Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 20 - Janvier 2016

Ce « flash » de l'ingérence économique évoque des actions dont des sociétés françaises sont régulièrement victimes. Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Vous comprendrez que, par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à : securite-economique@interieur.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

Flash n°20 Janvier 2016

Les déplacements à l'étranger, un risque important de captation d'informations

Un agent travaillant sur des questions de défense et de sécurité au sein d'une administration a récemment fait l'objet d'un contrôle intrusif en zone internationale de l'aéroport Roissy-Charles de Gaulle, alors qu'il s'apprêtait à partir en congés dans un pays étranger en compagnie d'une relation.

Au moment de l'enregistrement des bagages, deux agents se réclamant de la compagnie aérienne concernée les ont séparés et interrogés de façon concomitante. Outre les questions habituelles de sécurité (motif et adresse du séjour dans le pays de destination, voyages antérieurs, situation maritale, etc.), l'agent a posé à l'intéressé un certain nombre de questions précises sur sa profession et son employeur. Ce dernier a précisé la qualité de son employeur, sans pour autant révéler la nature réelle de ses fonctions. A la fin de l'interrogatoire, l'agent a ensuite signalé au fonctionnaire qu'il ferait l'objet d'un deuxième contrôle en zone internationale, après le passage en douane.

Arrivé à la salle d'embarquement, le fonctionnaire français a été interpellé par un autre agent de la compagnie aérienne qui lui a demandé de le suivre pour procéder, comme convenu, aux formalités de contrôle. L'intéressé a été conduit dans une salle sécurisée de l'aéroport, où les mêmes questions sur son environnement personnel et professionnel lui ont été posées. Le contenu de son bagage à main a par ailleurs été entièrement contrôlé et l'agent a également examiné pendant quelques instants son téléphone portable. Le fonctionnaire n'a pas pu constater les actions effectuées sur son téléphone, l'intervenant opérant dos tourné. En tout état de cause, le téléphone était verrouillé et le code d'accès n'a pas été sollicité.

De retour dans la salle d'embarquement, le fonctionnaire a reçu pour consigne de rester à proximité de l'agent qui l'avait interrogée la première fois, jusqu'à sa montée dans l'avion.

Arrivé dans le pays de destination, le téléphone de l'intéressé n'a pas fonctionné pendant trois jours, aucun appel ne pouvant être émis depuis l'appareil. Passé ce délai, le téléphone n'a plus présenté de dysfonctionnements. Par ailleurs, aucun problème n'a été constaté par le fonctionnaire pendant son séjour.

Commentaire

Cette situation pourrait s'avérer anecdotique si l'environnement professionnel et le contenu du téléphone de l'intéressé ne présentaient pas un caractère sensible. Il travaille en effet dans un service qui traite de questions liées à la sécurité de certaines informations stratégiques et son téléphone contenait les noms et coordonnées téléphoniques professionnelles et personnelles de ses collègues. De plus, sa messagerie professionnelle pouvait être consultée depuis Internet, donc depuis son téléphone, ce dernier pouvant conserver l'historique des messages échangés.

Dans le cas d'espèce, rien ne prouve que des informations sensibles ont été récupérées par l'agent ayant procédé à l'interrogatoire, dans la mesure où le téléphone était protégé par un code de verrouillage, ce qui rend l'accès au contenu de ce dernier plus difficile à mettre en œuvre. Néanmoins, à défaut, le risque de captation d'informations dans ce type de situation peut s'avérer bien réel, avec pour conséquences potentielles une captation de données se rapportant à des dossiers sensibles.

Sous couvert de lutte contre le terrorisme, les contrôles opérés par certains Etats dans les aéroports, bien que légitimes dans leur principe au vu des enjeux sécuritaires actuels, peuvent cependant donner lieu à des actions relevant de l'ingérence. Des agents appartenant à des services de renseignement étrangers peuvent agir dans les zones internationales des aéroports et profiter des vérifications de sécurité sur des passagers pour récupérer données et informations. Des cadres d'entreprises ont déjà fait l'expérience de ce type de contrôles intrusifs, y compris au moment du passage en douane une fois arrivés à destination (exigence de remise, aux fins de « vérifications », de smartphones ou d'ordinateurs portables par les autorités, la détention pouvant durer de longues minutes).

