L'affaire NSA-AT&T
La révélation d'une surveillance massive

Stéphane FOSSE
fosse.fr

19 octobre 2024

Résumé

En 2006, les révélations sur un programme de surveillance électronique massive mené par la NSA en collaboration avec AT&T ont secoué l'opinion publique américaine. Cet article examine les aspects techniques, juridiques et politiques de cette affaire qui a mis en lumière les tensions entre impératifs de sécurité nationale et protection des libertés individuelles à l'ère numérique.

Table des matières

1 La découverte d'un système de surveillance sans précédent

En mai 2006, un article publié dans *USA Today*[1] a bouleversé l'opinion publique américaine : la National Security Agency (NSA) aurait secrètement collecté les relevés d'appels téléphoniques de dizaines de millions d'Américains depuis les attentats du 11 septembre 2001. Cette collecte massive, réalisée sans mandat judiciaire, soulevait alors de graves questions sur le respect de la vie privée des citoyens et les limites du pouvoir exécutif en matière de surveillance intérieure.

Le journal s'appuyait sur des sources anonymes issues du gouvernement et des entreprises concernées. D'après ces témoignages, le programme visait à créer une gigantesque base de données regroupant l'historique des appels de la majorité des Américains. Si le contenu des conversations n'était pas enregistré, les métadonnées recueillies (numéros appelés, durée, etc.) permettaient d'établir des schémas de communication précis.

Ces révélations ont vite été renforcées par d'autres témoignages. L'un des plus marquants fut celui de Mark Klein, ancien technicien d'AT&T[2], qui affirma avoir participé à l'installation d'équipements permettant à la NSA d'accéder directement au réseau de l'opérateur. Il décrivit l'existence d'une mystérieuse **Salle 641A**[3] dans un centre de commutation d'AT&T à San Francisco, spécialement aménagée pour héberger les équipements de surveillance.

1.1 Le témoignage de Mark Klein

Mark Klein, qui avait travaillé chez AT&T pendant plus de 22 ans avant sa retraite en 2004, remarqua des activités suspectes dès 2002 lorsqu'il apprit qu'un agent de la NSA allait venir visiter leurs bureaux. En janvier 2003, lors d'une visite aux installations du bureau de Folsom Street à San Francisco, Klein commença à s'inquiéter d'une salle spéciale en construction au sixième étage.

D'après lui, cette salle contenait un *splitter* optique permettant de dupliquer l'intégralité du trafic Internet transitant par le centre. Ce dispositif renvoyait une copie parfaite du flux de données vers un puissant ordinateur Narus capable d'analyser ce trafic en temps réel. L'accès à cette salle était strictement limité : seul un technicien disposant d'une accréditation de sécurité délivrée par la NSA pouvait y entrer.

Mark Klein décida de révéler ces informations en 2006, après sa retraite, fournissant plus d'une centaine de pages de documents techniques authentifiés à l'Electronic Frontier Foundation[4]. Ces documents détaillaient l'installation et confirmaient que des équipements similaires étaient présents dans d'autres villes américaines, dont Seattle, Los Angeles et San Diego.

Le technicien est décédé le 8 mars 2025 à l'âge de 79 ans, laissant derrière lui un héritage important dans la lutte pour la protection de la vie privée à l'ère numérique.

2 Les implications techniques et juridiques

2.1 L'infrastructure technique de surveillance

Le cœur du dispositif de surveillance décrit par Klein reposait sur des technologies d'interception et d'analyse de données à grande échelle. Le *splitter* optique permettait de dupliquer le signal lumineux transportant les données sans perturber le trafic normal. Cette copie du flux était ensuite analysée par un superordinateur **Narus STA 6400** (Semantic Traffic Analyzer).

Ce système, conçu par la société Narus (rachetée plus tard par Boeing puis Symantec), possédait des capacités d'analyse impressionnantes :

— Traitement jusqu'à 10 Gigabits par seconde (1,25 Go/s) ;

— Inspection profonde des paquets (Deep Packet Inspection) ;

— Analyse sémantique en temps réel du contenu des communications ;

— Filtrage sophistiqué permettant d'identifier les communications présentant un intérêt ;

— Capacité de créer des profils d'utilisateurs basés sur leurs habitudes de navigation.

Cette technologie de surveillance, initialement développée pour aider les fournisseurs d'accès à facturer leurs services et prévenir les pertes de revenus (ce que Narus appelait *revenue leakage*), avait évolué après le 11 septembre 2001 pour intégrer davantage de capacités de surveillance "sémantique".

