L'affaire PRISM

Stéphane FOSSE
fosse.fr

3 juin 2024

Introduction

Le 6 juin 2013, les lecteurs du *Guardian* et du *Washington Post* découvrent une réalité qu'ils pouvaient jusqu'alors seulement soupçonner. Les deux journaux publient des documents classifiés qui révèlent l'existence d'un vaste programme de surveillance mené par la National Security Agency (NSA) américaine. Son nom : **PRISM**. Un acronyme qui résonne encore aujourd'hui comme un tournant majeur pour la vie privée et la sécurité nationale à l'ère numérique.

Après les attentats du 11 septembre 2001, les États-Unis, traumatisés, ont bouleversé leur doctrine sécuritaire. Cette date marque l'entrée du pays dans une nouvelle ère où la collecte massive de renseignements devient une priorité absolue. Dans cette configuration inédite, internet, devenu omniprésent, se transforme en terrain de surveillance privilégié.

La divulgation par Edward Snowden de l'existence de programmes tels que PRISM et XKeyscore a projeté sur la place publique une réalité jusqu'alors confidentielle, celle d'une surveillance électronique mondiale d'une ampleur sans précédent. Ces révélations ont soulevé des questions essentielles sur l'équilibre fragile entre impératifs de sécurité nationale et droits fondamentaux des citoyens.

Entre obscurité et transparence, entre pouvoir et contre-pouvoir, le cas PRISM illustre avec acuité les tensions qui traversent nos sociétés connectées au XXI^{e} siècle. Au cœur de cet enjeu se trouve la question cruciale : une démocratie peut-elle concilier efficacité sécuritaire et respect des libertés individuelles ?

1 Edward Snowden : de l'ombre à la lumière

Le 9 juin 2013, un visage inconnu s'affiche sur les écrans du monde entier. Edward Joseph Snowden, né le 21 juin 1983 à Elizabeth City en Caroline du Nord, vient de révéler l'un des secrets les mieux gardés des États-Unis. Ancien informaticien pour la CIA puis sous-traitant pour la NSA, ce jeune homme de 29 ans avait accès aux programmes les plus confidentiels du renseignement américain [1]. Son parcours, atypique et singulier, mérite qu'on s'y attarde pour mieux saisir la portée des documents qu'il a choisi de divulguer.

Snowden n'a jamais achevé ses études secondaires. Passionné d'informatique depuis son enfance, il s'engage dans l'armée américaine en 2003, dans un programme de formation des Forces spéciales. Une blessure aux jambes durant l'entraînement met fin à cette carrière militaire à peine entamée. Il trouve alors un emploi comme agent de sécurité dans un établissement secret de la CIA au Maryland, avant d'évoluer vers un poste en sécurité informatique [2].

Son expertise technique et son habilitation de sécurité lui ouvrent les portes de postes à responsabilité croissante. En 2007, la CIA l'envoie à Genève sous couverture diplomatique. Puis il devient consultant pour Dell en 2009, où il travaille sur des contrats NSA. En 2013, il rejoint Booz Allen Hamilton, autre sous-traitant majeur du renseignement américain, qui l'affecte à Hawaï dans une unité de la NSA. C'est là qu'il accède aux documents qui bouleverseront sa vie et ébranleront la confiance mondiale dans les services secrets américains.

Dans une interview au *Guardian*, Snowden livre ses motivations : « Je ne veux pas vivre dans un monde où tout ce que je fais et dis est enregistré. Ce n'est pas un monde que je suis prêt à cautionner » [2]. Cette phrase résume la conviction profonde qui l'a poussé à risquer sa liberté et sa sécurité.

Le choix de Hong Kong comme première destination de son exil n'est pas dû au hasard. Territoire semi-autonome, doté d'une tradition de liberté d'expression, Hong Kong lui permet de rencontrer les journalistes Glenn Greenwald et Laura Poitras pour leur transmettre des milliers de documents confidentiels. Leur premier rendez-vous, dans un centre commercial près de l'hôtel Mira, a quelque chose de romanesque : Snowden devait tenir un Rubik's Cube à la main pour être identifié [3].

La publication des premiers articles déclenche une onde de choc internationale. Les autorités américaines identifient rapidement Snowden comme la source des fuites. Le Département de la Justice dépose des accusations pour espionnage et vol de propriété gouvernementale. Contraint de fuir, il quitte Hong Kong pour Moscou, où il restera bloqué à l'aéroport pendant plusieurs semaines, son passeport ayant été annulé par les États-Unis [3].