Préconisations de la DGSI

Les déplacements à l'étranger impliquent une préparation avant le départ. Dans le cadre de ses missions de sécurité économique et de contre-ingérence, la DGSI émet les préconisations suivantes (liste non exhaustive) :

Avant le départ :

- Se renseigner sur la situation politique et sécuritaire du pays de destination, ainsi que sur les législations locales en termes de contrôle aux frontières. Cette préparation permet d'assurer la sécurité de la mission et d'anticiper les difficultés que pourraient poser des contrôles intrusifs opérés par/dans certains pays.

- Privilégier l'utilisation de matériels nomades dédiés exclusivement à la mission. Cette pratique permet de limiter le stockage d'informations et de documents sensibles/stratégiques aux seuls besoins de la mission. Les ordinateurs portables, tablettes et smartphones doivent

être expurgés de toutes données sensibles et l'accès à leur contenu doit être protégé par des mots de passe forts, personnels et secrets (comprenant idéalement 12 caractères alphanumériques).

Pendant le déplacement :

- Dès l'arrivée dans le pays, signaler sa présence aux autorités officielles françaises (ambassade ou consulat).

- Conserver sur soi, pendant toute la durée du déplacement, tous ses appareils électroniques et ne pas les laisser dans les coffres forts des hôtels. Le personnel des hôtels peut être amené à visiter votre chambre en votre absence et à ouvrir le coffre à l'aide d'un double de la clef ou d'un mot de passe « maître » pour se livrer à un vol d'informations. Si vous êtes contraint de vous séparer, par exemple, de votre smartphone, retirer et conserver sur vous la carte SIM, ainsi que la batterie dans la mesure du possible.

- Eviter autant que possible d'utiliser la connexion Wifi des hôtels. Dans certains pays, les accès Wifi des établissements hôteliers réputés pour accueillir des hommes d'affaires sont surveillés. Si l'utilisation du Wifi constitue votre seul moyen d'accéder à Internet, adaptez vos échanges en fonction de ce paramètre et changez vos mots de passe une fois rentré en France. Il est en effet facile de suivre vos déplacements et de s'introduire dans votre système informatique via ces canaux.

- Eviter de connecter ses appareils électroniques à des postes ou périphériques informatiques qui ne sont pas de confiance. Si vous avez besoin d'échanger des documents, privilégier l'utilisation d'une clé USB et effacer ensuite le contenu avec un logiciel d'effacement sécurisé.

- Apposer un filtre de confidentialité sur son écran d'ordinateur pour empêcher les regards indiscrets. A défaut, si vous travaillez dans les transports en commun, votre voisin peut jeter des regards sur votre écran d'ordinateur à votre insu.

- En cas de perte ou de vol de matériels, ou de contrôle par les autorités locales, informer immédiatement son responsable hiérarchique et demander conseil aux autorités officielles françaises (ambassade ou consulat) avant toute démarche auprès des autorités locales.

- Se méfier des rencontres professionnelles ou amicales « spontanées ». Ces rencontres peuvent aspirer à sympathiser avec vous pour vous faire parler.

Au retour :

- Rédiger un rapport d'étonnement à l'attention de son responsable hiérarchique et de son référent sûreté pour tout problème de sécurité et signaler tout comportement suspect qui aurait pu retenir l'attention. La DGSI pourra, au besoin, être alertée par les personnes référentes au sein de l'entité.

- Analyser ou faire analyser tout particulièrement les appareils électroniques ayant échappé à votre surveillance à un moment ou un autre.

A toutes fins utiles, vous trouverez diverses informations utiles à la préparation d'un voyage sur les sites Internet suivants :

- Site de la délégation interministérielle à l'intelligence économique : www.intelligence-economique.gouv.fr
- Site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
- Site du ministère des Affaires Etrangères et du Développement International : www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs.html
- Site du Club des Directeurs de Sécurité des Entreprises : www.cdse.fr