Argumentaire en faveur de l'adhésion des acteurs publics et privés au dispositif de protection du potentiel scientifique et technique de la nation

Qu'il s'agisse de propriété intellectuelle et industrielle, de sécurité, y compris face au terrorisme, ou de lutte contre la prolifération, notamment des armes de destruction massive, l'État se doit de veiller à ce que certaines activités sensibles de recherche, de production, d'essais, de développement de technologies innovantes soient correctement protégées pour respecter les engagements pris par la France au niveau européen et international et pour lutter contre les activités d'espionnage technologique susceptibles d'affaiblir la compétitivité de la nation ou ses capacités de défense.

Les mesures de protection adoptées dans le cadre de la réglementation PPST visent spécifiquement à limiter les risques de pillage ou de détournement à des fins malveillantes des savoirs, savoir-faire et technologies identifiés comme éléments essentiels du potentiel scientifique et technique de la nation et donc comme composante des intérêts fondamentaux de la nation. La réglementation, applicable sur l'ensemble du territoire de la République, offre une protection juridique et administrative fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues par les établissements publics ou privés. Elle repose sur deux mesures principales qui constituent le socle commun à toutes les entités adhérant au dispositif :

- la délimitation de zones à régime restrictif (ZRR) permettant une protection ciblée (physique et logique) des espaces renfermant les activités et informations de nature scientifique ou technique considérées comme stratégiques ou sensibles ;
- la mise en place d'une politique de sécurité des systèmes d'information visant à protéger les données numériques sensibles.

1 Un outil de sécurité pour parer aux nouvelles menaces auxquelles les acteurs économiques et scientifiques doivent faire face

Les services de renseignement constatent, année après année, une diversification et un accroissement du nombre d'opérations visant à capter des savoirs et des savoir-faire au sein des établissements français. Dans un contexte d'espionnage banalisé, accentué par la mondialisation et l'interdépendance des pays, le monde de la recherche et de l'innovation, aussi bien publiques que privées, est devenu une cible de choix. Ce constat est partagé par l'ensemble des pays qui disposent d'une R&D performante, tous s'efforçant désormais de mettre en place des outils, notamment réglementaires, visant à sécuriser les activités de recherche fondamentale ou appliquée.

Parmi la variété de modes opératoires utilisés, la majorité des incidents constatés relève des atteintes physiques sur site (notamment les intrusions et vols), souvent facilitées par des négligences humaines ou des failles de sûreté / sécurité au sein des établissements, ainsi que des atteintes aux données (notamment au travers de cyber-intrusions et d'attaques informatiques). Ces atteintes peuvent donner lieu à des captations technologiques pouvant entrainer une perte de compétitivité pour l'établissement ou à un détournement des savoir-faire à des fins malveillantes susceptibles d'entacher durablement la réputation de l'établissement.

Face à ces menaces, le dispositif PPST constitue un outil efficace au service des établissements publics et privés pour limiter les risques d'atteinte à leurs actifs scientifiques et techniques stratégiques, souvent acquis difficilement au prix de plusieurs années de développement et d'investissements. Il permet de protéger et de sécuriser spécifiquement le potentiel scientifique et technique détenu par l'entité (R&D, connaissances, savoir-faire, processus de production, données, etc.) afin de le préserver des risques de captation, de détournement ou d'utilisation frauduleuse et de prémunir la structure de tout risque de fragilisation (déstabilisation, altération de l'image, discrédit, détérioration de valeur, perte de chiffre d'affaires et d'opportunités contractuelles, etc.).

La démarche de protection implique avant tout de distinguer au sein de l'entité les informations de nature scientifique ou technique qui ont une portée stratégique[1]. En général, elles sont décisives pour l'avenir. C'est ce qui peut se traduire par l'idée de « potentiel » qui se trouve derrière chaque activité de recherche ou de production. L'identification et la localisation précise des éléments sensibles de l'entité au moment du processus de création des ZRR, ainsi que l'appréciation adéquate des différents risques auxquels chacune des activités est exposée, jouent un rôle essentiel dans l'efficacité de la protection.

2 Un dispositif dissuasif : décourager l'intrusion et la captation

Les tentatives de captation avortées ne sont pas directement comptabilisables. Cependant, la comparaison du nombre d'incidents constatés entre les entités mettant en œuvre la PPST et celles qui n'y ont pas recours permet de mettre en évidence l'effet dissuasif du dispositif.

