que la manière dont il affecte les droits fondamentaux des citoyens de l'UE, à l'étranger comme dans leur pays de résidence.

Gouvernance en matière de vie privée: les modèles européen et américain en concurrence

Une analyse approfondie et comparée des lois américaines relatives à la vie privée et du cadre de la protection des données dans l'Union démontre que les premières ne laissent que peu de possibilités réalistes aux individus de vivre leur vie en conservant le contrôle de leurs données personnelles. Cependant, l'un des principaux effets de la loi sur la protection des données est que si des données sont copiées d'un ordinateur vers un autre, pourvu que cette copie soit faite dans le respect de la loi, l'individu concerné ne peut s'opposer à la copie au motif que le risque pour sa vie privée augmente chaque fois que "ses" données vont être transmises[5]. Cela vaut si les données sont copiées sur mille ordinateurs au sein d'une seule organisation, ou si elles sont transmises à mille organisations, ou si elles sont envoyées sous un régime juridique différent dans un pays tiers. L'individu concerné par les données ne peut mettre fin à ce processus une fois qu'il a perdu le contrôle de ses données, tandis que si celles-ci étaient par exemple une "propriété intellectuelle", elles ne pourraient être reproduites que moyennant l'octroi d'une licence. Nous sommes tous les auteurs de notre vie, et il semble de plus en plus aberrant que les entreprises en ligne revendiquent la propriété des données qui enregistrent nos pensées et nos actions par le menu, tout en demandant aux personnes ayant produit ces données de sacrifier leur autonomie et de leur faire confiance pour ce qui est de la vie privée.

Le cadre de la protection des données dans l'Union est, en théorie, catégoriquement supérieur à la législation américaine en matière de vie privée; pourtant, en pratique, il est difficile de trouver des services en ligne conçus pour mettre en œuvre de manière pratique et sûre la protection des données prévue par le droit de l'Union.

La gouvernance en matière de vie privée à travers le monde a évolué autour de deux modèles concurrents: l'Europe a rendu inaliénables certains droits individuels et confié des responsabilités aux organismes de protection des données, tandis qu'aux États-Unis les entreprises ont ajouté des clauses de renonciation dans leurs contrats définissant les modalités et les conditions d'utilisation de leurs services[6], ce qui leur a permis d'exploiter les données de manière exhaustive (pratique appelée "notice and choice", ou "notification et choix").

Le scandale du programme PRISM est directement imputable à la domination émergente des services "gratuits" proposés depuis des entrepôts distants remplis de serveurs informatiques et par des entreprises opérant principalement sous juridiction américaine; ces services sont collectivement regroupés sous l'appellation "informatique en nuage". Afin d'expliquer le lien entre PRISM et l'informatique en nuage, il nous faut explorer plus en détail le cadre législatif américain en matière de sécurité nationale.

Portée et structure

Il est frappant de constater que depuis les premiers rapports faisant état d'écoutes illégales ces dix dernières années, et jusqu'à très récemment après les révélations concernant le programme PRISM, les médias européens ont abordé les controverses liées aux activités américaines de surveillance comme s'il s'agissait uniquement de querelles de paroisse sur les libertés civiles aux États-Unis, semblant ignorer que les activités de surveillances sont **dirigées vers le reste du monde**.

[5] Hondius, Frits W (1975), *Emerging data protection in Europe*. North-Holland Pub. Co.
[6] Voir le documentaire "Terms and Conditions May Apply" (2013, États-Unis) réalisé par Cullen Holback.

La présente note vise à documenter cet aspect de la question, souvent ignoré. Elle montrera que la modification en 2008 de la FISA a élargi son champ d'application au-delà de l'interception des communications, pour couvrir toutes les données hébergées par les services d'informatique en nuage. Cet élargissement présente des implications considérables en ce qui concerne le maintien de la souveraineté de l'UE sur ses données et la protection des droits de ses citoyens. Le but de cette note est de proposer un guide expliquant la manière dont la surveillance des communications sur l'internet par le gouvernement américain s'est développée, ainsi que les effets de cette surveillance sur le droit fondamental à la vie privée, en réalisant une analyse intégrée historique, technique et politique du point de vue des citoyens de l'UE[7]. La présente note comprendra donc:

- (I) Un historique des activités de surveillance des États-Unis à l'étranger, et les connaissances sur l'état actuel de ces activités

- (II) Une vue d'ensemble des principales controverses juridiques, tant du point de vue des États-Unis que des effets et des conséquences en ce qui concerne les droits des citoyens de l'UE

- (III) Les options stratégiques pour le Parlement européen et une série de recommandations

[7] De nouvelles informations basées sur les documents rendus publics par Edward Snowden ont été publiées tout au long de la rédaction de la présente note; bien que tout ait été fait pour veiller à l'exactitude de celle-ci, il est possible que des révélations ultérieures changent les interprétations données ici.

1. UN HISTORIQUE DES ACTIVITÉS DE SURVEILLANCE DES ÉTATS-UNIS.

PRINCIPALES CONCLUSIONS

- Un historique des différents programmes de surveillance des États-Unis (précurseurs d'ECHELON, PRISM, etc.) et de la législation des États-Unis en matière de surveillance (FISA et FAA) révèle que **les États-Unis ont systématiquement méprisé les droits fondamentaux des citoyens des pays tiers**.

- En particulier, la portée considérable de la FAA, associée à des définitions volontairement "politiques" de ce qui constitue des "renseignements étrangers", crée **un pouvoir de surveillance de masse ciblant spécialement les données des citoyens des autres pays** résidant en dehors des États-Unis, cette surveillance échappant au contrôle de la réglementation actuelle de l'UE en matière de protection des données et de la réglementation proposée dans ce domaine.

Un historique des programmes de surveillance américains donne le contexte de leur interprétation, laquelle est l'expression la plus récente de l'exceptionnalisme américain qui trouve ses origines dans la Seconde Guerre mondiale. Ces programmes représentent le plus grand défi actuel lancé à la protection des données, dans la mesure o ils intègrent des normes de traitement arbitraires et discriminatoires qui dépendent uniquement de la nationalité des personnes et d'alliances géopolitiques, des normes secrètes et incompatibles avec le droit de l'Union européenne.

1.1. La Seconde Guerre mondiale et les origines des traités UKUSA

C'est dans les années 1970 qu'ont été faites les premières révélations sur l'ampleur du succès des programmes alliés de cryptanalyse. Le monde a alors découvert l'histoire secrète de Bletchley Park (également appelé "Station X"), le quartier général du service de renseignements sur les transmissions de Churchill. L'histoire des partenariats internationaux secrets en matière de renseignement après la guerre est étroitement mêlée à la carrière personnelle d'Alan Turing, grand mathématicien et l'un des pères de l'informatique, qui a apporté une contribution essentielle à la conception de machines automatiques capables de déchiffrer les messages produits par une machine comme Enigma (utilisée pour de nombreuses communications au sein de l'armée allemande).

Alan Turing s'est rendu aux États-Unis en 1942 pour surveiller la production de masse par la marine américaine de machines de déchiffrage (appelées "bombes") pour la guerre dans l'Atlantique, et pour passer en revue le travail dans les laboratoires Bell sur un nouveau téléphone permettant de brouiller la communication entre chefs d'État. Malheureusement, Turing ne possédait aucune lettre d'autorisation et il fut donc considéré comme suspect par les autorités américaines et détenu jusqu'à ce que les représentants du Royaume-Uni à New York viennent le récupérer. Ce qui était censé être une visite de deux semaines dura en fin de compte des mois, parce que les autorités américaines n'avaient jamais auparavant connu de situation qui les aurait amenés à autoriser un étranger, même allié, à accéder aux laboratoires que Turing devait visiter. Plusieurs mois de tensions diplomatiques avec le Royaume-Uni et de querelles intestines entre la marine et l'armée de terre

américaines suivirent, cette dernière "n'ayant pas besoin de connaître" le programme Ultra (nom désignant les renseignements obtenus par déchiffrage à Bletchley Park). Le Royaume-Uni souhaitait que le secret soit partagé par le plus petit nombre de personnes possible, et la cacophonie qui suivit au sein des hiérarchies des services de sécurité de l'armée américaine fut appelée "l'affaire Turing".

Cette affaire est à l'origine du partenariat d'après-guerre dans le domaine du renseignement, conclu tout d'abord entre les États-Unis et le Royaume-Uni et auquel furent ensuite associés le Canada, l'Australie et la Nouvelle-Zélande, puis d'autres pays moins introduits. Ce traité est appelé UKUSA, et les détails de sa création sont connus parce que la NSA américaine a déclassifié le texte intégral des traités UKUSA[8] et la correspondance à leur sujet jusqu'aux années 1950 (le contenu actuel des traités est toujours secret). Le GCHQ[9] britannique n'a quant à lui déclassifié que peu d'informations, même si la déclassification a été présentée comme une décision commune des deux pays.

Le but des traités UKUSA était **de définir des domaines précis de coopération technique et d'éviter les conflits. Cependant, aucune disposition générale d'interdiction d'espionner n'apparaît dans les versions publiées jusqu'en 1950, mais simplement des affirmations de bonne volonté comparables à celles de traités publics.** Nous ignorons s'il existe un accord complet par lequel le Royaume-Uni et les États-Unis s'engagent à ne pas s'espionner mutuellement, et aucun de ces pays n'a fait de commentaire sur la question par voie législative ou exécutive.

1.2. ECHELON: le système de surveillance des communications des traités UKUSA

Dès la création de la NSA (Agence de sécurité nationale) en 1952 et tout au long de la guerre froide, le Royaume-Uni tout comme les États-Unis ont largement renforcé leurs capacités d'interception des communications, recueillant des informations aux points d'atterrissement des câbles sous-marins[10], interceptant les transmissions hertziennes à l'aide de satellites, et installant des réseaux d'antennes dans des bases militaires ou des ambassades. L'évolution et la nature de ces capacités ont été documentées à partir de recherches libres présentées dans deux rapports[11] destinés aux institutions européennes, qui ont abouti en 2000 à une enquête du Parlement européen concernant le programme ECHELON. ECHELON est en réalité le nom de code d'un système de surveillance précis, mais il est devenu dans l'usage courant une synecdoque désignant tout le système de surveillance des communications du traité UKUSA. La dernière réunion de la commission d'enquête du Parlement européen a eu lieu le 10 septembre 2001. La commission d'enquête a recommandé au Parlement européen que les **citoyens des États membres de l'UE chiffrent leurs communications afin de protéger leur vie privée**, car le programme ECHELON avait manifestement été utilisé par les agences américaines de renseignement à des fins d'espionnage économique.

[8] UKUSA Agreement Release 1940-1956 Early Papers Concerning US-UK Agreement – 1940–1944, NSA/CSS

[9] Quartier-général des communications du gouvernement (*Government Communications Head-Quarters*), l'organisation britannique de cryptologie et de renseignement responsable de la surveillance pour la sécurité nationale, héritière de Bletchley Park.

[10] Cette pratique a commencé dès les premiers câbles télégraphiques au 19e siècle, et elle a représenté un aspect important de l'affaire du télégramme Zimmermann, qui a été un des facteurs déterminants de l'entrée en guerre des États-Unis en 1917. Voir Desai, Anuj C. (2007), *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, Stanford Law Review, 60 STAN L. REV. 553 (2007).

[11] *STOA interception Capabilities* (2000) et EuroParl ECHELON (2001) – rapports de Duncan Campbell.

1.3. 1975-1978: le scandale du Watergate et la commission Church

Après que les États-Unis eurent été secoués par le scandale de Watergate, qui conduisit à la démission du président Richard Nixon, le sénateur Frank Church a été à la tête une commission parlementaire d'enquête sur les abus de pouvoir commis par les agences de répression et de renseignement qui avaient mis sur écoute des personnalités politiques et civiles avec l'accord du président et en violation du quatrième amendement de la Constitution américaine, qui protège la vie privée des citoyens en interdisant les perquisitions non motivées par un mandat, ce dernier devant être justifié par une "présomption sérieuse" (c'est-à-dire des éléments indiquant une probabilité d'au moins 50 % qu'un acte illégal a eu lieu).

La commission Church rendit un rapport sur la question de savoir si le quatrième amendement concernait l'interception et la collecte à grande échelle des communications internationales, dont la commission avait découvert qu'elles avaient étaient opérées en secret depuis les années 1940, en l'occurrence sur les télégrammes[12]. L'enquête a déterminé que **la collecte involontaire de données de citoyens américains transmises à travers les frontières était tolérable** si certaines procédures étaient prévues pour "réduire au minimum" l'accès non motivé (et si les erreurs n'étaient pas utilisées au préjudice de citoyens américains).

Cette idée a été codifiée dans la première **loi de 1978 sur la surveillance à l'étranger (Foreign Intelligence Surveillance Act ou FISA)**, qui réglemente l'interception de "renseignements étrangers" dans les communications internationales (et nationales) transmises par les opérateurs de télécommunications. Or, la collecte de données par tout État en dehors de son territoire représente un domaine absolu de non-droit qui n'est encadré par aucun accord international explicite.

1.4. Le contexte après le 11 septembre: l'élargissement des pouvoirs des services de renseignement

Après les attentats terroristes du 11 septembre 2001, la protection de la vie privée et des données a été profondément remise en question par des mesures exceptionnelles prises au nom de la sécurité et de la lutte contre le terrorisme.

Le "Patriot act" de 2001 a été adopté par le congrès des États-Unis le 26 octobre 2001, et son principal effet a été un vaste élargissement des pouvoirs des autorités répressives en ce qui concerne la collecte de renseignements à l'intérieur des États-Unis. La **loi de 2008 modifiant la loi sur la surveillance à l'étranger (Foreign Intelligence Surveillance Amendment Act ou FAA)**[13] a créé un pouvoir de surveillance de masse spécialement conçu pour la captation des données des citoyens des pays tiers vivant en-dehors du territoire des États-Unis. Ces deux lois américaines et leurs implications pour les citoyens de l'UE seront analysées dans la partie suivante (partie 2).

