Surveillance de la NSA : pourquoi le système des freins et contre-poids a été court-circuité

Steven R. Shapiro
Traduction Alix Meyer

Dans Politique américaine 2015/2 N° 24 , pages 11 à 27
Éditions L'Harmattan

ISSN 1771-8848
ISBN 9782343058474
DOI 10.3917/polam.024.0011
Date de mise en ligne : 06/05/2015

Surveillance de la NSA : pourquoi le système des freins et contre-poids a été court-circuité

Steven R. Shapiro*

Résumé

Les dernières révélations sur les activités de surveillance de la NSA aux États-Unis et dans le monde continuent de susciter le débat : leur ampleur est-elle justifiée ? Qu'est-ce que la vie privée dans un monde numérique ? Jusqu'à présent, les questions juridiques ont surtout porté sur le programme de recueil de métadonnées de connexion auprès des opérateurs de téléphonie mobile. Ces données ont été recueillies par la NSA sans que l'agence n''ait eu à cibler un suspect en particulier, à l'encontre de la tradition juridique américaine de protection de la vie privée des personnes face aux intrusions de l'État. Depuis, les médias ont révélé l'existence d'autres programmes de surveillance qui soulèvent des problèmes similaires.

Cet article propose de retracer l'histoire chaotique des efforts du législateur et du juge pour contrôler les méthodes de recueil du renseignement aux États-Unis avant d'explorer plus en avant en quoi le recueil en masse de métadonnées téléphoniques par la NSA constitue une menace pour la vie privée des personnes et comment le gouvernement américain a tenté de défendre la légalité de ses actions. Enfin, il s'agira d'expliquer les dysfonctionnements majeurs des mécanismes de contrôle par le législateur et les juges dont les failles ont été aggravées par les nouvelles contraintes très fortes qui pèsent aujourd'hui sur les journalistes qui cherchent à enquêter et à informer le public sur l'appareil de sécurité nationale.

Tout ce que nous savons sur la surveillance exercée par la NSA, nous le devons à Edward Snowden[2]. La question de savoir s'il s'est comporté en héros ou en traître continue d'alimenter la polémique. Il me semble que ce débat sert surtout à détourner l'attention pour éviter que l'on se pose d'autres questions beaucoup plus importantes : que doit-on penser de l'existence de cet appareil de surveillance d'État révélé par Snowden ? Le dispositif est-il légal ? Est-il justifié ? Et, enfin, comment expliquer que le système des freins etc contrepoidsontre-poids

* L'auteur est le *National Legal Director* de l'*American Civil Liberties Union* (ACLU).

2 Cf. Glen Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York, N.Y., Metropolitan Books (2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man*, New York, N.Y., Vintage Books (2014).

qui occupe une place si centrale dans notre conception de la démocratie constitutionnelle n'ait offert aucune résistance significative aux actions de la NSA ?

Bien entendu, la NSA ne s'est pas contentée de cibler uniquement les citoyens américains peut-être ne sommes-nous même pas les cibles principales. Malgré cela, j'ai choisi de me concentrer tout particulièrement sur le cas des citoyens américains plutôt que sur celui de tous ceux qui vivent en dehors des États-Unis pour une raison très simple. La loi américaine ne reconnaît aux étrangers qui vivent en dehors des États-Unis aucun droit dont ils peuvent se prévaloir devant les tribunaux américains. On peut cependant noter qu'à la suite des révélations de Snowden le président Obama a expliqué avoir décidé « d'étendre pour la première fois certaines des protections dont nous bénéficions en tant que citoyens américains au reste de la population mondiale »[3] tout en précisant qu'il s'agissait uniquement d'une décision politique de sa part et aucunement d'un changement de droit. Les protections qu'il évoquait alors concernaient la durée durant laquelle les données peuvent être conservées et comment elles peuvent être partagées.

Avant de s'occuper du présent, il est utile de commencer par faire un retour en arrière. Le terme de « vie privée » n'apparaît pas dans le texte de la Constitution américaine. Malgré cela, le Quatrième amendement intègre l'idée d'une protection de la vie privée puisqu'il précise que : « le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violé, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir. » Le quatrième amendement fut adopté en réponse à la pratique britannique qui consistait à délivrer des mandats de perquisition génériques qui permettaient aux soldats de la Couronne de fouiller les maisons des colons américains à la recherche de matériel de contrebande. La nécessité de se prévaloir d'une présomption sérieuse et individualisée constitue donc un élément central du Quatrième amendement. Dans le même temps, dans l'histoire américaine, le sens du Quatrième amendement a le plus souvent été intimement lié à la notion d'intrusion (*trespass*) développée par le droit coutumier (*common law*). En 1928, la Cour suprême des États-Unis a ainsi pu juger qu'une mise sur écoute non autorisée par un mandat de perquisition ne constituait pas une atteinte aux protections du Quatrième amendement tant que la police était capable d'installer le matériel de mise sur écoute sans pénétrer dans le domicile

3 Président Barack H. Obama, « Remarks by the President on Review of Signals Intelligence », 17 janvier 2014, en ligne : http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

du suspect[4]. Cette interprétation limitée du Quatrième amendement a prévalu jusqu'en 1967 lorsque, à l'occasion d'une autre affaire de mise sur écoute, la Cour suprême a choisi de renverser cette jurisprudence en expliquant que « le Quatrième amendement protège les personnes et non les lieux»[5].

Malgré cela, les activités de recueil de renseignements des agences américaines continuèrent sans aucune véritable régulation jusqu'au début des années 1970 lorsque deux événements majeurs se produisirent.

En 1972, la Cour suprême rejeta l'idée selon laquelle la notion de respect de la vie privée prévue par le Quatrième amendement puisse être écartée dans le cas d'un risque pour la sûreté nationale[6]. La Cour a jugé qu'en dehors d'une situation d'urgence, et au moins lorsqu'il s'agit d'une enquête sur le territoire américain, l'État n'a pas le droit de fouiller un domicile ou de mettre un téléphone sur écoute sans un mandat de perquisition. Cependant, la Cour a également bien pris le soin de limiter la portée de sa décision aux enquêtes sur le territoire américain, suggérant que les mêmes règles ne s'appliqueraient pas nécessairement pour le recueil de renseignements à l'étranger.

