Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Intérieur

INGERENCE ECONOMIQUE

Flash n° 30 - Février 2017

Ce « flash » évoque des actions d'ingérence économique 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° 30 Février 2017

La zone à régime restrictif (ZRR), un instrument de sécurité économique

Réformé en 2011, le dispositif de protection du potentiel scientifique et technique de la nation (PPST)[1] a pour objectif de prévenir les actes de malveillance qui pourraient être commis au sein d'établissements publics ou privés opérant dans des domaines stratégiques ou sensibles.

Il permet ainsi la création de *zones à régime restrictif* (ZRR) dans certains lieux identifiés et définis au préalable par l'établissement en concertation avec le ministère de tutelle. L'accès à ces zones repose sur un processus d'analyse des dossiers de demandes d'accès par les services ministériels compétents.

Ces procédures de contrôle visent à éviter que des personnes signalées et/ou mal intentionnées puissent avoir accès à certains savoir-faire et les utilisent dans le développement d'une arme (enjeux liés à la prolifération des armes de destruction massive, aux arsenaux) ou à des fins terroristes. Une ZRR peut par ailleurs être créée afin de protéger les activités présentant un intérêt économique pour la nation (ruptures technologiques, innovation, recherche et développement, informations relatives à des brevets ou à la propriété intellectuelle, etc.).

Les éléments matériels ou immatériels hébergés dans une ZRR peuvent être ainsi considérés comme des intérêts fondamentaux de la nation, ce qui leur confère une protection fondée sur le code pénal[2]. Les services de l'Etat se montrent donc particulièrement vigilants dès lors qu'un incident de sécurité est constaté dans une ZRR.

1er exemple

Le directeur d'une société classée ZRR est informé par son service informatique qu'une opération inappropriée est en cours au sein du bureau dédié aux activités de recherche et de développement. Le directeur se rend immédiatement sur les lieux et surprend un de ses employés en train de copier et de transférer sur un disque dur personnel des données industrielles sensibles. Le dirigeant a immédiatement mis à pied l'auteur des faits et déposé plainte. Le salarié encourt des sanctions pénales.

[1] Décret n°2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.
[2] Article 410-1 du code pénal relatif aux intérêts fondamentaux de la nation.

2ème exemple

Le responsable de la sécurité des systèmes d'information (RSSI) d'une société classée ZRR constate un redémarrage inexpliqué de plusieurs serveurs. L'analyse technique effectuée en interne permet de détecter une intrusion dans ces serveurs par l'intermédiaire d'un compte administrateur accessible depuis Internet. Plusieurs intrusions de ce type se sont produites en l'espace de quelques jours. Le dépôt de plainte a permis aux enquêteurs de mener des investigations plus poussées et de confirmer l'identité de l'auteur, un ex-salarié de la société qui avait présenté sa démission quelques mois auparavant. Placé en garde à vue, l'intrus a reconnu les faits et a été condamné à une peine de 3 mois d'emprisonnement avec sursis et 1500 euros d'amende pour accès et maintien frauduleux dans un système de traitement automatisé de données (article 323-1 du code pénal).

3ème exemple

Le directeur d'un laboratoire de recherche classé ZRR a déposé plainte pour le vol de matériels très innovants conçus à l'issue de deux années de recherche. Les premiers éléments de l'enquête ont conduit à privilégier l'hypothèse d'un vol ciblé, ne pouvant avoir été commis que par, ou avec la collaboration, d'un membre de l'équipe du professeur en charge des recherches. L'analyse du listing des accès par badge durant la période supposée de commission du vol a permis de détecter qu'un chercheur invité, de nationalité étrangère, recruté pour une durée d'un an au sein du laboratoire, avait accédé aux lieux le jour supposé du vol, jour où le laboratoire est normalement fermé. A la suite du dépôt de plainte, le parquet a chargé la DGSI d'une enquête sous les qualifications de sabotage et de livraison d'informations à une puissance étrangère (article 411-6 du code pénal).

Commentaires

La protection juridique et administrative qu'offre le statut de ZRR présente l'avantage d'induire une réaction rapide des services répressifs à la suite du dépôt de plainte du responsable de l'établissement victime. Les parquets compétents peuvent à ce titre saisir la DGSI pour mener les enquêtes à même de révéler d'éventuelles atteintes aux intérêts fondamentaux de la nation. Lorsqu'elles sont prouvées, le code pénal prévoit des sanctions pouvant aller, selon les cas, jusqu'à dix ans d'emprisonnement et 225 000 euros d'amende, voire jusqu'à vingt ans de détention criminelle et 300 000 euros d'amende[3].

[3] Livre IV, Titre Ier, Chapitre Ier.

Préconisations de la DGSI

- Tout établissement public ou privé, travaillant dans des domaines d'activité sensibles ou stratégiques, peut demander la création d'une ou plusieurs ZRR auprès des services ministériels spécifiquement en charge de ces questions (en général le service du haut fonctionnaire de défense et de sécurité du ministère compétent). Les demandes seront étudiées et des informations complémentaires sur l'intérêt d'adhérer au dispositif pourront être apportées.

- Tout incident de sécurité constaté au sein d'une ZRR (vol de matériel, de documents, etc.) doit être suivi d'un dépôt de plainte par le chef d'établissement. Les investigations ne pourront être diligentées par les services enquêteurs spécialisés qu'après cette formalité.

- Les établissements hébergeant des ZRR doivent sensibiliser les personnels habilités à y circuler et à y travailler aux risques liés aux intrusions et à la nécessité d'assurer l'intégrité des informations et supports qui y sont détenus.

- La création d'une ZRR implique, pour l'établissement, de se doter d'une politique de sécurité des systèmes d'information (PSSI). La PSSI est un document interne à l'établissement qui contribue à ce que chaque utilisateur adopte les bons réflexes d'hygiène informatique, tels que préconisés par l'Agence nationale de la sécurité des systèmes d'information.