Les sanctions pénales encourues par les contrevenants (clairement affichées sur les panneaux installés aux points d'entrée des ZRR), les informations précisées dans le règlement intérieur ainsi que les précédents (toutefois encore peu nombreux) d'infractions judiciarisées, exercent un rôle dissuasif vis-à-vis des personnes malveillantes extérieures à l'entité mais également vis-à-vis du personnel interne à l'entité.

Au-delà de la finalité de protection de l'accès aux recherches, études ou fabrications sensibles, ce volet dissuasif permet également de limiter d'autres formes d'intrusion. Par exemple, certains laboratoires de recherche sensibles abritant des animaleries ou travaillant sur des thématiques controversées par une partie de la société (comme les OGM), ont pu constater l'effet dissuasif des ZRR contre les intrusions de mouvements radicaux.

3 Un dispositif préventif : empêcher l'intrusion et la captation

Le dispositif repose sur une base juridique qui permet de réaliser un contrôle *a priori* des personnes souhaitant accéder à la ZRR pour y travailler et donc aux informations stratégiques qui y sont détenues. Ce mécanisme de contrôle préalable, qui passe par une vérification poussée de l'honorabilité des accédants, permet d'avoir recours à du personnel de confiance, ce qui peut s'avérer particulièrement intéressant dans le cadre de recrutements. La ZRR constitue dès lors un véritable espace de confiance. Ce contrôle peut s'exercer dès la phase de sélection finale des candidats, l'autorisation d'accès en ZRR devant dans tous les cas être délivrée préalablement à la signature du contrat ou à l'inscription du demandeur à des travaux de recherche se déroulant dans une ZRR.

Le dispositif prévoit également des mesures de sanction pénale à l'encontre des contrevenants en cas d'intrusion (les ZRR ont le statut de zone protégée). Les sanctions encourues sont renforcées en cas de captation de données protégées et de leur éventuelle livraison à des puissances étrangères (les éléments détenus au sein de la ZRR participent des intérêts fondamentaux de la nation). L'existence - et la connaissance par les acteurs - de ce mécanisme de sanction joue un rôle majeur pour éviter la survenue d'incidents et empêcher les captations.

Afin que la protection préventive soit optimale, il convient également de sensibiliser régulièrement l'ensemble du personnel de l'entité pour mieux responsabiliser chaque individu (la sécurité est l'affaire de tous) et instaurer progressivement une culture de la sécurité dans les pratiques de travail, la manipulation et l'échange d'informations. L'application de la PPST contribue ainsi à éviter certains comportements à risque *via* la sensibilisation des personnels et l'application de règles sur l'accès aux données (règlement intérieur renforcé, application d'une politique de sécurité des systèmes d'information, gestion rigoureuse des visiteurs et parcours adapté prédéfini, etc.).

Le lien privilégié que l'entité dotée d'une ZRR peut entretenir avec les services spécialisés compétents permet également à la structure d'être mieux informée de l'évolution des menaces.

---

[1] L'ancienne délégation interministérielle à l'intelligence économique (D2IE) donnait en 2015 la définition suivante : « *une information peut être qualifiée de stratégique lorsque sa possession donne à son détenteur un avantage certain et déterminant pour la suite du processus, par rapport à celui qui ne l'a pas. La valeur ajoutée économique potentielle de cette information est également un paramètre à prendre en compte.* »

Cela lui permet d'ajuster en conséquence son organisation interne et de mettre en œuvre des contre-mesures adaptées pour mieux prévenir les atteintes.

Le dispositif prévoit aussi un meilleur encadrement des projets de coopération de nature scientifique ou technique que l'entité souhaiterait engager avec des partenaires étrangers, notamment s'agissant de projets d'accord de collaborations relatives aux activités menées au sein des ZRR. L'examen préalable, éventuellement avec l'appui de l'État, de ces projets de coopération internationale permet de s'assurer que les termes du partenariat sont équilibrés et garantissent à court, moyen et long termes la préservation des intérêts de l'entité et, par extension, ceux de la nation. Il s'agit ainsi de prévenir les possibles atteintes au potentiel scientifique et technique susceptibles de s'opérer lors de la réalisation des échanges et du partage d'expertise inhérents à ces collaborations.