Trois ans plus tard, en 1975, le Congrès mit en place une commission d'enquête parlementaire chargée d'étudier les activités de surveillance des agences fédérales du renseignement accusées d'avoir commis des « fautes graves ». Selon les conclusions du rapport de la commission Church[7], les agences du renseignement « étaient passées outre les interdictions explicitement prévues par la loi, avaient porté directement atteinte aux droits des citoyens américains (y compris ceux des journalistes, des juges fédéraux et des membres du Congrès) tels que garantis par la constitution ». Enfin, pendant plus de quatre décennies, elles avaient « sciemment ignoré » les limites que la loi avait fixées à leurs activités de surveillance au nom de la sûreté nationale. La commission se montrait particulièrement inquiète de la manière dont les agences avaient « fait du recueil de renseignements par 'aspiration' » : sous prétexte de cibler des étrangers, il leur arrivait d'intercepter les communications de citoyens américains. La NSA avait ainsi pu s'appuyer sur un programme de surveillance de cibles étrangères pour « obtenir d'au moins deux opérateurs de télécommunication tous les télégrammes émis ou reçus des États-Unis, y compris des millions de communications privées des citoyens américains. » Lors d'une autre opération, la NSA avait écouté des milliers de conversations téléphoniques entre New York et une ville d'Amérique du Sud. Pour la commission Church, les atteintes systématiques

4 *Olmstead v. New York,* 237 U.S. 438 (1928).
5 *Katz v. United States*, 389 U.S. 347, 351 (1967).
6 *United States v. United States District Court*, 407 U.S. 297 (1972).
7 NdT – La commission prit le nom de son président, Franck Church, sénateur démocrate de l'Idaho.

aux libertés fondamentales qu'elle avait mises à jour étaient imputables à un dysfonctionnement des freins et contre-poids[8].

En 1978, suite au rapport de la commission, le Congrès vota une Loi sur la surveillance du renseignement extérieur (*Foreign Intelligence Surveillance Act* ou FISA)[9]. Pour la première fois, cette loi crée une procédure de mandat de perquisition pour encadrer les opérations de renseignement qui vise à mettre sur écoute des communications émises ou reçues par un individu aux États-Unis avec le reste du monde. Ces mandats doivent faire l'objet d'une demande auprès d'une nouvelle Cour de Surveillance du Renseignement Extérieur (Cour FISA) qui statue sur leur validité. En vertu de cette loi, la Cour FISA pouvait délivrer un mandat de perquisition pour autoriser une surveillance électronique à condition que la perquisition soit établie sous une présomption raisonnable et que la cible fût effectivement un espion engagé par une puissance étrangère. Le procédé fut ensuite étendu aux agents présumés d'une organisation terroriste étrangère. En 1998, la loi fut amendée afin que, dans le cadre d'une enquête sur des activités d'espionnage étranger, le gouvernement puisse demander à la Cour FISA d'enjoindre à des entreprises de transmettre certaines données commerciales. Là encore, le gouvernement devait démontrer qu'il y avait « des faits spécifiques clairs qui permettaient de penser que l'individu ciblé agissait pour le compte d'une puissance étrangère »[10]. À l'image des mandats de perquisition plus classique de la procédure pénale, un mandat FISA ne pouvait être délivré que sur la base d'une présomption individualisée.

Après le 11 septembre, ces normes furent très largement assouplies lorsque le Congrès adopta le PATRIOT Act en novembre 2001[11]. C'est désormais la section 215 de cette loi qui sert de cadre législatif à ces procédures. Après plusieurs amendements successifs, elle permet aujourd'hui au gouvernement d'obtenir de la Cour qu'elle ordonne la transmission du « moindre élément tangible » sans avoir à démontrer une quelconque présomption individualisée à condition que les documents demandés soient « liés à » une enquête sur du renseignement étranger ou encore à la protection contre le terrorisme international[12].

Bien entendu, le PATRIOT Act comportait beaucoup d'autres dispositions autorisant le gouvernement à étendre ses capacités d'enquête après les attentats du 11 septembre. Pour autant, cette loi ne lui permettait pas de mettre en place un mécanisme de surveillance électronique sur le sol américain sans mandat de perquisition. L'administration Bush a choisi d'ignorer ces limites et a pris

……..

8 Cf. « Final Report of the S. Select Comm. To Study Governmental Operations with Respect to Intelligence Activities » (Book II), S. Rep. n° 94-755 (1976) (*Church Committee Report*), en ligne: http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf.

9 Pub. L. No. 95-511, 92 Stat. 1783 (50 U.S.C. § 1801 *et seq.*).

10 50 U.S.C. §§ 1861-62 (2000).

11 USA PATRIOT Act of 2001, Pub.L. 107-56, 115 Stat. 272.

12 50 U.S.C. § 1861(b) (2) (A).

l'initiative sans en informer le Congrès et sans demander d'autorisation aux juges. De 2001 à 2007, un programme d'interception des courriels et conversations téléphoniques émis ou reçus par les États-Unis fut renouvelé à plusieurs reprises par le président George W. Bush. La seule condition requise était qu'un employé de la NSA – et non un juge – considère qu'il y avait « un motif raisonnable pour penser qu'une des parties prenantes à ces communications était membre d'Al Qaïda ou d'une de ses organisations satellites ou encore qu'elle contribuait à soutenir Al Qaîda »[13].

