L'Affaire XKeyscore : le symbole de la surveillance de masse

Stéphane FOSSE
fosse.fr

17 juin 2024

Le 31 juillet 2013, le journal britannique *The Guardian* publiait un article retentissant qui allait ébranler notre conception de la vie privée numérique. En s'appuyant sur des documents confidentiels fournis par Edward Snowden, il révélait l'existence d'un programme de surveillance mondial baptisé **XKeyscore**. Cette opération tentaculaire, moins médiatisée que le programme PRISM mais tout aussi invasive, conférait à la NSA un pouvoir de surveillance quasi illimité sur les communications électroniques mondiales.

Dépeint comme le « Google de la NSA », XKeyscore étaitun outil de collecte qui transformait la NSA en une sorte de divinité omnisciente du web. Les analystes pouvaient, sans autorisation judiciaire préalable, plonger dans d'immenses réservoirs de données : courriels, discussions instantanées, historiques de navigation et métadonnées diverses. Le système aspirait ces informations en temps réel via des serveurs stratégiquement répartis sur toute la planète. Plus alarmant encore, il conservait ces données pendant des jours, parfois des semaines, y compris des éléments sans rapport direct avec la sécurité nationale.

Ce dispositif déployait ses tentacules grâce à plus de 700 serveurs disséminés dans environ 150 sites à travers le monde, des États-Unis à la Chine en passant par la Russie et l'Inde. Cette gigantesque toile d'araignée numérique captait jusqu'à 20 téraoctets de données quotidiennement sur certains sites, un volume si colossal qu'il ne pouvait être stocké que pendant 24 heures. Seules les informations jugées pertinentes étaient ensuite conservées pour une durée pouvant atteindre cinq ans.

La véritable prouesse technique de XKeyscore résidait dans sa capacité à intercepter le trafic transitant par les câbles internet sous-marins, ces autoroutes de l'information qui constituent l'épine dorsale d'Internet. Cette méthode d'espionnage, réalisée en collaboration avec les services de renseignement britanniques, canadiens, australiens et néo-zélandais – le fameux groupe des « Five Eyes » – contournait toute restriction légale. L'interface utilisateur du programme, d'une simplicité déconcertante, permettait à n'importe quel analyste formé d'effectuer des recherches dans cette masse de données par simple requête, comme on le ferait sur un moteur de recherche ordinaire.

Aux États-Unis, ces révélations ont ravivé les discussions sur la section 702 du Foreign Intelligence Surveillance Act (FISA), cadre légal qui autorisait officiellement la surveillance des étrangers hors territoire américain. Bien que théoriquement limitée aux non-Américains, cette disposition permettait également de collecter « accidentellement » des données concernant des citoyens américains, soulevant de sérieuses questions constitutionnelles. L'American Civil Liberties Union (ACLU) n'a pas tardé à contester la légalité de ces pratiques devant les tribunaux.

La découverte que la NSA espionnait non seulement les citoyens, mais aussi les dirigeants de pays alliés, a déclenché une tempête diplomatique sans précédent. Le Brésil et l'Allemagne, particulièrement indignés, ont exigé des réformes pour encadrer la surveillance transfrontalière. Des nations ont remis en question leurs accords de partage d'informations avec Washington et renforcé leur propre sécurité numérique. L'Union européenne a fait de la protection des données un sujet central de ses négociations commerciales avec les États-Unis.

Au niveau national américain, le mouvement de réforme s'est accéléré. Des propositions ont émergé pour améliorer la transparence et le contrôle de ces programmes d'espionnage électronique. Un appel à rééquilibrer sécurité collective et respect des libertés individuelles s'est élevé, porté par un front composé d'organisations citoyennes, de spécialistes des technologies et de défenseurs des droits humains.

Sous la pression populaire, le Congrès américain a finalement voté en 2015 le USA FREEDOM Act. Cette loi a mis un terme à la collecte massive et systématique des métadonnées téléphoniques des Américains par la NSA. Elle a introduit l'obligation d'obtenir l'autorisation de la Cour FISA pour accéder aux données et transféré leur stockage aux opérateurs téléphoniques. La transparence a été renforcée avec la publication obligatoire de rapports détaillés sur les activités de surveillance. Néanmoins, ces réformes ont été jugées insuffisantes par de nombreux défenseurs des libertés, qui réclamaient des garde-fous plus stricts et plus contraignants.

Le USA FREEDOM Act présentait en effet deux principales mesures : transférer le stockage des données aux entreprises de télécommunications, avec accès uniquement sur décision de justice, et autoriser la NSA à traquer les suspects considérés comme des « loups solitaires ». Si ce texte représentait une avancée symbolique,

il a été critiqué pour son caractère trop limité. L'Electronic Frontier Foundation (EFF) a notamment relevé que la loi n'abordait pas la surveillance massive menée sous la section 702 du FISA, utilisée pour collecter les communications des utilisateurs du monde entier.

En Europe, les révélations de Snowden ont catalysé l'adoption du Règlement Général sur la Protection des Données (RGPD) en 2016. Cette réglementation ambitieuse, mise en application en mai 2018, visait à redonner aux citoyens le contrôle de leurs données personnelles tout en simplifiant l'environnement réglementaire des entreprises. Sans le séisme provoqué par Snowden, ce texte aurait probablement mis bien plus de temps à voir le jour. Le G29, devenu depuis le Comité européen de la protection des données, avait d'ailleurs souligné dès 2014 l'illégalité de la surveillance massive et systématique des citoyens européens, qui ne pouvait être justifiée par la seule lutte contre le terrorisme.