Le 31 juillet 2013, la Russie lui accorde finalement l'asile temporaire, qui sera transformé en permis de résidence de trois ans en 2014. Cette décision russe provoque une crise diplomatique avec Washington. En 2022, le président Vladimir Poutine lui octroie la nationalité russe par décret, actualisant encore le statut de cet exilé hors du commun [3].

L'impact de son geste dépasse largement sa personne. En 2014, l'édition américaine du *Guardian* et le *Washington Post* se voient décerner le prix Pulitzer pour la publication des révélations de Snowden, consacrant l'importance journalistique de cette affaire. Au-delà des récompenses, c'est la conscience publique qui a été durablement transformée par cette mise en lumière des pratiques de surveillance massives.

Aujourd'hui, Snowden reste une figure polarisante. Traître pour certains, héros pour d'autres, il incarne le dilemme moral entre loyauté institutionnelle et alerte éthique. Son cas soulève une question essentielle : où placer la frontière entre secret d'État nécessaire et droit du public à l'information quand les libertés fondamentales semblent menacées ?

2 PRISM : anatomie d'un système de surveillance

PRISM (Planning Tool for Resource Integration, Synchronization, and Management) est un dispositif complexe déployé par la NSA à partir de 2007 pour collecter et analyser des données de communication électronique à grande échelle. Son fonctionnement, révélé par les documents de Snowden, montre un accès privilégié aux données des géants américains du numérique [1].

Le cœur du programme repose sur une collaboration, volontaire ou contrainte, avec neuf entreprises technologiques américaines majeures : Microsoft (depuis 2007), Yahoo (2008), Google (2009), Facebook (2009), PalTalk (2009), YouTube (2010), AOL (2011), Skype (2011) et Apple (2012). Ces entreprises auraient fourni un accès direct à leurs serveurs, permettant à la NSA de collecter divers types de données : emails, discussions instantanées, vidéos, photos, fichiers stockés, détails de connexion, voire appels audio et vidéo.

La NSA affirme que PRISM ciblait uniquement les communications impliquant des individus non-américains situés à l'étranger. Mais les documents révélés suggèrent que le système captait aussi, « incidemment », des communications d'Américains. Cette collecte indiscriminée constitue l'un des aspects les plus controversés du programme.

Techniquement, PRISM fonctionnait par requêtes spécifiques envoyées aux entreprises, accompagnées de directives précisant les informations requises. Une fois obtenues, ces données étaient intégrées dans une base centralisée de la NSA, consultable par des analystes autorisés, permettant une surveillance en temps réel ou presque.

Les présentations PowerPoint divulguées par Snowden indiquent que PRISM collectait directement « à partir des serveurs » des entreprises concernées. Cette formulation a suscité des débats : s'agissait-il d'un accès automatisé aux données ou d'un processus plus contrôlé ? Les entreprises ont vigoureusement nié avoir accordé un accès direct et sans filtrage à leurs serveurs, affirmant qu'elles ne répondaient qu'à des demandes légales spécifiques [4].

La NSA soutenait que plusieurs niveaux de supervision étaient en place pour éviter les abus. Mais les critiques soulignaient le manque de transparence et les risques d'intrusion dans la vie privée. Les juges de la cour FISA, censés superviser ce programme, n'avaient qu'une vision limitée de son fonctionnement réel.

Au fil du temps, PRISM est devenu l'une des sources les plus importantes de renseignements pour la NSA. Selon les documents divulgués, il aurait fourni environ 91% des informations obtenues sur internet concernant des « cibles terroristes étrangères ». Ce chiffre révèle l'ampleur et l'efficacité perçue du programme aux yeux des services de renseignement.

Le programme PRISM partageait des informations avec d'autres services de renseignement, notamment britanniques, canadiens, australiens et néo-zélandais (les « Five Eyes »). Des documents ultérieurs ont même révélé que des agences françaises et allemandes y avaient aussi accès, malgré les protestations publiques de leurs gouvernements respectifs [5].