[12] Aucune autorité officielle n'existait pour le programme de collecte SHAMROCK (ni pour le programme d'interception MINARET), mais une bande magnétique contenant une copie de tous les télégrammes était livrée chaque jour à la NSA par un coursier, à la demande du gouvernement. Voir Snider, Britt L. (1999): Unlucky SHAMROCK - Recollections from the Church Committee's Investigation of NSA.

[13] Congrès américain (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, loi publique 110-261, 10 juillet 2008.

De nombreux nouveaux programmes et modalités de surveillance ont par ailleurs été proposés au président George Bush par le directeur de la NSA, le général Michael Hayden, sans autorisation légale explicite, et ils ont pourtant été autorisés. Ces programmes ont rétroactivement été déclarés légaux par des notes secrètes préparées par un juriste ayant relativement peu d'expérience[14], dans le cadre de l'autorisation d'utiliser la force militaire (AUMF) pour la guerre en Afghanistan et pour les opérations liées à la guerre contre le terrorisme.

Un de ces programmes, portant le nom de code *Stellar Wind* ("vent stellaire"), prévoyait l'installation de répartiteurs de fibre optique dans d'importants centre de commutation utilisés pour l'internet, et le tri en temps réel des énormes volumes de données y transitant à l'aide d'un petit ordinateur extrêmement performant (baptisé *deep packet inspection box*) qui renvoyait les données répondant à certains critères vers la NSA. C'est alors qu'on demanda à un responsable technique d'AT&T des bureaux de San Francisco d'aider à la construction d'une installation de ce genre (la "salle 641A"), lequel s'inquiéta, parce que cette activité violait de manière flagrante les protections garanties par la Constitution des États-Unis, le câble concerné transmettant non seulement des données internationales mais aussi des données nationales. Il rapporta donc les faits au *New York Times*, avec tous les éléments de preuve nécessaires, mais le journal ne publia un article[15] qu'un an plus tard, en 2005, après la réélection de George Bush.

D'autres *whistleblowers* ou accusateurs de la NSA, de la CIA et du FBI sortirent alors de l'anonymat, avec des récits de surveillance de masse illégale de téléphones portables, de communications sur l'internet et de satellites, et révélèrent même que les communications téléphoniques de Barack Obama[16] (alors sénateur) et de certains juges de la Cour suprême des États-Unis avaient été interceptées. Le scandale s'exacerba par le fait que deux ans auparavant, un ancien conseiller de la sécurité nationale[17] avait proposé un programme de recherche visant à la connaissance totale de l'information (*Total Information Awareness* ou TIA) et consistant en un système de surveillance de grande envergure de toutes les données numériques et leur traitement à l'aide d'algorithmes sophistiqués d'intelligence artificielle afin de détecter les possibles complots terroristes. La réaction immédiate des médias, très négative, avait poussé le Congrès américain à arrêter immédiatement le financement des recherches sur le système TIA, mais certaines rumeurs avaient persisté selon lesquelles ce programme avait été absorbé par une "caisse noire" consacrée aux activités de renseignement et se poursuivait.

Lorsque les premières allégations d'"écoutes illégales" firent surface dans une série de reportages du *New York Times*, du *Los Angeles Times* et du *Wall Street Journal*, on repensa forcément au programme TIA, prétendument annulé, et le malaise public s'intensifia.

[14] John Yoo, qui a également rédigé un avis secret selon lequel la torture par l'eau (*waterboarding*) n'était pas une forme de torture, et qu'elle pouvait donc être utilisée.
[15] *New York Times*, Bush Lets U.S. Spy on Callers Without Courts, Risen J, Lichtblau E, 16 décembre 2005.
[16] *Huffington Post*, Russ Tice, Bush-Era Whistleblower, Claims NSA Ordered Wiretap Of Barack Obama In 2004, 20 juin 2013.
[17] L'amiral John Poindexter, condamné lors de l'affaire Iran-Contra dans les années 1980 et gracié par le président Reagan.

1.5. Les révélations d'Edward Snowden et le programme PRISM

Le 5 juin 2013, le *Washington Post* et le *Guardian* ont publié un décret secret adopté au titre de l'article 215 du "Patriot act" et obligeant l'opérateur téléphonique Verizon à transmettre régulièrement à la NSA des détails sur toutes les communications téléphoniques à l'intérieur comme à l'extérieur des États-Unis. Le 6 juin, ces deux quotidiens ont révélé l'existence d'un programme de la NSA baptisé PRISM permettant à l'agence d'accéder aux données des grandes entreprises américaines travaillant dans le domaine de l'internet. À la fin de la journée, James Clapper (directeur de la NSA) a officiellement reconnu l'existence du programme PRISM et le fait qu'il s'appuie sur des pouvoirs conférés par l'article 702 de la FAA (article 1881a de la FISA). Le 9 juin, Edward Snowden a volontairement révélé son identité, et un entretien filmé dans lequel il s'exprime a été rendu public.

Les faits ont principalement été rapportés par trois journaux: le *Guardian*, le *Washington Post* et *Der Spiegel*. Quatre journalistes ont joué un rôle central dans l'obtention, l'analyse et l'interprétation des documents dévoilés: Barton Gellman, Laura Poitras, Jacob Appelbaum et Glenn Greenwald. Ces journaux ont ensuite été rejoints par l'édition américaine du *Guardian*, et par le *New York Times*, en collaboration avec l'organisation ProPublica, après que le gouvernement britannique eut exigé que la copie des documents d'Edward Snowden conservée dans les bureaux du *Guardian* à Londres soit effacée sous la supervision du GCHQ[18].

Ce que l'on peut appeler le "scandale PRISM" a révélé l'existence de plusieurs programmes de surveillance, parmi lesquels:

1.5.1 Le Programme “Upstream” (collecte de données en amont)

Les diapositives rendues publiques par Edward Snowden contiennent des références aux programmes de collecte de données dits «upstream» (en amont) de la NSA, obscurcis par divers noms de code. Les données sont copiées depuis des réseaux publics ou privés vers les serveurs de la NSA, à partir des points d'atterrissement des câbles de fibre optique et des centres de commutation des données de l'internet entre les grands fournisseurs d'accès; cette interception de données est basée sur des accords négociés avec les opérateurs de ces réseaux (ou sur la des injonctions judiciaires; ces interceptions ont sans doute également été opérées directement au niveau des câbles sous-marins[19] lorsque c'était nécessaire).

1.5.2 XKeyscore

Le système Xkeyscore a été décrit dans des diapositives[20] (datant de 2008[21]) publiées par le *Guardian* le 31 juillet 2013. Il s'agit d'un "outil d'exploitation/cadre analytique" permettant d'effectuer des recherches sur un "tampon de données défilant de 3 jours" regroupant une "collecte complète" de données stockées dans 700 serveurs de base de

[18] Une analyse complète des révélations dépasserait le cadre du présent rapport, mais le contenu de celui-ci part du principe que les diapositives et documents concernés sont authentiques, aucun élément crédible n'indiquant le contraire.
[19] L'existence de sous-marins américains spécialement équipés pour l'interception des câbles sous-marins a été décrite dans le rapport du Parlement européen publié en 2000 sur le programme ECHELON, cf. "Ivy Bells".
[20] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-programme-full-presentation
[21] Une offre d'emploi avait été publiée en juillet 2013 par un sous-traitant dans le domaine de la défense, indiquant que le programme était toujours actif.

données répartis sur 150 sites. Le système intègre les données[22] provenant des ambassades américaines, des transmissions satellites ou hertziennes (par le système anciennement appelé ECHELON) et les sources "upstream" décrites ci-dessus.

Le système Xkeyscore indexe les adresses courriel, les noms de fichier, les adresses IP et les numéros de port, les mouchards ("cookies"), les noms d'utilisateurs et les listes d'amis utilisés par les systèmes de messagerie électronique ou de discussion en ligne, les numéros de téléphone et les métadonnées liées aux sessions de navigation (y compris les mots saisis dans les moteurs de recherche ainsi que les lieux observés par l'intermédiaire de Google Maps). L'atout de ce système est qu'il permet aux analystes de découvrir des "critères forts" (c'est-à-dire des paramètres de recherche permettant d'identifier une personne cible ou d'extraire des données précises la concernant) et de rechercher les "événements anormaux", par exemple une personne "chiffrant ses communications" ou "recherchant des contenus suspects".

Les analystes peuvent également utiliser le résultat de ces recherches sur l'index pour "simplement extraire des données du site selon les besoins". Ce système de recherche unifiée permet d'effectuer des recherches rétrospectives portant sur les trois derniers jours (en 2008) d'une quantité bien plus considérable de données que ce qu'il est possible de copier en intégralité sur les serveurs de la NSA.

Le système permet également la "collecte de sessions personnelles", c'est-à-dire qu'un "événement anormal" qui pourrait caractériser un particulier ciblé peut déclencher la collecte automatique de données liées à l'événement sans nécessiter l'application d'un "critère fort". Il est également possible de repérer "toutes les machines exploitables dans un pays donné" en recoupant les "empreintes digitales" des configurations apparaissant dans les flux de données interceptés avec la base de données de vulnérabilités logicielles connues de la NSA. Les diapositives indiquent également qu'il est possible de repérer toutes les feuilles de calcul créées avec Excel "dont les adresses MAC proviennent de l'Iraq"[23].

La diapositive n° 17 est particulièrement remarquable dans la mesure où y figurent les premiers indices d'un contournement systématique des systèmes de chiffrage[24] (voir BULLRUN ci-dessous).

1.5.3 BULLRUN

BULLRUN[25] est le nom de code d'un programme de la NSA utilisé pendant la dernière décennie et consistant en un "effort agressif mené sur plusieurs fronts et visant à percer les technologies de chiffrage les plus couramment utilisées", qui a été révélé par un article

[22] http://theweek.com/article/index/247684/whats-xkeyscore

[23] Cette affirmation semble insolite car Microsoft n'intègre plus l'adresse MAC dans le GUID (*Global Unique Identifier* ou identifiant unique, permettant de créer un numéro unique pour l'indexation d'un document) depuis la version 2000 de Microsoft Office, et les adresses MAC ne sont pas liées à un pays précis (à moins que la NSA n'ait obtenu ou compilé une base de données complète spécifique pour l'Iraq, ou qu'elle soit en mesure de surveiller et d'intercepter des signaux Wi-Fi à longue portée et/ou de manière systématique).

[24] "Montrez-moi tous les fournisseurs de RPV dans tel pays, et présentez-moi les données qui me permettront de déchiffrer et de découvrir l'identité de leurs usagers" – un RPV (réseau privé virtuel) est un "tunnel chiffré" entre l'ordinateur d'un utilisateur et un fournisseur de RPV, faisant en sorte que le trafic Internet semble provenir du fournisseur de RPV et non de l'utilisateur lui-même, pour des raisons de sécurité et de protection de la vie privée.

[25] Le nom de code correspondant pour le programme de pénétration cryptographique jumeau utilisé par le GCHQ est EDGEHILL, mais celui-ci dépasse le cadre du présent rapport; curieusement, ces deux programmes ont été nommés d'après des batailles ayant eu lieu lors de guerres civiles aux États-Unis et au Royaume-Uni respectivement.

publié conjointement le 1er septembre 2013 par le *Guardian*[26] et le *New York Times*. De toutes les révélations d'Edward Snowden publiées jusqu'à présent, c'est le programme BULLRUN qui a suscité les plus vives réactions au sein de la communauté des experts de la sécurité en ligne, et des efforts acharnés sont mis en œuvre à travers le monde pour déterminer quels systèmes pourraient être vulnérables et pour mettre à jour ou en changer les clefs, les codes cryptographiques et les systèmes utilisés, notamment parce que les espions des pays hostiles tenteront à présent de découvrir les mécanismes de contournement qui n'étaient auparavant connus que de la NSA.

Ce programme dispose d'un budget de 250 millions d'USD par an, et il peut mettre en œuvre les méthodes suivantes: collaboration avec les fournisseurs de produits et de logiciels de sécurité informatique, cryptanalyse mathématique et attaques par canal auxiliaire, falsification de certificats de clés publiques, infiltration et manipulation d'organismes techniques afin de leur faire adopter des normes non sûres, et utilisation coercitive probable d'injonctions judiciaires obligeant les créateurs de solutions de chiffrage à introduire des portes dérobées (*backdoors*). Il est également important de souligner que rien n'indique (pour l'instant) que les algorithmes de chiffrage couramment utilisés ont été percés par un moyen mathématique, mais les doutes se sont multipliés au cours des dernières années concernant les vulnérabilités des "protocoles" complexes utilisés pour assurer la compatibilité entre les logiciels couramment utilisés.

L'article 702 de la FISA peut exiger d'un prestataire de services qu'il "fournisse immédiatement aux autorités toutes les informations, l'accès ou l'assistance nécessaires pour faire l'acquisition" de renseignements étrangers, et il pourrait donc à première vue obliger ces acteurs à dévoiler leurs clefs de chiffrage, y compris les clés SSL utilisées pour sécuriser les données en transit dans les grands moteurs de recherche, réseaux sociaux, portails de messagerie, et services d'informatique en nuage de manière générale. Nous ignorons à l'heure actuelle si ce pouvoir conféré par la FISA a été utilisé en ce sens.

[26] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

2. LES PROGRAMMES DE LA NSA ET LA LÉGISLATION CORRESPONDANTE: CONTROVERSES, LACUNES ET FAILLES, ET IMPLICATIONS POUR LES CITOYENS DE L'UE.

PRINCIPALES CONCLUSIONS

- La complexité et les interactions des diverses normes législatives des États-Unis relatives aux "renseignements étrangers", ainsi que leur interprétation par des tribunaux secrets et des notes rédigées par le pouvoir exécutif, ont conduit à des pratiques illégales **affectant à la fois les citoyens des États-Unis et ceux des autres pays**.

- Cette insécurité juridique, associée au fait que le quatrième amendement de la Constitution des États-Unis ne protège pas les citoyens des autres pays, signifie que les autorités américaines ne reconnaissent **aucun droit au respect de la vie privée des citoyens des autres pays** dans le cadre de la FISA.

- L'utilisation de plus en plus courante de **l'informatique en nuage fragilise encore plus la protection des données des citoyens de l'UE**.