2.2 Les questions juridiques soulevées

Sur le plan juridique, ce programme de surveillance soulevait de nombreuses interrogations quant à sa conformité avec les lois américaines existantes, notamment :

— Le *Stored Communications Act* (SCA)[5], qui réglemente l'accès aux communications électroniques stockées. La collecte systématique de métadonnées téléphoniques semblait contredire les dispositions du SCA exigeant généralement un mandat pour accéder à ce type d'informations ;

— Le *Wiretap Act*, qui encadre l'interception des communications en temps réel. L'utilisation de *splitters* optiques pour dupliquer l'intégralité du trafic Internet pouvait être considérée comme une forme d'écoute électronique généralisée, potentiellement en violation de cette loi ;

— Le *Pen Register Statute*, qui réglemente l'utilisation de dispositifs permettant d'enregistrer les numéros composés sur une ligne téléphonique. La collecte massive de métadonnées d'appels semblait dépasser largement le cadre prévu par cette loi.

Ces révélations ont rapidement conduit à des actions en justice, dont la plus notable fut l'affaire *Hepting v. AT&T*, intentée par l'Electronic Frontier Foundation au nom de clients d'AT&T. Cette plainte accusait l'opérateur d'avoir violé la vie privée de ses clients en collaborant avec la NSA sans autorisation légale.

3 Les réactions et les tentatives d'étouffement

Face à ces révélations embarrassantes, le gouvernement américain a rapidement tenté de faire obstacle aux poursuites judiciaires en invoquant le « privilège des secrets d'État ». Cette doctrine juridique permet au gouvernement de s'opposer à la divulgation d'informations en justice lorsque cela risquerait de nuire à la sécurité nationale.

Dans l'affaire *Hepting v. AT&T*, le ministère de la Justice est intervenu pour demander le rejet de la plainte, arguant que le simple fait de confirmer ou d'infirmer l'existence du programme de surveillance

constituerait une menace pour la sécurité nationale. Cette stratégie visait à empêcher tout examen judiciaire approfondi de la légalité du programme.

Parallèlement, l'administration Bush a tenté de justifier publiquement l'existence de ce programme de surveillance, le présentant comme un outil indispensable dans la lutte contre le terrorisme. Le président George W. Bush a notamment confirmé l'existence d'un « programme de surveillance terroriste » autorisé après le 11 septembre, tout en insistant sur son caractère ciblé et sa conformité avec la Constitution.

Ces tentatives de justification n'ont cependant pas suffi à apaiser les inquiétudes de nombreux juristes, parlementaires et défenseurs des libertés civiles. Le débat s'est cristallisé autour de la question de l'équilibre entre impératifs de sécurité nationale et protection des libertés individuelles dans un contexte de menace terroriste persistante.

4 Le Protect America Act de 2007

Face à la controverse grandissante et aux incertitudes juridiques entourant les programmes de surveillance de la NSA, le Congrès américain a finalement adopté en août 2007 le *Protect America Act*[6]. Cette loi, présentée comme une mise à jour nécessaire du *Foreign Intelligence Surveillance Act* (FISA) de 1978[7], visait à adapter le cadre légal de la surveillance électronique aux évolutions technologiques.

Les principales dispositions du *Protect America Act* comprenaient :

1. Une redéfinition de la notion de « surveillance électronique » excluant de facto du champ d'application du FISA toute surveillance visant une personne « raisonnablement considérée comme se trouvant hors des États-Unis ». Cette modification permettait à la NSA de surveiller plus facilement les communications internationales transitant par des infrastructures situées sur le sol américain ;
2. L'autorisation donnée au Directeur du Renseignement National et au Procureur Général d'ordonner, sans contrôle judiciaire préalable, la mise sur écoute de toute personne à l'étranger pour une durée pouvant aller jusqu'à un an ;
3. L'obligation pour les opérateurs de télécommunications de coopérer avec les services de renseignement pour la mise en place de ces surveillances, sous peine de sanctions ;
4. Une immunité rétroactive pour les entreprises ayant collaboré avec la NSA dans le cadre de programmes de surveillance antérieurs.

D'un point de vue technique, ces dispositions offraient une grande latitude aux services de renseignement pour déployer des systèmes de collecte et d'analyse de données à grande échelle. La loi permettait notamment l'interception massive de communications internationales transitant par les États-Unis, sans nécessité d'obtenir des autorisations individuelles pour chaque cible.

4.1 Les critiques du Protect America Act

Cette évolution législative a suscité de vives critiques de la part des défenseurs des libertés civiles, qui y voyaient une dangereuse extension des pouvoirs de surveillance de l'exécutif au détriment du contrôle judiciaire. Les partisans de la loi, en revanche, arguaient qu'elle était nécessaire pour adapter le cadre légal aux réalités technologiques du XXI^{e} siècle et aux menaces sécuritaires contemporaines.

