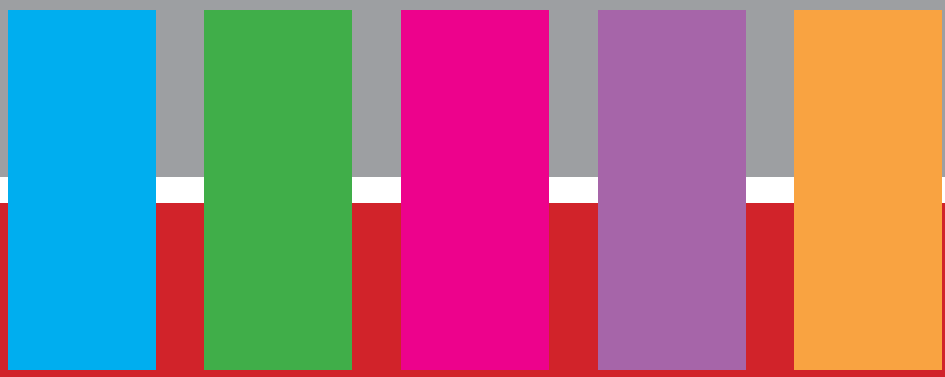
GUIDE DE L'INTELLIGENCE ÉCONOMIQUE POUR LA RECHERCHE



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DÉLÉGATION
INTERMINISTÉRIELLE
À L'INTELLIGENCE
ÉCONOMIQUE

PRÉFACE

Le monde est entré dans une « société de la connaissance » dans laquelle l'impact de la création et de la diffusion du savoir sur le développement économique est de plus en plus crucial. La recherche publique est le principal vecteur de cette création de savoir et joue à ce titre un rôle primordial pour l'économie d'un pays. C'est pour cette raison que le gouvernement a choisi d'investir massivement ces dernières années dans la recherche publique et l'enseignement supérieur, notamment en leur consacrant 22 milliards d'euros au travers du programme des investissements d'avenir.

Il est, dans ce contexte, essentiel que le monde académique s'intéresse aux questions d'intelligence économique. L'État s'est doté d'une politique publique en intelligence économique que chaque établissement d'enseignement supérieur et de recherche a vocation à décliner. Les principaux axes de cette politique sont la veille stratégique et la protection du patrimoine immatériel, le soutien à la compétitivité des entreprises et à la capacité de transfert des établissements de recherche publique, et la sécurité économique.

En pleine cohérence avec la Stratégie nationale de recherche et d'innovation, la politique d'intelligence économique développée par les universités, écoles d'ingénieurs, organismes et fondations de recherche doit permettre aux nouveaux savoirs et savoir-faire créés par ces établissements d'être diffusés dans le tissu économique et d'y devenir une semence pour l'innovation et la création d'emplois. Comme pour les autres grandes puissances scientifiques et techniques, cette stratégie doit aussi garantir la protection de notre potentiel scientifique et de notre patrimoine immatériel. Cela implique un travail de fond pour changer de nombreuses habitudes, créer de nouveaux réflexes, développer de nouvelles compétences au sein des établissements et atteindre de façon concrète un nouvel équilibre entre la diffusion des savoirs et des innovations et la protection de ce savoir.

Le présent guide de bonnes pratiques est une introduction à cette politique d'intelligence économique et vise à favoriser par des exemples sa mise en œuvre au sein des établissements. Il énonce des recommandations claires et renvoie à des documents de référence pour chacune des problématiques qu'il aborde. Il sera, j'en suis convaincu, des plus utiles pour tous les établissements de recherche et d'enseignement supérieur décidés à s'engager dans cette voie.

Si ce guide s'adresse au premier chef à la gouvernance des établissements, une politique d'intelligence économique ne sera pleinement efficace que lorsque tous les acteurs du système d'enseignement supérieur et de recherche se sentiront concernés et en appliqueront les bonnes pratiques au quotidien.

Je souhaite remercier la Délégation interministérielle à l'intelligence économique (D2IE) d'avoir pris l'initiative de réaliser ce guide avec la participation active du ministère de l'Enseignement supérieur et de la Recherche, d'autres administrations, universités et organismes de recherche. J'encourage pleinement les présidents et directeurs des établissements d'enseignement supérieur et de recherche à concevoir leur stratégie d'établissement en s'appuyant sur les recommandations de ce guide.

Laurent WAUQUIEZ
Ministre de l'Enseignement supérieur
et de la Recherche

SOMMAIRE

Pourquoi un guide de l'intelligence économique pour la recherche ?

La politique publique d'intelligence économique

Ce présent guide s'inscrit dans le cadre de la politique publique d'intelligence économique (IE), décrite dans la circulaire du Premier Ministre n° 5554/SG du 15 septembre 2011.

Cette politique s'organise autour de trois axes : la veille stratégique sur les évolutions et défis auxquels est confrontée l'économie française, le renforcement de la sécurité économique des entreprises et des établissements de recherche, et le soutien à la compétitivité de l'économie française. Sur ce dernier axe, la recherche académique a une place de choix, la politique publique d'IE préconisant de favoriser, dans un monde économique où l'innovation est le moteur de la croissance, le transfert des technologies issues du monde universitaire et de la recherche prioritairement vers l'industrie nationale ou communautaire, dans l'application d'une politique de retour sur investissement.

Ce guide s'adresse en priorité à la gouvernance des acteurs de la recherche publique, *i.e.* les universités, écoles, organismes de recherche et fondations, qui seront cités sous le vocable générique « établissements de recherche » dans le document.

L'intelligence économique et scientifique : un tabou pour la recherche ?

Si le monde de l'entreprise reconnaît aujourd'hui la nécessité d'intégrer l'intelligence économique dans sa politique de développement, celui de la recherche publique y reste encore relativement peu sensibilisé, se considérant généralement éloigné des préoccupations économiques et politiques, conscient de son devoir de diffusion et de libre accès aux savoirs et connaissances produits.

Les spécificités de la recherche

Bien que recherche publique et entreprises contribuent de concert à l'innovation et à la compétitivité économique nationale et communautaire, elles répondent à des logiques différentes et présentent des spécificités bien distinctes dans leur fonctionnement interne.

Les deux principales particularités du monde de la recherche, sont, d'une part, le caractère naturellement public de ses résultats et, d'autre part, le cadre de coopération internationale dans lequel il s'inscrit, même si tous les pays ne les appliquent pas avec la même intensité. En effet, l'idéologie de diffusion du savoir et la volonté de communication sur les activités et résultats sont à la base de l'esprit de la communauté scientifique. Cela pose un certain nombre de défis, notamment au niveau de la confidentialité nécessaire au transfert de technologie vers l'industrie et à la commercialisation des produits innovants. Sur le plan de la coopération internationale, le défi est d'évaluer et protéger la part qui revient à chaque partenaire et de préserver l'esprit de compétition indispensable à la créativité.

Enfin, le monde de la recherche a également la particularité d'être très fragmenté, parcellaire et hétérogène : force est de constater la grande dispersion géographique, sectorielle et fonctionnelle des établissements de recherche qui rend la définition et l'application d'une stratégie politique commune plus difficile.

Les responsabilités des établissements de recherche, sources de l'innovation et acteurs socio-économiques majeurs

Pour des raisons à la fois sociologiques, historiques et culturelles, associer le monde de la recherche académique à la politique publique d'intelligence économique ne semble pas aller de soi. Pourtant, il s'agit d'une entreprise tout à fait vitale et nécessaire. En effet, ces établissements sont des acteurs majeurs du paysage économique, se trouvant à la source même du « pipeline » de l'innovation. Il n'existe plus, dans le monde, d'économie qui ne soit

tirée par l'innovation, moteur de la croissance, créatrice d'emplois et garante de la vitalité de l'industrie.

Affirmer l'importance du rôle de la recherche, notamment publique, dans l'économie nationale et communautaire en termes de création d'emplois scientifiques et industriels, contribuer à une prise de conscience du milieu académique des retombées de ses activités pour l'intérêt général, sont autant d'ambitions centrales de ce guide.

Chaque établissement de recherche est intégré dans le système économique. En tant que source de l'innovation, la recherche est même le premier maillon de ce système et doit donc, en synergie avec sa mission de progrès et de diffusion des connaissances, tendre à maximiser son impact au profit de la société dans son ensemble. Son patrimoine scientifique constitue à ce titre un «bien commun» qu'il s'agit de protéger et de valoriser, de transformer en emplois sur le territoire national et en innovation, au service de la communauté.

Il ne s'agit pas de demander une valorisation industrielle immédiate de tous les résultats de la recherche. Il s'agit de mettre en place, d'une part, une politique de limitation des « fuites » du « pipeline de l'innovation », telles que les inventions transférées systématiquement pour exploitation à l'étranger avec une analyse insuffisante de la possibilité de les exploiter sur le sol national, les divulgations (conférences, salons, workshops, protection physique insuffisante des locaux et des systèmes d'information, etc.) ou les publications avant dépôt de brevet, et, d'autre part, une politique d'augmentation du débit du « pipeline », en limitant, notamment, le nombre d'inventions qui restent sur étagère.

Dans le cadre des indispensables coopérations internationales, l'identification de la « part » des travaux qui revient à la France n'est pas toujours facile, tant en termes de co-publications qu'en termes de dépôt et d'exploitation des brevets. Il conviendrait, là encore, de mettre en place une politique du « juste retour », de redynamiser l'esprit de compétition associé à celui de la coopération, pour permettre à la France de conserver sa place dans le peloton de tête des leaders scientifiques internationaux.

Associer recherche et enjeux économiques : la mise en place de schémas stratégiques d'établissement

Il s'agit bien de consacrer la compatibilité des missions de production et de diffusion du savoir et de contribution à la compétitivité économique nationale. Cela n'est toutefois possible qu'à condition que chaque établissement mette en place une politique adaptée, à laquelle ce guide donnera ses orientations générales. Cette politique passe notamment par une bonne gestion des domaines clés de l'établissement, dont les transferts de technologie vers l'industrie, la protection des données sensibles, la politique de propriété intellectuelle, mais aussi la promotion internationale de l'excellence de la formation et de la recherche dispensées par l'établissement. Ces défis déjà considérables sont encore complexifiés par l'internationalisation croissante des sujets de recherche et la multiplication des échanges transnationaux entre établissements de recherche (accueil de stagiaires ou de doctorants étrangers, partenariats de recherche internationaux, missions de chercheurs à l'étranger…). La politique de transfert de technologie requiert également la prise en compte de considérations juridiques et d'une vision stratégique d'ensemble de l'intérêt général.

La prise en compte de l'intelligence économique dans la politique d'un établissement consiste en la détermination et l'application d'une démarche visant à replacer la recherche académique au sein du système économique national, dans le dispositif de compétition internationale, qu'elle soit industrielle ou scientifique. La gouvernance des établissements pourra utiliser les recommandations de ce guide pour établir un schéma directeur de l'intelligence économique, à décliner dans ses différentes composantes, selon la structure de l'établissement.