- Un examen des mécanismes qui ont été mis en place par l'UE dans le domaine de l'exportation des données afin de protéger les droits des citoyens de l'UE démontre que ces mécanismes sont utilisés en réalité comme autant **d'échappatoires**.

Dans l'analyse des programmes de surveillance des États-Unis dont l'existence est connue et de la législation s'y rapportant, du point de vue de la protection des droits fondamentaux, les "zones grises" juridiques appartiennent à deux catégories qui interagissent en permanence[27]:

- un manque de sécurité juridique, qui se traduit par des violations du droit à la vie privée et d'autres irrégularités et abus potentiels commis aux États-Unis, par l'intermédiaire d'effets clairement involontaires sur les citoyens et les résidents légaux des États-Unis;

- les objectifs de la FISA et du "Patriot act", lois visant à recueillir des "renseignements étrangers" concernant des personnes qui ne sont ni citoyens des États-Unis ni résidents légaux.

[27] Forgang, Jonathan D., (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, volume 78, numéro 1, article 6, 2009.

2.1. Vides et insécurité juridiques dans le droit des États-Unis en matière de protection de la vie privée: implications pour les citoyens et les résidents des États-Unis

2.1.1 La doctrine de la "tierce partie" et les limitations au quatrième amendement

Dans deux affaires jugées aux États-Unis en 1976 et en 1979, une jurisprudence est apparue en vertu de laquelle, dans le cas de données confiées à une "tierce partie" ou nécessaires à l'utilisation d'un service fourni par celle-ci, par exemple une banque ou une compagnie téléphonique, les utilisateurs ne pouvaient raisonnablement s'attendre à ce que leur vie privée soit protégée; par conséquent, aucune garantie n'est assurée au titre du quatrième amendement de la Constitution des États-Unis, qui protège les citoyens contre les perquisitions non motivées par un mandat justifié par une "présomption sérieuse" (c'est-à-dire des éléments indiquant une probabilité d'au moins 50 % qu'un acte illégal a été commis). Dès lors, les données commerciales telles que les transactions par carte de crédit, les relevés bancaires et les factures téléphoniques détaillées peuvent être obtenues par les autorités répressives au terme de procédures administratives autorisées par l'agence concernée plutôt que par un juge indépendant, sans justifier d'aucune "présomption sérieuse".

Cette doctrine a fait l'objet de critiques répétées tandis que se développaient les moyens de communication mobiles enregistrant les déplacements des individus, les services internet enregistrant les sites visités et l'activité sur les moteurs de recherche, et les réseaux sociaux dans lesquels la structure et la dynamique de l'interaction sociale révèlent à elles seules des détails intimes[28] de la vie privée des utilisateurs[29]. Bien entendu, cette évolution ne pouvait être prévue par les tribunaux dans les années 1970; pourtant, toutes les tentatives de faire annuler cette jurisprudence ont jusqu'à présent échoué.

Les préoccupations concernant le respect de la vie privée ont été renforcées par l'article 215 du "Patriot act", qui a suscité une controverse importante. Cet article permet en effet d'obtenir des entreprises de l'internet des données commerciales "tangibles" sur la base d'injonctions judiciaires secrètes. S'il est vrai que les injonctions secrètes non judiciaires étaient déjà disponibles pour obtenir des données "sans contenu" (c'est-à-dire des métadonnées) dans le cadre d'une procédure appelée "lettre de sécurité nationale", l'article 215 du "Patriot act" peut s'appliquer à tous types de données "tangibles" détenues par un grand nombre d'entreprises du secteur privé.

Après les premières révélations sur le programme PRISM, le général Keith Alexander (directeur de la NSA) a confirmé dans deux audiences publiques devant les commissions parlementaires américaines de contrôle que la NSA collecte (à la fois aux États-Unis et en dehors de leurs frontières) des métadonnées sur les communications téléphoniques de tous les principaux opérateurs et qu'elle maintient une base de données contenant ces métadonnées pendant cinq ans[30]. De l'aveu de la NSA elle-même, ces données ne sont

[28] Agarwal, A., Rambow, O. & Bhardwaj, N. (2009) *Predicting Interests of People on Online Social Networks*, CSE 2009: conférence internationale sur la science et l'ingénierie informatique.

[29] Mislove, A., Viswanath, B., Gummadi, K.P. & Druschel, P. *You are who you know: inferring user profiles in online social networks*, actes de la troisième conférence de l'ACM sur les recherches en ligne et l'extraction de données, 2010, p. 251-260.

[30] Le *New York Times* a révélé le 1er septembre 2013, sur la base d'informations provenant d'une autre source qu'Edward Snowden, que l'entreprise AT&T conserve une trace de toutes les communications interurbaines et internationales depuis 1987, et qu'elle transmet ces listes à l'agence américaine de lutte contre le trafic de stupéfiants à des fins d'enquête dans le cadre d'un programme secret baptisé "HEMISPHERE". La conservation de

utilisées que pour déterminer s'il existe une "suspicion raisonnable claire" d'un lien avec une enquête en matière de lutte antiterroriste. Une recherche est effectuée sur la base de certaines données lorsqu'un numéro de téléphone ciblé est à trois "sauts" ou moins (c'est-à-dire lorsqu'il existe une "chaîne" de trois appels ou moins sur une période de cinq ans) d'une connexion associée à des activités terroristes.

2.1.2 CDR et "test de pertinence"

À l'heure actuelle, la controverse législative majeure aux États-Unis résultant des révélations d'Edward Snowden ne concerne pas le programme PRISM, mais la collecte généralisée de toutes les métadonnées de communications téléphoniques (enregistrements détaillés des appels ou CDR, pour *call detail records*), qui semble dépasser le cadre fixé par le "Patriot act". Les données ne peuvent être recueillies conformément à l'article 215 du "Patriot act" que si elles sont "pertinentes" pour une enquête autorisée. Le "Patriot act" a été modifié en 2006 pour inclure ce critère de pertinence en vue de limiter la collecte de données[31], mais il semble au contraire avoir été interprété comme justifiant la collecte généralisée de données.

Le raisonnement qui sous-tend cette collecte de données est donc douteux: comment justifier la constitution même de la base de données en s'appuyant sur le seul fait que le numéro de téléphone d'un suspect est relié par trois numéros intermédiaires à celui d'une personne soupçonnée de terrorisme? Comme l'explique un avocat, "ils se livraient à des enquêtes non fondées sur des soupçons afin d'obtenir les soupçons dont le tribunal FISA avait besoin pour ordonner des enquêtes"[32].

Les problèmes posés par la FISA ont été laissés à l'appréciation (au cours de procédures secrètes) de la cour de supervision du renseignement à l'étranger (*Foreign Intelligence Surveillance Court* ou FISC, et de la cour de révision des décisions sur le renseignement à l'étranger, FISCR) dont les juges sont désignés exclusivement par le juge en chef de la cour suprême des États-Unis. Il semble que les tribunaux FISA acceptent l'argument du gouvernement selon lequel il est courant, dans le cadre d'enquêtes, que des quantités illimitées de données soient considérées comme "pertinences" afin de découvrir des preuves réelles. Certains des avis des cours secrètes FISC et FISCR sont en cours de déclassification officielle, mais ils n'ont pas encore expliqué cette anomalie logique.

2.1.3. "Accès direct" aux centres de données accordé à des fins de surveillance?

Les entreprises désignées dans les diapositives liées au programme PRISM ont rapidement nié avoir donné aux autorités un "accès direct" à leurs centres de données, cet accès étant pourtant mentionné dans les diapositives révélant l'existence du programme PRISM. Leur position est qu'elles ont simplement respecté une injonction judiciaire et qu'elles n'avaient jamais entendu parler du programme PRISM (ce qui n'est pas surprenant puisqu'il s'agit

ce genre de données dans l'UE au-delà de la durée maximale de deux ans prévue par la directive de 2006 sur la conservation des données, serait illégale au titre de la directive de 2002 relative à la vie privée et aux communications électroniques (et de la directive "RNIS" adoptée précédemment, en 1998), celle-ci prévoyant que les données doivent être effacées ou rendues anonymes à l'expiration de toute utilité commerciale légitime.

[31] Selon le député américain Jim Sensenbrenner, *Patriot Act Architect Criticizes NSA's Data Collection,* NPR 20 août 2013.

[32] https://www.eff.org/deeplinks/2013/09/government-releases-nsa-surveillance-docs-and-previously-secret-fisa-court

d'un nom de code interne de la NSA désignant un programme très secret). Microsoft a affirmé n'avoir suivi les injonctions que lorsqu'elles mentionnaient des identifiants précis, et Google et Facebook ont nié posséder des "boîtes noires" dans leurs réseaux donnant l'"accès direct" aux autorités. Les entreprises sont soumises aux dispositions de l'article 702 sur la confidentialité et s'exposent en cas de violation à une inculpation pour outrage ou tribunal, voire pour espionnage[33]. Google et Microsoft ont entamé une procédure judiciaire contre le gouvernement afin d'être autorisés à publier les données sur le nombre des personnes concernées par les injonctions au titre de la FISA.

Cependant, il n'existe aucune contradiction importante entre les démentis soigneusement rédigés (et, semble-t-il, coordonnés[34]) publiés par les entreprises concernées et les rapports sur le programme PRISM. L'expression "accès direct" avait sans doute pour but d'établir une distinction entre cette modalité d'accès et le programme "upstream" (collecte de données en amont, voir plus haut), ce dernier ne signifiant pas nécessairement que les autorités sont capables d'extraire des données sans que le fournisseur de services en ait connaissance. Cependant, un "accès direct" n'est pas interdit par l'article 702 de la FAA, et il est possible que ce type d'accès ait déjà été autorisé par d'autres entreprises, ou qu'il soit à l'avenir autorisé par la FISC.

Un autre développement important a résulté d'un élément finement observé par le *New York Times*[35] le 8 août, qui a remarqué que dans le cadre des procédures de ciblage publiées le 20 juin, les "critères" de tri utilisés pour sélectionner les informations qui peuvent être lues au titre de l'article 702 pouvaient inclure des mots-clés arbitraires. Cela ne devrait pas surprendre, si l'on s'en tient à une simple lecture de l'article, mais la nouvelle a mis en lumière le fait que la vie privée des citoyens américains (et, bien entendu, celles des citoyens des autres pays) pouvait faire l'objet de recherches arbitraires portant sur une grande quantité de données, contrairement aux recherches faites sur des identifiants précis ayant au moins 50 % de chances de correspondre à des citoyens non américains. Un autre reportage a révélé[36] que le tribunal FISA a annulé en 2011 un arrêt précédent, permettant ainsi l'utilisation de critères de recherche arbitraires **même si** ceux-ci comprenaient des critères caractéristiques de citoyens américains.

Il semble donc que les mesures théoriques de sauvegarde, qui ne protégeaient selon la loi que les Américains, aient été fortement fragilisées[37] par les demandes de plus en plus étendues faites par les autorités aux tribunaux.

2.1.4 "Caisses noires" des agences de renseignement: dimension et coût des capacités des États-Unis

Le 31 août 2013, le *Washington Post* a publié des détails concernant le budget secret[38] ("caisse noire") de la communauté américaine du renseignement, qui s'élèverait à 50 milliards d'USD par an, ainsi qu'une ventilation des diverses catégories de dépenses. Selon les rapports, les États-Unis auraient dépensé plus de 500 milliards d'USD pour la

[33] http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

[34] Les formulations utilisées dans les déclarations faites par Google et Facebook présentent de nombreux points communs, ce qui permet de penser qu'elles proviennent d'un texte commun).

[35] http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?pagewanted=1&hp

[36] http://www.washingtonpost.com/politics/federal_government/report-surveillance-court-ruling-allowed-nsa-search-of-domestic-email/2013/09/08/4d9c8bb8-18c0-11e3-80ac-96205cacb45a_story.html

[37] Cloud, Morgan (2005), *A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment*, Ohio State Journal of Criminal Law, Vol. 3:33 2005.

[38] http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

collecte de renseignements secrets depuis les attentats du 11 septembre 2001. Le budget de la NSA est d'environ 10 milliards d'USD par an, mais les analystes ont été surpris de constater que le budget de la CIA avait connu une croissance rapide, atteignant 15 milliards d'USD et dépassant celui de la NSA.

2.2. Situation des citoyens et des résidents des autres pays que les États-Unis ("non-USPER")

Il est frappant de constater que jusqu'à présent, dans l'évolution de l'"Affaire Snowden", les commentaires politiques américains n'ont pour ainsi dire évoqué que les droits des *Américains*. Il ne s'agit pas ici d'une figure de style: aucune réciprocité ne devrait être tenue pour acquise[39] (que ce soit dans le domaine du droit ou du discours populaire) qui élargisse ces droits[40]. Les droits des citoyens des autres pays que les États-Unis n'ont quasiment jamais été évoqués par la législation ou les médias américains[41]. Il est encore plus surprenant d'observer qu'une analyse approfondie des dispositions de l'article 702 de la FISA indique clairement que deux régimes de traitement et de protection des données coexistent: le premier, réservé aux citoyens et aux résidents des États-Unis ("USPER"), et l'autre, qui n'accorde aucune protection, réservé aux personnes qui ne sont ni citoyens ni résidents des États-Unis ("non-USPER").

2.2.1 Les définitions politiques du "renseignement étranger"

La définition du "renseignement étranger" établie par la FISA a été modifiée à plusieurs reprises de manière à inclure des catégories particulières et explicites, par exemple le blanchiment d'argent, le terrorisme ou les armes de destruction massive, mais elle a toujours comporté deux branches dont la portée semble presque illimitée. Si l'on démêle la formulation, cette définition comprend[42]:

> *les informations relatives à une organisation politique basée à l'étranger **ou** à un territoire étranger qui sont **liées** et, dans le cas d'un citoyen ou d'un résident des États-Unis, sont **nécessaires** à la poursuite des activités des États-Unis dans le domaine des affaires étrangères.* [gras et soulignement ajouté]

Cette définition est d'une portée tellement générale que, du point de vue d'un non-USPER, il semble que **toute donnée susceptible d'aider la politique étrangère des États-Unis peut tomber sous le coup de cette définition, qui autorise de manière explicite la surveillance politique d'activités légales et démocratiques**.