Comme le raconta Mark Klein dans une interview accordée à PBS en 2007[8], sa motivation pour devenir lanceur d'alerte venait en partie de son expérience des années 1960 et des manifestations contre la guerre du Vietnam : « Je vois tout cela se reproduire, mais en pire. Quand la NSA s'est fait prendre dans les années 70 à faire de l'espionnage intérieur, c'était un grand scandale, et c'est pourquoi le Congrès a adopté la loi FISA... pour supposément régler ce problème. »

Il ajouta : « Une loi n'a de valeur que s'il existe une mémoire permettant aux gens de dire : 'Attendez une minute. Cela s'est déjà produit.' Et il faut s'avancer et dire : 'Je m'en souviens.' »

5 L'héritage de l'affaire NSA-AT&T

L'affaire NSA-AT&T de 2006 et les évolutions législatives qui ont suivi ont marqué l'histoire de la surveillance électronique aux États-Unis. Elles ont mis en lumière les tensions entre impératifs de sécurité nationale et protection des libertés individuelles à l'ère du numérique, soulevant des questions fondamentales sur les limites du pouvoir exécutif et le rôle du contrôle judiciaire dans un contexte de menace terroriste.

Si le *Protect America Act* visait à clarifier le cadre légal de la surveillance électronique, il n'a pas mis fin aux controverses. Les révélations ultérieures d'Edward Snowden en 2013 sur les programmes PRISM et XKeyscore ont montré que la NSA avait continué à développer des capacités de surveillance massive allant bien au-delà de ce que le public et même de nombreux parlementaires imaginaient.

Ces nouvelles révélations ont relancé le débat sur la nécessité d'un encadrement plus strict des activités de renseignement à l'ère numérique, illustrant les défis persistants posés par l'équilibre entre sécurité et liberté dans nos sociétés hyperconnectées.

Le décès récent de Mark Klein en mars 2025 a rappelé l'importance de son témoignage. Sept ans avant Edward Snowden, il avait tenté d'alerter sur les programmes de surveillance massive de la NSA. Son action

courageuse, même si elle n'a pas reçu la même attention médiatique que celle de Snowden, reste une contribution majeure à la compréhension de l'évolution des capacités de surveillance gouvernementale à l'ère numérique.

6 Conclusion

L'affaire NSA-AT&T a révélé l'existence d'infrastructures techniques permettant une surveillance sans précédent des communications numériques et soulevé des questions essentielles sur l'équilibre entre sécurité nationale et libertés individuelles.

L'évolution de la législation américaine suite à ces révélations illustre les difficultés à encadrer juridiquement des technologies de surveillance en constante évolution. Le *Protect America Act* de 2007, loin de résoudre ces tensions, a plutôt confirmé une tendance à l'expansion des pouvoirs de surveillance au nom de la lutte contre le terrorisme.

Les questions soulevées par cette affaire restent d'actualité. À l'heure où les technologies de surveillance deviennent toujours plus sophistiquées et omniprésentes, le témoignage de lanceurs d'alerte comme Mark Klein permet de garantir la transparence et le débat démocratique sur ces enjeux fondamentaux.

Références

[1] L. Cauley, NSA has massive database of Americans' phone calls, *USA Today*, 11 mai 2006.

[2] Z. Farooqui, Mark Klein, AT&T technician who helped expose NSA spying, dies at 79, *The Washington Post*, 14 mars 2025.

[3] S. R. Farber et W. E. Forsyth, « The NSA, AT&T, and the Secrets of Room 641A, » SSRN, rapp. tech., 2023.

[4] Electronic Frontier Foundation, In Memoriam: Mark Klein, AT&T Whistleblower Who Revealed NSA Mass Spying, Electronic Frontier Foundation, 12 mars 2025.

[5] M. Detrich, The Stored Communications Act (SCA) Explained - Minc Law, sept. 2024.

[6] A. C. L. Union, ACLU Fact Sheet on the "Police America Act" | American Civil Liberties Union — aclu.org, 2007.

[7] B. of Justice Assistance, The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance — bja.ojp.gov.

[8] PBS Frontline, Interviews - Mark Klein, Spying on the Home Front, PBS, 9 jan. 2007.

[9] C. Osborne, AT&T technician Mark Klein, who exposed secret NSA spying, dies, *TechCrunch*, 14 mars 2025.

[10] K. Crockford, NARUS, deep packet inspection and the NSA, Privacy SOS, 13 juin 2013.

[11] M. Klein, Wiring Up the Big Brother Machine... And Fighting It. BookSurge Publishing, 2009, isbn : 9781439229019.

[12] J. Bamford, The Shadow Factory : The NSA from 9/11 to the Eavesdropping on America. New York : Doubleday, 2008, isbn : 9780385521321.