Un guide s'adressant à l'ensemble des établissements de recherche publique

De nombreux guides spécifiques à un secteur, un type d'activité (valorisation, politique de sécurité des systèmes d'information ou PSSI, etc.) ou encore une catégorie particulière d'établissement ont déjà été publiés. Le présent guide s'adresse aux établissements de recherche publique dans leur ensemble, en tenant compte de ce qui fait leur

spécificité en tant que groupe et en choisissant ainsi d'aborder des problématiques qui concernent chacun d'entre eux. Il ne s'agit pas de formuler un nouveau texte réglementaire. Ce guide a été conçu pour souligner la nécessité de l'élaboration au sein de chaque établissement d'une vision stratégique comprenant impérativement un certain nombre de points incontournables. Ce texte entend fournir et mettre à disposition de l'ensemble des établissements de recherche des conseils et recommandations, mais surtout pointer les problématiques les plus fréquentes que les gouvernances d'établissement seront amenées à gérer.

En 2001, les ministères en charge de l'enseignement supérieur et de la recherche produisaient un texte de « recommandations pour l'adoption d'une charte de propriété intellectuelle (PI) par les établissements publics d'enseignement supérieur et de recherche ». Le présent document se situe dans la lignée du précédent, tout en replaçant les pratiques dans le contexte actuel de la mondialisation.

Construction du guide

Cinq fiches thématiques viendront donc nourrir la réflexion quant à la construction du schéma stratégique de l'établissement et aux objectifs qui devront lui être associés : assurer un bon positionnement français sur les marchés internationaux (objectif de compétitivité économique et progrès socio-économiques…) et favoriser le rayonnement de la recherche française.

- Fiche 1 : Veille stratégique
- Fiche 2 : Gestion du patrimoine immatériel
- Fiche 3 : Politique de Sécurité des Systèmes d'Information
- Fiche 4 : Développement de l'interface entre la recherche publique et le monde socio-économique
- Fiche 5 : Politique internationale

Les différents thèmes abordés ne constituent pas des domaines séparés. Ils doivent au contraire être mis en perspective afin d'assurer la cohérence globale du guide et du futur schéma stratégique de l'établissement qui orientera les décisions de l'établissement vers la mission de contribution à la compétitivité nationale. Il s'agit de rationnaliser et optimaliser les activités de l'établissement (publications, production de brevets, transfert de technologies…), d'éviter l'éparpillement des énergies et des efforts et d'avancer dans une direction commune et stratégique.

Les fondamentaux pour mettre en œuvre une politique d'Intelligence économique

• Engagement fort de la direction de l'établissement : initier la politique et mettre en œuvre ses principes de base au niveau de la direction, quotidiennement.
• Créer un service ou une fonction responsable et identifiable au sein de l'établissement pour le déploiement et le suivi de la politique d'intelligence économique.
• Ce service sera plus efficace s'il est directement rattaché à la présidence de l'établissement.
• Le périmètre de son action doit être clair et reconnu au sein de l'établissement. Il doit avoir les moyens de son ambition.
• En premier lieu, il doit donc définir son plan de travail. Il est indispensable, dans un premier temps, qu'il se concentre sur la mise en œuvre des bonnes pratiques les plus basiques pour que le déploiement de la politique d'intelligence économique soit concret et visible. Il doit définir ensuite une charte de l'IE et la déployer à tous les niveaux.
• Les responsables de la politique d'intelligence économique doivent sensibiliser tous les personnels de l'établissement sur l'intérêt de mettre en œuvre une telle politique. La pédagogie est indispensable (identifier des exemples internes ou externes évidentsqui démontrent la nécessité d'une telle politique).
• Dans certains cas, la formation des personnels à certains principes de base d'IE sera nécessaire. De nombreuses écoles, universités et CCI (chambres de commerce et d'industrie) proposent des modules ou des formations à l'IE. Un partenariat peut être des plus efficaces. Une identification préalable des compétences locales est nécessaire.
• Il est nécessaire d'identifier au sein de l'établissement, ou bien à l'extérieur (en région par exemple), les compétences utiles ou indispensables à la mise en œuvre d'une politique d'intelligence économique (services ou personnes en charge de la valorisation, de la veille, de la sécurité, de la sécurité des systèmes d'information, de l'international, laboratoires de recherche en IE, laboratoires ou chercheurs appliquant les principes de l'IE …).
• La politique d'intelligence économique de l'établissement sera plus efficace si ces conditions fondamentales sont réunies. La structure créée doit en être pleinement responsable.
• Concernant le déploiement de la politique d'IE en région, prendre connaissance des SRIE (schéma régional d'IE) et SRDE (schéma régional de développement économique).
• Les structures des différents établissements s'étant engagés sérieusement dans la mise en œuvre d'une politique d'intelligence économique devraient à terme être mises en réseau de façon à favoriser les échanges de bonnes pratiques et assurer une actualisation constante des politiques d'intelligence économique des établissements.

Les services qui peuvent vous aider

(liste non exhaustive)

• La D2IE (délégation interministérielle à l'intelligence économique) est chargée, par décret du 17 septembre 2009, de l'élaboration et de la mise en place de la politique publique d'Intelligence Economique (PPIE).
• Des correspondants ministériels IE sont en charge, dans chaque ministère, de la mise en œuvre de la politique publique d'IE.
• Les préfets de région sont pilotes du dispositif régional d'intelligence économique. Ils développent et font vivre un SRIE (schéma régional d'intelligence économique) et un SRDE (schéma régional de développement économique).
• Le DRRT (directeur régional de la recherche et de la technologie) participe au dispositif régional.
• Sur le plan de la sécurité économique, la DDRI (direction départementale du renseignement intérieur) et la gendarmerie assurent des missions régaliennes de protection du patrimoine et proposent des audits de sécurité et des actions de sensibilisation.
• Un correspondant IE des ministères économique et financier (chargé de mission régional en matière d'intelligence économique-CRIE) est placé auprès des DIRECCTE (directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi).
• Les CCI (chambres de commerce et d'industrie) proposent souvent des formations à l'IE ou des audits.
• L'INPI propose des pré-diagnostics de propriété industrielle, gratuits pour l'entreprise ou l'établissement. L'institut dispose de relais en région.
• AFNOR dispose de relais en région et propose des conseils en normalisation ou pré-normalisation.
• Des universités et des écoles proposent des formations à l'IE

1

Veille stratégique

Introduction

On peut distinguer au sein d'un établissement de recherche deux types de veille :

• la veille scientifique et technique pratiquée et maîtrisée au quotidien par les chercheurs dans leurs activités de recherche ;

• la veille stratégique pratiquée par la gouvernance de l'établissement.

La présente fiche thématique entend aborder de façon spécifique le second type de veille. La veille stratégique est une méthode visant à fournir les informations, puis l'analyse nécessaires à la gouvernance d'établissement. Dans le cas de l'intelligence économique, elle appuie la construction d'une politique ayant pour objectifs finaux, d'une part, le développement de l'innovation et des transferts maîtrisés de technologies vers l'industrie, prioritairement nationale et communautaire, dans un but de création d'emplois sur le territoire et, d'autre part, la préservation de la place scientifique et économique dans la concurrence internationale. Ces objectifs corrélés nécessitent une bonne maîtrise de l'environnement socio-économique de l'établissement. La veille stratégique peut y contribuer à travers l'identification :

• des différentes opportunités de développements technologiques ;

• des évolutions des politiques publiques ;

• des évolutions des contextes économiques et internationaux.

La première tâche est de déterminer le périmètre de la veille en fonction des objectifs fixés et des secteurs d'activités. Ensuite, une réflexion sur le mode d'organisation de la veille au sein de l'établissement et aux différents niveaux de l'organisme peut permettre de gagner en efficacité.

Types de besoins en information

Les besoins informationnels d'un établissement de recherche concernent de nombreux domaines :

• informations technologiques ;

• informations scientifiques et techniques ;

• informations réglementaires, normatives et juridiques ;

• informations financières et commerciales ;

• informations géopolitiques, sociologiques, socio-économiques et culturelles.

Les informations collectées doivent concourir à la maîtrise de l'environnement socio-économique en vue de la conduite de la politique stratégique de l'établissement. Bien connaître son environnement, bien connaître ses partenaires de coopération et la politique scientifique et d'innovation de leur gouvernement, permet de faire des choix de coopération plus efficaces et plus fructueux.

Cet objectif nécessite une veille sur les domaines suivants :

- les évolutions des sujets de recherche, les grandes tendances internationales. Il est notamment indispensable de positionner les sujets de recherche par rapport aux frontières technologiques, où la recherche est la plus productive en termes de publications et de brevets. Cette veille favorise également la détection de niches ;

- les classements nationaux et internationaux : il est indispensable de positionner l'établissement dans les environnements international et national et d'estimer sa part dans les résultats nationaux ;

- le suivi des résultats des partenaires académiques, industriels et commerciaux. Il est indispensable de situer en continu la qualité des partenaires scientifiques d'un établissement. Ceci permet d'éviter l'enlisement de coopérations improductives et permet l'identification de nouveaux partenaires potentiels en fonction de leurs résultats académiques.

- les appels à projets institutionnels nationaux et internationaux (notamment pôles de compétitivité en France, PCRD en Europe, appels nationaux…) ;

- les tendances et marchés dans le domaine de l'innovation ;

- la veille sociologique et le suivi des opinions publiques ;

- l'analyse pays : environnement juridique, politique (notamment de politique scientifique), économique, indicateurs scientifiques (publications, brevets, etc.) des pays partenaires scientifiques ou des pays potentiellement partenaires ;

- les programmes de recherche et de formation des pays et établissements étrangers, afin de profiter des occasions de coopération intéressantes (soit pour le sujet, soit pour le financement) et d'avoir une vision claire de la politique scientifique du pays et de ses objectifs économiques ;

- les pratiques d'intelligence économique dans les établissements de recherche étrangers ;

- l'e-réputation sur l'établissement. Il est

important de veiller à l'image que l'on renvoie, la réputation d'un établissement contribuant à celle d'un pays ;

- la veille réglementaire et normative nationale, européenne et internationale, notamment en termes de valorisation et d'innovation ;

- la détection de contrefaçon de brevets détenus par l'établissement ;

- la détection de plagiat d'articles scientifiques, ou d'usage indu de nom d'établissement.

Les sources

Une maîtrise des sources d'informations est nécessaire. Celles-ci doivent être hiérarchisées en fonction de leur fiabilité estimée.