L'analyse technique de PRISM révèle une sophistication impressionnante dans sa conception. Le système permettait des recherches ciblées par mots-clés, métadonnées ou caractéristiques spécifiques. Cette puissance analytique, couplée à d'autres programmes comme XKeyscore, offrait aux analystes une capacité sans précédent à suivre et profiler des individus à travers leurs activités numériques.

PRISM illustre l'évolution des méthodes de renseignement à l'ère numérique, où la collecte massive de données remplace progressivement les méthodes traditionnelles de surveillance ciblée. Cette industrialisation de la surveillance soulève des questions sur la proportionnalité et la nécessité de tels moyens dans une société démocratique.

3 Cadre juridique et zones d'ombre

La légalité du programme PRISM repose principalement sur la section 702 du Foreign Intelligence Surveillance Act (FISA), ajoutée par les amendements de 2008. Cette disposition autorise la surveillance des communications électroniques de personnes non américaines situées à l'étranger, sans nécessiter un mandat spécifique pour chaque cible.

La section 702 a mis en place un système de supervision différent des procédures traditionnelles. Plutôt que d'exiger des mandats individuels, elle permet à la NSA d'obtenir une autorisation annuelle de la Foreign Intelligence Surveillance Court (FISC) pour ses programmes de collecte. Cette autorisation globale constitue un changement significatif par rapport aux principes antérieurs du FISA, qui exigeaient des approbations au cas par cas [6].

Les entreprises technologiques seraient légalement obligées de fournir des données en réponse aux ordres émis sous l'autorité de la section 702. En théorie, ce processus comporte des garde-fous : les requêtes doivent viser des renseignements étrangers significatifs et ne peuvent « intentionnellement » cibler des Américains [4].

Dans la pratique, les zones d'ombre et les ambiguïtés juridiques sont nombreuses. L'une des principales préoccupations concerne la collecte « par accident » de communications d'Américains en contact avec des cibles étrangères. Ces communications peuvent être conservées et consultées sans mandat supplémentaire, créant une faille dans les protections constitutionnelles.

La question de la juridiction territoriale pose également problème. Internet ne connaît pas de frontières claires, et les données circulent mondialement. Les serveurs de nombreuses entreprises américaines stockent des informations relatives à des utilisateurs du monde entier. PRISM exploite cette réalité technique pour accéder à des données globales, soulevant des questions sur la souveraineté numérique et les droits des non-Américains.

Le fonctionnement secret de la FISC a fait l'objet de critiques sévères. Cette cour spécialisée opère à huis clos, sans procédure contradictoire. Entre 1979 et 2012, elle aurait rejeté seulement 11 demandes sur plus de 33 900, soulevant des doutes sur l'efficacité de ce contrôle judiciaire [7].

En janvier 2025, un développement significatif est survenu quand un tribunal fédéral a estimé que les recherches sans mandat dans les bases de données de la section 702 violaient le Quatrième Amendement de la Constitution américaine, qui protège contre les perquisitions et saisies déraisonnables [8]. Cette décision a concerné le cas d'Agron Hasbajrami, un résident américain accusé de soutien au terrorisme, dont les communications avaient été interceptées via la section 702 [9].

Le tribunal a rejeté l'argument du gouvernement selon lequel une « exception de renseignement étranger » justifierait ces recherches sans mandat. Le juge a statué que « l'intérêt public seul ne justifie pas des recherches sans mandat » [9], remettant en question une pratique établie depuis des années. Cette jurisprudence pourrait avoir des implications majeures lors du prochain renouvellement de la section 702, prévu pour 2026.

Au niveau international, le cadre juridique est encore plus flou. La surveillance transfrontalière échappe largement aux traités existants. Les révélations sur PRISM ont montré que certains pays européens, tout en condamnant publiquement ces pratiques, bénéficiaient des renseignements obtenus ou menaient des programmes similaires.

L'Union européenne a réagi en renforçant sa législation sur la protection des données, aboutissant au Règlement général sur la protection des données (RGPD) en 2016. Ce texte ambitieux peut être vu comme une réponse directe aux révélations de Snowden, cherchant à redonner aux citoyens européens un contrôle sur leurs données personnelles.

L'affaire Schrems II en 2020 illustre les tensions persistantes entre les régimes juridiques américain et européen. La Cour de justice de l'Union européenne a invalidé le *Privacy Shield*, mécanisme qui facilitait les transferts de données vers les États-Unis, jugeant insuffisantes les protections contre la surveillance gouvernementale américaine.