En décembre 2005, le *New York Times* fut le premier à révéler l'existence de ce programme d'écoutes non autorisées. Il s'ensuivit un débat national assez proche de celui qui agite aujourd'hui auxles États-Unis, quant aux limites du droit à la vie privée. Barack Obama qui n'était alors que simple sénateur faisait partie des critiques les plus virulents des actions de l'administration Bush qui prétendait pouvoir ignorer la loi et le respect de la vie privée des citoyens américains. Pour autant, juste avant l'élection présidentielle de 2008, Obama apporta sa voix à la majorité sénatoriale pour adopter une nouvelle réforme de la Loi sur la surveillance du renseignement étranger (*FISA Amendements Act*)[14] ;, texte qui consistait très largement à légaliser les actions que l'administration Bush avait entreprises sans autorisation. Plus précisément, selon la section 702 de la loi[15], le gouvernement pouvait désormais obtenir un mandat de perquisition général (*blanket warrant*) qui l'autoriserait à surveiller, sans aucun ciblage, les messages électroniques et les appels téléphoniques pour une durée maximale d'un an tant que le procureur général des États-Unis[16] et le Directeur du renseignement (*Director of National Intelligence* - DNI) auraient certifié conjointement que les procédures mises en place étaient « établies de manière raisonnable » afin de garantir que cette surveillance ne concernait que des personnes (hors citoyens américains) dont « on pourrait raisonnablement croire » qu'elles ne se trouvaient pas sur le territoire américain[17]. Ces protocoles sont très différents du critère de la nécessaire définition d'une cible individualisée qui prévalait jusque-là. En vertu de la nouvelle loi FISA, si le gouvernement américain est capable d'identifier des courriels et des appels téléphoniques émis depuis la ville française de Lyon, il peut ainsi demander une autorisation pour intercepter

13 Cf. Office of the Inspector Gen. of the Dep't of Def. et al., *Unclassified Report on the President's Surveillance Program* (2009), en ligne: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/report_071309.pdf

14 Pub. L. No. 110-261, 122 Stat. 2436.

15 50 U.S.C. § 1881a.

16 NdT – équivalent de notre ministre de la Justice.

17 De plus, le procureur général des États-Unis et le DNI doivent également certifier que la surveillance se fera selon des procédures autorisées par les tribunaux pour minimiser les risques d'interception et de stockage d'informations privées concernant des citoyens américains sans aucun lien avec le renseignement extérieur.

tous ces courriels et ces appels téléphoniques, même si c'est un citoyen américain qui est à l'autre bout du fil.

L'ACLU s'est pourvu en justice en arguant que la Constitution américaine ne permettait pas au gouvernement de faire de la surveillance électronique une « pêche au filet dérivant » (*dragnet surveillance*). Elle a dit : « Nous avons porté l'affaire devant les tribunaux au nom des citoyens américains et des organisations américaines qui avaient eu des communications avec le reste du monde ou qui avaient travaillé à l'étranger et qui étaient donc susceptibles d'avoir été prises pour cibles par les autorités américaines. Parmi nos clients, on dénombrait *Amnesty International, Human Rights Watch*, des journalistes de renom qui publiaient régulièrement sur les questions de terrorisme international ainsi que des avocats américains qui défendaient des détenus de la prison de Guantanamo. Malheureusement, la Cour suprême a refusé la saisine dans notre affaire et donc elle ne s'est pas prononcée sur le fond. Par une majorité de cinq juges contre quatre, la Cour, usant d'une logique kafkaïenne, a jugé que nos clients ne pouvaient légitimement remettre en cause les pouvoirs de surveillance du gouvernement tels que prévus par la nouvelle loi FISA qu'à condition d'être absolument certains d'avoir été mis sur écoute. Or, ils ne pouvaient pas être absolument certains d'avoir été mis sur écoute puisque cette information était tenue secrète par le gouvernement qui refusait de la confirmer ou de l'infirmer[18].

Les quatre juges dissidents s'étaient montrés plus pragmatiques. Ils affirmaient qu'on ne pouvait pas demander à nos clients de démontrer avec certitude quelque chose que le gouvernement tenait absolument à garder secret. Ils ont même estimé que la probabilité selon laquelle « au moins quelques-unes » des conversations privées de nos clients aient pu être interceptées par la NSA devait être vue comme comparable à celle qui « permet d'estimer l'occurrence des événements futurs à l'aune du bon sens et de la plus simple connaissance de la nature humaine »[19].

Nous craignions qu'en écartant ainsi nos requêtes, la Cour allait, de fait, immuniser le programme de surveillance de la NSA contre toute remise en cause par une partie adverse. En guise de réponse, la majorité de la Cour avait repris les interprétations du gouvernement, selon lesquelles les autorités ne pouvaient pas utiliser de preuves obtenues dans le cadre d'une communication interceptée sous couvert de sûreté nationale sans en aviser l'accusé. Ce dernier pouvait dès lors légitimement remettre en cause la constitutionnalité de cette surveillance et demander à ce que ces preuves ne soient pas utilisées contre lui

18 *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013).
19 *Id.* 1155.

au pénal[20]. Cet argument était bien conforme aux textes mais la suite révéla que, dans la pratique, le gouvernement ne respectait pas ce principe[21].

En juin 2013, deux mois après l'arrêt de la Cour Suprême dans l'affaire *Amnesty*, le journal *The Guardian* publia son premier article à partir des documents fournis par Edward Snowden. L'article révélait qu'en avril de cette même année, dans une décision jusque-là restée secrète, la Cour FISA s'était appuyée sur cette même Section 215 pour donner ordre à *Verizon Business Network Services*, l'un des principaux opérateurs de téléphonie mobile du pays, de fournir à la NSA « en continu... toutes les informations sur les détails des appels, les 'métadonnées téléphoniques' de tous les appels lancés depuis son réseau à l'international ou sur le territoire américain pour une période de 60 jours de mi-avril à mi-juin 2013 » . Rappelons que la Section 215 permet au gouvernement de demander des « éléments tangibles », y compris des documents commerciaux, dans le cadre d'une enquête sur le renseignement étranger ou sur le terrorisme. Ces « métadonnées téléphoniques » que Verizon était ainsi obligé de transmettre comportaient le numéro de téléphone de la personne qui avait émis l'appel, celui-ci téléphone de la personne qui l'avait reçu ainsi que l'heure et la durée de l'appel. On apprit ensuite que le gouvernement avait renouvelé cette demande à de multiples reprises et obtenu des ordres similaires pour les autres opérateurs de téléphonie mobile américains.