L'information brevet[1][2]

Il est important d'insister sur le rôle particulier que jouent les documents brevets pour la veille d'un établissement de recherche. En effet, outre leur mission de protection de la propriété intellectuelle, les brevets constituent une des sources les plus intéressantes pour la veille stratégique d'établissement. L'ensemble des informations publiées dans un document de brevet ou qui peuvent être tirées de statistiques relatives aux brevets[3] (ce que l'on appelle « l'information brevet ») comprend à la fois des données techniques, juridiques, commerciales, portant sur l'évolution des dépôts dans un domaine ou dans un pays donné. L'étude et l'exploitation de ces données, par exemple à travers l'élaboration de cartographies de brevets, permettent d'aboutir à une analyse très fine et complète de l'environnement d'un établissement de recherche, tant au plan de l'état de la recherche qu'à celui du contexte économique et commercial. Ces analyses peuvent permettre d'évaluer la brevetabilité d'une invention, de détecter les tendances technologiques et techniques et d'identifier les équipes scientifiques travaillant sur ces problématiques.

Les bases de données de brevets sont un excellent outil de diffusion des connaissances : les brevets contiennent 70 % à 80 % de l'information scientifique et technologique. L'accès aux textes des brevets est simple et gratuit. Rappelons aussi qu'en Europe, la loi énonce que l'utilisation des brevets à des fins de recherche et développement est libre et gratuite (par exemple, en France, voir le Code de la Propriété Intellectuelle, article L. 613.5.b).

- Bases de données brevets gratuites : OEB / WIPO : Patentscope / INPI : FR-esp@cenet / Bases de données étrangères (notamment SIPO pour la Chine).

Il existe également des bases de données « brevets » payantes, dédiées en particulier aux professionnels.

Les normes

Les normes sont également une source majeure pour la veille stratégique appliquée à un établissement de recherche. Identifier les normes existantes dans les secteurs où la recherche est menée permet d'éviter de passer à côté de règles du jeu importantes pour le développement de ces technologies. De plus, faire une veille sur les normes existantes dans certains secteurs et les besoins en normes est susceptible de faire émerger des besoins en nouveaux programmes de recherche et de contribuer à leur définition. Les normes existantes reflètent en effet l'état de l'art, au-delà duquel on peut toujours innover. Enfin, les normes permettent souvent un effet de levier sur les transferts de technologie.

Autres sources

D'autres types de documents ou de manifestations constituent des sources pertinentes. Il s'agit de :

- les colloques, salons, conférences ;
- les rapports de réunions, de conférences ou groupes de travail dans les instances internationales scientifiques (fond des débats mais aussi évolutions de participations à ces manifestations) ;
- les sites scientifiques et les sites de publications scientifiques ;
- les sites internet des entreprises, des ONG, des lobbys… ;
- forums, blogs et réseaux sociaux professionnels et scientifiques (sont représentatifs des tendances même s'ils sont encore des sources peu fiables) ;
- Les textes de lois, les règlements nationaux, européens et internationaux (la veille réglementaire est particulièrement importante pour les chercheurs traitant de sujets à composante sociétale controversée comme les OGM, les cellules souches…) ;
- les retours d'expérience des chercheurs et

(1) PIR2 ET INPI : Guide de l'information brevet

(2) PALAZZOLI Fabien, Exploitation de l'information brevets dans un laboratoire de recherche public : identification de niches de développement technologique en bio-production et thérapie génique

(3) OMPI/WIPO, Les brevets comme moyen d'accès à la technologie

enseignants-chercheurs impliqués dans des coopérations internationales (la mise en place d'un dispositif de remontée et de traitement d'informations est nécessaire dans ce cas).

Les outils de veille

Il existe des outils gratuits en ligne, tels que :

• les fils RSS et les agrégateurs de flux RSS ; il conviendra d'identifier préalablement les sites ;

• les alertes proposées par de nombreux sites ; l'abonné est averti par email dès qu'un nouvel article correspondant aux mots-clés ou aux thématiques sélectionnés est publié ;

• les outils de veille réputationnelle ;

• …

Des chercheurs ou des entrepreneurs ont dressé des panoramas des outils de recherche gratuits proposés en ligne.

Il convient toutefois d'appeler à la prudence quant à la nature des recherches à effectuer avec ces outils gratuits et non protégés et la fiabilité des sources peut parfois être mise en doute. Pour la veille sur les sujets les plus sensibles et les projets stratégiques ou de diversification scientifique, des outils protégés sont à privilégier.

Il existe également des logiciels de veille non gratuits et plus spécifiques :

• des explorateurs de web souvent associés à des plateformes de diffusion de l'information

• des bases de données professionnelles d'information brevet

• des logiciels de veille réglementaire

• des outils de cartographie de l'information et des acteurs

• des outils dédiés à la recherche scientifique : un panorama des outils spécifiques à la recherche est disponible à l'adresse suivante : Quels outils pour la veille scientifique au CEMAGREF ? : *http ://halshs.archives-ouvertes.fr/docs/00/06/20/83/PDF/sic_00000122.pdf*

• …

Un outil de veille est un investissement. Toutefois, certains outils sont particulièrement coûteux. L'opportunité d'en faire l'acquisition doit être discutée.

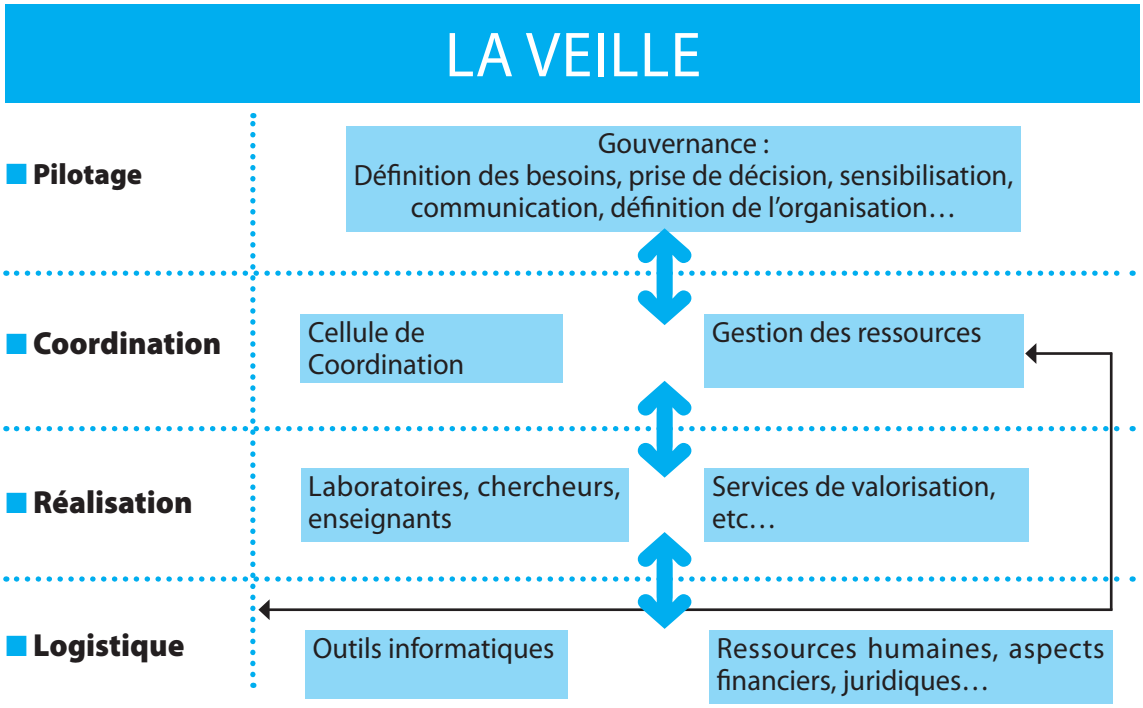
Structure organisationnelle de la veille stratégique au sein de l'établissement

La collecte aléatoire des informations ne suffit pas à constituer une politique de veille. La veille stratégique est à la fois une organisation et une « culture d'établissement », dont la définition peut se rapprocher de celle de « l'intelligence stratégique », élaborée par l'AFNOR[4] et le Comité Européen de Normalisation (CEN), soit « l'engagement d'un ensemble de démarches hiérarchisées et ordonnées permettant d'aboutir à la formulation d'analyses à haute valeur décisionnelle et une prise de décision de la part de la direction ». Ces démarches se traduisent par la mise en place d'une organisation spécifique à la veille au sein de l'établissement, chargée de la collecte, de la diffusion et du partage optimal des informations, ainsi que de l'orientation générale des recherches d'informations. La première tâche qui incombe donc à la gouvernance de l'établissement est une réflexion sur le mode d'organisation de la veille. Un audit de l'existant en matière de veille peut aider à mieux saisir les besoins de l'établissement et ainsi déterminer le périmètre de la veille. Ces besoins devront être réévalués de façon régulière.

Le schéma suivant a été élaboré, à titre d'illustration et d'exemple. Il présente une possible structure de veille à mettre en place, et s'inspire librement du schéma du système de management de l'intelligence stratégique de l'AFNOR. Il permet de mieux visualiser les différents acteurs mais aussi les échanges et les flux d'information nécessaires à l'efficacité et à l'intérêt d'une politique de veille. Tous les niveaux de gouvernance sont concernés par la veille, depuis le laboratoire jusqu'à la direction générale et chacun a un rôle à y jouer. Il conviendra de déterminer, en premier lieu, les périmètres dévolus à chaque niveau de gouvernance.

De nombreuses pratiques existent déjà à différents niveaux des structures, y compris dans les laboratoires. Une consultation préalable des acteurs, une adhésion de ceux-ci au système et une harmonisation des pratiques seront les garants de l'efficacité du dispositif.

(4) AFNOR, Le management de l'intelligence stratégique », Fascicule de Documentation FD X50-052 , mai 2011



Pilotage

La fonction du pilotage de la veille stratégique revient à la gouvernance. Il s'agit de définir les besoins, les orientations et le périmètre de la veille, en adéquation avec la programmation scientifique et technique, ainsi qu'avec la politique de gestion du patrimoine immatériel de l'établissement et la politique de coopération internationale. La sensibilisation et la communication en interne sur l'importance de la politique de veille font aussi partie de ses prérogatives. Enfin, en s'appuyant sur les produits de cette politique que sont l'information et l'analyse, la gouvernance prend les décisions relatives à la politique stratégique de l'établissement.

Réalisation

L'activité de veille stratégique à proprement parler, c'est-à-dire la collecte organisée des informations stratégiques, est réalisée principalement par les services d'information scientifique et technique, les services de valorisation, les chercheurs et autres personnels d'établissement, au titre de leur expertise scientifique, et des experts compétents sur les questions juridiques, financières ou commerciales.

Coordination

Les informations collectées par les acteurs chargés de la réalisation de la veille sont «nettoyées» (en fonction de leur pertinence et de leur fiabilité) et traitées, c'est-à-dire analysées et mises en perspective, par le service de coordination. Celui-ci fait le lien entre la gouvernance et les autres niveaux de l'établissement et s'assure que les activités de veille correspondent toujours à un réel besoin et que les informations collectées ont bel et bien une application et une utilité concrète.