Ces développements montrent que le débat juridique ouvert par les révélations sur PRISM reste vivace et continue d'évoluer, remodelant progressivement l'équilibre entre sécurité nationale et droits fondamentaux dans le monde numérique.

4 Répercussions et héritage

L'affaire PRISM a provoqué des ondes de choc dans presque tous les secteurs de la société, redéfinissant notre rapport à la vie privée et à la sécurité numérique. L'impact s'est fait sentir sur le plan diplomatique, juridique, économique et sociétal, créant un « avant » et un « après Snowden » dans notre conscience collective.

Sur le plan diplomatique, les révélations ont détérioré les relations entre les États-Unis et plusieurs alliés. Quand il est apparu que la NSA avait espionné les communications personnelles de dirigeants comme Angela Merkel, chancelière allemande, la confiance s'est érodée. Le Brésil et l'Allemagne ont porté la question devant les Nations Unies, appelant à de nouvelles normes internationales pour encadrer la surveillance numérique [5].

Pour les géants américains de la technologie, l'impact a été double. D'une part, leur réputation a souffert de leur apparent manque de protection des données utilisateurs. D'autre part, ils ont subi des pertes économiques estimées entre 35 et 180 milliards de dollars sur trois ans, selon le *New America Foundation*. Des entreprises comme Cisco, dont les équipements présentaient des *backdoors*[10], ont vu leurs ventes chuter dans certains marchés internationaux, particulièrement en Chine, où la méfiance envers les technologies américaines s'est accentuée.

Face à cette crise, l'industrie technologique a réagi par une adoption plus large du chiffrement. Google, Apple et d'autres ont intensifié leurs efforts pour protéger les données des utilisateurs, y compris contre l'accès gouvernemental. Le chiffrement de bout en bout est devenu un argument marketing et une nécessité technique, illustrant un changement dans l'équilibre des pouvoirs entre entreprises privées et agences gouvernementales.

Aux États-Unis, l'administration Obama a dû réagir aux critiques croissantes. En janvier 2014, le président a annoncé des réformes modestes, dont une plus grande transparence et des limitations sur la collecte de métadonnées téléphoniques. Le USA Freedom Act de 2015 a formellement mis fin à la collecte massive de relevés téléphoniques, bien que des programmes de surveillance significatifs aient perduré sous d'autres formes.

Au niveau législatif global, l'héritage de PRISM se manifeste dans des textes comme le RGPD européen, qui a refondu l'approche réglementaire des données personnelles. Cette influence s'étend désormais à d'autres régions, avec la Californie, le Brésil ou l'Inde adoptant des législations inspirées du modèle européen.

Pour les citoyens ordinaires, les révélations ont transformé la perception de leur vulnérabilité numérique. Une enquête Pew Research de 2015 montrait que 52% des Américains se disaient « très préoccupés » par la surveillance gouvernementale, contre 33% avant les révélations. Cette prise de conscience a stimulé l'adoption d'outils de protection de la vie privée comme les réseaux privés virtuels (VPN), les messageries chiffrées ou les navigateurs axés sur la confidentialité.

Les mouvements de défense des libertés civiles ont gagné en influence. Des organisations comme l'Electronic Frontier Foundation (EFF) ou l'American Civil Liberties Union (ACLU) ont vu leur audience et leurs ressources augmenter. La question de la surveillance numérique est passée d'un sujet de niche à un enjeu politique majeur, débattu lors des campagnes présidentielles et législatives.

Dans le monde universitaire et intellectuel, l'affaire a stimulé une réflexion profonde sur les implications éthiques de la surveillance de masse. Des philosophes comme Giorgio Agamben ont analysé le passage d'un « État de droit » à un « État de sécurité », où l'exception devient la règle. Cette réflexion nourrit un débat essentiel sur les valeurs fondamentales de nos démocraties à l'ère numérique.

L'un des héritages les plus durables de l'affaire PRISM réside dans la sensibilisation du grand public. Avant 2013, peu de personnes comprenaient l'ampleur de la collecte de données numériques. Après les révélations, des termes comme « métadonnées », « chiffrement » ou « surveillance de masse » sont entrés dans le vocabulaire courant, révélant une prise de conscience collective des enjeux numériques.

