	Call for evidence **Boosting Research Security in the EU** *Contribution du Centre National de la Recherche Scientifique*	Janvier 2024

Propos liminaire

Comme l'a identifié l'Union européenne le 20 juin dernier, la sûreté de la recherche (*Research Security*) est un maillon incontournable de l'approche globale pour le renforcement de la sécurité économique européenne. Au-delà du champ économique, protéger la recherche c'est aussi contribuer à la protection de nos valeurs communes européennes : « *Si nous ne portons pas au niveau français et européen cette recherche, on décide stratégiquement de dépendre de ceux qui la feront. (…) nous ne pouvons pas mésestimer le fait que nous sommes dans un monde qui se refracture et où il y a derrière des choix géopolitiques qui iront avec des choix de recherche* » (propos du Président de la République française, le 26 novembre 2019 à l'occasion des 80 ans du CNRS). En tant qu'organisme de recherche fondamentale multidisciplinaire au service de la société, le CNRS soutient la démarche de *Research Security* européenne.

Le CNRS est, en effet, particulièrement concerné par cette démarche européenne naissante et ce à double titre : en tant qu'acteur de premier plan de la recherche européenne (1er organisme de recherche européen par le nombre de salariés, 1er bénéficiaire des programmes cadres depuis 40 ans …) mais également en tant qu'acteur de longue date du dispositif français de Protection du Potentiel Scientifique et Technique (PPST).

Le CNRS souhaite donc être partie prenante du déploiement d'une *Research Security* européenne au-delà de cette seule participation au *Call for evidence* – dont le très court délai de réponse impose, malheureusement et à ce stade, de se concentrer sur certains points clé.

1. Dispositif existant en France et au CNRS

En France, il existe depuis 2012 un dispositif réglementaire national pour protéger les travaux scientifiques (publics comme privés) contre les ingérences étrangères, les captations indues ou encore contre les détournements à des fins non souhaitées. Le cœur du dispositif est l'affirmation, dans notre Code pénal (art. 410-1), que le potentiel scientifique et technique fait partie **des intérêts fondamentaux** de la nation. Il s'agit du dispositif dénommé PPST.

Ce dispositif constitue une **protection juridique forte** basée sur l'identification des savoirs et savoir-faire stratégiques ainsi que des technologies sensibles et sur leur protection par des mesures limitatives dont des **Zones à Régime Restrictif** (ZRR). Il s'agit de créer un **espace de confiance** pour conduire et partager la recherche par le contrôle des accès à ces zones réglementées. Toute personne doit être dûment autorisée pour y travailler : cela s'applique à tous **sans distinction de nationalité**.

L'identification des travaux sensibles repose sur l'analyse de **quatre critères de risque** en cas de captation, détournement ou ingérence étrangère :

- Risque d'atteinte aux intérêts économiques de la nation. *Nota :* dans le cas de la recherche publique, ce risque s'entend également comme un risque d'atteinte au rayonnement scientifique de la nation ;
- Risque de renforcement d'arsenaux militaires étrangers ou d'affaiblissement des capacités de défense de la nation ;
- Risque de contribution à la prolifération d'armes de destruction massive et leurs vecteurs ;
- Risque d'utilisation à des fins terroristes sur le territoire national et à l'étranger.

Comme le laisse entendre l'utilisation de ces quatre critères, la PPST est également un outil de conformité vis-à-vis d'autres dispositions légales (exportations de matériels de guerre, biens à double usage, traités internationaux, *etc.*)

Indépendamment de la création de ZRR, la PPST s'applique à de nombreux niveaux : recrutements, coopérations internationales, mobilités, *etc.*

Le fonctionnement de la PPST dans son ensemble est particulièrement **centralisé** et repose sur une chaîne d'acteurs. En premier lieu, la PPST est pilotée et coordonnée de manière interministérielle par le Secrétariat général de la défense et de la sécurité nationale (SGDSN – service de la Première Ministre). Le SGDSN dispose d'un relais fonctionnel au sein de chaque ministère, les Hauts Fonctionnaires de Défense et de Sécurité (HFDS), qui – à leur tour – disposent de relais dans chaque établissement. Ainsi, le HFDS du Ministère de l'enseignement supérieur et de la recherche peut s'appuyer sur son réseau de Fonctionnaires de Sécurité et de Défense (FSD) : chaque établissement (universités comme organismes nationaux de recherche) dispose d'un FSD.

