Lutter contre l'espionnage technologique

Le dispositif de protection du potentiel scientifique et technique de la nation

« Les États n'ont pas d'amis, ils n'ont que des intérêts »
Charles de Gaulle

Pilotée par le Secrétariat général de la défense et de la sécurité nationale, il s'agit d'une protection juridique et administrative de l'accès aux savoirs, savoir-faire stratégiques et technologies sensibles d'établissements publics et privés.

Passé au second plan à la suite des attentats terroristes de 2015, l'espionnage – et notamment l'espionnage technologique – est aujourd'hui un sujet d'une brûlante actualité qui concerne tant le secteur public (laboratoires de recherche, écoles, universités…) que le monde de l'entreprise. Sachant que ces activités d'espionnage peuvent être menées par des services de renseignement, des entités privées mais également des organisations criminelles travaillant au profit d'États.

La protection du potentiel scientifique et technique de la nation (PPST) est conçue comme un outil de sécurité économique destiné à favoriser la protection du potentiel scientifique et technique d'un établissement (R&D, savoir-faire, processus de production, données, etc…) face aux menaces d'ingérences directes ou indirectes (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information etc...). L'idée est que, grâce à ce dispositif, l'État mette à la disposition de l'établissement concerné – public ou privé – les outils réglementaires, techniques et humains dont il dispose pour maîtriser les risques pesant sur ce potentiel. Celui-ci est alors intégré aux intérêts fondamentaux de la nation et bénéficie à ce titre de la protection juridique instituée par le code pénal.

Ce dispositif s'appuie notamment sur la création de zones dont l'accès est réglementé, ainsi que par la mise en place d'une une politique de sécurité des systèmes d'information basée sur les préconisations de l'ANSSI[1].

Établir des espaces clos réglementés

La protection des contenants est assurée par la création de zones protégées au sens de l'article 413-7 du code pénal. L'accès à ces zones, dénommées zones à régime restrictif (ZRR) est réglementé et soumis à l'avis favorable du ministre de rattachement de l'établissement concerné. Une ZRR est généralement constituée d'un bâtiment – ou d'une partie de bâtiment – et non de l'ensemble d'un site. Elle est créée par arrêté ministériel, après enregistrement au répertoire national des ZRR par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) qui fournit un numéro d'identifiant. La décision est alors notifiée au chef de l'établissement et communiquée au préfet territorialement compétent.

L'ensemble du personnel travaillant physiquement dans une ZRR, ou qui est amené à s'y connecter à distance, doit bien entendu être informé du statut de celle-ci, des règles qui la régissent et des poursuites pénales auxquelles s'expose un contrevenant.

L'accès à la ZRR – qu'il soit physique ou virtuel – au titre d'un recrutement (CDD, CDI, intérimaire…), d'un stage (doctorant, activité de recherche…), de prestations de service, etc... doit recueillir l'avis favorable du ministère concerné avant d'être autorisée par le chef d'établissement. Une simple visite, elle, ne nécessite que l'autorisation du chef d'établissement.

1 : Agence nationale de la sécurité des systèmes d'information.

Il n'existe pas de normes techniques obligatoires pour protéger une ZRR. La PPST impose seulement qu'elle soit un espace clos, doté à chacun de ses accès extérieurs d'une signalétique informant de son statut et des conséquences pénales auxquelles s'exposent les contrevenants. En d'autres termes, ce dispositif n'impose aucune dépense liée à la protection ! Chaque entité décide, selon ses moyens et son besoin de protection, si elle souhaite (et surtout comment) protéger sa ZRR.

Définir les objectifs et procédures de sécurité informatique

En parallèle, les établissements concernés doivent mettre en place une politique de sécurité des systèmes d'information. Celle-ci définit les objectifs et procédures en matière de sécurité informatique. Ce document interne contribue à ce que chaque utilisateur adopte les bons réflexes d'hygiène informatique, dans le but de réduire les incidents de sécurité et les coûts associés. Dans ce cadre, un responsable de la sécurité des systèmes d'information doit être désigné comme interlocuteur privilégié pour toutes les questions relatives à la sécurité informatique et à la responsabilité de la mise en œuvre de la politique de sécurité des systèmes d'information.