Logistique

Le service de coordination gère également ce qui relève de la logistique, c'est à dire les outils :

- il juge de l'opportunité d'un investissement dans un outil de veille performant, mais potentiellement onéreux ;
- les ressources humaines : il peut choisir d'externaliser une partie des activités de veille ;
- le nouveau patrimoine que constituent les informations collectées (politique de gestion du patrimoine immatériel : voir fiche 2).

RECOMMANDATIONS

1. VEILLE STRATÉGIQUE

Pourquoi une veille stratégique ?

- La veille stratégique permet d'avoir une bonne connaissance de son environnement socio-économique, et notamment : d'identifier les opportunités de développements technologiques, de suivre les évolutions des politiques publiques et des contextes économiques et internationaux.
- La veille stratégique consiste en la collecte, la diffusion et le partage optimal des informations au sein de l'établissement.

Mettre en œuvre une politique de veille stratégique

- Trois étapes clés pour la mise en œuvre d'une activité de veille stratégique :
  1. s'assurer de l'adhésion des acteurs des laboratoires et des services ;
  2. déterminer le périmètre de la veille en fonction des objectifs ;
  3. déterminer un mode d'organisation de la veille optimal/adapté à l'établissement.
- Il est recommandé de créer une fonction de coordination de la veille.
- Il est nécessaire d'identifier les types de besoins en information (techniques, juridiques…), ainsi que leurs sources (brevets, normes…) et les outils de veille.
- Il est indispensable de hiérarchiser les sources d'information par niveau de fiabilité estimée.
- La veille « brevets » ou la veille « normes » sont indispensables au niveau international.
- La veille « pays » permet un meilleur pilotage de la coopération internationale.

Opportunités et points à discuter

- Il existe des outils de veille gratuits proposés en ligne. Il faut être prudent quant à la nature des recherches à effectuer avec ces outils : pour les sujets les plus sensibles, des outils protégés sont à privilégier.
- L'opportunité d'acheter un logiciel coûteux doit être discutée en regard des objectifs fixés et des besoins identifiés.
- Des cartographies d'acteurs ou de brevets sont des outils intéressants.

Bibliographie

- **AFNOR :** « Prestations de veille et prestations de mise en place d'un système de veille », Norme Expérimentale XP X50-053, Avril 1998. *http://www.boutique.Afnor.org/NEL5DetailNormeEnLigne.aspx?&nivCtx=NELZNELZ1A10A101A107&ts=5610196&CLE_ART=FA047502*
- **BODART Marie Gabrielle, FALIZE Caroline,** « Mise en place d'un service de veille collective pour la recherche : déroulement du projet, évaluation et perspectives », *Documentaliste-Sciences de l'Information*, vol 43, n° 2/2006, p. 108-120.
- **CENTRE DE RECHERCHE HENRI TUDOR (Luxembourg),** *Veille scientifique, technique, réglementaire et concurrentielle au centre de recherche Henri Tudor*, 2005.
- **SCIE,** *Guide des bonnes pratiques en matière d'intelligence économique*, février 2009. *http ://www.economie.gouv.fr/demarche-d-intelligence-economique*
- **PIR2 ET INPI :** Guide de l'information brevet, site de la PI et des PME. *http ://www.pi-r2.org/*
- **OMPI/WIPO,** *Guide de l'OMPI sur l'utilisation de l'information en matière de brevet. http ://www.wipo.int/freepublications/fr/patents/434/wipo_pub_l434_03.pdf*
- **OMPI/WIPO,** *Les brevets comme moyen d'accès à la technologie. http ://www.wipo.int/freepublications/fr/patents/434/wipo_pub_l434_02.pdf*
- **PALAZZOLI Fabien,** Exploitation de l'information brevet dans un laboratoire de recherche public : identification de niche de développement technologique en bio-production et en thérapie génique. *http ://www.univ-tours.fr/these-de-fabien-palazzoli-doctorat-de-sciences-de-la-vie-et-de-la-sante-202976.kjsp*
- **PALAZZOLI Fabien & al.,** « Les brevets, une source d'informations stratégiques pour les acteurs privés et académiques », *Biotech finances*, n°477, Editions européennes de l'innovation, 4 octobre 2010.
- **CEMAGREF** Quels outils pour la veille scientifique au CEMAGREF ?. *http ://halshs.archives-ouvertes.fr/docs/00/06/20/83/PDF/sic_00000122.pdf*
- **Base de données brevets WIPO/OMPI :** *http ://www.wipo.int*
- **Base de données brevets esp@cenet :** *http ://fr.espacenet.com/*
- **Base de données brevets Chine :** *http ://www.sipo.gov.cn/sipo_English2008/*

2

Gestion du patrimoine immatériel

Introduction

« La propriété intellectuelle est un outil primordial pour mettre en valeur, protéger l'innovation, organiser les partenariats de toutes sortes, et faciliter le transfert des laboratoires de recherche publics vers le secteur économique. La propriété intellectuelle en général, et le brevet en particulier, sont connus pour leur capacité de structuration des partenariats de recherche et développement entre organisations. En effet, le brevet permettant de matérialiser, d'identifier, et d'évaluer au moins une partie des apports intellectuels et des résultats d'un partenariat, il contribue à la sécurisation de la circulation entre partenaires d'une partie des flux de savoir partagés et/ou échangés[5]. »La propriété intellectuelle est donc un outil important et indispensable de la politique de recherche des établissements de recherche publique, dont elle est indissociable.

Le patrimoine immatériel d'un établissement de recherche public comprend non seulement des informations scientifiques, comme l'ensemble des informations se rapportant aux technologies qu'il développe, les connaissances, savoir-faire et compétences de ses ingénieurs et de ses chercheurs, ses résultats de recherche (fondamentale et appliquée) sous formes de brevets, de savoir-faire ou d'articles, ses bases de données, mais encore des informations d'organisation, telles que son portefeuille de contrats et de collaborations de recherche ou ses données nominatives, ou des informations « d'image », comme sa réputation auprès de la communauté scientifique internationale.

La gestion de ce patrimoine nécessite la mise en place de mesures de protection, qu'elles soient juridiques ou opérationnelles, visant à préserver l'intégrité, la disponibilité et la confidentialité de l'ensemble de ces informations. Elle nécessite également la mise en place de mesures de valorisation de ce patrimoine, au bénéfice de l'établissement mais également à celui de l'État, notamment en termes de création d'emplois industriels et scientifiques[6].

Gestion et protection des informations

L'information et sa circulation ont dans notre société actuelle une importance croissante. Une information peut être notamment une donnée, une connaissance, un renseignement ; elle peut être commerciale, organisationnelle, scientifique et technique ou de toute autre nature. L'information a toujours un support, qu'il s'agisse d'un support papier, informatique, télématique ou encore de la mémoire humaine ; elle peut également être incorporée dans un produit, un procédé ou un service, voire dans un matériel biologique ou vivant. L'information peut en outre être transportée par tout medium approprié ou être transférée via un tel medium. Par ailleurs, l'information a un caractère objectif, intrinsèque : elle n'est pas liée à son support : elle peut circuler, se « cloner » ou être copiée, dénaturée, modifiée, se multiplier et se propager. Finalement, l'information est un actif, de nature incorporelle, et a toujours une utilité. Il convient toutefois de signaler qu'une information n'est pratiquement jamais unique ou isolée ; elle s'insère dans un ensemble d'informations présentant une cohérence et un caractère pratique ou opératoire, notamment dans le cas de savoir-faire.

Tout établissement de recherche est exposé au risque de perte ou de détournement d'informations : vols de supports informatiques, diffusion involontaire d'information, suscitée ou non, interception de communications, manipulation du personnel, vol de documents (notamment les cahiers de laboratoire)… Les atteintes peuvent tout aussi bien toucher ses données scientifiques ou technologiques que ses outils ou moyens scientifiques, techniques et humains. **Les informations sensibles, ou stratégiques, peuvent être définies comme celles dont la perte ou la diffusion pourrait faire perdre à l'établissement le fruit de son travail ou une occasion de création d'emplois scientifiques ou industriels, en France ou en Europe.**

La protection des informations est une préoccupation de l'ensemble des acteurs impliqués dans l'établissement. Il est essentiel que chacun ait conscience de la sensibilité et de la vulnérabilité des informations qu'il détient, des pratiques frauduleuses

(5) *AFNOR FD-X50-146 ; Management de l'innovation - Management de la propriété intellectuelle* ; décembre 2010

(6) Ministère de la Jeunesse, de l'Éducation et de la Recherche, Ministère délégué Recherche et Nouvelles Technologies : *Protection et valorisation de la recherche publique*, Septembre 2003. p. 22

existantes et de la nécessité d'une diffusion maîtrisée de cette information en interne comme en externe. La politique de gestion des données doit permettre d'en préserver l'intégrité, la disponibilité et, dans certain cas, la confidentialité. Les mesures à mettre en place doivent permettre de travailler en toute confiance avec ses collaborateurs mais aussi d'être mieux armé pour se défendre face à des méthodes déloyales (piratage d'informations, espionnage économique, contrefaçon…).

Traçabilité et organisation du patrimoine de l'établissement

Assurer la traçabilité de son patrimoine immatériel consiste à donner un support, daté et signé, à chacune de ses informations. Bien organiser ses données, c'est accroître les potentialités de transfert maîtrisé de son patrimoine, notamment pour le savoir-faire secret qui n'est pas toujours intégralement codifié, mais doit l'être au maximum. En cela, c'est une étape préparatoire nécessaire à la politique de gestion du patrimoine et de confidentialité.

Mais c'est également **se doter d'éléments de preuve en cas de contentieux relatifs à la paternité de résultats ou à la propriété de données.** Ces informations peuvent ainsi se révéler utiles dans nombre de situations comme par exemple dans le cadre d'une collaboration de recherche où la traçabilité des informations est un gage précieux de prévention de conflits concernant la propriété des données fournies par chacun des partenaires et leur utilisation exclusive pour le projet. Il en est de même en cas de contentieux en revendication de la propriété de résultats (par exemple dans le cadre d'une procédure en interférence aux États-Unis notamment depuis la modification de la législation américaine à la suite de l'accord sur les ADPIC (Aspects des Droits de Propriété Intellectuelle qui touchent au Commerce) ou lors de la revendication de la propriété sur un logiciel). Toutes ces situations et informations sensibles doivent être identifiées.

Ce type de politique permet également de conserver une trace des informations, et cela même après le départ potentiel de leur auteur. En effet, il faut attirer l'attention sur le fait que le départ de certains personnels au savoir-faire unique, (codifié ou tacite), peut diminuer la valeur du patrimoine de l'établissement.