---

[39]. Corradino, Elizabeth A., (1989), Fordham Law Review, *The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far?* volume 57, numéro 4, article 4, janvier 1989.
[40]. Cole, David, (2003), Georgetown Law: The Scholarly Commons, *Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?* 25 T. Jefferson L. Rev. 367-388.
[41] Kenneth Roth (directeur de l'organisation Human Rights Watch), le 4 septembre 2013, a appelé le président Barack Obama à "reconnaître le droit à la vie privée des citoyens des pays autres que les États-Unis".
[42] 50 USC §1801(e)2(B) - http://www.law.cornell.edu/uscode/text/50/1801

2.2.2. Pouvoirs spéciaux concernant les communications des non-USPER

Afin de mettre fin au scandale[43] des "écoutes illégales" de citoyens américains, le Congrès des États-Unis a adopté[44] la loi intérimaire sur la protection des États-Unis (PAA) en 2007, qui modifie la FISA de 1978 et crée un nouveau pouvoir d'interception des communications des non-USPER situés à l'extérieur du territoire des États-Unis (soit 95 % du reste du monde). L'enjeu politique qui a fait l'objet des débats les plus vifs portait sur la question de savoir si les entreprises de télécommunications avaient, en coopérant avec les autorités, violé la législation relative à la protection de la vie privée de leurs clients. Si le recours à l'autorisation d'utiliser la force militaire (AUMF) à des fins de surveillance sur des citoyens américains s'était avéré illégitime, la responsabilité des entreprises concernées aurait pu être engagée pour des milliards de dollars de dommages. Les opérateurs de télécommunications et les prestataires de services en ligne ont affirmé qu'elles ne coopéreraient à l'avenir que si leur immunité civile totale était garantie. Il est essentiel de souligner à ce stade que cette controverse portait sur les effets de la législation sur la protection de la vie privée des Américains, et que la surveillance des étrangers situés à l'extérieur du territoire des États-Unis au moyen de l'interception de leurs données acheminées vers **ou transitant par** les États-Unis était tenue pour acquise et constituait une prérogative nationale[45].

2.2.3. Le quatrième amendement de la Constitution des États-Unis ne s'applique pas aux non-USPER qui se trouvent à l'extérieur du territoire américain

Nous pouvons à présent expliquer le rapport entre la controverse sur l'article 215 du "Patriot act" et l'utilisation des pouvoirs conférés par l'article 702 de la FISA dans le cadre du programme PRISM. La base de données contenant 5 années d'informations détaillées sur les communications téléphoniques intérieures et internationales a été utilisée pour établir une justification liée à la lutte contre le terrorisme (selon le principe des "trois sauts"). Une vérification était alors effectuée dans une deuxième base de données, celle-ci contenant une liste de numéros de téléphone dont la NSA estime qu'ils appartiennent à des citoyens américains. Si cette vérification indiquait que le numéro concerné n'était probablement pas celui d'un Américain, l'article 702 de la FISA permettait d'écouter le contenu de l'appel, sans qu'une autre autorisation soit nécessaire. En revanche, si le numéro appartenait probablement à un citoyen américain, l'obtention d'un mandat autorisant l'écoute était nécessaire (au titre d'un autre article de la FISA), et ce mandat devait être justifié de manière bien plus précise et porter sur un cas individuel.

Cependant, une lecture attentive de l'article 215 révèle qu'un autre but des écoutes (en plus de la lutte antiterroriste) peut être "*l'obtention de renseignements étrangers ne concernant pas un citoyen ou un résident des États-Unis*"[46]. Du point de vue des pays tiers, il pourrait s'agir là d'un facteur important qui n'a jusqu'à présent pas été pris en considération dans les analyses de la situation faites aux États-Unis, et il est malaisé de déterminer dans quelle mesure cette disposition interagirait avec l'écheveau déjà complexe de la légalité contestée de cette loi. Cependant, cette disposition **représente un exemple**

[43] Bloom, Stephanie Cooper (2009), *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, Public Interest Law Journal Vol 18:269.
[44] Congressional Research Service (2007), P.L. 110-55, *the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, 23 août 2007.
[45] Congressional Research Service (2007), *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, August 23, 2007* et Congressional Research Service – Liu, Edward C. (2013), *Reauthorization of the FISA Amendments Act*, 7-5700, R42725, 2 janvier 2013.
[46] http://www.law.cornell.edu/uscode/text/50/1861

supplémentaire de discrimination de la législation des États-Unis entre les mesures de protection que la Constitution garantit aux citoyens américains et le traitement réservé aux citoyens des autres pays.

L'ancien directeur de la NSA, le général Michael Hayden, a fait des déclarations remarquables à l'occasion d'entretiens, soulignant que "*le quatrième amendement* [qui interdit les perquisitions et les saisies non motivées, et exige que tout mandat soit délivré dans le cadre d'une procédure judiciaire et motivé par une présomption sérieuse] *n'est pas un traité international*"[47], et que les États-Unis ont l'avantage de jouer sur leur propre terrain et peuvent donc librement intercepter toute communication étrangère passant par le territoire des États-Unis et consulter toute donnée étrangère stockée sur le territoire des États-Unis.

Ces propos ont de quoi déranger si on les compare aux discours et aux déclarations des représentants du département d'État des États-Unis avant 2012 lors de forums tels que la conférence "Octopus" du Conseil de l'Europe sur la cybercriminalité et la conférence internationale des commissaires à la protection des données et de la vie privée. Ces déclarations vantaient les protections offertes par le quatrième amendement de la Constitution américaine[48] et, puisqu'elles avaient pour but de rassurer un public international sur le respect de la vie privée par les États-Unis, elles ne peuvent en rétrospective qu'être considérées comme trompeuses[49]. En 2012, l'auteur de la présente note a demandé publiquement à un représentant américain d'affirmer catégoriquement que le quatrième amendement s'appliquait aux non-USPER (situées en dehors du territoire américain), et aucune réponse n'a été donnée.

2.2.4. Les risques de l'informatique en nuage pour les non-USPER

La loi intérimaire de 2007 sur la protection des États-Unis ("Protect America act" ou PAA), évoquée plus haut, devait expirer peu avant l'élection présidentielle de 2008, et son champ d'application était limité à l'interception de données auprès des opérateurs téléphoniques et des fournisseurs d'accès à l'internet. Barack Obama, alors candidat, a approuvé un accord soutenu par les deux grands partis américains visant à intégrer de manière permanente la PAA et ses mesures d'immunité pour les entreprises de télécommunications au sein de la FAA (loi modifiant la FISA), accord promulgué en juillet 2008.

Lors que la FAA a été introduite, elle contenait trois mots supplémentaires que personne ne semble avoir remarqués[50]. En ajoutant la notion de "services de télétraitement" (terme défini dans la loi de 1986 sur la protection de la vie privée dans les communications électroniques, qui porte sur l'accès des *autorités de répression* aux communications stockées), **cette loi a considérablement élargi son champ d'application, auparavant limité aux communications téléphoniques et sur l'internet, pour inclure l'informatique en nuage**.

---

[47] CBS News, le 30 juin 2013; pour une analyse approfondie, voir YOUNG (2003), op. cit.

[48] Voir Medina, M. Isabel, (2008) Indiana Law Journal, *Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment* volume 83, numéro 4, article 14, janvier 2008.

[49] Dans les remarques de l'ambassadeur des États-Unis auprès de l'UE, William E. Kennard, 3e conférence européenne de Forum Europe sur la protection des données et de la vie privée, 4 décembre 2012, les assurances données concernant le droit pénal ne s'appliquent pas à la FISA, ce qui n'est pas mentionné; voir aussi Département d'État des États-Unis (2012), *Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US*.

[50] Pour une analyse des services de télétraitement dans le cadre de la loi américaine sur la protection de la vie privée dans les communications électroniques, voir Pell, Stephanie K. (2012), *Systematic government access to private-sector data in the United States*, International Data Privacy Law, 2012, Vol. 2, No 4.

L'informatique en nuage peut être définie de manière générale comme le traitement de données effectué sur plusieurs ordinateurs distants par l'intermédiaire du réseau internet. Le secteur de l'internet vante depuis 2007 les atouts de l'informatique en nuage auprès des entreprises, des autorités et des décideurs, à commencer par Google qui a rapidement été suivi par Microsoft et d'autres, cette activité devenant une nouvelle branche du secteur de l'informatique professionnelle.

En 2012, la commission LIBE a commandé au Centre d'études de la politique européenne (CEPS) et au Centre d'études sur les conflits, liberté et securité (CCLS) une note d'information sur la lutte contre la cybercriminalité et la protection de la vie privée dans le nuage, à laquelle l'auteur de la présente note a été invité à contribuer[51]. Certaines parties de la note en question **affirment clairement que l'informatique en nuage et la législation américaine dans ce domaine représentent une menace sans précédent contre la souveraineté des données de l'UE**.

Elle souligne clairement ce qui suit[52]:

- *[Les prestataires de services d'informatique en nuage] ne peuvent se conformer à aucun des principes sur lesquels se fonde l'accord sur la sphère de sécurité. Ce problème n'a jamais été résolu de manière satisfaisante par la Commission avant la conclusion hâtive de l'accord malgré les objections des autorités européennes chargées de la protection des données. Par conséquent, de nombreux prestataires américains de services d'informatique en nuage affirment respecter l'accord sur la sphère de sécurité et prétendent, sans qu'il soit possible de le justifier, que cela permet de transférer des données des États-Unis dans des nuages américains en toute légalité; par ailleurs, depuis 2009, certains de ces acteurs ont même modifié leurs documents d'autocertification pour s'attribuer le statut contradictoire d'acteurs de "traitement au sein de la sphère de sécurité". Dans un avis publié récemment, le groupe de travail "Article 29" sur la protection des données (WP29) a indiqué que cela n'était pas suffisant.*

- *Les prestataires de services d'informatique en nuage sont des entreprises internationales aux prises avec des problèmes de droit public international. Elles choisissent quelle législation suivre en fonction des sanctions auxquelles elles s'exposent, des besoins de la situation et, en pratique, de l'allégeance de la majorité des dirigeants de l'entreprise. Jusqu'à présent, toute l'attention portée à ces conflits s'est concentrée sur le "Patriot act" américain, mais les implications de la loi de 2008 modifiant la loi sur la surveillance à l'étranger (FAA) n'ont pour ainsi dire pas été abordées. L'article 1881a de la FAA crée, pour la première fois, un pouvoir de surveillance de masse visant particulièrement les données des non-USPER situés en dehors du territoire des États-Unis et pouvant s'appliquer à l'informatique en nuage. Bien que tous les concepts concernés aient été définis dans des lois précédentes, leur association constitue une nouveauté (…); le changement le plus significatif a entièrement échappé à tout commentaire ou débat public. La portée de la surveillance a été élargie pour ne plus concerner uniquement l'interception des communications mais aussi la consultation de toute donnée stockée dans un nuage*

[51] Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), *Fighting cyber crime and protecting privacy in the cloud*, étude pour le Parlement européen, PE 462.509.

[52] Des avertissements similaires ont également été formulés par Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012), *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*, IVIR, Institute for Information Law, université d'Amsterdam, novembre 2012 (traduction en anglais). Voir aussi les mises en garde sur l'incompatibilité de la FAA avec la CEDH en 2010: LoConte, Jessica (2010), *FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?*, Pace International Law Review Online Companion 1-1-2010.

public. Ce changement résulte de la seule introduction des "services de télétraitement" dans la définition d'un "prestataire de services de communication électronique".

- *(…) des implications très importantes pour la souveraineté des données de l'UE et la protection des droits de ses citoyens. Les implications concernant les droits fondamentaux de l'UE trouvent leur origine dans la définition donnée au concept de "renseignement étranger", celle-ci comprenant les informations relatives à une organisation politique basée à l'étranger ou à un territoire étranger qui sont liées à la poursuite des activités des États-Unis dans le domaine des affaires étrangères. En d'autres termes, la surveillance des données appartenant à des étrangers stockées dans les nuages «évoluant au-dessus du» territoire américain est légale aux États-Unis. Le problème fondamental est que l'informatique en nuage fait exploser le cadre juridique des transferts internationaux de données, qui est vieux de quarante ans. La principale mesure souhaitée serait la signature d'un traité international complet garantissant la pleine réciprocité des droits, et des exceptions ("dérogations") pourraient être reconnues dans des circonstances particulières, pourvu que soient prévues des mesures de sauvegarde adaptées à la situation. L'informatique en nuage contrevient à la règle d'or selon laquelle "l'exception ne doit pas devenir la règle". Une fois les données transférées dans le nuage, la souveraineté de ces données est abandonnée. En résumé, il est difficile d'éviter de conclure que **l'UE n'apporte pas de réponse adéquate à la perte irrévocable de sa souveraineté sur ses données** et permet aux erreurs commises lors des négociations sur la sphère de sécurité en 2000 de se consolider au lieu de les corriger.*

- *Une attention particulière devrait être consacrée à la législation américaine qui autorise la surveillance des données des non-USPER stockées dans le nuage. Le PE devrait demander que soient menées d'autres enquêtes portant sur la FAA américaine, sur le statut du quatrième amendement vis-à-vis des non-USPER, et sur le "Patriot act" (notamment son article 215).*

- *Le PE devrait envisager une modification du règlement sur la protection des données afin d'obliger l'affichage d'avertissements à destination des personnes concernées par les données (indiquant que les données pourraient faire l'objet d'une surveillance à des fins politiques) avant toute exportation de données de l'UE vers les États-Unis. Aucune personne ne devrait être laissée dans l'ignorance concernant le f des données sensibles la concernant sont exposées à un système de surveillance régi par un pays tiers. Les dérogations existantes concernant le nuage doivent être annulées, en raison du risque systémique de perte de souveraineté sur les données. L'UE devrait ouvrir de nouvelles négociations avec les États-Unis en vue d'une reconnaissance du droit fondamental à la protection de la vie privée garantissant aux citoyens de l'UE les mêmes protections devant les tribunaux américains que celles dont bénéficient les citoyens américains.*

- *L'UE doit mettre en place une politique sectorielle visant à la création d'une capacité autonome d'informatique en nuage. La communication de la DG INFO publiée en octobre 2012 ne répond pas aux enjeux analysés dans la présente note. Un objectif à envisager pourrait être qu'à l'horizon 2020, 50 % des services publics de l'UE soient hébergés sur une infrastructure informatique en nuage entièrement sous la juridiction de l'UE.*

Cette étude a également souligné que depuis l'affaire SWIFT, un groupe de contact de haut niveau de l'UE a conduit en 2011 des négociations avec les autorités américaines sur un

accord-cadre portant sur les transferts de données à des fins de répression. Jusqu'à présent, les États-Unis ont affirmé la main sur le cœur qu'un tel accord ne prévoirait pas l'accès par les autorités américaines aux données de l'UE hébergées par les acteurs privés américains, et qu'il exclurait ainsi de manière spécifique le cas de l'informatique en nuage[53].