4 Un dispositif permettant de mieux sanctionner les actes délictueux

Le cadre réglementaire sur lequel repose le dispositif permet de se retourner juridiquement contre un contrevenant qui s'introduirait sans autorisation au sein de la ZRR. Les sanctions sont renforcées en cas de captation ou de détournement de données, savoirs ou savoir-faire détenus au sein de la ZRR.

Sans cette protection juridique spécifique, le responsable de l'entité est presque totalement démuni en cas d'incident. Seuls le viol de la propriété privée, le vol ou la dégradation de biens peuvent alors être invoqués, avec l'écueil de la charge de la preuve et des peines applicables (traitement comme n'importe quel délit de droit commun) qui ne prennent pas en compte l'impact réel du préjudice associé à la captation de données stratégiques (absence de reconnaissance de ces données comme participant aux intérêts fondamentaux de la nation).

Le dispositif présente l'avantage d'induire une intervention rapide des services spécialisés à la suite d'un dépôt de plainte, ce qui donne lieu à des investigations poussées permettant de limiter au maximum l'impact de l'incident reporté.

Les mesures particulières actionnées en cas d'incident survenant dans une ZRR permettent également de préserver l'image et donc la réputation de l'entité.

5 Un dispositif offrant un accompagnement étatique privilégié et personnalisé dans la démarche d'élévation du niveau global de sécurité de l'entité

Le dispositif de la PPST permet aux entités concernées d'établir avec l'administration et les services spécialisés un lien privilégié au travers d'un accompagnement rapproché de la démarche de protection de leurs intérêts économiques, scientifiques et techniques ou simplement réputationnels.

La protection est en effet assurée par concertation entre les pouvoirs publics et les entités intéressées. Cela se traduit par un dialogue renforcé entre, d'une part, l'administration en charge de la protection des intérêts fondamentaux de la nation et, d'autre part, les établissements détenteurs des éléments constitutifs du potentiel scientifique et technique de la nation. La « communauté » des ZRR offre ainsi un lieu d'échange entre « détenteur des savoirs et savoir-faire » et pouvoirs publics.

Au travers de ce dialogue étroit entre les services de l'État et les acteurs publics ou privés, la réglementation PPST vise ainsi à mieux concilier liberté de la recherche, dynamique des relations économiques et besoin de protection des activités « sensibles ».

L'administration favorise ainsi les actions de prévention et le dialogue afin d'évaluer la nécessité de prendre des mesures de protection qui soient adaptées à l'exposition des entités aux risques et menaces pouvant porter atteinte au potentiel scientifique et technique de la nation.

Dans le cadre de l'activité de la ZRR, l'État apporte un appui administratif au travers de la procédure d'avis ministériel préalable à toute autorisation d'accès. Par délégation du ministre compétent, le service du haut fonctionnaire de défense et de sécurité instruit le dossier de demande d'accès et émet un avis fondé sur une double analyse, technique (pertinence des travaux

envisagés au regard des informations relatives au demandeur) et de sécurité (honorabilité du demandeur évaluée par les services enquêteurs spécialisés). Chaque avis ministériel résulte d'une analyse bénéfice/risque qui prend donc aussi en compte les avantages offerts par l'accueil du candidat. En cas de doute, des adaptations peuvent être proposées au travers de réserves à suivre par l'entité afin de limiter les risques.

Les services spécialisés assurent également une mission de conseil auprès des entités abritant des ZRR, en entretenant des contacts réguliers, par le biais d'entretiens bilatéraux, de visites in situ lorsqu'elles s'avèrent nécessaires, ou encore au travers de conférences de sensibilisation à l'attention des personnels travaillant dans les ZRR. Ces contacts directs avec les établissements permettent un accompagnement personnalisé des laboratoires et des entreprises adhérant au dispositif afin que les activités/données sensibles détenues ne soient pas mises en situation de vulnérabilité.

Au total, l'adoption par l'entité de la « démarche » PPST assure une montée progressive de son niveau global de sécurité qui peut être complétée - par choix de l'entité et sans obligation réglementaire - par des mesures additionnelles de protection (clôtures sur l'emprise du bâtiment, lecteurs de badges, gardes de sécurité, etc.).