Plusieurs mesures concrètes peuvent illustrer cette politique :

- effectuer des dépôts auprès d'intermédiaires agréés ou officiels (enveloppes Soleau[7] auprès de l'INPI, dépôts de droit d'auteur contrôlés pour les logiciels et bases de données, actes probants par officiers ministériels, huissiers, notaires, etc.)[8] ;
- tenir à jour les cahiers de laboratoires[9], constituer des rapports scientifiques et techniques, tous éléments probants en cas de litiges et en matière d'interférence et permettant de codifier le savoir-faire secret non breveté ;
- archiver méthodiquement les données : assurer l'intégrité, l'authenticité des documents, ainsi que leur disponibilité (formats des supports informatiques adaptés) et leur imputabilité, mais aussi la protection des locaux d'archives en tenant compte des impératifs de confidentialité ;
- effectuer des copies de sauvegarde ; utiliser des logiciels de gestion de la configuration pour les logiciels (traçabilité des différentes versions...) ; utiliser un marquage des documents confidentiels ;
- assurer le transfert des connaissances des personnels permanents, des stagiaires et des doctorants avant leur départ du laboratoire.

Référentiels de sensibilité

La protection des informations sensibles et de leur support suppose une hiérarchisation des informations en fonction de leurs besoins de protection. L'identification des informations stratégiques reste un préalable à toute bonne politique.

Il s'agira également de déterminer un mode de diffusion et d'accès adapté à chaque niveau. Il est néanmoins à rappeler[10] que surprotéger des informations en les sur-qualifiant de sensibles et ne les divulguer qu'à quelques privilégiés risque de créer un climat de méfiance et peut nuire à l'activité de l'établissement, puisque l'information ne sera pas

(7) INPI : *L'enveloppe Soleau, tout ce qu'il faut savoir avant de déposer une enveloppe Soleau*

(8) Ministère de la jeunesse, de l'éducation et de la recherche, Ministère délégué Recherche et Nouvelles Technologies : *Protection et valorisation de la recherche publique, op cit, p. 9*

(9) *CNRS/MESR, Le cahier de laboratoire national*, Février 2010

(10) *SCIE, Guide des bonnes pratiques en matière d'intelligence économique*, Février 2009, p. 16

accessible au collaborateur qui en aura besoin et qui saura la valoriser. De nombreux classements sont envisageables.

On peut par exemple réfléchir à quatre niveaux :

• l'information est **générale, non protégée**, ouverte à l'ensemble du personnel, et en cas de divulgation en dehors de l'établissement les conséquences sont nulles ou minimes ;

• l'information est un atout promotionnel au service de la réputation de l'établissement, elle est « **à diffuser** », i.e. à mettre en valeur dans le cadre d'une politique de communication. Ces atouts choisis sont susceptibles de contribuer à l'aspect influence de la politique d'intelligence économique de l'établissement. Il conviendra néanmoins de les sélectionner avec soin afin de ne pas dévoiler au grand public des informations sensibles ou stratégiques. Dans le cadre de la consultance notamment, il doit être rappelé que les recommandations évoquées dans ce guide s'appliquent d'autant plus scrupuleusement dans ces situations en externe, présentant un danger potentiel de fuite d'information, dommageable pour l'établissement, mais également pour l'emploi et l'intérêt général ;

• L'information est **restreinte** car sa divulgation peut nuire de façon importante à l'établissement et à l'intérêt public : la divulgation d'informations concernant les partenaires industriels, par exemple, peut se traduire par une perte de confiance de ces derniers ;

• l'information est **strictement confidentielle** car sa divulgation porterait lourdement préjudice à l'établissement (secrets de fabrication, stratégie de l'établissement, stratégie du MESR, de l'État …) et/ou à l'intérêt public : pertes de chances de créer de l'emploi territorial, pertes financières élevées, graves atteintes à la notoriété / image de marque.

Politique de contrôle d'accès aux informations[11]

Les fuites d'informations sont réalisées selon deux modes principaux :

- l'accès indu aux informations, par intrusion dans les locaux, par intrusion informatique, par vol d'ordinateurs ou de supports électroniques (disques durs, clés USB, etc.), par vol ou copie de documents, etc. ;

- la diffusion indue de ces informations, volontaire ou non (conférences, salons, discussions téléphoniques ou dans les espaces publics, discussions informelles, rapports de stage etc.) et éventuellement suscitée (audits intrusifs, questionnement par téléphone ou direct lors de conférences, discussions informelles etc.).

Pour maîtriser les fuites d'informations, il convient de mettre en place des politiques de :

- **protection des accès aux locaux**. Les plus sensibles sont notamment les locaux abritant des produits dangereux, les calculateurs et moyens informatiques centraux, les espaces de stockage, les laboratoires abritant des activités de recherche stratégiques, les archives, les cahiers de laboratoires, etc. Il conviendra dans un premier temps de les identifier et de les répertorier, puis de déterminer sous quelles conditions ils doivent être accessibles au personnel de l'établissement et aux personnes extérieures, en application des dispositions règlementaires en vigueur. Ces modes d'accès doivent toujours apparaître dans les contrats, notamment dans le cas des unités mixtes. Il est important de s'assurer que tous les personnels sont couverts et que chaque unité dispose d'un règlement intérieur incluant la question des contrôles d'accès. La fermeture de ces accès et des comptes informatiques, ainsi que la restitution du matériel lors de la fin du contrat d'un membre du personnel de l'établissement, des stagiaires, intérimaires et chercheurs invités est également à organiser ;

- **protection des systèmes d'information** (voir fiche 3 PSSI) ;

- **sensibilisation des personnels**. Une grande partie des pertes d'information provient d'erreurs humaines, souvent involontaires et qu'une sensibilisation ou une formation appropriée suffit à réduire. La mise en œuvre effective d'une politique de sensibilisation des personnels, la définition de règles de bonnes pratiques pour les déplacements à l'étranger, les accords de coopération, la gestion des stagiaires et visiteurs ou la protection intellectuelle, est préconisée. De même la remontée d'informations (sous forme, par exemple, de rapport d'étonnement sur tout incident interne ou externe, comme par exemple une tentative de diffusion suscitée d'informations sensibles ou une tentative d'intrusion) doit être mise en place. Le fonctionnaire de sécurité et de défense (FSD) doit être informé et consulté pour tout incident notable. Un incident localisé s'insère

(11) CEA : *Livret du référent : Accueil d'un collaborateur. Protection du patrimoine scientifique et technique du CEA*, Juin 2011.

souvent dans un schéma plus global et prend alors une importance accrue ;

- **prévoir la PI dans les contrats**. Les droits et les responsabilités de chacun seront d'autant plus clairs qu'ils auront été formalisés à travers des outils juridiques et contractuels (contrats, chartes, conventions de stage…), avant le démarrage d'une coopération ou avant une embauche[12]. Ces documents confèrent un caractère visible et explicite à la politique de protection du patrimoine de l'établissement et permettent de sensibiliser et d'alerter le personnel sur ces problématiques. Cette politique de contractualisation s'applique tout autant, si ce n'est plus, aux partenaires extérieurs (sous-traitants, prestataires, donneurs d'ordres, laboratoires extérieurs nationaux ou internationaux, entreprises…). En effet, la mise en place d'un partenariat ne signifie pas le partage total de toutes les informations, même dans le cas d'un audit commandité par un donneur d'ordre. En toutes circonstances, la diffusion d'information se doit de rester maîtrisée. Chaque partenariat implique un accord sur les responsabilités relatives à leur protection. Des clauses spécifiques doivent être incluses dans les contrats de travail des employés concernés par les partenariats (clauses de confidentialité restant valides après la rupture du contrat, habilitations, clauses de restitutions de données confidentielles, clauses de non-concurrence, attribution sans ambiguïté des inventions et de la propriété intellectuelle à l'employeur, etc.), et des chartes de confidentialité ou de bonnes pratiques peuvent être diffusées afin de recueillir l'engagement des personnels à respecter les règles de sécurité et de confidentialité de l'établissement. Il est par ailleurs recommandé d'effectuer une cartographie précise des activités des prestataires extérieurs de l'établissement afin de pouvoir définir de manière optimale leurs besoins en matière d'accès aux locaux et aux informations.

Cas particulier : au sens de la défense des intérêts fondamentaux de la Nation, des informations, des secteurs ou des structures sont gérés selon un régime spécifique et il conviendra de porter alors une attention particulière aux textes suivants, dont le non-respect peut entraîner des poursuites pénales.

Dispositif réglementaire en vigueur relatif à la protection du potentiel scientifique et technique de la Nation (PPST)

Le dispositif réglementaire en vigueur a pour objectif de renforcer la protection des activités scientifiques dans les unités de recherche. Il ne porte pas préjudice aux échanges et coopérations qui découlent naturellement de ces activités. Ce dispositif s'appuie sur un décret et deux arrêtés qui précisent la mise en œuvre de mesures de protection spécifiques :

- Il définit des secteurs scientifiques et techniques dits « protégés » qui font l'objet d'une concertation avec les pouvoirs publics pour la mise en place de mesures de protection minimale, notamment dans le cadre des coopérations internationales et des congrès.
- Les unités de recherche plus sensibles, qui mènent des activités dont les risques de récupération ou de captation peuvent porter atteinte aux intérêts fondamentaux de la Nation, bénéficient d'une protection renforcée notamment pour les visites, inscriptions en thèse, stages ou autres contrats passés avec l'unité.
- Le dispositif prévoit également la création de zones spécifiques dites « zones à régime restrictif » (ZRR) dans les unités où l'activité est considérée comme très sensible, dont l'accès est réglementé.

À noter : les FSD des établissements de recherche et les hauts fonctionnaires de défense et de sécurité (HFDS) des ministères de tutelle sont chargés de la mise en œuvre du dispositif. Ils peuvent fournir au besoin toutes les informations sur les modalités de concertation entre les unités de recherche et les pouvoirs publics.

(12) *SCIE, op cit*. p. 21

Textes en vigueur :

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.
Code pénal. Livre IV : Des crimes et délits contre la nation, l'État et la paix publique, titre Ier « Des atteintes aux intérêts fondamentaux de la nation »
- **Article 410 -1**.
- **chapitre I, section 3 :** « De la livraison d'informations à une puissance étrangère » : Articles 411-6 à 411-8.
- **chapitre III, section 1 :** « des atteintes à la sécurité des forces armées et aux zones protégées intéressant la défense nationale » : Articles R 413-1 à R 413-5-1 et article 413-7.
- **chapitre III, section 2** « Des atteintes au secret de la défense nationale » : Article 413-10-1.

Secret, informations classifiées, contrôle des exportations, textes en vigueur

Code pénal. Livre II : Des crimes et délits contre les personnes, chapitre VI, section 4, §1 : « Atteinte au secret professionnel » : Articles 226-13 à 226-14
Code de la défense. Livre III : Régimes juridiques de défense d'application permanente. Protection du secret de la défense nationale :
Articles R2311 à R2311-9 : Informations et supports classifiés.
Articles L1332-1 à L1332-7 : Protection des installations d'importance vitale.
Articles L1333-1 à L1333-7 : Protection et contrôle des matières nucléaires.
Instruction Générale Interministérielle n°1300 / SGDSN du 30 novembre 2011 portant sur la protection du secret de la défense nationale.
Règlement européen (CE) n° 428-2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit des biens à double usage.
Recueil de mesures de protection des SI traitant d'informations sensibles non classifiées de défense du Niveau Diffusion Restreinte. Document issu du GT Refonte de l'IIM n°486 (Mars 2011).

