L'affaire Snowden, une rupture stratégique : ces données personnelles qui constituent la mémoire vivante de la NSA

Le déroulement du scandale ainsi que les données révélées par Edward Snowden sont décortiqués et analysés dans ce livre. Il permet de mieux comprendre le bouleversement stratégique que cet ancien sous-traitant de la NSA a déclenché au nom de la défense des libertés individuelles. Extrait de "L'affaire Snowden, une rupture stratégique", de Quentin Michaud et Olivier Kempf, publié chez Economica (1/2).

Avec Quentin Michaud
Avec Olivier Kempf

PRISM, la cheville ouvrière

En physique, le prisme est un bloc de verre taillé de façon à difracter la lumière d'une certaine manière. PRISM agit avec la même logique. Lorsque l'accord est donné par l'unité *Targeting and Mission Management* (S343) pour aspirer un flux de données, PRISM opère de façon automatisée. Un logiciel Pintaura autogère cette opération en accordant des codes (P1, P2, P3) pour chaque support depuis lequel la donnée est extraite, respectivement *Facebook*, *Microsoft* et *Google*. Un logiciel *Unified Targeting Tool* agit ensuite comme un moteur de recherche pour rechercher un élément précis dans cette masse de données. Les personnels de la NSA disposant d'un accès à PRISM peuvent alors y puiser des informations en tapant simplement un nom ou une adresse email. Les métadonnées stockées par PRISM se chiffrent en millions. Les documents d'Edward Snowden montrent que 117 675 noms de personnes surveillées par la NSA soupçonnés d'intervenir dans des activités terroristes étaient répertoriés au sein de PRISM, le 5 avril 2013.

Autre information distillée par ces premiers documents, PRISM coûte chaque année 20 millions de dollars. Une goutte d'eau dans un budget de plus de 10 milliards de dollars pour la NSA. En premier lieu, le programme a commencé la collecte de données avec *Microsoft*, le 9 novembre 2007. Ont suivi *Yahoo!* et *Google* l'année suivante, *Facebook* en mars 2009, puis *Apple* en octobre 2012. Ces collectes qui visent des données particulières sont en constant développement. *Der Spiegel* a ainsi affirmé dans un livre *Der NSA Komplex*, paru en mars 2014, que le service *cloud SkyDrive* de Microsoft a été intégré à PRISM en mars 2013. Cet accord a été conclu après plusieurs mois de négociation entre le FBI et le géant informatique américain. Cette coopération suggère alors que la NSA n'est pas la seule à gérer les partenariats avec les grands groupes américains, alors que leur exploitation repose sur des logiciels mis en œuvre uniquement par cette même Agence. Parmi les exploitations de données les plus importantes figurent celles sur *Yahoo!*, *Google* et *Microsoft*. Ces trois géants américains représentent 98 % des données stockées par PRISM. Le logiciel de messagerie instantanée *Paltalk* a lui aussi fourni des informations importantes à la NSA notamment au cours du printemps arabe en Tunisie et en Égypte, ainsi que sur les échanges entre les rebelles en Syrie.

Concernant le SSO, les chiffres donnent le tournis. Selon le *Washington Post*, cette unité a recueilli en 2012 444 743 emails *Yahoo!*, 105 068 emails *Hotmail*, 82 857 comptes *Facebook* ou encore 33 697 emails *Gmail*. Chaque année, cela représente un volume total de 250 millions de données liées aux emails. Cela ne comprend pas la teneur des échanges dans les messages électroniques, les informations liées aux heures d'envoi et de réception ainsi que les pièces jointes échangées, ce que l'on appelle les métadonnées.

Les scoops se succèdent

Dès lors, les événements s'enchaînent très rapidement. En moyenne, un scoop impliquant les activités de la NSA avec des chiffres très précis est publié tous les trois jours. Le 7 juin, Glenn Greenwald publie un autre article « Boundless Informant: the NSA's secret tool to track global surveillance data ». L'affaire Verizon devient alors une affaire beaucoup plus importante qui gagne en texture grâce aux informations apportées par le journaliste américain. Elle prend une dimension différente révélant l'existence d'un programme de la NSA avec des documents très précis à ce sujet.