Les géants technologiques américains, éclaboussés par leur collaboration présumée avec la NSA, ont dû réagir pour regagner la confiance de leurs utilisateurs. Ils ont nié avoir accordé un accès direct à leurs serveurs et multiplié les promesses de transparence. Pour restaurer leur crédibilité, ces entreprises ont généralisé le chiffrement des communications et durci leurs protocoles internes. Par l'intermédiaire de leurs lobbies, elles ont plaidé en faveur d'une réforme des lois sur la surveillance, tout en restant soumises aux pressions gouvernementales. Ces révélations ont néanmoins affecté leur réputation à l'international, alimentant la méfiance envers les technologies américaines et encourageant le développement de solutions alternatives en Europe et en Asie.

L'opinion publique, jusque-là largement ignorante de l'ampleur de cette surveillance, a connu un brutal réveil. Les citoyens se sont davantage sensibilisés aux méthodes de protection de leur vie numérique. Des organisations comme l'EFF ont vu leur audience croître, tandis qu'une coordination mondiale des défenseurs des libertés s'organisait pour réguler la surveillance de masse. La question est devenue un enjeu électoral dans plusieurs démocraties, forçant les responsables politiques à se positionner.

Malgré ces avancées, le dilemme entre sécurité collective et libertés individuelles reste entier. Avec la multiplication des objets connectés et l'avènement de l'intelligence artificielle, de nouveaux défis émergent, nécessitant une actualisation permanente du cadre juridique et éthique. L'affaire **XKeyscore**, par son ampleur et ses ramifications, reste emblématique de la vigilance nécessaire pour préserver nos vies privées dans l'ère numérique.

Dans cette bataille, certains acteurs majeurs ont pris des mesures concrètes. Jimmy Wales, cofondateur de Wikipédia, a annoncé dès août 2013 un renforcement de la sécurité de l'encyclopédie collaborative avec l'activation par défaut du protocole HTTPS. Facebook a généralisé la connexion sécurisée de ses utilisateurs à la même période. Google a commencé à prioriser les sites web en HTTPS à partir de 2015. Ces initiatives ont constitué les premières réponses techniques au problème soulevé par les révélations sur XKeyscore.

Cette affaire a aussi provoqué un changement de positionnement des géants du numérique vis-à-vis du gouvernement américain. Face aux critiques concernant leur coopération avec la NSA, certaines entreprises ont manifesté une volonté accrue de résister aux demandes des autorités. Le refus d'Apple d'accorder au FBI l'accès à ses données téléphoniques en 2016 illustre cette nouvelle posture.

Pour l'avenir de nos sociétés démocratiques, l'affaire XKeyscore nous rappelle que la vigilance citoyenne reste le meilleur rempart contre les dérives sécuritaires. L'équilibre fragile entre protection collective et respect des libertés individuelles ne sera préservé que par un débat permanent et une transparence accrue des pouvoirs publics. Le combat est loin d'être gagné, mais la prise de conscience mondiale déclenchée par Edward Snowden constitue déjà une victoire essentielle pour la défense de nos droits fondamentaux.

Références

[1] G. Greenwald, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', *The Guardian*, juill. 2013.

[2] France24, XKeyscore, le meilleur outil de la NSA pour surveiller Internet, *France 24*, juill. 2013.

[3] Le Programme XKeyScore, Edward Snowden face à la NSA, mars 2016.

[4] XKeyscore, l'autre programme d'espionnage informatique des renseignements américains, *L'Usine Digitale*, avr. 2015.

[5] AFP, US: XKeyscore, un programme de surveillance d'internet encore plus intrusif, *ArcInfo*, août 2013.

[6] La NSA, de XKeyscore à PRISM, *Radio-Canada*, août 2013.

[7] XKeyscore, le logiciel anti cyber criminalité de la NSA, *Le VPN*, fév. 2021.

[8] O. Peguy, Surveillance : ce qui change avec le "USA Freedom act", *Euronews*, juin 2015.

[9] NSA : le Freedom Act adopté et promulgué après moult remous aux États-Unis, *Euronews*, juin 2015.

[10] Le Sénat américain adopte une réforme symbolique des pouvoirs de la NSA, *Le Temps*, juin 2015.

[11] Elodie, Le Sénat vote l'USA Freedom Act et réforme (un peu) la NSA, *Journal du Geek*, juin 2015.

[12] P. Martin, L'USA Freedom Act : un cache-sexe pour l'espionnage illégal, *World Socialist Web Site*, 2015.

[13] H. Bernard, Edward Snowden : les conséquences de ses révélations sur la surveillance de masse par les États-Unis, *Rotek*, nov. 2021.

[14] Affaire PRISM : avis du G29 sur la surveillance massive des citoyens européens, *CNIL*, jan. 2016.

[15] A. Zitouni, La petite histoire du RGPD, du minitel à Edward Snowden, *Indexel*, mars 2020.

[16] É. D. D. L. Riviére, Impact des révélations de Snowden : comprendre les conséquences sur la surveillance, *Secret Defense*, juin 2024.

[17] D. Lyon, La surveillance globale dans un monde post-Snowden, *Communiquer*, n° 20, p. 49-65, sept. 2017.

[18] Surveillance de masse: les droits des citoyens de l'UE encore en danger, *Parlement européen*, oct. 2015.

[19] E. Snowden, Mémoires vives. Editions du Seuil, 2019, Autobiographie.