Cette révélation relança complètement le débat sur les atteintes à la vie privée aux États-Unis car elle faisait voler en éclats la douce illusion selon laquelle les citoyens américains qui n'avaient rien à se reprocher ne seraient jamais victimes de l'insatiable soif de données de leur gouvernement. Face aux critiques grandissantes, les autorités usèrent de différents arguments pour défendre leur programme de recueil de données en masse. Premièrement, le gouvernement insista bien sur le fait que les interceptions ne concernaient que les métadonnées téléphoniques et non le contenu des conversations. Deuxièmement, il prétendait que ces métadonnées étaient consultées uniquement s'il y avait « un motif raisonnable et intelligible de soupçonner » qu'un numéro de téléphone était lié, d'une manière ou d'une autre, à une activité terroriste. Enfin, selon les autorités, ce recueil en masse de métadonnées téléphoniques constituait un

……..

20 *Id.* 1154.

21 Adam Liptak, « A Secret Surveillance Program Proves Challengeable in Theory Only », *The New York Times*, 15 juillet 2013, en ligne: http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?hp. Plus tard, le gouvernement a changé sa politique pour se mettre en conformité avec la loi et avec la manière dont elle avait été présentée devant les tribunaux. cf. Patrick C. Toomey, « Government Reverses Course on Wireless Wiretapping in Criminal Case, Admits Duty to Notify Defendants », en ligne: https://www.aclu.org/blog/national-security/government-reverses-course-warrantless-wiretapping-criminal-case-admits-duty . Suite à ce changement, plusieurs nouvelles procédures ont été entamées devant les tribunaux pour remettre en cause le pouvoir de surveillance du gouvernement en vertu de la section 702 révisée de la loi FISA.

élément absolument central du dispositif mis en place pour empêcher de futurs attentats terroristes.

Malheureusement pour le gouvernement, à bien y regarder, aucun de ces arguments ne se révèle très convaincant. Bien qu'il ne s'agisse que de recueillir des métadonnées, à une si grande échelle, ces informations permettent au gouvernement d'en apprendre énormément sur les réseaux de relations dans lesquels nous nous inscrivons et sur nos diverses activités. Dans son avis d'expert dans l'affaire *Clapper*, Edward W. Felten, professeur et directeur du *Center for Information Technology Policy* à l'université de Princeton, expliquait ainsi que « les métadonnées reflètent le contenu des messages »[22]. Numériques, elles sont très faciles à analyser et « peuvent révéler une somme extraordinaire d'informations sur nos habitudes et nos relations »[23]. On peut ainsi savoir si quelqu'un a appelé les numéros spéciaux qui permettent de signaler des violences conjugales ou un viol, SOS suicide, les Alcooliques Anonymes, les numéros dédiés aux adolescents homosexuels en difficulté ou encore ceux pour les vétérans qui éprouvent des difficultés à se réadapter à une vie normale. Comme l'explique le professeur Felten : « Lorsqu'on agrège des métadonnées sur la durée et que l'on pioche dans cette mine d'informations on peut, par simple association, y découvrir encore plus d'informations personnelles » sur nos relations les plus intimes et nos orientations politiques[24].

Même en admettant que le gouvernement disait la vérité lorsqu'il prétendait ne pas regarder les métadonnées interceptées à moins d'avoir « un soupçon raisonnable et intelligible », c'est la NSA et non un juge qui se chargeait de décider s'il y avait bien « un soupçon raisonnable et intelligible ». De plus, une fois que la NSA avait décidé d'examiner les métadonnées d'un numéro de téléphone particulier, l'agence pouvait explorer jusqu'à trois « maillons » supplémentaires en examinant les métadonnées de toutes les personnes qui avaient contacté une personne qui avait contacté une personne qui avait contacté une personne qui avait contacté la personne suspectée au départ. Ainsi, ce sont très vite des centaines de milliers voire des millions d'individus qui se retrouvaient pris dans les mailles du filet.

Enfin, l'argument selon lequel ces recueils de données en masse par la NSA étaient justifiés par le besoin d'assurer la sûreté nationale s'est lui aussi révélé assez galvaudé. Selon une étude du Bureau de protection de la vie privée et des libertés individuelles (*Privacy and Civil Liberties Oversight Board*), une

22 « *metadata is often a proxy for content* ». Déclaration sous serment (*Affidavit*) de Edward W. Felton, en date du 23 août 2013, en soutien à la requête des plaignants dans l'affaire *American Civil Liberties Union v. Clapper*, Dkt. No. 13-cv-03994 (S.D.N.Y), 39, en ligne: https://www.aclu.org/sites/default/files/assets/202013.08.26_aclu_pi_brief_and_declarations.pdf.

23 *Id.* at 46.

24 *Id.* at 47.

agence indépendante au sein de l'administration, on ne trouve « pas un seul exemple d'enquête sur une menace d'attaque terroriste contre les États-Unis dont le résultat ait été affecté de manière notable par le recours aux données téléphoniques »[25].

Une commission spéciale nommée par le président Obama suite aux révélations de Snowden arriva à la même conclusion : « Même sans intercepter et stocker les métadonnées téléphoniques en masse, le gouvernement dispose d'autres moyens pour remplir ces objectifs tout à fait légitimes sans porter atteinte à la vie privée des personnes et rendre possibles des abus de pouvoir »[26].