2.2.5. Les autorités américaines ne reconnaissent aucun droit à la vie privée aux non-USPER dans le cadre de la FISA

La collecte de "renseignements étrangers" dans le cadre du programme PRISM nécessite que les autorités suivent les procédures de "réduction au minimum"[54] et de "ciblage"[55], qui ont été dévoilées (non censurées) par le *Guardian* le 20 juin 2013. Mises ensemble, ces procédures appuient fortement l'idée que les non-USPER ne bénéficient aux yeux des autorités américaines d'aucun droit à la vie privée dans le cadre du programme PRISM et des autres programmes associés. Les documents dévoilés sont très tautologiques et pleins de jargon bureaucratique, mais une lecture attentive ne révèle absolument aucune reconnaissance des droits des non-USPER. On peut donc supposer que **la pratique opérationnelle des États-Unis n'impose aucune limite à l'exploitation ou à la violation de la vie privée d'un citoyen «non-USPER», pourvu que les critères vagues définissant les *renseignements étrangers* soient respectés**.

Par ailleurs, en mai 2012, dans une lettre envoyée aux commissions parlementaires américaines responsables de la surveillance des activités de renseignement[56], le gouvernement affirmait que:

> *La NSA ayant déjà déterminé que les critères utilisés dans le cadre des procédures de ciblage approuvés par la FISC donneraient des résultats liés à l'étranger, le rôle du FBI en matière de ciblage est différent de celui de la NSA. Il ne peut être demandé au FBI de remettre en question le ciblage effectué par la NSA (…).*

Les versions des procédures de ciblage qui ont été dévoilées sont génériques, mais l'union américaine pour les libertés civiles (ACLU)[57] a obtenu des copies censurées de diapositives sur la formation du personnel du FBI abordant de manière spécifique la FAA dans le cadre de la lutte antiterroriste. La lettre se poursuit:

> *Une fois acquises, toutes les communications sont transmises à la NSA. La NSA peut également demander que les communications répondant à des critères donnés acquises dans le cadre du programme PRISM soient "envoyées en copie" à d'autres acteurs de la communauté du renseignement.* (soulignement ajouté)

Cela signifie que des agences comme la CIA, parmi les seize agences qui constituent la communauté américaine du renseignement, peuvent recevoir leurs propres flux de données en vue d'un stockage et d'une analyse, après application par la NSA d'un filtre

[53] Document officieux sur les négociations menées en 2011 entre l'UE et les États-Unis sur la protection des données

[54] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

[55] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

[56] https://www.aclu.org/files/assets/ltr_to_hpsci_chairman_rogers_and_ranking_member_ruppersberger_scan.pdf (document déclassifié le 21 août 2013)

[57] Demande faite par l'ACLU conformément à la loi sur la liberté de l'information (2010), Introduction to FISA Section 702, (2010), ministère américain de la justice, document déclassifié en décembre 2010.

correspondant à une possibilité de 50 % que ces données concernent des non-USPER. Aucun reportage sur les documents rendus publics par Edward Snowden, ni aucun autre commentaire, n'a mentionné cet "envoi en copie" ni l'utilisation finale des données.

Selon les "procédures de ciblage" de la FAA dévoilées par Edward Snowden (datant de 2009), la NSA utilise une base de données de numéros de téléphone et d'identifiants Internet[58] pour purger les USPER de la liste afin qu'ils ne soient pas visés au titre de l'article 702. Les analystes ne peuvent accéder aux "données de contenu" au titre de l'article 702 que si la personne concernée a plus de 50 % de chances d'être un non-USPER situé à l'extérieur du territoire américain, puisqu'il a été déterminé que le quatrième amendement ne s'appliquait pas dans ce cas. Si ce critère n'est pas respecté, un mandat doit être obtenu suivant une procédure décrite dans une autre partie de la FISA.

Ces procédures démontrent que la "présomption sérieuse", qui exigeait des éléments indiquant une probabilité de 50 % qu'un *acte criminel* a été commis, a été convertie en une probabilité de 50 % que la personne soit de *nationalité américaine*. Cette interprétation peut être observée pour la première fois dans une décision de 2008 de la cour de révision des décisions sur la surveillance à l'étranger (FISCR), dont une version censurée avait été brièvement publiée en 2010 puis retirée du site Web officiel (mais une copie[59] en a été conservée par une ONG œuvrant dans le domaine de la transparence).

Le raisonnement de la FISCR était que **la surveillance, à des fins de renseignement étranger, de sujets dont il est raisonnable de supposer qu'ils se trouvent à l'extérieur des États-Unis, répond aux critères d'une dérogation à l'exigence de mandat fixée par le quatrième amendement sur la base de "besoins spéciaux"[60].** La constitutionnalité de ce jugement est contestée par plusieurs procédures judiciaires entamées par des organisations américaines de défense des libertés civiles, car ce critère de "pile ou face" signifie que de nombreuses interceptions de communications d'USPER sont opérées en infraction aux dispositions de la Constitution américaine.

2.3. Exportation des données: fausses solutions et protections insuffisantes

Pour conclure cette partie, l'auteur souhaite attirer l'attention du Parlement européen sur certaines difficultés liées aux dérogations et/ou aux mesures de protection actuellement proposées pour remédier aux implications pour les citoyens de l'UE présentées plus haut. Cette partie vise à souligner les lacunes et les vides juridiques qui existent dans plusieurs mécanismes mis en place pour l'exportation des données. De l'avis de l'auteur, ces mécanismes ne devraient pas être considérés comme garantissant la protection des droits des citoyens de l'UE.

[58] Il semble s'agir d'une base de données différente, contenant un répertoire plutôt que des métadonnées acquises de manière controversée au titre de l'article 215. Nous ignorons comment et sous l'autorité de qui ce répertoire est compilé (par exemple en surveillant les réseaux de communication), mais il contient de toute évidence plus d'informations que les annuaires téléphoniques commerciaux.
[59] www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf
[60] Anzalda, Matthew A. et Gannon, Jonathan W. (2010), *In re Directives...: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance* (article payant), Texas Law Review, Vol 88:1599 2010.

2.3.1 Sphère de sécurité, règles d'entreprise contraignantes pour les prestataires et informatique en nuage

L'accord conclu par les États-Unis et l'UE en 2000 sur la sphère de sécurité a mis en place un processus permettant aux entreprises américaines de respecter la directive 95/46/CE sur la protection des données personnelles. Si une entreprise américaine déclare adhérer aux principes de la sphère de sécurité, un contrôleur européen peut exporter des données vers cette entreprise (un contrat écrit est toutefois nécessaire).

Parfois décrit comme une "déclaration unilatérale simultanée", l'accord ne précisait pas s'il s'appliquait à la situation dans laquelle des données sont traitées aux États-Unis à la demande de contrôleurs situés sur le territoire de l'UE. Notamment dans le cas de l'informatique en nuage, ces prestataires de services à distance seraient vraisemblablement incapables d'appliquer les principes de la sphère de sécurité, ces derniers devenant donc, selon les autorités américaines, nuls. L'accord était-il toujours valable pour l'exportation sans restrictions de données de l'UE en vue d'un traitement à distance dans le contexte d'un cadre essentiellement auto-réglementé? En 2000, la Commission européenne a rejeté les objections de la société civile et de certaines DPA (autorités chargées de la protection des données) afin de parvenir à un accord.

Les négociateurs américains du ministère du commerce ont travaillé en étroite collaboration avec les lobbies commerciaux américains afin d'élaborer une liste de "questions fréquemment posées" permettant aux entreprises américaines d'interpréter l'accord sur la sphère de sécurité de manière à réduire les droits de l'UE en matière de protection de la vie privée, indiquant comment contourner les règles liées aux données identifiables, refuser les droits d'accès, et se soustraire à tout devoir de finalité ou à toute demande de suppression. La sphère de sécurité s'est avérée tellement complexe que pendant de nombreuses années, aucun citoyen de l'UE n'a suivi toutes les étapes du processus bureaucratique pour déposer une plainte.

L'étude officielle de l'UE[61] relative à la sphère de sécurité qui a été réalisée en 2004 a sous-estimé la FISA et n'a pas donné à l'expression "*renseignement étranger*" l'interprétation politique mentionnée plus haut désignant les non-USPER, et a indiqué que "*les dispositions controversées du 'Patriot act' ne sont dans l'ensemble pas pertinentes en ce qui concerne les flux de données dans le cadre de la sphère de sécurité*".

Une grande partie de l'analyse juridique étayant la théorie selon laquelle les dispositions de l'accord sur la sphère de sécurité s'appliquent à l'informatique en nuage remonte au travail de Christopher Kuner[62], qui a organisé pendant de nombreuses années un lobby regroupant à Bruxelles des responsables de la protection de la vie privée venant principalement d'entreprises multinationales américaines et qui a acquis une influence auprès de la Commission et des DPA. M. Kuner a également représenté la Chambre de commerce internationale lors de discussions avec l'UE sur la protection des données et a été le conseiller de grandes entreprises de l'internet. Le manuel de M. Kuner sur le droit commercial en matière de protection des données a été cité dans le cadre d'une étude commandée par Microsoft[63], qui affirme que l'accord sur la sphère de protection est

[61] Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), *Safe Harbour Decision Implementation Study*, Commission européenne, DG marché intérieur, contrat PRS/2003/A0-7002/E/27.
[62] Kuner, Christopher (2008), *Membership of the US Safe Harbor Program by Data Processors*, The Center For Information Policy Leadership, Hunton & Williams LLP.
[63] Hon, W. Kuan et Millard, Christopher (2012), *Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4*, QMUL Cloud Legal Project: "Il existe une certaine incertitude concernant l'application ou non de l'accord sur la sphère de sécurité aux transferts de données vers un sous-traitant (et non un contrôleur), par exemple un prestataire de services d'informatique en nuage.

suffisant pour couvrir l'informatique en nuage. Les États-Unis ont récemment resservi cet argument de manière explicite[64].

Dans ce contexte, un groupe de travail de l'autorité chargée de la protection des données (la DPA) a entamé les discussions vers 2009 avec les grandes entreprises de l'internet concernant une proposition de nouvelle dérogation qui pourrait inclure l'informatique en nuage. Celle-ci est connue sous le nom de *Binding Corporate Rules for data processors* , "règles d'entreprise contraignantes pour les sous-traitants de données".

L'idée était qu'un prestataire américain de services d'informatique en nuage (ou d'un autre pays tiers) pourrait se voir délivrer une habilitation de sécurité pour une plate-forme logicielle complète par un auditeur réputé, en suite de quoi, moyennant le respect d'une série de procédures organisationnelles élaborées par le WP29[65], un contrôleur de l'UE pourrait alors exporter des données personnelles vers le nuage de ce prestataire en toute légalité. Cette liste imposait (et, dans une mesure limitée, renforçait) des conditions et des formulations similaires à celles qui avaient déjà été élaborées par la Commission pour les clauses "modèles" (voir plus bas).

Sans doute en réponse aux avertissements concernant la FISA, deux mois avant les révélations d'Edward Snowden, le WP29 a publié une "clarification" apparemment mineure, ajoutant[66] que la liste de procédures à suivre

> *"ne fait **que** créer un processus d'information qui ne légitime pas les transferts à lui seul. En cas de conflit de lois, **on** se référera aux traités et aux accords internationaux qui s'appliquent à la question"* [gras ajouté]

Il ne semble pas très avisé de placer la charge de la responsabilité d'une évaluation aussi critique[67] liée à des conflits de droit international sur une entreprise étrangère ayant un intérêt direct dans le résultat de l'évaluation et pouvant être accusée d'espionnage pour avoir respecté le droit de l'UE.

Les règles d'entreprise contraignantes pour les sous-traitants peuvent sembler être une variante des règles d'entreprise contraignantes existantes (pour les contrôleurs), mais elles représentent en réalité un risque bien plus important pour la protection de la vie privée des citoyens de l'UE. Le risque stratégique pour la souveraineté des données de l'UE, qui découle directement de la notion de règle d'entreprise contraignante pour les prestataires, est que le secteur mondial de l'informatique en nuage est dominé par les "plates-formes" logicielles de Microsoft, de Google, d'Amazon et de quelques autres. Depuis 2010, l'objectif commercial de Microsoft dans le secteur public est de répondre à tous les appels d'offres des gouvernements dans le

---

Vraisemblablement, c'est le cas (…)." Voir aussi Walden, Ian (2011), *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, QMUL Cloud Legal Project, document de recherche nº 74/2011, note de bas de page nº 119.

[64] US Department of Commerce International Trade Administration (2013), *Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*.

[65] ART29WP - Groupe de travail "Article 29" sur la protection des données (2012), Document de travail 02/2012 établissant un tableau reprenant les éléments et les principes des règles d'entreprise contraignantes applicables aux sous-traitants, WP 195, adopté le 6 juin 2012).

[66] ART29WP - Groupe de travail "Article 29" sur la protection des données (2013), *Explanatory Document On The Processor Binding Corporate Rules*, WP 204, document adopté le 19 avril 2013.