6 Un savoir-faire reconnu par l'Etat et l'appartenance à une communauté de confiance favorable aux partenariats industriels ou de recherche

Le dispositif PPST constitue un outil de sécurité intéressant pour le développement de collaborations :

- il démontre une certaine maturité de l'entité dans la protection des informations sensibles qu'elle détient ;
- il confère une certaine crédibilité pour initier des partenariats avec des acteurs exigeants en terme de sécurité ;
- il est la reconnaissance par l'Etat du caractère stratégique de ce que l'entité développe ou produit.

L'adhésion au dispositif est en effet bien perçue par les entreprises privées qui y voient souvent un gage de qualité et de sécurité permettant de préserver les données sensibles industrielles et le potentiel économique. Les ZRR constituent en ce sens un réseau de confiance, favorable au développement de partenariats industriels, de recherche ou pour l'exécution de contrats publics sensibles. Cela peut permettre également de répondre à l'exigence de certains clients ou fournisseurs.

Enfin, l'adhésion au dispositif peut permettre, dans certains cas, de mettre en avant un niveau de sécurité qui peut répondre aux exigences imposées par certains régimes réglementaires à portée extraterritoriale. Un échange de notes verbales entre la France et les Etats-Unis datant de 2014 a permis de placer le régime de la PPST, au même titre que celui de l'habilitation au secret de la défense nationale, comme garantie suffisante vis-à-vis des exigences de sécurité de la réglementation américaine *International Traffic in Arms Regulations* (ITAR)[2].

7 Un dispositif flexible offrant une protection ciblée, sur mesure, adaptée aux besoins identifiés et aux moyens pouvant être consentis par l'entité

La concertation établie avec l'administration vise à prendre en compte les spécificités de chaque entité. Les mesures concrètes sont adaptées au cas par cas, selon les risques, et en fonction des moyens disponibles. En cas d'incompatibilité avec certaines préconisations opérationnelles, un diagnostic peut être établi en concertation étroite avec les services de l'administration afin de définir les mesures (techniques ou organisationnelles) qui pourront s'adapter au mieux à un contexte donné tout en garantissant un niveau de protection optimal.

[2] La réglementation américaine impose notamment que les personnels étrangers ou binationaux qui sont amenés à manipuler au sein des entreprises françaises des produits ou données non classifiés ITAR fassent l'objet d'une enquête de sécurité conforme aux exigences du Département d'Etat.

Il revient aux entités de définir les contours de la future ZRR ainsi que les modalités d'organisation au sein de la ZRR et les ressources qui pourront y être apportées. L'objectif est de rendre le tracé acceptable et accepté, et la gestion de la ZRR la moins contraignante possible tout en s'assurant que les éléments qui relèvent du potentiel scientifique et technique de la nation sont bien couverts.

Il n'existe pas de normes techniques obligatoires pour protéger une ZRR. Le dispositif 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, la PPST n'impose aucun frais lié à la protection physique des ZRR. Chaque entité décide selon ses moyens et ses besoins de protection de déployer ou non des barrières supplémentaires (lecteur de badge, caméra de surveillance, etc.).

La gestion des dossiers de demandes d'accès aux ZRR peut néanmoins entrainer un coût en termes de ressources humaines, dans l'éventualité où un nombre important et régulier de demandes d'accès devait être instruit.

Les visites dans une ZRR ne sont pas soumises à la procédure de l'avis ministériel favorable préalable. La prise en charge de visiteurs amenés à pénétrer dans une ZRR repose alors sur un accueil responsable, avec un accompagnement des personnes au travers d'un parcours adapté défini à l'avance afin de limiter les risques de captation.

Le dispositif PPST offre ainsi :

- une protection ciblée pour ne protéger que ce qui doit l'être, le périmètre des ZRR étant ajustable au « juste besoin de protection » afin de ne pas perturber le fonctionnement de l'entité ;
- une évaluation adaptée du niveau des différents risques pour chaque activité considérée comme « sensible » au titre de la PPST et hébergée dans une ZRR, contribuant ainsi à « filtrer » au mieux les accès pouvant présenter une vulnérabilité potentielle en termes de captation et/ou de détournement de savoirs et savoir-faire ;
- une flexibilité, le périmètre des ZRR étant facilement modifiable pour rester en adéquation avec les éléments et activités qu'elle protège et qui peuvent évoluer dans le temps ;
- des normes techniques minimales permettant aux entités qui ont peu de moyens financiers de bénéficier de la protection juridique renforcée des ZRR et de l'accompagnement étatique pour augmenter progressivement leur niveau global de sécurité en fonction de leurs ressources.