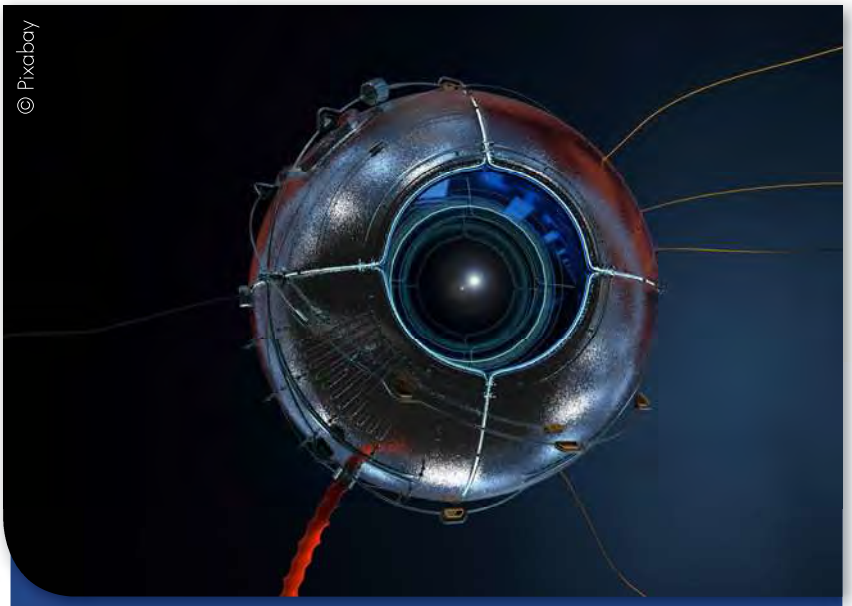
D'un point de vue pénal, les personnes qui pénètrent sans autorisation dans une ZRR encourent une peine de 6 mois d'emprisonnement et 7 500 € d'amende. De plus, une ZRR abritant des éléments essentiels du potentiel scientifique et/ou économique de la nation, les faits de nature à porter atteinte à ces intérêts sont sanctionnés jusqu'à 15 ans de détention criminelle et 225 000 € d'amende.

Face à un espionnage technologique – cyber et humain – de plus en plus offensif, tant dans le secteur public que privé, le dispositif de protection du potentiel scientifique et technique de la nation apporte une réponse à la fois simple et juridiquement robuste, en liaison étroite avec les services spécialisés. Outil puissant, mais encore trop méconnu, il mérite toute l'attention des entités de recherche du secteur public et des entreprises technologiques, notamment les PME.

Patrice Lefort-Lavauzelle

Pour aller plus loin :

- Site du SGDSN : www.sgdsn.gouv.fr – Contact PPST au SGDSN : ppst@sgdsn.gouv.fr
- Plaquette *La protection du potentiel scientifique et technique de la nation.* SGDSN. Janvier 2017.
- Flash Ingérence économique La zone à régime restrictif (ZRR) un instrument de sécurité économique, DGSI. Février 2017.
- *La protection du patrimoine scientifique et technique de la nation (PPST) : outil de lutte contre l'espionnage technologique.* DPID. Mai 2017.
- *Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) : un outil de lutte contre l'espionnage technologique particulièrement adapté aux PME qui travaillent avec la Défense.* Fiche Entreprises & Défense (FED). Association des entreprises partenaires de la Défense. Octobre 2017.


© Pixabay

Pilotée par le Secrétariat général de la défense et de la sécurité nationale, il s'agit d'une protection juridique et administrative de l'accès aux savoirs, savoir-faire stratégiques et technologies sensibles d'établissements publics et privés.

La Zone à régime restrictif en résumé

Protection juridique	L'intrusion constitue un délit
Protection physique	Adaptée aux besoins et aux moyens
Recrutement	Avis favorable après enquête administrative
Prestataires	Enquête administrative portant sur la personne morale et les personnes physiques
Stages	Avis favorable après enquête administrative
Visites	Accord du responsable avec accompagnement de la personne
Evolution de la structure capitalistique ou juridique	Doit être signalée. Des mesures de protections additionnelles peuvent être préconisées.
Sécurité des systèmes d'information	Mise en place d'une politique de sécurité des systèmes d'information (PSSI), basée sur les règles de protection préconisées par l'ANSSI.

Protection du secret de la défense nationale et PPST : des objectifs différents

SI la protection du secret de la défense nationale vise à protéger des informations et des supports classifiés de toute compromission, la PPST a pour but la protection d'informations stratégiques.

Ainsi, les régimes de contrôles d'accès sont différents. Les enquêtes administratives menées dans le cadre de la protection du secret (pour une habilitation, ou pour l'accès à une zone réservée, par exemple) détectent les vulnérabilités des personnes physiques ou morales.

Les contrôles effectués au titre des zones à régime restrictif prennent en compte le risque que représente les personnes physiques au regard de leur pays d'appartenance et de la nature des activités exercées au sein de la ZRR.