Dès que les activités de surveillance de la NSA furent rendues publiques, deux procès furent intentés. Les juges parvinrent à des conclusions diamétralement opposées dans les deux affaires. Le premier procès eut lieu à Washington et le second, lancé à l'instigation de l'ACLU, à New York. Le juge chargé de l'affaire à Washington décrit le recueil en masse de métadonnées téléphoniques comme « quasiment digne de George Orwell » et vraisemblablement anticonstitutionnel[27]. À l'inverse, seulement six jours plus tard, le juge chargé de l'affaire à New York conclut que le recueil en masse de métadonnées téléphoniques ne constituait pas une atteinte au respect de la vie privée des personnes garanti par la loi[28]. Ces deux arrêts ont fait l'objet d'appels qui n'ont pas encore été jugés à l'heure où nous écrivons ces lignes.

Pendant ce temps, en août 2013, le gouvernement avait déclassifié un arrêt de la Cour FISA qui autorisait lui aussi le recueil des métadonnées téléphoniques par la NSA[29]. De manière tout à fait remarquable, bien que le programme ait été mis en place depuis 2001 et que sa légalité ait été affirmée à de multiples reprises par la Cour FISA depuis 2006, c'était la première fois que la cour explicitait le raisonnement juridique qui sous-tendait sa décision.

Quels sont donc les problèmes juridiques soulevés dans ces diverses affaires ? Premièrement, le programme de recueil en masse des métadonnées téléphoniques par la NSA est-il autorisé par la section 215 du PATRIOT Act ? Il

25 Privacy and Civil Liberties Oversight Board, « Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court », 23 janvier 2014, p. 146, en ligne: http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf.

26 « Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies », 12 décembre 2013, p.118, en ligne: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf .

27 *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013).

28 *American Civil Liberties Union v. Clapper*, 959 F.Supp.2d 724 (2013). Les débats devant la cour furent télévisés aux États-Unis. La vidéo est en ligne: http://www.c-span.org/video/?321163-1/aclu-v-clapper-oral-argument-phone-record-surveillance .

29 *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted],* Br. 13-109 (FISC 29 août 2013), en ligne: http://www.uscourts.gov/uscourts/ fisc/br13-09-primary-order.pdf.

s'agit d'une pure question d'interprétation du texte de loi[30]. Ensuite, comment faut-il comprendre les instructions du Congrès lorsqu'il autorise la Cour FISA à faire des mandats de réquisitions pour obtenir des éléments matériels tangibles *en rapport* avec une opération de renseignement extérieur ou une enquête terroriste ? Aux yeux du gouvernement, les données de chaque communication téléphonique sont toujours *tpertinentes* dans le cadre de ses efforts dans la lutte antiterroriste puis qu'in ne sait pas à l'avance quelles données pourront finalement se révéler utiles. Notre réponse consiste simplement à dire que la manière dont le gouvernement définit le mot « pertinent » revient à le vider de tout son sens. Selon cette même logique, au moindre crime, le gouvernement devrait avoir le droit de pénétrer dans toutes les habitations d'une ville et de les feuiller sans cibler de suspect en particulier puisqu'il ne sait jamais à l'avance dans quelle maison il va pouvoir trouver des preuves.

La question de constitutionnalité est encore plus fondamentale. En vertu du Quatrième amendement, le gouvernement ne peut pas faire de perquisition sans avoir identifié un suspect et obtenu un mandat d'un juge. Pourtant, durant les dernières décennies, la Cour suprême a développé une exception à cette règle appelée « doctrine de la tierce partie ». Selon cette théorie, le droit des individus au respect de leur vie privée ne s'applique pas aux données commerciales détenues par une tierce partie quand bien même ces données contiendraient des détails très personnels auxquels le gouvernement n'aurait normalement pas accès sans mandat. En 1979, en application de cette règle, la Cour a jugé que la police n'avait pas besoin d'un mandat de perquisition pour installer un « mouchard » sur la ligne d'un homme suspecté d'avoir téléphoné à une femme à de multiples reprises pour la menacer et l'injurier après avoir cambriolé son domicile quelques jours auparavant[31]. Le mouchard, un instrument qui enregistre tous les numéros composés depuis un poste spécifique, a permis de rapidement confirmer que la police avait identifié le bon suspect et il fut ensuite arrêté.

La position défendue par le gouvernement est la suivante : puisqu'il n'était pas nécessaire d'obtenir un mandat de perquisition pour récupérer les numéros de téléphone composés depuis un seul poste sur une période de quelques jours après avoir identifié un suspect précis, alors il n'est pas nécessaire d'obtenir un mandat de perquisition pour récupérer les métadonnées téléphoniques

30 Sur ce point, se pose, de plus, la question de savoir si les individus clients des opérateurs de téléphonie peuvent légitimement se constituer partie civile. Les deux cours fédérales qui se sont intéressées à la question ont jugé que les plaignants ne pouvaient pas remettre en cause la légalité du texte en arguant que seuls les destinataires de ces ordres basés sur la Section 215, c'est-à-dire les opérateurs de téléphonie mobile comme *Verizon Business Network Service,* pouvaient se pourvoir devant une Cour FISA. Malgré tout, le juge de New York a finalement tranché la question de la légalité du texte de loi en faveur du gouvernement puisqu'il a jugé que le programme en question entrait bien dans le périmètre de la Section 215.

31 *Smith v. Maryland*, 442 U.S. 735 (1979).

de millions d'Américains sur une période de plusieurs années sans avoir identifié le moindre suspect. Donnez-lui long comme le doigt, et le gouvernement réclame long comme le bras. En dernier ressort, c'est bien la Cour suprême qui va devoir trancher ce débat et il est fort difficile de prédire quelle sera sa réponse. Ces dernières années, elle a semblé pourtant prendre la mesure de l'ampleur inédite des atteintes à la vie privée rendues possibles par la révolution numérique. Elle paraît prête à reconnaître que les règles qui gouvernent la protection de la vie privée doivent évoluer pour s'adapter à cette nouvelle donne [32]. L'année dernière, le juge Roberts, Président de la Cour, a fait l'observation suivante : prétendre comparer le fait de pouvoir consulter sans mandat de perquisition le contenu d'un téléphone portable saisi au cours d'une arrestation avec le fait de consulter le contenu du portefeuille ou le carnet d'adresses d'une personne qui vient d'être arrêtée « revient à dire qu'il n'y aurait pas vraiment de différence fondamentale entre une balade à cheval et une expédition lunaire »[33].