Boundless Informant constitue une base de données de la NSA permettant de connaître en temps réel l'état de la surveillance pratiquée sur les réseaux dans les pays du monde entier. Telle une carte mondiale des activités de la NSA, *Boundless Informant* informe de manière pédagogique et le plus simplifié possible les personnels de l'Agence sur les cyberopérations en cours. Ces activités semblent concerner uniquement des missions d'interception et non pas des

cyberopérations offensives de l'Agence.

La NSA dispose donc d'outils de cyberespionnage mais également de capacités de suivi et de contrôle de ces mêmes opérations de cybersurveillance. Le programme symbolise à lui seul ce qu'Edward Snowden souhaite avant tout dénoncer : la quantité incommensurable de données numériques collectées et stockées par les États-Unis. Les documents d'Edward Snowden indiquent que l'Iran faisait partie en 2007 des pays les plus espionnés au monde. Cette base de données qui se traduit sous la forme d'une carte géographique mondiale met en exergue une surveillance poussée des communications des Américains sur le sol national. En 2007, 2 892 000 000 communications auraient ainsi été interceptées aux États-Unis, selon les documents d'Edward Snowden publiés dans le *Guardian*. Dès ces premières révélations, Edward Snowden et les journalistes qui publient ses documents laissent entendre clairement que des données des citoyens américains sont stockées par la NSA. Pour autant, le directeur national du renseignement, James Clapper, répondait, au début de l'année 2014, lors d'une audition aux parlementaires de la commission américaine du renseignement « *No sir* » à la question de savoir si la NSA collectait des données sur les Américains aux États-Unis.

Boundless Informant permet d'apprendre concrètement que la NSA avait recueilli, entre le 1er et le 31 mars 2013, 97 milliards de données téléphoniques. Les données fournies sont donc très récentes. Et c'est cela qui accrédite encore plus les informations divulguées par ce *whistleblower* (« lanceur d'alerte ») unique en son genre. Le programme est géré par une unité au rôle déterminant de la NSA, la *Global Access Operations* chargée de superviser l'ensemble des opérations d'interception réalisées en dehors du territoire américain. En clair, elle s'assure du bon fonctionnement de l'ensemble des programmes de collecte et de stockage des données téléphoniques copiées depuis les câbles sous-marins, les satellites ou encore les métadonnées de navigation sur Internet.

Cette encyclopédie constitue la mémoire vivante de la NSA. Le programme se nourrit des données engrangées par les principaux logiciels pour dresser l'activité de l'Agence partout dans le monde. Parmi les logiciels que *Boundless Informant* scanne en permanence figure *Bullrun*. Il s'agit d'une collaboration entre la NSA et son homologue britannique, le GCHQ, visant à mettre en commun leurs activités liées au décryptage des clefs de chiffrement utilisées dans le cadre de la sécurisation des transactions en ligne. Dans le cadre de la surveillance des échanges financiers dans le monde, les deux Agences ont effectivement décidé – comme le révèlent les documents d'Edward Snowden – de mutualiser leurs moyens dédiés à casser les clefs de chiffrements les plus courantes pour crypter les numéros de compte et les montants des transactions opérées partout dans le monde.

Parmi les autres programmes qui nourrissent *Boundless Informant* citons également *Egotistical Giraffe* mis au point pour surveiller spécifiquement le réseau *Tor*. Ce réseau informatique est utilisé par des hackers mais aussi par des journalistes pour échanger de façon cryptée des informations de nature sensible. La NSA examine ainsi les profils des personnes et les informations échangées sur ce réseau censé être inviolable. Par ailleurs, *Muscular* est le nom d'un programme de la NSA établi pour pénétrer tous les réseaux privés de *Google* et *Yahoo!*. L'objectif est alors de s'introduire dans toutes les messageries ou tchats privés pour identifier des personnes et extraire des données. Enfin, *Olympia* permet quant à lui de surveiller uniquement les communications au sein du ministère brésilien des Mines et de l'Énergie.

Extrait de "L'affaire Snowden, une rupture stratégique", de Quentin Michaud et Olivier Kempf, publié chez Economica, 2014. Pour acheter ce livre, cliquez ici.