PLL

Comment la Chine tenterait de recruter des Français[2]

La République populaire de Chine aurait approché ces dernières années 4 000 personnes – dont 1 700 travaillant dans la fonction publique – via les réseaux sociaux professionnels, en particulier LinkedIn, et ce à l'aide de 500 faux profils. Une opération d'une ampleur sans précédent dans le seul but de contacter des « *cibles* » ayant un profil intéressant dans des domaines stratégiques tels que les télécommunications, l'informatique, les nanotechnologies, le nucléaire, la santé ou pouvant servir de relais d'influence… Dans un premier temps la « *cible* » est invitée à fournir des notes, un travail de synthèse… moyennant une petite rétribution. Elle est ensuite invitée – tous frais payés – à participer à une conférence en Chine dans son domaine d'expertise, ou à rencontrer un client potentiel. Des photos « *compromettantes* » sont alors prises, la trace des paiements évidemment conservée, et la victime est alors contrainte de collaborer si elle veut éviter d'être dénoncée aux services français. Plusieurs centaines de personnes seraient entrées dans un processus de compromission assez abouti. Certaines auraient même été incitées à passer des concours administratifs afin d'infiltrer des ministères.

PLL

2 : Notamment, www.lefigaro.fr/actualite-france/ et www.lci.fr/justice/

Et si les États-Unis se passaient d'étudiants chinois ?

Alors que la Chine est le pays qui a le plus d'étudiants aux États-Unis – 350 000 – c'est l'une des propositions qui a été faite par Stephen Miller, l'un des conseillers à la Maison Blanche, au président Trump. Destinée à limiter le nombre d'espions potentiels chinois, l'idée a été évoquée auprès du président qui l'aurait finalement écartée après une discussion avec l'ambassadeur des États-Unis en Chine. S'il n'a pas opté pour une décision radicale – refuser tout visa aux étudiants chinois –, le président américain étudierait toutefois une méthode douce : les limiter en nombre.

L'espionnage par la République populaire de Chine inquiète en effet énormément outre-Atlantique. Selon l'administration américaine, la Chine recourt à des pratiques de collecte offensive de l'information qui dépassent largement le cadre du ciblage des industries dites stratégiques du complexe militaro-industriel ou des secteurs-clés de l'énergie ou des nouvelles technologies. Ainsi, tout membre de la communauté chinoise au sens large (diaspora, étudiants, stagiaires « *post-doc* »…) serait potentiellement au service de la communauté du renseignement, y compris si nécessaire sous la menace de s'en prendre à des proches restés en Chine. Les services chinois pourraient également s'appuyer sur les associations d'étudiants et les Instituts Confucius (plus de 1 500 centres dans le monde) dont les responsables ne sont nommés qu'avec l'agrément de l'ambassade du pays concerné. En février dernier, le directeur du FBI Christopher Wray disait craindre toutes les méthodes « non traditionnelles » de l'espionnage moderne par les Chinois, dont les étudiants, les professeurs ou les scientifiques. « *Cela ne se passe pas que dans les plus grandes villes, ça se déroule partout* », avait-il déclaré avant de reconnaître que les États-Unis avaient un « haut niveau de naïveté » sur ces questions. D'après une étude réalisée par le FBI auprès de 165 sociétés, la moitié d'entre elles a déclaré avoir subi un espionnage économique. Et 95 % de ces entreprises ont suspecté la Chine d'en être responsable.

L'espionnage industriel est souvent plus économique que de lourds investissement de R&D. Outre-Atlantique, le FBI a lancé une campagne de sensibilisation des entreprises américaines aux dangers de l'espionnage économique.

A quand un CIFIUS au niveau européen ?

Les États-Unis disposent depuis 1975 d'un comité, le *Committee on Foreign Investment in the US* (CIFIUS), chargé de surveiller les investissements étrangers. Avec obligation, depuis une loi votée au mois d'août dernier, de soumettre un dossier au CIFIUS si, directement ou indirectement, la transaction donne à une société étrangère – même minoritaire – un accès à des technologies dites « *critiques* ». Une réforme du comité faisant suite à un rapport du Pentagone publié en février 2017 qui démontrait comment des intérêts chinois, par le biais de fonds d'investissements actifs dans la Silicon Valley, ont mis la main sur des technologies sensibles.

L'approche du CIFIUS est très pragmatique, il ne s'agit pas de protéger les sociétés américaines en situation difficile, de défendre des filières ou de protéger l'emploi. Mais bien d'empêcher des technologies américaines d'être transférées à des pays qui pourraient ensuite utiliser celles-ci contre les États-Unis.

PLL