[67] Pour une analyse de tels conflits, voir: Radsan, John A. (2007), *The Unresolved Equation of Espionage and International Law*, Michigan Journal of International Law, Vol 28:595 2007.

domaine du traitement de données[68]. Les économies induites par le traitement dans le nuage peuvent être extrêmement importantes (le coût peut parfois représenter un dixième de celui du traitement "sur place" par le contrôleur, d'après les arguments de vente des prestataires dans ce secteur). Les économies sont dues aux coûts d'équipement, aux frais généraux et de personnel opérationnel (les coûts d'expertise en matière de cybersécurité sont de plus en plus élevés) moins considérables, et les grands prestataires de services d'informatique en nuage peuvent bénéficier d'économies d'échelle et d'un taux d'utilisation plus élevé en répartissant la charge des calculs sur plusieurs fuseaux horaires. Il existe donc déjà une pression économique, qui ira croissant à l'avenir, pour la migration de données européennes "locales" vers un modèle d'informatique en nuage, et l'UE ne possède à l'heure actuelle aucune plate-forme logicielle importante capable de faire concurrence (en matière de coûts, de fonctionnalité ou de fiabilité) aux grands fournisseurs américains. Les logiciels libres et ouverts sont l'exception à ce tableau sombre, puisqu'ils ont produit des «piles» puissantes d''informatique en nuage, capables de concurrencer les logiciels et les services propriétaires.

À cet égard, les règles d'entreprise contraignantes pour les sous-traitants peuvent être considérées comme une stratégie efficace à la fois pour la Commission et pour les autorités chargées de la protection des données (DPA) souhaitant maintenir l'apparence d'un contrôle juridique sur les données de l'UE, ainsi que pour les prestataires de services d'informatique en nuage qui estiment que le régime existant de l'UE en matière de protection des données est peu attrayant, notamment du point de vue fiscal[69]. La Commission reconnaît le statut juridique de la notion de règles d'entreprise contraignantes pour les sous-traitants dans le texte du nouveau projet de règlement[70]. Les DPA n'auraient dès lors plus d'autre choix que d'accepter la validité de ces règles une fois qu'elles sont établies. Jusqu'à présent, seule une douzaine de règles d'entreprise contraignantes pour les contrôleurs ont été approuvées[71], et la pratique concernant leur respect est peu rassurante[72].

2.3.2. Contrats modèles

Depuis 2001, la Commission européenne a rédigé et approuvé des clauses "modèles" destinées à être introduites dans les contrats des contrôleurs et des sous-traitants situés à l'extérieur de l'UE, en vue de protéger la vie privée des individus de la même manière que si les données restaient à l'intérieur de l'UE.

[68] L'auteur de la présente note a été le conseiller principal en matière de protection de la vie privée des quarante responsables nationaux de la technologie de Microsoft (chargé de la liaison avec les autorités publiques) jusqu'en 2011, et a bénéficié d'une formation spéciale dans le domaine de la vente soulignant l'objectif de la section «nuage» de répondre à tous les appels d'offres des gouvernements, quel que soit le caractère sensible des données. Lorsqu'il a été demandé si cela n'était pas une erreur, cet objectif a été réaffirmé.

[69] Les grandes entreprises de l'internet ont tendance à choisir de s'installer dans les États membres ayant les impôts les plus bas et la réglementation la moins stricte en matière de protection de la vie privée. Si ces deux aspects ne coïncident pas, les départements juridiques des entreprises concernées doivent élaborer des contrats complexes et coûteux permettant de respecter les exigences techniques de contrats "modèles".

[70] Les règles d'entreprise contraignantes ne sont plus considérées comme une "dérogation" (article 44), voir Commission européenne (2012), Proposition de règlement général sur la protection des données, 25/01/2012, COM(2012) 11 final 2012/0011.

[71] L'observation d'une douzaine d'entreprises de la liste a révélé que la plupart d'entre elles ne publient pas les règles d'entreprise contraignantes sur leur site, alors qu'elles sont en principe obligées de le faire.

[72] L'auteur a déposé une plainte à des fins de test auprès de la DPA du Luxembourg concernant le manque absolu de connaissance des règles d'entreprise contraignantes par le personnel d'assistance de PayPal (PayPal ne peut respecter ces règles si son personnel ne connaît ni leur existence ni les obligations qui y sont liées). Malgré plusieurs rappels, après un an aucune nouvelle n'a été donnée sur le résultat de l'enquête.

L'erreur conceptuelle de cette approche générale est qu'elle part du principe que les systèmes informatiques peuvent être "vérifiés" en vue de garantir les trois exigences essentielles de la sécurité des informations: la confidentialité, l'intégrité et la disponibilité. S'il est vrai qu'une vérification de l'intégrité[73] et de la disponibilité des données est techniquement et logiquement possible, ce n'est pas le cas pour la confidentialité. Il est impossible de savoir avec certitude si un acteur interne ou externe, autorisé ou non, a accédé aux données ou les a copiées. Même si les données sont chiffrées à l'aide d'un algorithme puissant, l'implémentation de celui-ci peut présenter des défauts logiciels, ou la clef peut être révélée ou acquise de manière secrète.

Les révélations concernant le programme PRISM illustrent de manière frappante le caractère insensé de ce stratagème juridique. Aucune autorité ne peut, dans un contexte civil impliquant des acteurs privés, garantir le droit au respect de la vie privée lorsqu'un acteur tel que la NSA enfreint ce droit en tentant d'accéder à des données en opérant selon des règles qui lui sont propres et de manière légale à ses yeux.

La clause 5(d)1[74] a prévu que le responsable du traitement des données doit aviser l'exportateur de données de l'UE de toute "demande juridiquement contraignante" de divulguer des données, **à moins** que cela ne soit interdit, **par exemple** en vertu d'une interdiction relevant du droit pénal visant à préserver la confidentialité d'une enquête pénale La formulation "par exemple" semble indiquer que les lois relatives à la sécurité nationale l'emportent à priori sur toute obligation contractuelle. Bien que l'UE conserve le pouvoir de mettre fin aux transferts de données, cela nécessite une justification concrète, ce qui signifie que les règles intègrent dès le départ une tentation structurelle de fermer les yeux.

Tous les acteurs organisationnels ont en effet de bonnes raisons de vouloir ignorer ces dispositions: la Commission, parce que cela lui permet d'affirmer qu'un "niveau élevé" de protection des données est garanti; les DPA, afin de ne pas exposer leurs limitations techniques et de ne pas épuiser leurs ressources limitées en procédures judiciaires coûteuses; les États membres, dont les autorités de sécurité bénéficient d'un accès aux informations liées aux activités américaines de lutte antiterroriste, et les entreprises européennes et américaines qui souhaitent simplement exercer leurs activités sans que ne leur soient sans cesse posées des questions gênantes concernant la surveillance de masse par l'État. Même la société civile de l'UE[75] semble apathique depuis la mise en place du programme ECHELON, se concentrant principalement sur les questions liées aux droits des consommateurs[76] au lieu de poser des questions pertinentes sur l'impact des flux de données commerciales vers les États-Unis sur les droits fondamentaux et la souveraineté de l'UE.

En leur qualité réputée de mécanismes juridiques de protection des droits et d'obtention de réparations en cas de mesures de sécurité insuffisantes ou de mauvaises pratiques en matière de protection de la vie privée, ces contrats (et leurs clauses "modèles") se sont avérés inutiles, dans la mesure où ils n'ont donné lieu à aucune procédure juridique. Dans la plupart des situations où un

[73] Pour vérifier l'intégrité des données, une fonction de hachage leur est appliquée, qui permet de créer une "empreinte digitale" pouvant servir à des fins de comparaison.
[74] Décision de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE (2002/16/CE).
[75] On remarquera l'exception du Chaos Computer Club, en Allemagne.
[76] Certaines exceptions prometteuses existent toutefois, comme la campagne internationale de lutte contre la surveillance de masse, lancée en 2005 et qui n'a pas duré longtemps (le site Web n'existe plus, mais une copie en a été conservée ici) et le niveau généralement élevé de vigilance au sein de la société civile allemande, que l'on peut interpréter comme un désir de ne pas répéter l'histoire.

contrôleur européen souhaiterait obtenir des dommages-intérêts pécuniaires auprès d'un sous-traitant ou d'un contrôleur d'un pays tiers, cette démarche pourrait nuire de manière irréversible à sa réputation (p. ex. en rendant publique une divulgation de données). En théorie, cet effet dissuasif sera éliminé par les dispositions du projet de règlement obligeant[77] les entreprises à informer les DPA des fuites de données, mais les DPA ont indiqué qu'elles n'exigeraient pas nécessairement que les sujets des données soient informés (ce qui rendrait public un tel incident), en partie afin de prémunir les contrôleurs contre les atteintes à leur réputation. Les règlements à l'amiable et sans publicité permettent aux entreprises de se soustraire à la fonction que remplirait un litige contractuel, à savoir informer les contrôleurs de la fiabilité de ceux vers qui ils pourraient exporter des données. Dans le cadre de cette approche, bien entendu, ceux que les données concernent ne savent absolument pas quand leurs droits ont été violés.

[77] L'exigence actuelle d'information en cas de divulgation de données, fixée par la directive révisée relative à la vie privée et aux communications électroniques, ne s'applique qu'aux entreprises de télécommunications et aux fournisseurs d'accès à l'internet, et non aux prestataires de services informatiques proposés sur des sites tels que les réseaux sociaux et les moteurs de recherche, ni aux contrôleurs de données.

3. OPTIONS STRATÉGIQUES ET RECOMMANDATIONS POUR LE PARLEMENT EUROPÉEN

3.1. Réduire l'exposition au risque et mettre en place un secteur européen de l'informatique en nuage

Comme nous l'avons expliqué plus haut, le mécanisme de règles d'entreprise contraignantes pour les sous-traitants, qui est en apparence conçu pour faciliter le flux de données de l'UE vers des nuages hébergés dans des pays tiers, ne suffit pas à la protection des droits. Il présente une lacune qui permet la surveillance illégale. Il est donc plutôt surprenant qu'aux diverses étapes de son développement, ce mécanisme ait bénéficié du soutien du groupe de travail "article 29" sur la protection des données[78] (WP29), du contrôleur européen de la protection des données[79] (CEPD), et de la Commission nationale de l'informatique et des libertés (CNIL), en France, qui a dirigé le travail d'élaboration de ces règles. Depuis, rien n'a permis d'établir que ces DPA ont compris le glissement structurel de souveraineté des données[80] produit par le passage à l'informatique en nuage. Il semble plutôt qu'une vision irréaliste et légaliste ait conduit ces autorités à négliger la protection des citoyens de l'UE.

Recommandations:

- Des avis visibles devraient être affichés sur tout site Web américain proposant des services dans l'UE afin de demander aux utilisateurs l'autorisation de capturer leurs données. Les utilisateurs devraient être informés que leurs données pourront faire l'objet d'une surveillance (au titre de l'article 702 de la FISA) par le gouvernement des États-Unis à toutes fins utiles à la politique étrangère des États-Unis. L'ajout d'une obligation de renseigner les citoyens sensibilisera ces derniers aux questions de vie privée et favorisera le développement de services placés entièrement sous la juridiction de l'UE. Une telle mesure aurait des effets économiques sur les entreprises américaines et ferait pression sur le gouvernement américain pour qu'il parvienne à un accord.

- Les autres mécanismes principaux concernant l'exportation des données (contrats modèles, sphère de sécurité) ne constituant pas une protection contre la FISA ou le "Patriot act", ils devraient être annulés et renégociés. Dans tous les cas, l'obligation de consentement informé décrite ci-dessus, incluant un avis visible affiché sur les sites, devrait concerner toute donnée recueillie, dans le passé ou le futur, par un contrôleur public ou privé au sein de l'UE, avant qu'elle ne puisse être exportée vers les États-Unis à des fins de traitement dans le nuage.

- Une politique sectorielle complète visant au développement d'une capacité

[78] ART29WP - Groupe de travail "article 29" sur la protection des données (2012), Avis sur l'informatique en nuage, WP 196, adopté le 1er juillet 2012

[79] Contrôleur européen de la protection des données - Hustinx, Peter (2010), Protection des données et informatique dématérialisée dans le droit européen, discours, troisième journée européenne de sensibilisation à la cybersécurité, BSA, Parlement européen, 13 avril 2010, groupe de discussion IV: Vie privée et informatique dématérialisée.

[80] De Filippi, Primavera, and McCarthy, Smari (2012), *Cloud Computing: Centralization and Data Sovereignty*, European Journal of Law and Technology 3, 2.

européenne en matière d'informatique en nuage exploitant des logiciels libres et ouverts devrait être soutenue. Une telle politique réduirait la mainmise des États-Unis sur le sommet de la chaîne de valeur des services en lignes utilisant l'informatique en nuage ainsi que sur le marché européen de la publicité en ligne. Les données européennes sont actuellement vulnérables à la manipulation commerciale, à la surveillance par des puissances étrangères, et à l'espionnage industriel. L'investissement dans un secteur européen de l'informatique en nuage présentera donc des avantages économiques, tout en posant les bases d'une souveraineté durable des données.

3.2. Rétablir l'"article 42"

La version publiée[81] du nouveau règlement omet l'"article 42" (selon la numérotation d'un projet de règlement[82] divulgué deux mois avant la version finale), à la suite - semble-t-il - de pressions considérables des lobbyistes représentant les intérêts américains[83]. L'article 42 interdit aux pays tiers (comme les États-Unis et tout autre État non membre de l'UE) d'accéder aux données personnelles des citoyens de l'UE à la demande d'une cour ou d'une autorité administrative extérieure à l'UE sans y avoir été préalablement autorisés par une autorité européenne de protection des données. Cet article a été décrit comme la "clause anti-FISA".

Recommandations: L'effet dissuasif de l'"article 42" devrait être évalué avant que cet article ne soit rétabli, et les questions suivantes devraient en particulier être examinées:

- Bien que l'article 42 atténue en principe les aspects controversés de la FISA, il ne semble pas que la mesure sera efficace, puisque les dirigeants des entreprises américaines pourraient se voir accusés d'espionnage pour avoir suivi cette disposition. Comme l'a indiqué récemment le PDG de Yahoo!: "*nous aurions pu aller en prison si nous avions dévoilé les secrets liés à la surveillance de la NSA*"[84]

- L'efficacité des sanctions pour ce qui est de garantir le respect des dispositions devrait également être évaluée du point de vue des gains et des pertes économiques. À titre d'exemple, l'autorité européenne de contrôle de la concurrence a mené de longues poursuites contre Microsoft pour son monopole sur les réseaux locaux, et le géant américain s'est vu infliger une amende d'un milliard d'USD (la plus importante jamais imposée par l'UE). L'avocat responsable de la stratégie de Microsoft n'a pas été congédié pour incompétence, mais promu au poste de conseiller général adjoint. En effet, grâce à son monopole, Microsoft a réalisé au cours de la décennie précédente au moins vingt fois le montant de l'amende, ce que les experts de l'entreprise avaient prévu.