Politique de propriété intellectuelle(13)

Le dépôt de propriété intellectuelle répond à deux objectifs : garantir ou exiger des droits d'exploitation d'une invention ou d'un modèle (notamment applicable par le dépôt de titres) et assurer le moyen de preuve d'antériorité pour protéger des droits a posteriori, *i.e.* pour démontrer qu'on avait une connaissance antérieure au dépôt par un tiers (notamment applicable par la déclaration bases de données publiques, le dépôt d'enveloppes Soleau, les cahiers de laboratoire …).

Deux grandes catégories existent :

• la propriété industrielle avec les brevets (inventions techniques), les marques (signes distinctifs), les dessins et modèles (protections de formes), les connaissances techniques (savoir-faire secret, topographie de semi-conducteurs, certificats d'obtentions végétales). Elle s'acquiert par un dépôt de titres (brevets, marques, modèles d'utilité, etc.) et parfois par usage (dénomination sociale, nom commercial et enseignes). En France, les modèles d'utilité ne sont pas utilisés ;

• la propriété littéraire et artistique avec le droit d'auteur, le droit des bases de données(14) et les droits voisins (qui incluent le droit des artistes-interprètes et le droit des producteurs de phonogrammes, vidéogrammes et entreprises audiovisuelles). Elle s'acquiert sans formalités, du fait même de la création de l'œuvre.

(13) *Charte de propriété intellectuelle et de transfert de technologie et de connaissance des instituts Carnot*, politique relative à la propriété intellectuelle (p. 2, paragraphes 1 à 7)

(14) *Concernant les bases de données : Code de la PI* : L341-1 à 341-2 / L34265 / L343 à L343-7 et Code du patrimoine, Titre III Dépôt légal, articles L131 à L133

Le logiciel est concerné par ces deux aspects : le droit d'auteur protège sa forme d'expression, le brevet d'invention protège ses fonctionnalités techniques[15].

La politique de propriété intellectuelle d'un établissement de recherche revêt diverses fonctions[16]. Parmi elles, on peut compter la protection du patrimoine scientifique et technologique, la lutte contre la contrefaçon, mais aussi la mise en valeur des titres (gestion de portefeuille de brevets) en vue d'un développement maîtrisé des partenariats et projets collaboratifs avec des acteurs de la recherche ou de l'industrie[17]. Construite en adéquation avec la programmation scientifique et technique de l'établissement, la politique de propriété intellectuelle est un outil important de compétitivité, qui permet de structurer la recherche et les partenariats pendant les phases ultérieures de R&D, puis d'optimiser les chances de transfert bien contrôlé de technologies sous des formes diverses (contrats de partenariats de recherche et de développement, contrats de licence, créations de *start-up*, etc.[18]). Il est à souligner que la perte, ou l'exploitation non optimale des titres de propriété intellectuelle a des conséquences néfastes (notamment financières) pour l'établissement, mais aussi et surtout pour la compétitivité économique et la création d'emplois en France et en Europe. Ces risques sont d'autant plus sérieux s'il s'agit d'un partenariat international, c'est-à-dire si l'un des partenaires dépend d'une juridiction étrangère, hors UE. Il est cependant possible pour un établissement de mettre en place des mesures afin d'éviter que les retombées positives des travaux de ses chercheurs ne profitent, au détriment des intérêts français et communautaires, à d'autres économies. Les conseils et recommandations préconisés dans cette fiche doivent donc être considérés dans ce contexte particulier.

Brevet, secret ou publication ?

Le brevet n'est pas le seul moyen de protéger les résultats de la recherche d'un établissement. En effet, les moyens de protection[19] diffèrent en fonction de la nature de « l'objet » à protéger : il est parfois nécessaire de maintenir le secret autour d'un procédé, savoir-faire, etc. Il faut donc trouver un autre moyen de protéger des résultats car un brevet est destiné à être rendu public. En effet, un brevet fera obligatoirement l'objet d'une publication 18 mois[20] après le dépôt de la demande et une politique de secret n'est donc plus envisageable.

Le secret est une forme très efficace de protection d'une invention, à condition qu'il soit maintenu, ce qui est particulièrement difficile à réaliser, notamment lorsque l'invention est issue des résultats de la recherche publique[21]. Lorsqu'il peut être conservé, celui-ci pourra être préféré au brevet, par exemple lorsque la contrefaçon est difficile, voire impossible à démontrer. Si le secret ne peut pas être maintenu, notamment parce que l'inventeur divulguera son invention, le dépôt d'une demande de brevet sera privilégié.

Il est donc possible d'avoir dans un premier temps une politique de secret, puis dans un second temps une politique de brevet ; l'inverse est en revanche impossible.

Les chercheurs hésitent parfois à recourir au dépôt de brevet, craignant que ce dépôt ne se fasse au détriment de la publication scientifique. Il est pourtant important de souligner que **dépôt de brevet et publication ne sont pas incompatibles**. Les

(15) *Concernant le logiciel : Code de la propriété intellectuelle* : L122-6 à 122-6-2 / L113-9 / L122-4

(16) *MINEFI, La propriété industrielle*

(17) *CEA, La valorisation au CEA, dossier de presse, Juin 2008, p. 10*

(18) *Document AFNOR fd x50-146, Management de la propriété intellectuelle ; décembre 2010, op cit*

(19) *Université de Strasbourg, Service de Valorisation, Guide des bonnes pratiques de valorisation , Juin 2009*

(20) *INPI : Le brevet, les 16 étapes clés, p. 12*

(21) MEJR, *op cit,* p.39

publications portant sur des résultats scientifiques, même amenés à être brevetés et exploités sont tout à fait possibles, dans la mesure où ces publications interviennent chronologiquement après le dépôt du brevet. Le contraire n'est cependant pas possible en raison du critère de nouveauté absolue nécessaire à la validité du brevet[22]. Il est donc à retenir que la culture du brevet n'est nullement contradictoire avec celle de la publication. En l'absence de dépôt de brevet, une publication sans divulgation du savoir-faire technique est parfois possible si la publication se limite à l'énoncé du problème scientifique et à la description des résultats scientifiques, sans décrire la solution technologique sous –jacente qui permet de passer du problème à la solution.

Stratégie de valorisation

La mise en place d'une politique stratégique[23] implique, au-delà de l'objectif général d'accroissement du nombre de dépôts de brevets, une approche de la gestion des brevets par domaines technologiques et/ou par marchés applicatifs visés. Un ensemble cohérent de brevets représente en effet une valeur économique supérieure à la somme des brevets individuels et constitue un atout pour l'exploitation industrielle des résultats. Une politique de propriété intellectuelle et la constitution de portefeuilles de brevets doivent aussi être élaborées dans un souci de rationalisation et n'ont de véritable sens que si chaque dépôt de brevet correspond à une exploitation future.

La mise en œuvre de cette stratégie implique au départ une politique d'encouragement au dépôt de brevet[24] (des réductions de redevances sont notamment accordées aux organismes à buts non lucratifs). Elle requiert ensuite une sélection des brevets maintenus et/ou étendus sur la base d'un plan de valorisation bien défini. Si dans les phases amont, le dépôt de brevet est encouragé, la sélectivité s'accroît par la suite lors des phases de publication et d'extension internationale des brevets ; elle tient compte de l'environnement technique du brevet (exemples : l'invention est antériorisée ou la détection de la contrefaçon est impossible) mais aussi d'appréciations plus subjectives liées à la politique scientifique, technologique et de valorisation de l'établissement.

Cette sélection se fait également en conformité avec les avis d'experts scientifiques, juridiques et commerciaux chargés par la gouvernance de valoriser les projets et privilégie l'exploitation des brevets par des entreprises françaises ou européennes.

Cette politique peut impliquer la recherche d'accords avec des partenaires disposant de brevets complémentaires, pour pouvoir constituer des portefeuilles suffisamment garnis.

Dans le cadre des programmes d'investissements d'avenir, sont mises en place des « sociétés d'accélération du transfert de technologies » (SATT) ayant vocation à proposer leurs services à l'ensemble des établissements et organismes de recherche du territoire national. Elles auront pour principale mission le financement et l'accompagnement de projets de R&D en phase de maturation. L'intelligence économique reste toutefois une fonction non externalisable des établissements, qui restent maîtres de leur politique de valorisation.

Les SATT devront ainsi veiller à faire bénéficier prioritairement le tissu industriel et de services français ou communautaire des résultats de la recherche académique, dans le cadre de l'application de la circulaire interministérielle 5554/SG du 15 septembre 2011 « actions de l'État en matière d'intelligence économique ».

Dans cette optique, la question de l'introduction de capitaux étrangers dans les SATT devra être bien étudiée en tant que de besoin.

(22) *INPI : Ce qui peut être breveté. Nouveauté*

(23) *CEA La valorisation au CEA, Dossier de Presse, 2010, p. 10*

(24) *INPI : Tarif des procédures*

Dangers et dérives du « business » de la valorisation :

Celle-ci ne doit pas avoir pour but de vendre et transférer de la propriété intellectuelle au plus offrant, sans vision stratégique de long terme pour l'industrie nationale. Ainsi, la valorisation ne devrait pas être optimisée en fonction des redevances perçues, mais en termes d'emplois créés, préférentiellement sur le sol national ou européen(25). Le marché de la propriété intellectuelle ne doit pas être un marché comme les autres, il a vocation à être une semence pour des projets industriels innovants et créateurs d'emploi. La France exporte plus de DPI (droits de propriété intellectuelle) à l'étranger qu'elle n'en importe : le transfert de technologies françaises vers l'étranger représente en 2009 un montant de 9,4 milliards d'euros (vente de licences), et l'achat de licences étrangères représente 5,3 milliards d'euros, soit une balance exportatrice excédentaire de 4,1 milliards d'euros(26). Dans le même temps la désindustrialisation perdure : « … sur la période 1980-2007, l'industrie française est passée de 5,3 à 3,4 millions d'emplois, soit une baisse de 36 %. La part de l'industrie dans l'emploi total a reculé de 11 points (passant de 24 % à 13 %)(27).

