Le dispositif de protection du potentiel scientifique et technique de la Nation (PPST) : outil de lutte contre l'espionnage technologique

Patrice Lefort-Lavauzelle

Patrice Lefort-Lavauzelle, chef de cabinet du directeur de la Protection des Installations, moyens et activités de la Défense (DPID) nous présente le dispositif de protection du potentiel scientifique et technique de la Nation. Face à l'espionnage technologique, tant dans le secteur public que privé, le dispositif de protection du potentiel scientifique et technique de la Nation (PPST) apporte une réponse à la fois simple et pratique, en liaison étroite avec les services spécialisés. Ce dispositif s'appuie notamment sur la création de zones à régime restrictif (ZRR) dont l'accès est réglementé, ainsi que sur la mise en place d'une politique de sécurité des systèmes d'information (PSSI) basée sur les préconisations de l'ANSSI.

Directement rattachée au ministre des Armées, la DPID est la direction fonctionnelle du ministère, tête de chaîne de la fonction « Défense - Sécurité ». Cette fonction couvre la protection physique, la cyber-sécurité, la protection du secret, ainsi que la protection du potentiel scientifique et technique de la Nation (PPST) et la continuité d'activité.

Si la menace terroriste est aujourd'hui prégnante, celle-ci ne doit pas faire oublier les activités liées à l'espionnage - notamment technologique - que celles-ci soient le fait de services de renseignement, d'entités privées, voire d'organisations criminelles travaillant au profit d'États...

Les atteintes au potentiel scientifique et technique de la Nation (PPST) se sont multipliées depuis ces dernières années et ont amené le gouvernement à réviser le dispositif de protection du patrimoine scientifique et technique qui datait de 1972, et dont la précédente réforme remontait à 1993.

Juridiquement plus robuste, le nouveau dispositif de protection du potentiel scientifique et technique de la Nation est fondé sur le Code pénal et s'organise principalement autour d'un décret du Premier ministre en Conseil d'État [1][1], d'un arrêté du Premier ministre [2][2] et d'une circulaire interministérielle du Premier ministre [3][3].

Il vise à protéger les accès aux savoirs, savoir-faire et technologies les plus « sensibles » des établissements publics, mais également privés, dont le détournement ou la captation pourraient :

- porter atteinte aux intérêts économiques de la Nation (risque R1);
- renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense de la Nation (risque R2);
- contribuer à la prolifération des armes de destruction massive et de leurs vecteurs (risque R3);
- être utilisés à des fins terroristes sur le territoire National ou à l'étranger (risque R4).

Ce dispositif est opposable « erga omnes » (« opposable à tous ») et écarte donc tout risque de discrimination. Chaque ministère adapte les modalités de mise en œuvre avec ses propres directives, et ce, en fonction des spécificités de son domaine de compétences.

Les mesures de protection

Le dispositif prévoit la mise en œuvre de mesures de protection qui s'appliquent aux éléments essentiels du potentiel scientifique et technique de la Nation et notamment aux savoirs et savoir-faire et technologies relatifs aux secteurs scientifiques et techniques protégés listés en annexe de l'arrêté du 3 juillet 2012.

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 donc être informé du statut de celle-ci, des règles qui la régissent et des poursuites pénales auxquelles s'expose un contrevenant.

Le dispositif PPST d'une manière pratique

Pourquoi intégrer ce dispositif ?

La protection du potentiel scientifique et technique de la Nation est un outil de sécurité économique destiné à favoriser la protection du potentiel scientifique et technique d'un établissement (R&D, connaissances, savoir-faire, processus de production, données, etc.) face aux menaces d'ingérences directes ou indirectes (utilisation frauduleuse d'informations, vol ou captation de

1 *[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 *[2] Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la Nation.*

3 *[3] Circulaire interministérielle du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la Nation*

données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information etc.).

C'est également un outil destiné à lutter contre la prolifération des armes de destruction massive (ADM) et contre l'expansion du terrorisme grâce au contrôle des accès aux informations et aux biens susceptibles d'y contribuer (connaissances, savoirs et savoir-faire). Le dispositif robuste ainsi constitué permet à la France de respecter ses engagements internationaux en termes de lutte contre la prolifération et contre le terrorisme.

L'État met à la disposition de l'établissement concerné les outils réglementaires, techniques et humains dont il dispose pour maîtriser les risques pesant sur ce potentiel. Le potentiel de l'établissement concerné est intégré aux intérêts fondamentaux de la Nation et bénéficie à ce titre de la protection juridique instituée par le Code pénal.

Comment créer une zone à régime restrictif (ZRR) ?

Lorsqu'il existe un risque lié à la captation d'informations susceptibles d'affaiblir le potentiel scientifique et technique de la Nation, le chef de service, d'établissement ou d'entreprise et le ministre de rattachement s'entendent sur la nécessité de créer une zone à régime restrictif.