Les FSD sont responsables du déploiement de la PPST dans leur établissement et sont le point de contact naturel pour les agents de l'établissement pour toute question en lien avec la PPST.

Au CNRS, plus particulièrement, notre démarche est fondée sur la confiance en nos chercheurs, l'adhésion de tous, la responsabilisation de chacun et le pragmatisme des mesures de protection.

2. Réflexions sur le projet de Recommandation présenté

2.1. Principes généraux/*Guiding Principles*

➞ "*Emphasis on self-governance by the sector in full respect of academic freedom and institutional autonomy*"

La protection de la recherche vis-à-vis des ingérences étrangères relève des intérêts nationaux des États membres. Ainsi, s'il convient que le secteur de la R&I s'empare de la question au niveau européen, **cette auto-gouvernance devra également s'inscrire dans le respect des dispositifs nationaux existant ou à venir, qui sont, eux, du ressort des États**. Cela n'est pas exclusif de l'élaboration et de l'adoption d'un socle commun européen de mesures de protection de la recherche et de l'innovation.

Nous attirons l'attention sur la protection juridique des chercheurs qu'offre l'établissement d'un cadre réglementaire national. La *Research Security* est une démarche de maîtrise des risques et, aussi aboutie soit-elle, il restera toujours un risque résiduel de captation indue ou de détournement à des fins malveillantes. En cas d'incident avéré, un chercheur ayant respecté le dispositif réglementaire en vigueur, verra sa responsabilité dégagée. En France, les atteintes aux intérêts fondamentaux de la nation (dont fait partie le potentiel scientifique) sont punies par les articles 410-1 à 414-9 du Code pénal. Dans le cadre de la PPST, la responsabilité des décisions les plus sensibles est déportée vers les établissements et le ministère de tutelle. Demander aux chercheurs d'assumer une part de responsabilité trop large, c'est aussi courir le risque que les chercheurs s'autocensurent en appliquant trop systématiquement et trop largement un principe de précaution (ex : arrêt total des collaborations avec tel ou tel pays).

➞ "*Taking an all-of-government framework towards supporting and empowering the sector, notably by linking R&I and security expertise*"

Plus généralement, l'équilibre des bénéfices et des risques des potentielles collaborations internationales nécessite une approche globale, car les avantages et les inconvénients ne sont pas nécessairement supportés par les mêmes acteurs (recherche, relations diplomatiques, défense, économie, …). Une **approche interministérielle** (ou inter Directions générales) au sein des États peut être nécessaire : la question de la protection de la recherche dépasse parfois la seule compétence d'un secteur ou d'un ministère (DG).

Une fois un cadre posé, la politique de *Research Security* peut ensuite être déclinée dans chaque ministère impliqué dans le secteur de la recherche et de l'innovation mais **nécessite toujours un dialogue** entre les secteurs de la recherche, de l'innovation, de la sécurité, émission de visa *etc*.

➞ "*Supporting an all-of-sector approach, including basic and applied research as well as higher education*"

Le CNRS souligne qu'il existe un continuum entre recherche fondamentale et appliquée. Aussi les préoccupations de sûreté doivent-elles couvrir tout le spectre de la recherche et de l'innovation, en prenant en compte les spécificités et les enjeux associés à chaque niveau de TRL.

➞ "*Proportionality of safeguarding measures based on a risk-based approach*"

Les mesures de protection doivent, en effet, être mises en place selon un principe de proportionnalité vis-à-vis du risque identifié. **Cela présuppose que des critères d'évaluation du risque soient clairement établis et partagés par tous.** Cela suppose également une **harmonisation de ce qui est considéré comme une mesure de protection faible, médiane ou forte**.