La politique de valorisation d'un portefeuille de brevets d'établissement de recherche publique doit bénéficier prioritairement à l'économie nationale ou communautaire et lui assurer des avantages compétitifs. Elle doit être tournée vers la relance du tissu industriel national et le développement de produits, procédés et services nouveaux à valeur ajoutée. Elle doit participer au développement d'une industrie performante créatrice d'emplois nationaux. Elle doit prendre en compte les recommandations décrites dans la politique publique d'intelligence économique, définie en novembre 2010 :

« l'État doit donc concentrer son action dans trois directions majeures :

– La valorisation de la recherche publique en priorité au profit des entreprises françaises ou européennes. Le transfert technologique depuis la recherche publique doit fournir à l'industrie et aux services français ou européens des avantages technologiques leur permettant de gagner des marchés à l'export, dans le respect des règles et impératifs liés au contrôle des exportations de biens et technologies sensibles. Il doit leur garantir un haut niveau d'innovation et d'autonomie nationale. Les investissements consentis par la France dans son système de recherche public et privé doivent générer un retour sur investissement, qui permettra le maintien du niveau actuel de qualité du système de recherche national.

– ….»

(25) *Managing university Intellectual Property in the Public Interest ; National Research Counsil ; USA* ; October 2010 ; The national academies press

(26) *World Bank statistics ; royalties and licences fees payments ; royalties and licenses fees receipts* ; 2011

(27) *Lettre Trésor-Eco de septembre 2010* – « Le recul de l'emploi industriel en France de 1980 à 2007 : quelle est la réalité ?

La valorisation dans l'économie nationale ou régionale, des exemples internationaux :

Plusieurs grands pays leaders dans le domaine de l'innovation technologique ont pris des mesures pour favoriser l'exploitation préférentielle des résultats de la recherche publique sur leur territoire national. Il conviendra que les établissements de recherche français en tiennent compte dans leurs accords de coopération scientifique avec ces pays.

Des mesures, incitatives ou prescriptives, sont de type « nécessité d'un accord gouvernemental pour le transfert ou la concession de DPI vers des pays tiers » ou « remboursement de tout ou partie des subventions allouées aux établissements ou entreprises pour le développement des technologies innovantes ». Selon l'OMPI, il s'agit des cinq premiers pays déposants de brevets par leurs résidents (hors Office Européen des Brevets)(28).

Les États-Unis ont été les premiers à adopter ce type de mesures en 1980, à travers le Bayh-Dole Act. L'OCDE indique, dans son rapport *Turning science into business : patenting and licensing at public research organizations (OECD Breakfast series ; 28/05/2003* p10), que l'Allemagne(29), la Corée du Sud et le Japon ont adopté des mesures d'objectif comparable.

La Chine(30) a adopté des mesures pour promouvoir l'innovation nationale et le développement de l'industrie nationale dans sa loi de décembre 2007 (*Law of the People's Republic of China on Progress of Science and Technology*).

Protection des titres de propriété intellectuelle

Mener à bien une politique de protection du patrimoine immatériel et plus particulièrement des titres de propriété intellectuelle nécessite de bien identifier les situations dans lesquelles les titres de propriété intellectuelle peuvent être sous-exploités, sous-évalués, contournés, ou encore perdus. La production de propriété intellectuelle est le fruit d'un investissement important à la fois financier et humain, qui restera vain si elle n'est pas exploitée de manière optimale. Ces situations de diminution de la valeur de la propriété intellectuelle d'un établissement sont susceptibles de porter préjudice à l'établissement et à l'économie.

• **Concession de licences d'exploitation** (exclusives ou non)(31). La propriété intellectuelle n'a de véritable valeur que si elle est correctement exploitée dans un projet innovant industriel et commercial, qui sera créateur d'emplois et de croissance. La prudence est donc de mise quant à la concession de licence d'exploitation : il s'agit de s'assurer que le partenaire unique à qui sera confiée l'exploitation de la propriété industrielle sera réellement en mesure de remplir cette mission. À cet égard, les licences exclusives, qui dans beaucoup de cas sont nécessaires pour donner au licencié une véritable position concurrentielle, lui permettant de développer ses activités et de créer des emplois de manière significative, devront être assorties obligatoirement des dispositions suivantes préservant l'intérêt public :

(28) *OMPI/WIPO Stats : C.1 Demandes déposées par des résidents, par office*

(29) *Nebenbestimmungen für Zuwendungen auf Kostenbasis des Bundesministeriums für Bildung und Forschung an Unternehmen der gewerblichen Wirtschaft für Forschungs- und Entwicklungsvorhaben (NKBF 98) Stand : April 2006 ; clause 16.2*
Besondere Nebenbestimmungen für Zuwendungen des Bundesministeriums für Bildung und Forschung zur Projektförderung auf Ausgabenbasis (BNBest-BMBF 98) Stand : April 2006 ; clause 10.2

(30) *Law of the People's Republic of China on Progress of Science and Technology* (Adopted at the 2nd Meeting of the Standing Committee of the Eighth National People's Congress on July 2, 1993 and amended at the 31st Meeting of the Standing Committee of the Tenth National People's Congress on December 29, 2007)

(31) Aux USA, 40 à 45% des licences de la recherche publique sont exclusives ; voir notamment *AUTM Licensing Survey*, FY 2005 à 2009

– définition d'un domaine d'exploitation exclusif, permettant au laboratoire de valoriser dans d'autres domaines afin de maximiser les retombées industrielles ;

– fixation de seuils d'exploitation minimale en deçà desquels le licencié perd l'exclusivité ;

– fixation d'un minimum garanti de redevances, incitant le licencié à exploiter. Laisser la propriété intellectuelle sans application, c'est perdre une occasion de participer à l'effort économique, mais c'est aussi rendre inutiles les moyens et les travaux de recherche mis en œuvre par l'établissement de recherche pour en arriver au dépôt de brevet.

• **Création de *spin off***. La participation à la création d'une entreprise innovante peut constituer une formidable opportunité pour un établissement de recherche public, à condition de parvenir à garder le contrôle sur les activités de l'entreprise et sur ses titres de propriété intellectuelle. Dans le cas particulier où l'établissement choisit d'abandonner sa propriété intellectuelle à la *spin-off* au moment de sa création (ce cas devrait rester minoritaire vu les risques décrits ci-après), il conviendra notamment de bien évaluer le risque de dilution de la valeur de l'apport de propriété intellectuelle de l'établissement en cas d'augmentation massive de fonds par un autre contributeur. La valeur relative des titres de la propriété intellectuelle peut être grandement diminuée et l'établissement perdra ainsi le contrôle d'une société pourtant créée grâce aux fruits de ses travaux scientifiques et techniques. Cette dimension sera à prendre en compte lors des négociations d'un contrat de création d'entreprise issue de la recherche publique.

À cet égard, le mode de transfert de technologie préféré en cas de création de start-up devrait suivre les recommandations suivantes :

• définition d'un domaine d'exploitation exclusif, permettant au laboratoire de valoriser dans d'autres domaines afin de maximiser les retombées industrielles ;

• fixation de seuils d'exploitation minimale en deçà desquels le licencié perd l'exclusivité ;

• fixation d'un minimum garanti de redevances, incitant le licencié à exploiter.

Par ailleurs, la poursuite de la collaboration avec la *spin-off* sous forme d'accord de R&D postérieur à l'accord de licence initial, permet de continuer à créer de la valeur économique qui sera exploitée par la start-up, tout en renforçant l'ancrage de l'activité sur le sol national. Le laboratoire commun entre l'établissement public et la spin-off est la forme la plus aboutie de cet ancrage.

• **Contrefaçon**

La défense des droits, suite à l'identification d'une contrefaçon, est également un élément fort de la stratégie de valorisation(32). Il est important que l'établissement de recherche soit reconnu sur le marché comme un acteur défendant fermement ses droits. Tous les salariés doivent se sentir concernés. Parmi ceux-ci, l'inventeur est la personne la plus à même de détecter une contrefaçon ainsi que les « responsables de portefeuilles ».

Il importe de prendre en compte également le risque de contentieux généré par la diffusion sous forme de logiciels libres des codes sources qui ont leur origine dans des logiciels propriétaires auxquels les chercheurs ont eu accès via des collaborations.

Si la recherche d'un accord à l'amiable avec un contrefacteur reste évidemment à privilégier, il est toutefois nécessaire de prévoir le cas où le contentieux s'engage sur le terrain judiciaire. Des solutions intermédiaires peuvent également être envisagées permettant à l'établissement de limiter les frais de procédure à engager (cofinancement avec un industriel ou bien encore prise en charge par l'industriel des coûts liés à la procédure judiciaire avec une juste rétribution de ce dernier en cas de succès). Il est important de noter qu'aujourd'hui, de plus en plus de brevets font l'objet de litiges, les actions en contrefaçon ou les oppositions (au niveau européen) sont considérées comme un élément clé de la politique de protection du patrimoine immatériel. Un établissement de recherche doit prendre en compte le fait qu'une procédure(33) en contrefaçon peut présenter des risques s'il existe des failles juridiques dans la rédaction du brevet, voire dans la traçabilité insuffisante des activités de recherche ayant conduit au brevet. Celui-ci peut être invalidé suite à une procédure en contrefaçon pourtant lancée par l'établissement.

• **Les brevets en partenariat**

Quelques notions de base sur la propriété

(32) *CEA, La valorisation au CEA, dossier de presse, Juin 2008*, p. 13

(33) *Code de la PI* : Action civiles : L615-1 à L615-10 /Action pénales : L615-12 à L615-16

intellectuelle doivent être rappelées aux chercheurs et enseignants-chercheurs.

« Toute invention doit faire l'objet d'une déclaration de l'employé vers son employeur, même si le travail menant à l'invention a été réalisé en dehors des missions de l'employé et des locaux de l'employeur. Selon le Code de la propriété intellectuelle, le titulaire des droits de propriété industrielle est a priori l'employeur du ou des inventeurs »[34].

De plus, il est à noter que l'inventeur français a l'obligation de faire d'abord un dépôt à l'INPI avant d'étendre sa protection à l'étranger[35]. Cela est à prendre en compte en particulier dans le cadre d'une mission réalisée à l'étranger par un chercheur employé par un établissement de recherche public français ou dans le cadre des laboratoires internationaux, surtout si la loi du pays d'accueil prévoit des dispositions similaires.

Le cas des personnels non permanents et sans contrats de travail (stagiaires, boursiers, chercheurs invités non salariés de l'établissement) est à étudier quand ils participent à des travaux menant au dépôt de brevet. En effet, un personnel non salarié de l'établissement a des droits individuels de propriété intellectuelle sur les résultats des travaux de recherche. Il est donc important pour l'établissement de contractualiser avec ces personnels avant le début de leurs travaux. Un accord de cession de l'ensemble des droits avec contrepartie financière en cas d'utilisation commerciale sera privilégié.

• Co-publications internationales

Lors de la parution d'une co-publication internationale impliquant un chercheur, un laboratoire ou un établissement français (50 % des publications « françaises » sont écrites en partenariat), il est important que la contribution française à l'article scientifique soit reconnue à sa juste proportion. Le nom de l'établissement français de tutelle des auteurs doit apparaître pour qu'une part de la publication soit attribuée à la France dans les comptes fractionnaires bibliométriques internationaux. L'établissement doit également veiller à ce que des chercheurs ou établissements étrangers n'ayant pas participé à la rédaction ne soient pas associés à l'article.