- Si un grand prestataire de services d'informatique en nuage venait à ne pas respecter l'article 42, cela mènerait à une violation irréversible mais secrète des droits de millions de citoyens, et le règlement devrait prévoir le statut de grave délit pénal pour ce type d'infraction. Mais à l'heure actuelle, la plupart des transpositions par les États membres de la directive 95/46 de l'UE traitent les violations du droit en matière de protection des données comme des infractions mineures, et certains

[81] Commission européenne (2012), Proposition de règlement général sur la protection des données, 25/01/2012, COM(2012) 11 final 2012/0011.
[82] Commission européenne (2011), [Projet de] proposition de règlement sur la protection des données.
[83] Washington pushed EU to dilute data protection, *Financial Times* 12 juin 2013.
[84] *The Guardian* 12 septembre 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance?CMP=twt_gu

États membres n'appliquent même aucune sanction pénale. Cette situation ne dissuadera pas les acteurs prêts à adopter une stratégie calculée visant à ignorer la législation européenne, au vu des sanctions imposées par le droit des États-Unis.

- De manière générale et au-delà du champ d'application particulier de l'article 42, les amendes imposées en cas d'infraction dans le cadre du nouveau règlement sur la protection des données doivent être augmentées de manière importante. Elles ont été réduites à 2 % du revenu d'une entreprise, alors que les versions précédentes divulguées faisaient état d'amendes supérieures. L'exemple mentionné plus haut de l'affaire impliquant Microsoft dans le domaine de la concurrence montre que certaines entreprises disposent de ressources extrêmement importantes et de stratégies pointues grâce auxquelles elles anticipent des amendes de milliards de dollars et les prennent même en considération dans leur modèle économique. Une amende à hauteur de 20 % du revenu mondial de ces entreprises pourrait être nécessaire afin de les convaincre de prendre au sérieux les dispositions de l'article 42.

- Malgré le programme BULLRUN, la cryptographie est probablement encore intacte en théorie[85], mais les experts ignorent quelles implémentations de chiffrage et quels logiciels pourraient avoir été décryptés par la NSA. **Il convient donc de prendre en considération un élargissement du champ d'application de l'"article 42" afin qu'il s'applique également aux distributeurs de systèmes et de produits (en plus des contrôleurs et des sous-traitants) sur les marchés de l'UE.** Les certifications existantes concernant les produits de chiffrage, à fortiori si elles ont été influencées par la NSA ou le GCHQ, doivent par ailleurs être considérées comme suspectes.

3.3. Mesures de protection et d'incitation pour les *whistleblowers / accusateurs*

Recommandation: Le nouveau règlement devrait comporter des mesures systématiques de protection et d'incitation pour les dénonciateurs. Ceux-ci devraient recevoir de solides garanties d'immunité et d'asile, ainsi que 25 % de toute amende résultant de leurs révélations[86]. Le dénonciateur pourrait avoir à vivre le restant de ses jours dans la peur des mesures punitives appliquées par son pays, et devoir prendre des précautions pour éviter l'extradition illégale, c'est-à-dire d'être enlevé. Paradoxalement, la législation américaine prévoit déjà des récompenses de l'ordre de 100 millions d'USD pour les personnes dénonçant la corruption (en matière de marchés publics et d'entente sur les prix)[87].

3.4. Réforme institutionnelle

À une étape très précoce de la consultation, la Commission européenne a rejeté la possibilité de mettre en place une nouvelle autorité centrale paneuropéenne chargée de la

[85] En effet, si la NSA était parvenue à décrypter le chiffrage de certaines données, elle ne dépenserait pas autant de ressources pour le contourner par des moyens indirects (à moins qu'elle ne cherche à brouiller les pistes à grande échelle).
[86] Ce principe est attesté depuis longtemps dans le droit, sous le terme de "qui tam".
[87] http://www.theguardian.com/business/2010/oct/27/glaxosmithkline-whistleblower-wins-61m

protection des données, car cela semblait une mesure disproportionnée dans le contexte du principe de subsidiarité. Elle a donc décidé de faire évoluer le rôle du WP29, qui deviendrait le nouveau conseil de protection des données. Mais une possibilité intermédiaire aurait pu être envisagée: la création d'une nouvelle autorité centrale chargée des affaires liées aux flux de données vers les pays tiers.

Recommandation: Il faudrait créer un service central d'enquête chargé des affaires liées aux flux de données vers des pays tiers. Ce service devrait disposer de l'autorité et des ressources nécessaires pour entamer des procédures complexes à charge des entreprises internationales, qui disposent souvent d'importants départements juridiques qui leur permettent de gagner du temps et de faire appel des décisions pendant de nombreuses années. Les DPA nationales demeureraient compétentes pour les affaires strictement nationales, et conformément au principe de subsidiarité, elles pourraient lancer leurs propres enquêtes nationales ou porter une affaire devant le service central.

3.5. Autorités de protection des données et gouvernance

Le scandale PRISM et les révélations d'Edward Snowden n'étaient pas les premières mises en garde adressées aux institutions de l'UE concernant les droits des citoyens européens. Les associations de défense de la vie privée ont averti la Commission en 2000 que l'accord sur la sphère de sécurité présentait de dangereuses lacunes[88]. Plus récemment, la note mentionnée plus haut concernant l'informatique en nuage et élaborée pour la commission LIBE du Parlement européen soulignait clairement les lacunes de la FISA et les conséquences de celles-ci sur les droits et la protection des citoyens de l'UE[89].

La Commission a même organisé une audience[90] au cours de laquelle cette note a été présentée, à la suite d'une séance sur la stratégie de l'UE en matière de cybersécurité, le 20 février 2013. Les membres du Parlement européen ont ensuite demandé que des propositions soient présentées immédiatement, afin de respecter le délai de dépôt des amendements[91] par la commission LIBE concernant le règlement sur la protection des données. Mais à partir du mois de mars, l'intérêt pour cette note a baissé et il semblait très peu probable que le Parlement apporte son soutien à une révision fondamentale du règlement sur la protection des données. À la suite du scandale PRISM et après les révélations d'Edward Snowden, ces mises en garde et les préoccupations qui y sont liées ont toutefois acquis une nouvelle légitimité. Une question demeure: pourquoi les DPA n'ont-elles pas réagi?

Sur les 150 avis du groupe de travail "article 29" publiés depuis les événements du 11 septembre 2001, seul le premier mentionne le "Patriot act" (dans une note de bas de page) et aucun la FISA, ni même le terme de "renseignement étranger". Les DPA nationales[92], le CEPD[93] et les autres institutions[94] semblaient ignorer la législation

[88] L'auteur de la présente note (alors directeur de la FIPR) et d'autres ont demandé à des représentants de l'UE si cet accord permettait la mise en place de mécanismes de surveillance de masse de type ECHELON, mais nous n'avons reçu aucune réponse.
[89] Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), *Fighting cyber crime and protecting privacy in the cloud*, étude pour le Parlement européen, PE 462.509.
[90] 20/02/2013, audition de la commission LIBE du Parlement européen sur le rapport sur la cybercriminalité et l'informatique en nuage (vidéo, à partir de 17:08:18).
[91] Les amendements LIBE n^{os} 806/2531/2748/2950 du nouveau règlement sont le résultat de ces propositions.
[92] Exception faite des DPA allemandes, qui ont été vigilantes. Voir Weichert, Thilo (2011), *Cloud Computing and Data Privacy*, The Sedona Group Conference Working Group Series, février 2011. Voir aussi International Working

américaine et le fait que le programme PRISM était légalement possible. Aucun de ces acteurs n'a tiré la sonnette d'alarme pour les citoyens de l'UE, malgré des avertissements[95], et malgré le scandale impliquant les États-Unis largement relaté dans les médias, avant 2008. Cela pourrait s'expliquer par le fait que les DPA, l'ENISA[96] et l'unité "confiance et sécurité" de la DG Connect[97] sont toutes ambivalentes sur la question de savoir si la dérogation à la compétence de l'UE pour la "sécurité nationale" signifie ou non qu'elles doivent défendre la vie privée de leurs citoyens contre les agences de renseignement étrangères.

Dans leur dernier état des lieux avant que l'affaire Snowden n'éclate, les CEPD ont pris note de l'amendement de la commission LIBE, mentionné plus haut, portant sur un avertissement visible à l'attention de ceux qui sont concernés par des données avant qu'ils ne donnent leur consentement à leur transfert sur le nuage, mais ils l'ont rejeté[98] au motif qu'il n'était pas "technologiquement neutre".

Il semble que les DPA de l'UE connaissent certaines difficultés structurelles qui doivent être résolues. En particulier, les DPA possèdent manifestement des capacités insuffisantes en matière d'expertise technique. Seules quelques dizaines de membres du personnel des DPA (sur deux mille à travers l'UE) ont un parcours lié à l'informatique, et encore moins un diplôme d'études supérieures dans le domaine de la protection de la vie privée dans l'univers numérique. Il existe une conception profondément ancrée selon laquelle, puisqu'il est préférable de rédiger la loi de manière technologiquement neutre[99], les régulateurs sont dispensés d'avoir à en comprendre les aspects techniques. Par exemple, le WP29 n'a jamais procédé à aucune étude sur les technologies sophistiquées de protection de la vie privée, ni publié d'avis appelant à leur utilisation, même lorsque de nombreux éléments indiquaient que le marché ne les adopte pas volontairement.

Recommandations: Une réforme du système de désignation des autorités européennes chargées de la protection des données devrait être mise en œuvre. Le nouveau règlement n'aborde pas cette question, alors qu'il s'agit d'un élément critique visant à prévenir à la fois l'inertie et le blocage dans le contexte des questions liées à une technologie particulière. Les possibilités visant à améliorer la gouvernance et les capacités de l'UE en matière de protection des données pourraient inclure:

Group on Data Protection in Telecommunications (2012), *Working Paper on Cloud Computing - Privacy and data protection issues - Sopot Memorandum*, 51e réunion, 23 et 24 avril 2012.

[93] Bowden, Caspar (2012), *Is EU data safe in US Clouds?* (diapositives), Académie de droit européen, Trier, septembre 2012. Le CEPD et son adjoint étaient tous deux présents à l'audience, ainsi que des fonctionnaires de haut rang du Conseil, de la Commission et d'autres DPA, qui ont reçu par courriel une copie de la note.

[94] Voir 28.6.12 - Audience des Verts sur la protection des données (diapositives) (vidéo, t=2h43m); voir aussi 10/10/2012, réunion interparlementaire de la commission LIBE

[95] Bowden, Caspar (2011), *Government Databases and Cloud Computing* (diapositives), The Public Voice, Mexique, octobre 2011.

[96] Le 14/06/2013, le service de presse de l'ENISA a répondu à une question que l'auteur de la présente note avait posée au directeur, indiquant que la défense contre les activités de la NSA ne relevait pas de la compétence de l'agence, mais réalisant sans doute que cette position était intenable, il a ensuite publié le 06/09/2013 une déclaration qui nuance cette réponse et qui sous-entend de manière incorrecte (dans la note de bas de page no 21) que l'ENISA avait averti l'UE des risques liés à des activités du type de celles de la FISA en 2009.

[97] Déclaration du représentant de la DG Connect lors de l'atelier sur la sécurité de l'informatique en nuage organisé le 28/05/2013 pour discuter des mises en garde de l'auteur de la présente note juste avant les révélations d'Edward Snowden.

[98] Contrôleur européen de la protection des données (2013), *Additional EDPS Comments on the Data Protection Reform Package*.

[99] Contrôleur européen de la protection des données (2011), Avis sur la communication intitulée "Une approche globale de la protection des données à caractère personnel dans l'Union européenne", Bruxelles, 14 janvier 2011.

- l'inclusion au sein du conseil de protection des données d'au moins un commissaire spécial ayant pour mandat d'accorder la priorité à la protection des droits des citoyens, et disposant d'un personnel indépendant à l'effectif réduit, éventuellement élu par un vote populaire (mais apolitique) au moment des élections européennes ou par le Parlement;

- l'inclusion d'un commissaire technique spécial, désigné par une assemblée d'experts en informatique du milieu universitaire spécialisés dans les questions de protection de la vie privée, et éventuellement d'un autre commissaire issu du domaine des sciences de la surveillance, disposant aussi tous deux d'une petite équipe indépendante;

- l'obligation pour les commissaires chargés de la protection des données d'être désignés par les parlements nationaux et non par le pouvoir exécutif;

- un minimum de 25 % du personnel technique des DPA ayant des qualifications appropriées (ou une expérience équivalente) et des possibilités d'évolution de carrière[100] vers les plus hauts postes;

- une allocation de fonds visant à soutenir le secteur de la société civile; notons toutefois qu'il convient d'accorder une attention particulière à la circonscription de cette allocation. Les fonds devraient être distribués de manière équitable et sur la base du mérite, tout en évitant l'effet d'étouffement dû à la bureaucratie ainsi que le risque d'emprise institutionnelle[101]. Aux États-Unis, la culture de philanthropie et les grandes organisations de la société civile permettent l'existence de quatre ONG nationales très professionnelles[102], adoptant des approches différentes, qui lancent des procédures dans des affaires importantes liées à la protection de la vie privée et à la liberté d'information et qui publient des critiques très techniques et de classe mondiale des politiques du gouvernement. Par contraste, l'UE possède encore un ensemble disparate de dizaines d'ONG qui, à cause de leur manque de ressources et de leur manque de capacité stable de travailleurs à temps plein affectés à la recherche n'ont pas fait de campagne contre la FISA avant l'affaire Snowden.

[100] Les DPA indiquent qu'elles ne sont pas en mesure d'embaucher ou de conserver des membres du personnel technique ayant des connaissances à jour parce que leurs salaires ne peuvent concurrencer ceux du secteur privé. Les plans de carrière au sein des DPA pourraient donc assurer une parité de rémunération raisonnable entre le personnel technique et juridique, ce qui contribuerait à résoudre le problème.