Afin de garantir cette notion de proportionnalité, il paraît nécessaire qu'une flexibilité suffisante soit laissée aux responsables nationaux dans l'appréciation de chaque cas particulier.

Il ne faudrait pas non plus se limiter à une approche « *risk-based* » mais tendre vers une approche où les risques pris sont évalués au regard des opportunités/bénéfices envisagées (« ***benefit/risk-based approach*** »)

➞ "*Focus on national security risks as well as ethics and integrity considerations*"

Si les enjeux de sécurité nationale prévalent, il est nécessaire de trouver le plus grand dénominateur commun de nos valeurs partagées au niveau UE, dans le respect des spécificités de chacun en matière de sécurité nationale.

Nous insistons sur la nécessité d'aboutir à la **définition commune des valeurs cœur à partager**. À défaut d'une dynamique collective de montée en puissance en matière de *Research Security*, les possibilités de contournement des dispositifs nationaux par des entités malveillantes resteront nombreuses : il faut éviter un « maillon faible » européen qui servirait de « *back door* » pour capter des résultats de la recherche européenne.

➞ "*Taking a country-agnostic approach avoiding all forms of discrimination and stigmatisation*"

Les mesures de protection mises en œuvre doivent s'appliquer à tous dans une approche *erga omnes* : aussi bien aux ressortissants nationaux, aux ressortissants UE et aux ressortissants non-UE.

Il est cependant explicite que l'élaboration d'une politique de protection de la recherche européenne vise à la protéger de captations extra-européennes.

2.2. Actions politiques clé/*Key policy actions*

➞ « *Adopt a comprehensive and coherent approach at national as well as R&I sector level on safeguards while aiming for increasing levels of consistency across Europe at all levels*"

Nous partageons la nécessité de cette approche exhaustive et cohérente, tant aux niveaux nationaux qu'au niveau européen. L'organisation et les critères d'appréciation des risques varieront nécessairement d'un État à l'autre, notamment en raison des questions de souveraineté nationale. À l'échelle de l'Union européenne, il conviendrait donc de développer des **liens de confiance** entre les acteurs de la *Research Security* et de s'assurer de **l'acceptation mutuelle des contraintes et des lignes rouges** de chacun. Une divergence dans l'appréciation des lignes rouges entre deux partenaires ne saurait faire obstacle à la participation de ceux-ci à un même consortium.

➞ "*Invest in a better understanding of the sector-specific threat landscape and the sector's resilience*"

Nous partageons également cette nécessité mais nous relevons tous les défis que cela pose. Le paysage de la menace est en **constante évolution**. Il peut être **très variable en fonction des thématiques scientifiques ou des partenaires envisagés** et relève de la souveraineté nationale de chaque État Membre.

➞ "*Support research performing organisations in their efforts to develop due diligence and risk management procedures and assign responsibilities within the organisation*"

Les procédures de maîtrise des risques et de *due diligence* sont effectivement en cours de structuration au sein des établissements. L'identification claire des acteurs et des responsabilités est une étape nécessaire à la mise en place d'une protection efficace.

➞ "*Promote that national funding agencies incentivise beneficiaries to identify and address Research Security issues in their projects.*"

De façon complémentaire, les **agences nationales et européennes de financement devraient être elles-mêmes des acteurs de la *Research Security*** et intégrer cette dimension dans leur fonctionnement. Les choix de financement devraient prendre en compte et faciliter la *Research Security* au sein de programmes de recherche.

2.3. Initiatives au niveau de l'Union européenne/*EU level initiatives*

➞ « *Facilitate peer learning and coordination among Member States and stakeholders and create communities of practice across Europe*"

En tant qu'organisme de recherche français, le CNRS souhaite être partie prenante de ces discussions et de ces communautés d'échange. Nous proposons que ces communautés se structurent en groupes de confiance : la nature des enjeux de la *Research Security* nécessite un certain niveau de confiance dans ses interlocuteurs et que les participants à ces groupes aient un niveau d'implication similaire (éviter les discussions à sens unique).