Celui-ci adresse un dossier de demande de création de ZRR aux entités concernées, sachant que chaque ministère a ses procédures propres. Au sein du ministère des Armées, le dossier est instruit par la Direction générale de l'armement (DGA) en liaison avec la Direction du renseignement et de la sécurité de la défense (DRSD), la DGA signant les arrêtés de création de ZRR.

Comment la procédure de demande d'accès en zone à régime restrictif fonctionne-t-elle ?

La procédure de demande d'accès s'effectue en trois étapes :

- Le demandeur formalise sa demande au moyen d'un formulaire type fourni par le ministère de rattachement. La délivrance de l'autorisation d'accès est un préalable à la signature du contrat de travail ou à l'inscription du demandeur à des travaux de recherche se déroulant dans une ZRR ;
- Le responsable de la ZRR ou directeur de recherche, accuse réception du dossier et complète la demande par les données scientifiques demandées ;
- Le ministre, qui s'exprime le cas échéant par l'intermédiaire du haut fonctionnaire de défense et de sécurité (HFDS) ou par délégation du fonctionnaire de sécurité et de défense, rend un avis. Lorsque l'avis est favorable, l'accueillant peut - ou non - faire droit à la demande d'accès.

Les autorisations d'accès sont délivrées pour une durée maximale de cinq ans et peuvent être révisées à tout moment. Il est intéressant de noter que, pour les personnes habilitées au secret de la défense nationale, il n'est pas nécessaire d'effectuer une demande d'accès, les habilitations (avis de sécurité...) sont réputées autoriser l'accès à une ZRR.

Une demande d'accès virtuel à la ZRR doit-elle être traitée au même niveau qu'une demande d'accès physique ?

Tout accès à la ZRR, qu'il soit physique ou virtuel, est soumis à autorisation du chef d'établissement, après avis favorable du ministre. Les documents de la ZRR ne peuvent donc être consultés que par les personnes y ayant été autorisées par le chef d'établissement.

Quelle est la différence entre un accès à une ZRR et une visite de ZRR ?

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 ou de missions doit recueillir l'avis favorable du ministère concerné avant d'être autorisée par le chef d'établissement.

Une visite se caractérise par son aspect temporaire et par l'absence de participation directe aux activités scientifiques et techniques de la ZRR. L'avis ministériel n'est pas requis, seule l'autorisation du chef d'établissement est nécessaire. Une visite se différencie également de la prestation de services - nécessitant une autorisation d'accès - par l'absence de contrat.

Quels sont les coûts de la mise en œuvre de la PPST pour un établissement abritant une ZRR ?

Il n'existe pas de normes techniques obligatoires pour protéger une ZRR. La PPST impose seulement que la ZRR soit un espace clos, doté à chacun de ses accès extérieurs d'une signalétique informant du statut de ZRR 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.

Il est néanmoins important de noter que la gestion des dossiers de demandes d'accès aux ZRR peut avoir un coût en termes de ressources humaines, dans l'éventualité où un nombre important et régulier de demandes sont déposées.

Quelles sont les peines encourues par les personnes qui pénètrent sans autorisation dans une ZRR ?

En application de l'article 413-7 du Code pénal, les personnes qui pénètrent sans autorisation dans une ZRR risquent une peine de 6 mois d'emprisonnement et 7.500 € d'amende.

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

La protection du secret de la défense nationale vise à protéger des informations et des supports classifiés (ISC) de toute compromission. La PPST a pour but la protection d'informations stratégiques au regard des quatre risques cités plus haut, notamment R1 « atteintes aux intérêts économiques de la Nation ».
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 ZRR prennent eux 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.

Modèle de signalétique d'une ZRR

Les mesures d'interdiction sont rendues apparentes au moyen de panneaux rectangulaires de 50 x 40 cm placés aux endroits appropriés du périmètre extérieur. Elles doivent être en nombre suffisant pour être obligatoirement vues, y compris de nuit.
Dans le cas particulier où les limites de ZRR se confondent avec celles d'une ZP existante, ces panneaux ne seront placés qu'aux portes d'accès de la ZRR.
Ces panneaux doivent porter d'une façon lisible l'inscription :

ZONE A REGIME RESTRICTIF

Interdiction de pénétrer
sans autorisation
Article R 413-1 du Code pénal

Tout contrevenant s'expose
aux peines prévues par
l'article 413-7 du Code pénal

A quelles peines s'expose la personne détournant ou dérobant des informations ou du matériel détenus dans une ZRR ?

La ZRR abrite des éléments essentiels du potentiel scientifique et/ou économique de la Nation, définis, conformément à l'article 410-1 du Code pénal, comme des intérêts fondamentaux de la Nation. À ce titre, l'article 411-9 du Code pénal sanctionne les faits de nature à porter atteinte à ces intérêts jusqu'à 15 ans de détention criminelle et 225.000 € d'amende.

La protection juridique et administrative qu'offre le statut de ZRR présente l'avantage d'assurer une réaction rapide des services de l'État à la suite du dépôt de plainte du responsable de l'établissement victime.

Qu'impose la PPST en matière de sécurité informatique ?