Dix ans après, l'équilibre entre sécurité nationale et vie privée reste fragile. D'un côté, les agences de renseignement soulignent la menace persistante du terrorisme et des cyberattaques. De l'autre, les défenseurs des libertés civiles rappellent que la surveillance préventive et indiscriminée menace les fondements mêmes de la démocratie. Ce dialogue tendu mais nécessaire constitue peut-être l'héritage le plus important de l'affaire PRISM.

5 Conclusion

L'affaire PRISM a marqué notre relation au numérique. Au-delà des aspects techniques et juridiques, elle nous confronte à des questions fondamentales sur le type de société que nous souhaitons construire à l'ère digitale. Que sommes-nous prêts à sacrifier au nom de la sécurité ? Quelle valeur accordons-nous réellement à notre vie privée ? Comment concilier innovation technologique et protection des droits fondamentaux ?

Les révélations d'Edward Snowden ont déchiré le voile d'opacité qui entourait les pratiques de surveillance numérique. Cette transparence forcée a permis l'émergence d'un débat public informé, première étape indispensable vers des choix démocratiques sur ces enjeux. Si l'équilibre idéal entre sécurité et liberté reste à trouver, la conscience collective des risques et des opportunités du monde connecté s'est considérablement affinée.

Dans la lignée des grands lanceurs d'alerte de l'histoire, Snowden nous rappelle le rôle essentiel du contre-pouvoir dans les démocraties modernes. Son parcours singulier illustre le dilemme moral qui traverse chaque citoyen face à un système qui semble s'éloigner de ses valeurs proclamées. Sa décision controversée de révéler ces informations nous oblige à réfléchir à notre propre responsabilité face aux dérives potentielles des institutions.

L'avenir des questions soulevées par PRISM reste ouvert. D'un côté, les capacités techniques de surveillance continuent de s'étendre, avec l'intelligence artificielle et l'internet des objets créant de nouvelles possibilités de collecte et d'analyse de données. De l'autre, une conscience accrue des enjeux pousse vers un renforcement des protections juridiques et techniques de la vie privée.

Dans cette tension permanente, chaque citoyen, chaque entreprise, chaque gouvernement est appelé à prendre position et à contribuer à façonner un avenir numérique qui préserve à la fois notre sécurité collective et nos

libertés individuelles. Cet équilibre fragile, constamment à reconstruire, constitue l'un des plus grands défis démocratiques du XXI^{e} siècle.

Références

[1] G. Greenwald et E. MacAskill, NSA Prism program taps in to user data of Apple, Google and others, *The Guardian*, juin 2013, Consulté le 5 mai 2025.

[2] M. J. Schwartz, 9 Facts About NSA Prism Whistleblower, *Dark Reading*, juin 2013, Consulté le 5 mai 2025.

[3] Wikipedia, Edward Snowden, *Wikipédia*, avr. 2025, Consulté le 5 mai 2025.

[4] B. Gellman et A. Soltani, Here's everything we know about PRISM to date, *The Washington Post*, juin 2013, Consulté le 5 mai 2025.

[5] L'Usine Digitale, Best-of 2013 : les révélations d'Edward Snowden, *L'Usine Digitale*, déc. 2013, Consulté le 5 mai 2025.

[6] Office of the Director of National Intelligence, Section 702 Basics, *Office of the Director of National Intelligence*, sept. 2017, Consulté le 5 mai 2025.

[7] Electronic Frontier Foundation, EFF Urges Supreme Court to Take On Unconstitutional NSA Surveillance, *Electronic Frontier Foundation*, août 2017, Consulté le 5 mai 2025.

[8] American Civil Liberties Union, Court Rules Warrantless Section 702 Searches Violated the Fourth Amendment, *American Civil Liberties Union*, jan. 2025, Consulté le 5 mai 2025.

[9] J. Oates, Court rules FISA Section 702 surveillance unconstitutional, *The Register*, jan. 2025, Consulté le 5 mai 2025.

[10] L. Armasu, Backdoors Keep Appearing In Cisco's Routers — tomshardware.com, [Accessed 06-05-2025], juill. 2018.

[11] A. Crocker et M. Guariglia, VICTORY! Federal Court (Finally) Rules Backdoor Searches of 702 Data Unconstitutional, *Electronic Frontier Foundation*, jan. 2025, Consulté le 5 mai 2025.