➞ "*Support the development of practical guidance and due diligence tools for research performing organisations*"

Le développement de tels outils serait bénéfique pour l'ensemble des acteurs européens. Actuellement les outils de *due diligence* adaptés au monde de la recherche manquent encore. Afin de garantir des décisions souveraines et en accord avec nos valeurs communes, il conviendrait qu'il s'agisse d'**outils européens propres**. Le recours aux outils proposés par des acteurs extra-UE est une source de risque de dépendance dans nos prises de décision.

Ces outils devraient être rendus disponibles pour l'ensemble de la communauté de la *Research Security* européenne. En revanche, l'accessibilité de ses outils devrait être limitée aux acteurs en ayant besoin pour leurs prises de décision. En particulier, une accessibilité totale (ex : publication sur internet) exposerait au monde nos éléments de vigilance et faciliterait les contournements de nos dispositifs par des acteurs malveillants.

➞ "*Monitor the Member States' uptake of the Recommendation's guiding principles and key policy actions.*"

L'application de ces recommandations et leur suivi devra s'effectuer dans le respect de la responsabilité des établissements vis-à-vis de leurs dispositifs nationaux.

3. Éléments complémentaires

- Il existe une responsabilité au niveau des États vis-à-vis des engagements internationaux qu'ils ont pris, ex : traité de non-prolifération des armes nucléaires, conventions internationales sur les armes chimiques et biologiques, arrangement de Wassenaar, régime de contrôle de la technologie des missiles, traité de Nagoya … La *Research Security* européenne doit pouvoir s'articuler avec le bon respect par les États de leurs engagements.

- Les principes généraux devraient prévoir une notion d'indépendance et de résilience du dispositif de *Research Security* vis-à-vis de l'action d'États tiers non européens. Le dispositif ne doit pas pouvoir être instrumentalisé par un acteur extra-UE afin d'orienter la politique européenne de protection de la recherche selon une orientation donnée.

- La dimension « sécurité économique » ne doit pas être négligée. Le développement économique étant un objectif majeur de l'UE, la protection de nos atouts est essentielle.

- Dans notre dispositif national, nous constatons que les acteurs de la sûreté de la recherche n'ont pas de parcours ou de profil-type : il peut s'agir de juristes, de scientifiques, de chargés de relations internationales, d'anciens militaires, d'informaticiens … C'est une richesse dans le cadre d'un fonctionnement en réseau où chacun apporte son expertise. **La diversité des compétences est certainement à encourager dans le déploiement d'une *Research Security* européenne**, cela contribuerait à éviter que les initiatives qui émergeront se cristallisent sur certains aspects au détriment des autres (ex : sur la conformité légale, sur les questions cyber, *etc.*) En parallèle, l'initiative européenne en matière de sûreté de la recherche pourrait inclure la mise en place de formations spécifiques, afin que – dans leur diversité – les acteurs de la *Research Security* partagent **un socle commun de compétences**.

- Les « *EU level initiatives* » pourraient inclure un soutien à la formation et à la sensibilisation de l'ensemble des personnels de recherche. En particulier, **les jeunes chercheurs seraient une cible pertinente à atteindre** afin de développer cette dimension sécurité au plus tôt.

- Les dispositifs de *Research Security* déployés devront être accompagnés de dispositifs de sécurité des systèmes d'information performants et cohérents.

- Le document décrivant le *Call for evidence* indique que le niveau de prise de conscience de la problématique « *Research Security* » peut être très variable d'un État de l'UE à l'autre, ce qui pourrait aboutir à des pressions pour exclure d'un consortium européen des partenaires issus d'États qui n'ont pas ou peu de mesures relatives à la maîtrise des risques. Notre expérience pratique est inverse : il arrive qu'un partenaire qui dispose d'un dispositif plus contraignant subisse des pressions par des partenaires qui n'ont pas le même niveau protection. Les règles de fonctionnement des consortia doivent prendre en compte les différences d'appréciation par les partenaires des questions de *Research Security*.