Les établissements concernés doivent avant tout mettre en place une politique de sécurité des systèmes d'information (PSSI). La PSSI est un document interne qui diffuse les « bonnes pratiques » et fixe les objectifs et procédures de l'établissement en matière de sécurité informatique. Ce document 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 (RSSI) doit être désigné. Il est l'interlocuteur privilégié pour toutes les questions relatives à la sécurité informatique et a la responsabilité de la mise en œuvre de la PSSI.

Qu'impose la réglementation à un établissement public ou privé dès lors qu'il conduit des activités relevant d'un ou plusieurs secteur(s) protégé(s) ou qui souhaite coopérer avec un partenaire étranger dans un domaine relevant de ces secteurs ?

Les secteurs protégés listés en annexe de l'arrêté du 3 juillet 2012 ont été définis en fonction de l'intérêt stratégique qu'ils présentent pour la Nation, ou pour ceux qui les convoitent, et de la nécessité de préserver le potentiel scientifique et technique. La règlementation prévoit que l'établissement relevant d'un ou plusieurs de ces secteurs protégés fasse remonter certaines informations vers le haut fonctionnaire de défense et de sécurité du ministère concerné, ou le HFCDS pour le ministère des Armées. À titre d'exemple, le HFDS doit être tenu informé des projets de congrès, séminaires ou autres événements organisés par l'établissement.

La ZRR en résumé

Protection juridique	L'intrusion constitue un délit
Protection physique	Adaptée aux besoins et aux moyens
Recrutement	Avis favorable après enquête administrative (EA)
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
Évolution de la structure capitalistique ou juridique	Doit être signalée. Des mesures de protection 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.

L'entité qui souhaite coopérer avec un partenaire étranger doit bien entendu en informer le HFDS du ministère en charge du secteur dont il relève. Le HFDS émet alors un avis sur le projet.

Le dispositif PPST s'adresse tout particulièrement aux PME technologiques - notamment les sous-traitants des grands industriels du secteur Aéronautique, Défense & Sécurité (ADS) - à la recherche d'un dispositif à la fois simple et juridiquement robuste dans le cadre de la protection de matériels (prototypes...) ou d'informations (R&D, innovation...) et ce, en liaison étroite avec les services spécialisés. Outil puissant mais encore trop méconnu, il a toute sa place dans la « boîte à outils » des professionnels de la sûreté et devrait connaître un net développement. ■

Patrice Lefort-Lavauzelle,
Chef de cabinet du DPID

Bibliographie

Instruction interministérielle n° 901 relative à la protection des systèmes d'informations sensibles. ANNSI. 28 janvier 2015.

O. de Maison Rouge « Le droit du renseignement, renseignement d'État, renseignement économique » Lexis Nexis. 2016.

Lettre d'information de la Direction de la sécurité économique en zone Paris. DRSD. Novembre - décembre 2016.

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.

Liste des secteurs scientifiques et techniques protégés

Les secteurs scientifiques et techniques protégés sont identifiés par un nombre

Biologie, médecine et santé :

11 • Aspects moléculaires et cellulaires de la biologie.
12 • Biomolécules, pharmacologie, thérapeutique.
13 • Physiologie, biologie des organismes, populations, interactions.
14 • Recherche clinique, innovation technologique, santé publique.

Chimie :

21 • Chimie des matériaux.
22 • Chimie organique, minérale, industrielle.
23 • Chimie théorique, physique, analytique.
24 • Génie des matériaux.

Mathématiques et leurs interactions :

31 • Mathématiques et leurs interactions.

Physique :

41 • Constituants élémentaires et physique théorique.
42 • Plasmas chauds.
43 • Milieux denses, matériaux et composants.
44 • Milieux dilués et optique fondamentale.
45 • Physique nucléaire.

Sciences agronomiques et écologiques :

51 • Biologie de l'environnement, des populations, écologie.
52 • Biologie des organismes ; biotechnologies animales, végétales et microbiennes.
53 • Biotechnologies agroalimentaires, sciences de l'aliment.

Sciences de la terre et de l'univers, espace :

61 • Astronomie, astrophysique.
62 • Terre solide et enveloppes superficielles.
63 • Terre, enveloppes fluides.

Sciences et technologies de l'information et de la communication :

71 • Automatique, productique.
72 • Traitement du signal et des images.
73 • Électronique, microélectronique, nanoélectronique et micro-ondes.
74 • Micro-nanosystèmes et capteurs.
75 • Systèmes optiques et photoniques.
76 • Informatique et applications.

Sciences pour l'ingénieur :

81 • Génie des procédés.
82 • Plasmas froids.
83 • Electronique de puissance.
84 • Génie électrique.
85 • Acoustique.
86 • Bio-mécanique et bio-ingénierie.
87 • Energétique, thermique, combustion.
88 • Mécanique des milieux fluides.
89 • Génie civil.
810 • Génie mécanique, productique, transport.
811 • Mécanique des solides, des matériaux, des structures et des surfaces.
812 • Missiles, armes, sciences et techniques de défense.