Ce qui est sûr c'est que le public américain réagit de manière bien plus marquée lorsqu'il pense que les programmes antiterroristes du gouvernement sont dirigés contre d'innocents citoyens américains. Or, c'est exactement ce qui s'est passé ici. Après que Snowden eut révélé l'existence du programme de métadonnées téléphonique qui était jusque-là tenu secret, le président Obama a affirmé qu'il se félicitait de voir ces questions débattues sur la place publique. Bien entendu, rien ne l'obligeait à attendre Edward Snowden pour ouvrir ce débat mais, pourtant, il ne l'avait jamais fait. Une fois qu'il apparut clairement que le problème ne disparaîtrait pas tout seul, le président Obama, et c'est à mettre à son crédit, proposa une série de réformes. Au lieu de laisser la NSA choisir seule sur quel numéro de téléphone elle allait se pencher, il lui donna l'ordre de demander l'accord de la Cour FISA pour chaque enquête. De plus, il annonça qu'au lieu d'explorer trois « maillons » à partir du numéro de téléphone ciblé, la NSA devrait désormais se contenter de deux maillons. Enfin, il déclara qu'il demanderait un vote au Congrès pour avaliser ces changements[34].

C'est une avancée significative mais qui demeure limitée. Le Congrès peut encore rejeter les propositions présidentielles. Mieux vaut deux maillons plutôt que trois, mais cela signifie quand même que des centaines de milliers d'Américains vont se retrouver mis sous surveillance par la NSA. Enfin, les propositions de réformes présidentielles ne concernent que le programme de métadonnées téléphoniques sur lequel se sont concentrés l'attention des médias

32 Le juge Sotomayor l'a reconnu explicitement en ce qui concerne la doctrine de la tierce partie dans son opinion individuelle pour l'arrêt *United States v. Jones*, 132 S.Ct. 945, 954 (2012).

33 *Riley v. California*, 134 S.Ct. 2473, 2488 (2014).

34 Fact Sheet, « The Administration's Proposal for Ending the Section 215 Bulk Telephony Program », 27 mars 2014, en ligne: http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m

et les critiques. La NSA continue de travailler sur une multitude d'autres programmes dont on commence tout juste à apprendre l'existence.

Tout cela nous ramène à notre point de départ : comment la mise sous surveillance a-t-elle pu devenir la norme plutôt que l'exception ? Un premier élément de réponse est à chercher dans l'étendue des progrès technologiques. C'est parce que lea placementmise sous surveillance massifve est technologiquement possible qu'elle a été mise en place. L'offre crée sa propre demande.

L'explication ne saurait s'arrêter là. L'administration aime à répéter que les activités de surveillance de la NSA en général et le programme de métadonnées téléphoniques en particulier ont été dûment évalués et autorisés par les trois pouvoirs. Sans doute, mais il faut aussi rappeler que le système constitutionnel démocratique américain est fondé sur l'idée que c'est la concentration des pouvoirs qui représente le plus grand danger contre les libertés fondamentales et que, par conséquent, leur séparation entre le législatif, l'exécutif et le judiciaire constitue le meilleur moyen de préserver les libertés en laissant à chaque pouvoir les moyens de juguler les autres.

Ici, le système a clairement failli. Ni le Congrès ni la Cour FISA créée par le Congrès n'ont vraiment su juguler la NSA dans sa boulimie de données à recueillir. Au Congrès, la supervision des agences de renseignement est presque entièrement réservée à des commissions spécialisées soumises au secret Défense. Ces commissions avaient bien eu connaissance du programme de métadonnées téléphoniques et elles n'avaient rien vu à redire. Peut-être les membres de ces commissions pensaient-ils que ce programme était légal et nécessaire, mais le fait que cette conviction n'ait jamais eu à souffrir d'aucune contradiction dans la mesure où ils n'entendaient que la version de la NSA demeure problématique. Même les autres membres du Congrès étaient largement tenus à l'écart. Dans les rares cas où des membres du Congrès qui ne faisaient pas partie de ces commissions spécialisées étaient autorisés à consulter des documents classés confidentiels, la procédure était la suivante : ils devaient se rendre seuls, sans aucun de leurs collaborateurs, dans une salle entièrement condamnée. Ils ne pouvaient pas prendre de notes et rien de ce qu'ils avaient vu ne pouvait être rendu public. Dans le meilleur des cas, il faut déjà beaucoup de courage politique pour remettre en cause un programme que les élites du renseignement décrivent comme absolument fondamental pour assurer la sûreté nationale. Lorsqu'il y a une telle asymétrie dans l'accès à l'information, c'est encore plus difficile.

Les membres des commissions du renseignement avaient donc accès à plus d'informations que leurs collègues. Certains d'entre eux ont essayé de forcer l'administration à une plus grande transparence mais leurs efforts furent mis à mal par les règles qui entourent le secret Défense. Ainsi, au cours d'une

audience publique devenue célèbre, Ron Wyden, sénateur de l'Oregon devenu très critique à l'égard des agences du renseignement, demanda à James Clapper, Directeur du renseignement (DNI), si « la NSA recueillait la moindre donnée, quelle qu'elle soit, concernant des millions ou des centaines de millions d'Américains. », ce à quoi Clapper répondit : « Non... pas volontairement ». Au moment de cette déposition, la NSA imposait aux opérateurs de téléphonies mobiles de lui transmettre en masse les métadonnées téléphoniques des Américains. Après les révélations d'Edward Snowden, de nombreuses voix se sont élevées pour accuser Clapper d'avoir menti au Congrès des États-Unis. Il s'est défendu en disant que, au vu des circonstances, il avait répondu de manière « aussi peu mensongère » que possible. Car le programme de surveillance était classé secret et le sénateur Wyden n'avait pas pun poursuivre l'affaire sous le regard du public[35].

