Données sensibles, écoutes, piratage: comment sont sécurisés les téléphones des chefs d'État

Par Marius François

La sécurité des télécommunications des gouvernements est un sujet sensible. *Jonathan Ernst/REUTERS - Gonzalo Fuentes/REUTERS*

Le président des États-Unis en fait l'économie. La sécurité des téléphones des dirigeants est pourtant un enjeu essentiel. *Le Figaro* fait le point sur les risques et les moyens mis en place pour les éviter.

Donald Trump n'est pas très à cheval sur la protection de son smartphone. Jusqu'en 2017, il utilisait un Samsung Galaxy S3, qui n'est plus mis à jour depuis 2015. Fin mai, Politico rapportait que le milliardaire refusait de se plier au protocole d'inspection de ses iPhone. Il en posséderait deux: un pour Twitter, un pour ses appels téléphoniques. Cette décision du chef d'État américain soulève une problématique importante: la protection des télécommunications des dirigeants et des gouvernements. Quelles sont les solutions envisagées pour éviter les risques d'écoute et de piratage?

De par leur statut, les chefs d'État sont amenés à échanger des informations confidentielles. De simples conversations peuvent avoir des conséquences diplomatiques, économiques ou politiques. Si des données fuitent ou si des pirates prennent le contrôle du téléphone d'un dirigeant, les retentissements peuvent être dramatiques. «Aujourd'hui, on utilise majoritairement des téléphones qui sont créés soit par des Américains soit par des Chinois. Même si les opérateurs sont français, on ne peut pas savoir précisément ce que les fournisseurs de solutions téléphoniques font réellement avec les téléphones qu'ils produisent», explique le cabinet de Mounir Mahjoubi, secrétaire d'État au Numérique, interrogé par *Le Figaro* , «On ne peut pas se permettre une quelconque imprécision dans ce domaine-là surtout vu les échanges qu'il peut y avoir au niveau de l'État».

Utiliser des appareils ultrasécurisés mais peu fonctionnels

Le chiffrement de bout en bout des communications est une nécessité pour les chefs d'État. Des constructeurs ont donc développé des appareils très sécurisés mais à l'ergonomie quelque peu dépassée. Ainsi, aux États-Unis, Boeing a développé le Boeing Black, un smart phone tactile capable de s'autodétruire logiciellement en cas de problème (***← photo***).

En France, l'entreprise Thalès a sorti, non sans une pointe d'humour, son Teorem ***(photo →),*** un téléphone à clapet sécurisé. La Direction Générale des Armées en a

commandé 14.140 exemplaires à sa sortie. L'appareil est capable, entre autres, de se connecter au réseau de téléphonie et télécopie Rimbaud (Réseau Interministériel de base uniformément durci) qui regroupe pas moins de 4500 abonnés au sein des ministères. Entre 2006 et 2017, Jacques Chirac, Nicolas Sarkozy puis François Hollande possédaient donc cet appareil au style retro en plus de leur téléphone personnel.

Sécuriser des smartphones grand public

La sécurisation d'appareils grand public semble être la solution plébiscitée par les présidents et dirigeants. Barack Obama a, par exemple, réussi à obtenir un Blackberry avec un ajout logiciel SecurVoice. Malheureusement pour lui, une fois les Blackberry dépassés, il a fallu attendre des années pour qu'il puisse prendre en main un iPhone ou un appareil Android. «On m'a donné le téléphone et on m'a dit «Monsieur le président, pour des raisons de sécurité, vous ne pouvez pas prendre de photos, vous ne pouvez pas envoyer des textos, le téléphone ne marche pas, vous ne pouvez pas mettre de la musique dessus…»», a déclaré Barack Obama sur le plateau du Tonight Show, «Grosso modo, ça ressemble à un téléphone pour enfant de trois ans...»

C'est également la solution choisie par Emmanuel Macron à son arrivée à l'Élysée. Il a été doté par Orange Cyberdéfense d'un Samsung Galaxy S7 Edge équipé de la technologie CryptoSmart développée par l'entreprise Ercom en partenariat avec le laboratoire Recherche & Développement de Samsung. «Tous les ministres sont équipés de téléphones sécurisés avec une solution cryptée au sein de leur mobile. La solution Ercom est labellisée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)», explique le cabinet de Mounir Mahjoubi.

Pas de partage de photos à l'horizon ni de partie endiablée de Candy Crush Saga, le téléphone du président permet uniquement de communiquer de manière sécurisée. Les échanges vocaux et SMS sont cryptés de bout en bout par une clé de chiffrement unique. En cas de perte ou de vol, une puce spéciale insérée sous le capot de l'appareil permet de détruire les données à distance.

Mettre en place des protocoles de sécurité

Une messagerie chiffrée développée par le gouvernement est également en cours de test auprès d'une trentaine de fonctionnaires du secrétariat d'État au Numérique. Le projet vise à remplacer l'usage de Telegram et WhatsApp, deux applications respectivement russe et américaine, par les députés et les ministres. La nouvelle messagerie du gouvernement devrait sortir dans le courant de l'été et «n'a rien coûté car elle utilise un code en open source: ce sont des développeurs en interne qui ont passé quelques heures par-ci par-là pour l'agrémenter».

«On voit la DGSI très régulièrement pour s'assurer qu'il n'y a pas eu de pénétration dans nos téléphones portables», rappelle le cabinet de Mounir Mahjoubi. De plus, les services de la sécurité intérieure exigent «des mesures de sécurité extrêmement importantes quand on [le chef de l'État, les ministres et leur cabinet, NDLR] rentre dans certains pays. On nous demande parfois de ne pas emporter nos téléphones et de partir avec une solution très sécurisée distribuée par l'État». En effet, des régimes comme la Chine ou Israël, par exemple, ont une politique de censure et de contrôle très stricte des télécommunications.

Si les smartphones grand public ont leur succès auprès des dirigeants, leur usage est prohibé pour les dossiers les plus sensibles. «Pour les sujets qui sont vraiment considérés comme Confidentiel Défense ou Secret-Défense, il n'y a absolument rien qui passe par les téléphones portables des ministres ou des cabinets», confie le cabinet de Mounir Mahjoubi, «Pour ça, on continue à utiliser des téléphones fixes, des solutions extrêmement poussées en matière de sécurité et des réseaux internes».