[101] Par exemple, la stratégie "no disconnect" oblige les ONG à faire appel à des consultants afin de préparer des offres minutieuses, ce qui a pour effet d'exclure les petites ONG et est contraire à l'esprit de la société civile.

[102] L'Electronic Frontier Foundation (EFF), le centre d'informations sur la protection de la vie privée dans le monde numérique (Electronic Privacy Information Center, EPIC), l'Union américaine pour les libertés civiles (American Civil Liberties Union, ACLU), et le centre pour la démocratie et la technologie (Center for Democracy and Technology, CDT).

CONCLUSION

Comme il a été observé plus haut, un des aspects les plus extraordinaires de l'affaire PRISM est non seulement le fait que les droits des non-USPER n'ont pas fait l'objet de discussions aux États-Unis, mais le fait qu'ils n'ont même pas fait l'objet de discussions dans les médias européens pendant plusieurs mois après les premières révélations. Les droits des non-USPER ont rarement été mentionnés, et un lecteur moyen ne comprendrait pas que les activités de surveillance de la NSA ciblaient ces non américains, totalement dépourvus de droits.

Il semble que la seule solution susceptible de résoudre le scandale PRISM doive passer par des changements apportés à la législation américaine, et cela devrait constituer l'objectif stratégique de l'UE. **Mais l'UE doit examiner de manière très attentive[103] le type précis d'accord proposé dans le cadre de toute entente future avec les États-Unis.** Des mécanismes pratiques[104] mais efficaces sont également nécessaires pour vérifier que les divulgations de données aux États-Unis à des fins d'enquête motivée ne font pas l'objet d'abus.

Dans l'évaluation des conséquences des révélations d'Edward Snowden, trois éléments techniques devraient être pris en considération lors de la recherche de réponses efficaces.

(1) Les données ne peuvent être traitées que sous forme déchiffrée, ce qui signifie que tout prestataire de services d'informatique en nuage peut se voir ordonner, au titre de l'article 702 de la FISA, de remettre aux autorités une clef de déchiffrage, ou les données elles-mêmes sous leur forme déchiffrée. Le chiffrage est vain lorsqu'il s'agit d'empêcher la NSA d'accéder aux données traitées dans les nuages basés aux États-Unis (mais il est toujours utile pour se prémunir contre des adversaires externes, par exemple des pirates informatiques). L'utilisation du nuage comme espace de stockage distant n'offre pas la même compétitivité ou la même modularité que son utilisation pour le traitement de données. **Il n'existe aucune solution technique au problème[105].**

(2) L'exposition de grandes quantités de données à la surveillance de masse exercée sur le nuage est un abandon de la souveraineté sur les données, et la conservation des données au sein de l'UE est préférable en attendant l'adoption de solutions de nature juridique. Bien que la NSA dispose de la capacité de cibler certains systèmes sur le territoire de l'UE, cela est plus difficile et plus risqué. Une réforme fondamentale du nouveau règlement est nécessaire, sans quoi ces deux situations seront *en pratique* traitées de la même manière, et les services d'informatique en nuage seront commandés au prestataire le moins cher.

(3) Même si une entreprise basée dans l'UE et exerçant son activité aux États-Unis est également exposée aux conflits entre le droit de l'UE en matière de protection des données et la FISA américaine, il est moins probable en pratique qu'elle se voie donner ce type d'injonction secrète, car ses dirigeants et son personnel juridique opposeraient vraisemblablement une résistance plus importante, les citoyens de l'UE étant moins

[103] Concernant les pouvoirs présidentiels "inhérents" non soumis à l'autorité du congrès, voir: Fein, Bruce (2007), *Presidential Authority to Gather Foreign Intelligence*, Presidential Studies Quarterly, mars 2007.
[104] Wills Aidan and al., *Parliamentary Oversight of security and Intelligence Agencies in the EU*, note pour le Parlement européen, PE 453.207
[105] La technique exotique de "chiffrement homomorphique" est parfois proposée comme une solution possible, mais elle n'est pas applicable à l'activité des entreprises car son adoption ne serait pas compétitive et elle ralentirait le traitement de manière très importante.

vulnérables aux lois américaines en matière d'espionnage. Les "nuages" peuvent être limités à une zone précise, et les arguments selon lesquels cela provoquerait une "balkanisation" de l'internet[106] sèment la confusion entre la question de la censure et celle de la protection de la confidentialité des données.

* * *

Il est impossible de faire marche arrière sur les pensées suscitées dans l'esprit du public par les révélations d'Edward Snowden. Elles ont d'ores et déjà modifié la société dans laquelle nous vivons. Chacun, à présent, sait que la communauté américaine du renseignement peut avoir connaissance de n'importe quel secret personnel envoyé sous forme électronique dans le champ d'action de la NSA. Ces nouvelles pourraient être extrêmement déstabilisantes pour les sociétés démocratiques, puisqu'elles sont contradictoires avec l'exercice des droits politiques et humains fondamentaux et créent une nouvelle forme de pouvoir omniscient instantané et coercitif.

Il existe une symétrie historique entre la violation des droits conférés aux Américains par le quatrième amendement et le mépris pour le droit au respect de la vie privée des personnes du monde entier. Dans la période précédant la guerre d'indépendance des États-Unis en 1776, les Britanniques ont employé des "mandats généraux" les autorisant à effectuer des recherches sans suspicion, et c'est le ressentiment[107] envers ce pouvoir et son abus qui ont motivé le quatrième amendement de la Constitution des États-Unis.

L'article 702 (ou article 1881a) constitue un mandat général permettant aux autorités américaines de recueillir des données et d'intercepter des informations liées aux affaires étrangères des États-Unis, mais la vie privée des Américains est juridiquement sacro-sainte (même si ce n'est qu'en théorie) à moins que ne soit satisfait le seuil juridique de "nécessité" ne soit franchi. Ce qui a particulièrement indigné les révolutionnaires américains du 18e siècle, c'est qu'une célèbre affaire[108] avait, dix ans auparavant, conduit à l'interdiction de ce type de mandat général au Royaume-Uni. Ils ont donc perçu comme une forme d'hypocrisie le fait que des lois qu'ils n'avaient pas écrites et ne pouvaient changer protégeaient la vie privée de leurs dirigeants mais non celle des sujets vivant dans les colonies. C'est le même principe qui est en jeu aujourd'hui.

[106] Département américain du commerce (conseiller général) – Kerry, Cameron F. (2013), discours prononcé devant le German Marshall Fund of the United States, 28 août 2013.
[107] https://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf
[108] Entick vs. Carrington 1765

RÉFÉRENCES

- ACLU FOIA request (2010), Introduction to FISA Section 702, (2010) Course Information, US Department of Justice, publié en décembre 2010
- Anzalda, Matthew A. and Gannon, Jonathan W. (2010), In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance (paywall), Texas Law Review, Vol 88:1599 2010
- ART29WP - Article 29 Data Protection Working Party (2012), Opinion on Cloud Computing, WP 196, adopté le 1er juillet 2012
- ART29WP - Article 29 Data Protection Working Party (2012), Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 195, adopté le 6 juin 012
- ART29WP - Article 29 Data Protection Working Party (2013), Explanatory Document On The Processor Binding Corporate Rules, WP 204, adopté le 19 avril 2013
- Bigo Didier, Boulet Gertjan, Bowden Caspar, Carrera Sergio, Jeandesboz Julien, Scherrer Amandine (2012), Fighting cyber crime and protecting privacy in the cloud, étude pour le Parlement européen, PE 462.509
- Bloom, Stephanie Cooper (2009), What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform, Public Interest Law Journal Vol 18:269
- Bowden, Caspar (2011), Government Databases and Cloud Computing (slides), The Public Voice, Mexico, octobre 2011
- Bowden, Caspar (2012), Is EU data safe in US Clouds? (slides), Academy of European Law, Trier, septembre 2012
- Cloud, Morgan (2005), A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment, Ohio State Journal of Criminal Law, Vol 3:33 2005
- Cole, David, (2003), Georgetown Law: The Scholarly Commons, Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens? 25 T. Jefferson L. Rev. 367-388
- Congressional Research Service - Bazan, Elizabeth B. (2008), The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, mis à jour le 7 juillet 2008, RL34279
- Congressional Research Service – Liu, Edward C. (2013), Reauthorization of the FISA Amendments Act, 7-5700, R42725, 2 janvier 2013
- Congressional Research Service (2007), P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, 23 août 2007
- Corradino, Elizabeth A. (1989), Fordham Law Review, The Fourth Amendment Overseas: Is Extraterritorial Protection of Foreign Nationals Going Too Far? Volume 57, Issue 4, Article 4, janvier 1989
- De Filippi, Primavera, and McCarthy, Smari (2012), Cloud Computing: Centralization and Data Sovereignty, European Journal of Law and Technology 3, 2
- Desai, Anuj C. (2007), Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy, Stanford Law Review, 60 STAN L. REV. 553
- Dhont J., Asinari M.V.P., Poullet Y., Reidenberg J., Bygrave L. (2004), Safe Harbour Decision Implementation Study, Commission européenne, DG Marché intérieur,

contrat PRS/2003/A0-7002/E/27

- Dulles, Allen Welsh (1963), The Craft of Intelligence, New York: Harper&Row.
- Commission européenne (2011), [projet de] proposition de règlement général sur la protection des données
- Commission européenne (2012), proposition de règlement général sur la protection des données, 25.1.2012, COM(2012) 11 final 2012/0011
- Commissaire européen - Reding, Viviane (2013), Letter to the Attorney General, Ref. Ares (2013)1935546 - 10/06/2013, Bruxelles, 10 juin 2013
- Contrôleur européen de la protection des données - Hustinx, Peter (2010), Data Protection and Cloud Computing Under EU Law, speech, Third European Cyber Security Awareness Day, BSA, Parlement européen, 13 avril 2010, Panel IV: Privacy and Cloud Computing
- Contrôleur européen de la protection des données (2011), Opinion on the Communication - "A comprehensive approach on personal data protection in the European Union", Bruxelles, 14 janvier 2011
- Contrôleur européen de la protection des données (2013), Additional EDPS Comments on the Data Protection Reform Package
- Fein, Bruce (2007), Presidential Authority to Gather Foreign Intelligence, Presidential Studies Quarterly, mars 2007
- Forgang, Jonathan D. (2009), "The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Volume 78, Issue 1, Article 6, 2009
- Hoboken, J.V.J., Arnbak, A.M., Van Eijk, N.A.N.M (2012), Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, IVIR, Institute for Information Law, University of Amsterdam, novembre 2012 (traduction anglaise)
- Hon, W. Kuan and Millard, Christopher (2012), Data Export in Cloud Computing - How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4, QMUL Cloud Legal Project, 4 avril 2012
- Hondius, Frits W (1975), Emerging data protection in Europe. North-Holland Pub. Co.
- International Working Group on Data Protection in Telecommunications (2012), Working Paper on Cloud Computing - Privacy and data protection issues - Sopot Memorandum, 51e réunion, 23-24 avril 2012
- Kuner, Christopher, (2008), Membership of the US Safe Harbor Program by Data Processors, The Center For Information Policy Leadership, Hunton & Williams LLP
- LoConte, Jessica (2010), FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?, Pace International Law Review Online Companion 1-1-2010
- Medina, M. Isabel, (2008) Indiana Law Journal, Exploring the Use of the Word "Citizen" in Writings on the Fourth Amendment Volume 83, Issue 4, Article 14, janvier 2008
- Pell, Stephanie K. (2012), Systematic government access to private-sector data in the United States, International Data Privacy Law, 2012, Vol. 2, No. 4
- Radsan, John A. (2007), The Unresolved Equation of Espionage and International Law, Michigan Journal of International Law, Vol 28:595 2007
- Snider, Britt L. (1999): Unlucky SHAMROCK - Recollections from the Church Committee's Investigation of NSA

- U.S. Ambassador to the EU (2012), Remarks by William E Kennard, Forum Europe's 3rd Annual European Data Protection and Privacy Conference, 4 décembre 2012
- U.S. Commerce Department (General Counsel) – Kerry, Cameron F. (2013), Keynote Address at the German Marshall Fund of the United States, 28 août 2013
- US Congress (2008), Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 122 Stat. 2436, Public Law 110-261, 10 juillet 2008
- US Department of Commerce International Trade Administration (2013), Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing, 4 décembre 2012
- US State Department (2012), Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the EU and the US
- Vandekerchkhove, Wim (2010), European whistleblower protection: tiers or tears?, in D. Lewis (ed) A Global Approach to Public Interest Disclosure, Cheltenham/Northampton MA, Edward Elgar, pp 15-35.
- Walden, Ian (2011), Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, QMUL Cloud Legal Project, Research Paper N° 74/2011
- Weichert, Thilo (2011), Cloud Computing and Data Privacy, The Sedona Group Conference Working Group Series, février 2011
- Wills Aidan, Vermeulen Mathias, Born Hans, Scheinin Martin, Wiebusch Micha, Thornton Ashley, Parliamentary Oversight of security and Intelligence Agencies in the EU, note pour le Parlement européen, PE 453.207.
- Young, Stewart M, (2003) Michigan Telecommunications and Technology Law Review, Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases, Volume 10, Rev. 139

PARLEMENT EUROPÉEN

CATALOGUE BA-02-13-390-FR-C

DIRECTION GÉNÉRALE DES POLITIQUES INTERNES

DÉPARTEMENT THÉMATIQUE C
DROITS DES CITOYENS ET AFFAIRES CONSTITUTIONNELLES

Rôle

Les départements thématiques sont des unités de recherche qui fournissent des conseils spécialisés aux commissions, délégations interparlementaires et autres organes parlementaires.

Domaines

- Affaires constitutionnelles
- Liberté, sécurité et justice
- Égalité des genres
- Affaires juridiques et parlementaires
- Pétitions

Documents

Visitez le site web du Parlement européen: **http://www.europarl.europa.eu/studies**

SOURCE PHOTO: iStock International Inc.

ISBN 978-92-823-5062-1
doi: 10.2861/31596

Office des publications