Si la Cour FISA n'a pas su remplir son rôle de contrôle sur la NSA, c'est aussi parce que c'est un tribunal secret. Ses délibérations sont tenues secrètes et, traditionnellement, même ses injonctions étaient tenues secrètes. De plus, ce n'est pas la Cour elle-même, mais le pouvoir exécutif, qui peut choisir de déclassifier ses injonctions. Avec l'évolution du rôle de la Cour FISA, le problème n'a fait que s'aggraver. À l'origine, elle devait simplement être chargée d'établir des mandats de perquisition et des autorisations de mise sur écoute dans le cadre d'enquêtes sur le renseignement extérieur, une mission de routine et sans grandes conséquences. Aujourd'hui, on lui demande d'approuver des activités de surveillance à très grande échelle, comme le programme de métadonnées téléphoniques, qui ne ciblent aucun suspect en particulier et qui imposent à la Cour d'interpréter des textes de loi d'une grande complexité, souvent sans pouvoir s'appuyer sur aucun précédent. La Cour doit donc se contenter des éléments que lui donne le gouvernement. Dans des documents rendus publics, la Cour elle-même pestait contre toutes les fois où le gouvernement ne lui avait pas dit la vérité. De même, seul le gouvernement peut présenter ses arguments devant la Cour. Du point de vue du raisonnement juridique pur, un tel système ne peut pas aboutir aux meilleurs résultats. Il donne naissance à un ordre légal secret, dont seul le gouvernement connaît l'existence et auquel le public est soumis à son insu. On est tenté de citer cet éminent juge fédéral qui, après le 11 septembre et en d'autres lieux avait eu cette formule : « le huis clos tue les démocraties »[36].

Enfin, même si cela pourrait sembler étrange après que les révélations de Snowden ont fait les unes du *Guardian,* du *Washington Post* et du *New York Times*, force est de constater que les médias n'ont pas pu remplir pleinement

35 James Risen, « Lawmakers Question White House Account of an Internet Surveillance Program », *The New York Times*, 3 juillet 2013, disponible à http://www.nytimes.com/2013/07/04/us/lawmakers-question-white-house-account-of-an-internet-surveillance-program.html .

36 *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 683 (6 th Cir. 2002).

leur rôle de contrôleur contre les abus gouvernementaux. Leur efficacité a été mise à mal par la férocité avec laquelle le gouvernement s'est mis à poursuivre en justice leurs sources au sein de l'appareil d'État. L'administration Obama a entamé des poursuites contre un nombre record de personnes accusées d'avoir divulgué des informations et contre des lanceurs d'alerte. De fait, elle a poursuivi autant de personnes pour divulgation d'informations confidentielles que toutes les administrations précédentes réunies.

C'est en partie la conséquence d'un vrai choix politique, mais cela s'explique aussi par les développements de ce monde numérique dans lequel nous vivons désormais. Par certains côtés, le fait que l'information soit numérisée rend plus faciles que jamais les fuites d'une masse de données absolument inédite. Dans un monde sans numérique, Wikileaks n'existerait pas. En même temps, comme nous laissons toujours derrière nous une trace numérique, l'identification des responsables de ces fuites est beaucoup plus aisée. Aujourd'hui, Snowden est mis en examen par la justice américaine mais il n'est pas le seul. Tout cela contribue à faire réfléchir à deux fois aussi bien les lanceurs d'alerte que les journalistes qui souhaiteraient révéler des secrets d'État.

Les journalistes, mais surtout leurs sources au sein de l'État, prennent de grands risques. Le cadre législatif qui régit la transmission d'informations concernant la sûreté nationale est demeuré largement inchangé depuis qu'il a été fixé pendant la Première Guerre mondiale. Aux États-Unis, divulguer une information sur la sûreté nationale à une personne non autorisée est donc normalement passible de poursuites en vertu de la Loi contre l'espionnage de 1917[37]. Un tel acte étant considéré comme une forme d'espionnage, les sanctions potentielles sont sévères. La Loi contre l'espionnage ne fait aucune distinction entre le fait de transmettre des informations confidentielles à l'ennemi et le fait de les transmettre à la presse. De même, elle ne fait aucune distinction entre la publication dans la presse d'informations confidentielles et la transmission d'informations confidentielles par des agents de l'État dont on peut penser qu'ils auraient plutôt intérêt à garder le secret.

Pendant de nombreuses années, il était convenu qu'en vertu du Premier amendement la presse ne serait pas punie par la loi pour avoir publié des informations obtenues de manière légale et sans doute ne pourrait pas l'être. Une distinction fondamentale était faite entre une information reçue d'un lanceur d'alerte et une information que la presse aurait obtenue en sollicitant directement un agent de l'État ou encore par un vol. De même, il était généralement admis qu'il y avait une différence fondamentale entre transmettre des informations à la presse et les transmettre à l'ennemi.

……..
37 18 U.S.C. § 793(e).

De nos jours, tout cela paraît beaucoup moins clair. Chelsea/Bradley Manning a été poursuivi devant un tribunal militaire pour avoir transmis à Wikileaks des milliers de documents classés confidentiels qui furent ensuite mis en ligne sur internet. Durant ce procès, le gouvernement a défendu l'idée selon laquelle transmettre des informations confidentielles à Wikileaks ou au *New York Times* et les donner directement à Al Qaïda revenait bien au même puisque, comme tout un chacun, Al Qaïda pouvait aller sur internet ou lire le *New York Times*[38].

Dans une autre affaire récente, le gouvernement, enquêtant sur des fuites d'informations, avait entamé des démarches pour obtenir un mandat de perquisition contre un journaliste accusé de crime en bande organisée pour avoir simplement fait ce que ces collègues avaient pris l'habitude de faire depuis plusieurs décennies : il avait publié un article contenant des informations confidentielles obtenues d'une de ses sources dont il protégeait l'anonymat[39]. L'idée que le gouvernement pourrait entamer des poursuites pénales contre un journaliste suscita un tel tollé que la procédure fut abandonnée. Cependant, lorsqu'il s'agit d'attaquer des journalistes, l'arsenal du gouvernement ne se limite pas aux poursuites pénales. Les autorités usent de plus en plus souvent de leur pouvoir d'assignation (*subpeona power*) pour forcer des journalistes à révéler leurs sources. En cas de refus, ces derniers peuvent être poursuivis pour outrage à la Cour (*contempt of the court*) et risquer une peine de prison[40].

Enfin de manière tout à fait significative, et contrairement à la décision récente de la Cour Européenne des Droits de l'Homme dans l'affaire *Bucur* [41], aux États-Unis, une source gouvernementale poursuivie pour avoir divulgueréé des informations confidentielles ne peut pas demander au tribunal de jauger si les révélations concernées servent suffisamment l'intérêt général pour compenser les risques pour la sûreté nationale tels que présentés par le gouvernement.

Personne ne demande au gouvernement de rendre publics les noms des individus qu'il surveille. Cependant, dans une démocratie, l'ampleur des pouvoirs de surveillance dont se parent les autorités peut et doit faire l'objet d'un contrôle de la part du public, tout particulièrement lorsqu'elle espionnent leurs propres

……..

38 Ben Wizner, « The Bradley Manning Prosecution Sends an Antidemocratic Message », *The New York Times*, 1er août 2013, en ligne: http://www.nytimes.com/roomfordebate/2013/07/31/ripples-of-the-bradley-manning-verdict/the-bradley-manning-prosecution-sends-an-antidemocratic-message.

39 Tom McCarthy, « James Rosen: Fox News Reporter Targeted as 'Co-Conspirator' in Spying Case », *The Guardian*, 21 mai 2013, en ligne: http://www.theguardian.com/world/2013/may/20/fox-news-reporter-targeted-us- government.

40 cf. Adam Liptak, « Supreme Court Rejects Appeal from Times Reporter over Refusal to Identify Source », *The New York Times*, 2 juin 2014, disponible à: http://www.nytimes.com/2014/06/03/us /james-risen-faces-jail-time-for-refusing-to-identify-a-confidential-source.html .

41 *Bucur and Toma v. Romania*, ECHR, No. 40 238/02 (01/08/ 2013).

citoyens. Pour reprendre l'expression de Louis Brandeis, l'un des plus grands juges de l'histoire de la Cour suprême : « la lumière du soleil est le meilleur des désinfectants ». La NSA agit dans l'ombre depuis trop longtemps.

Texte traduit de l'anglais (américain) par Alix Meyer

☑

Bibliographie indicative

Glen Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York, N.Y., Metropolitan Books (2014).

Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man*, New York, N.Y., Vintage Books (2014).

Adam Liptak, « Supreme Court Rejects Appeal from Times Reporter over Refusal to Identify Source », *The New York Times*, 02/06/2014, en ligne :

http://www.nytimes.com/2014/06/03/us/james-risen-faces-jail-time-for-refusing-to-identify-a-confidential-source.html .

Adam Liptak, « A Secret Surveillance Program Proves Challengeable in Theory Only », *The New York Times*, 15/07/2013 en ligne : http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?hp .

Tom McCarthy, « James Rosen: Fox News Reporter Targeted as 'Co-Conspirator' in Spying Case », *The Guardian*, 21/05/2013, en ligne :

http://www.theguardian.com/world/2013/may/20/fox-news-reporter-targeted-us-government .

Barack H. Obama, Remarks by the President on Review of Signals

Intelligence,17/01/2014, en ligne :

http://www.whitehouse.govthe-press-office/2014/01/17/remarks-president-review-signals-intelligence.

Privacy and Civil Liberties Oversight Board, « Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court », 23/01/2014, en ligne :

http://www.pclob.gov/Library/215-Report_on_the_Telephone_ Records_ Program.pdf .

James Risen, « Lawmakers Question White House Account of an Internet

Surveillance Program », *The New York Times*, 03/07/2013, en ligne :

http://www.nytimes.com/2013/07/04/us/lawmakers-question-white-house-account-of-an-internet-surveillance-program.html .

Patrick C. Toomey, « Government Reverses Course on Wireless Wiretapping in Criminal Case, Admits Duty to Notify Defendants », en ligne :

https://www.aclu.org/blog/national-security/government-reverses-course-warrantless-wiretapping-criminal-case-admits-duty .

President's Review Group on Intelligence and Communications Technologies, « Liberty and Security in a Changing World: Report and Recommendations », 12/12/2013, en ligne :

http://www.whitehouse.gov/ sites/default/files/docs/2013-12-12_rg_final_report.pdf.

The White House, « Fact Sheet: The Administration's Proposal for Ending the Section 215 Bulk Telephony Program », 27/03/2014, en ligne :

http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

Ben Wizner, « The Bradley Manning Prosecution Sends an Antidemocratic

Message », *The New York Times*, 01/08/2013, en ligne :

http://www.nytimes.com/roomfordebate/2013/07/31/ripples-of-the-bradley-manning-verdict/the-bradley-manning-prosecution-sends-an-antidemocratic-message .

U.S. Department of Defense, Office of the Inspector General, *Unclassified Report on the President's Surveillance Program* (2009), en ligne :

http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/report_071309.pdf .

U.S. Senate, *Final Report of the S. Select Comm. To Study Governmental Operations with Respect to Intelligence Activities* (Book II), S. Rep. No. 94-755 (1976), en ligne :

http://www.intelligence.senate.gov/pdfs94th/ 94755_II.pdf.