La protection et l'exploitation du logiciel

- Protection : le logiciel[36] est concerné par les deux aspects de la propriété intellectuelle. Le droit d'auteur protège sa forme d'expression, le brevet d'invention protège ses fonctionnalités techniques.

- Exploitation : quelle que soit la protection choisie pour lui, le logiciel peut être diffusé sous différents modèles :

• le modèle du logiciel propriétaire ;
• le modèle du logiciel libre ;
• les modèles mixtes libre/propriétaire.

Dans le cas du logiciel libre, la mise en ligne d'un code source d'un logiciel (*Open source*), peut dans certains cas être considérée comme une divulgation mondiale massive puisque le code source est téléchargeable sur internet. Elle ne devrait donc être effectuée que s'il a été démontré auparavant que ceci ne constitue pas un danger potentiel de fuite d'information, dommageable pour l'emploi national et l'intérêt général (par exemple pertes de chances de développements économiques sur la base de modèles propriétaires ou mixtes).

En règle générale, les modes de valorisation du logiciel de type propriétaire ou mixte libre/propriétaire (couches basses de faible valeur : logiciel libre ; couches métiers ou applicatives à forte valeur ajoutée : logiciel propriétaire) devraient être privilégiés.

Normalisation

La normalisation joue un rôle fondamental pour renforcer la compétitivité des entreprises : elle constitue un outil majeur pour accélérer le temps d'accès au marché et favoriser la « légitimation » des résultats de la recherche et de l'innovation. Du fait de son mode d'élaboration et de son impact économique, la normalisation est donc un outil stratégique majeur pour les organisations, qu'elles soient publiques ou privées. Il convient donc que les chercheurs participent à l'élaboration des normes dans les secteurs qui les concernent. Les intérêts pour eux sont multiples :

• apporter leur connaissance et expertise scientifique et technique pour garantir la qualité des

(34) *Université de Strasbourg, Service de Valorisation, Guide des bonnes pratiques de valorisation*, Juin 2009 p. 16

(35) *INPI : Se protéger à l'étranger / Code de la PI* : article R612-1 : Dépôts des demandes / Art. R614-21 : demandes internationales

(36) *Concernant le logiciel : Code de la propriété intellectuelle* : L122-6 à 122-6-2 / L113-9 / L122-4

documents normatifs, pour le bien de la communauté ;

• faire une veille technologique sur les évolutions dans les secteurs où s'exercent leurs recherches ;

• identifier de nouveaux champs de recherche potentiels ;

• faire partie d'un réseau d'experts reconnus dans son secteur et acquérir de la notoriété ;

• faciliter le transfert de technologies issues de la recherche vers le marché ;

• protéger les fruits de la recherche en élaborant des normes fondées sur les performances de nouvelles technologies, non sur leur description.

Les interactions entre normes et brevets

Contrairement à une idée répandue, les normes n'empêchent pas la propriété intellectuelle ; la norme est formulée le plus souvent en termes de résultats à atteindre, pas en termes de solution technique. Elle porte généralement sur l'interopérabilité et les interfaces, sans décrire techniquement la solution déployée.

Une norme peut cependant, lorsqu'aucune autre solution ne paraît possible, passer par l'utilisation d'un brevet (identifié comme « brevet essentiel »). Les organismes de normalisation internationaux (ISO, CEI et UIT), mais également européens (CEN, CENELEC et ETSI) et nationaux, ont adopté une politique sur la gestion des droits de propriété intellectuelle (DPI). Ces règles sont désignées « règles FRAND » (*Fair, Reasonable And Non Discriminatory*).

Selon ces règles, l'existence d'un brevet doit être signalée le plus en amont possible lors de l'élaboration d'une norme (déclaration « ex-ante »). Le détenteur des droits de propriété industrielle doit alors donner l'assurance qu'il consent à négocier des licences avec tout demandeur, à des termes et conditions raisonnables et non discriminatoires.

Les normalisateurs n'interviennent pas dans le montant des licences accordées, qui relèvent de négociations entre les parties. L'industriel doit alors accorder des licences à des montants raisonnables qui favoriseront l'adoption de la norme, mais qui lui permettront tout de même de rentabiliser ses efforts de recherche et de développement. Les licences peuvent également être gratuites dans certains cas, ce qui permet à l'entreprise de se faire mieux connaître sur le marché. Dans tous les cas, la déclaration du détenteur des droits de propriété industrielle est enregistrée dans les bases de données de l'ISO, la CEI ou l'UIT pour organiser une traçabilité du dispositif. Toute licence doit également faire l'objet d'une démarche d'inscription auprès du registre national des brevets de l'INPI pour être opposable aux tiers[37].

Les avantages à citer un brevet dans une norme sont en effet de plusieurs natures :

- orienter le marché vers une technologie ;
- augmenter le nombre d'utilisateurs de cette technologie et développer un marché ;
- augmenter ses revenus avec le montant des licences accordées ;
- acquérir de la notoriété.

(37) *INPI : La vie de votre brevet*

2. GESTION DU PATRIMOINE IMMATÉRIEL

Qu'est ce que le patrimoine immatériel ?

■ Le patrimoine immatériel comprend trois types d'informations : scientifiques (connaissances, savoir-faire, compétences, publications, brevets…), d'organisation (portefeuille de contrats et de collaborations…), d'image (réputation).
■ Tout établissement de recherche est exposé au risque de perte ou de détournement d'informations (vols de supports informatiques, de cahiers de laboratoires, diffusion involontaire d'informations sensibles, manipulation du personnel…).

Comment mettre en œuvre une politique de gestion du patrimoine immatériel ?

■ La veille stratégique de l'établissement contribue à la gestion éclairée/intelligente du patrimoine immatériel de l'établissement.
■ La gestion du patrimoine immatériel nécessite la mise en place de mesures de protection juridiques et/ou opérationnelles visant à préserver l'intégrité, la disponibilité et la confidentialité de l'ensemble des informations de l'établissement.
■ Il est essentiel que chacun dans l'établissement se sente concerné.
■ Trois étapes clés dans la gestion et la protection des informations :

1. assurer la traçabilité des informations et de leur circulation ;
2. établir un référentiel de sensibilité des informations (générale, de communication externe, à diffusion restreinte, confidentielle) et identifier l'information stratégique, en prenant soin de ne pas surprotéger inutilement les informations ;
3. adopter une politique de contrôle d'accès aux informations et une politique de PI.

La traçabilité des informations concrètement

■ Appliquer des mesures concrètes :

- effectuer des dépôts auprès d'intermédiaires agréés ou officiels (enveloppe Soleau auprès de l'INPI…) ;
- tenir à jour les cahiers de laboratoires, constituer des rapports scientifiques et techniques (qui permettent de codifier le savoir-faire secret non breveté) ;
- archiver méthodiquement les données ;
- effectuer des copies de sauvegarde ;

• assurer le transfert de connaissances des personnels avant leur départ du laboratoire.

– Garantir la confidentialité : accords de confidentialité, marquage des documents confidentiels, cryptage éventuel de données…

La politique de contrôle d'accès aux informations concrètement

■ Appliquer des mesures concrètes :

• identifier et répertorier les locaux sensibles puis en déterminer les conditions d'accès pour le personnel de l'établissement et les personnes extérieures (ces conditions doivent toujours apparaître dans les contrats) en se conformant aux obligations règlementaires en vigueur ;

• s'assurer de la fermeture des accès et des comptes informatiques lors de la fin du contrat d'un membre du personnel, d'un chercheur invité, d'un stagiaire, d'un intérimaire… ;

• protéger les systèmes d'information (voir fiche 3) ;

• sensibiliser les personnels et définir des règles de bonnes pratiques (déplacements à l'étranger, accords de coopération…) car une grande partie des pertes d'information provient d'erreurs humaines souvent involontaires (voir fiche 5) ;

• organiser la remontée d'informations sur tout incident interne ou externe (rapports d'étonnement ou fiches d'alerte …) ;

• réaliser une cartographie des activités des prestataires extérieurs de l'établissement afin de pouvoir définir de manière optimale leurs besoins en matière d'accès aux locaux et aux informations.

Gestion de la propriété intellectuelle

■ S'assurer de la bonne gestion de la PI dans les contrats de l'établissement avant le démarrage des travaux dans le cadre d'une coopération ou avant une embauche.

■ Utiliser la PI comme outil de structuration de la recherche et des partenariats, au service et en conformité avec la politique de recherche et de partenariats de l'établissement.

■ Le secret est une forme très efficace de protection d'une invention. S'il ne peut être maintenu, le dépôt d'une demande de brevet doit être privilégié.

■ Responsabiliser les chercheurs sur l'intérêt économique de leurs travaux et la création d'emplois.

■ Valoriser les brevets prioritairement dans l'économie nationale et communautaire.

■ Informer les chercheurs sur les règles de la PI, notamment dans le cadre international.

■ Chaque établissement doit se doter d'une charte de bonnes pratiques de gestion de la propriété intellectuelle et du transfert de technologie, comme le recommande la Commission européenne (*résolution du Conseil européen 10323/08 du 30/05/2008*).

■ Lors de concessions de licences exclusives et de création de *spin-off*, et pour s'assurer d'une bonne valorisation de la PI, quelques bonnes pratiques devraient être observées dans la plupart des cas :

- définition d'un domaine d'exploitation exclusif permettant au laboratoire de valoriser dans d'autres domaines afin de maximiser les retombées industrielles ;
- fixation de seuils d'exploitation minimums en deçà desquels le licencié perd l'exclusivité ;
- fixation d'un minimum garanti de redevances, incitant le licencié à exploiter.

■ Contrefaçon : il est important que l'établissement de recherche soit reconnu sur le marché comme un acteur défendant fermement ses droits. Il doit s'appuyer sur son licencié et sur l''inventeur pour mener sa politique de veille. Une procédure en contrefaçon peut néanmoins présenter des risques s'il existe des failles juridiques dans la rédaction du brevet : il peut être invalidé.

■ Co-publications internationales : le nom et l'adresse de l'établissement français de tutelle des auteurs doivent apparaître pour qu'une part de la publication soit attribuée à la France dans les comptes fractionnaires bibliométriques internationaux.

■ Logiciels libres : ne diffuser un logiciel en licence libre qu'après avoir analysé que ce n'est pas dommageable pour l'emploi national et l'intérêt général (par exemple pertes de chances de développements économiques sur la base de modèles propriétaires ou mixtes).

■ Normalisation : organiser une veille sur les normes et les activités de normalisation en cours, s'interroger sur la pertinence du développement de nouvelles normes dans un champ innovant. Il convient que les chercheurs participent à l'élaboration des normes dans les secteurs qui les concernent.

Bibliographie

- **Site de l'INPI :** *http ://www.Inpi.fr*
- **Site de l'AFNOR :** *http ://www.Afnor.org*
- **AFNOR FD-X50-146 ;** *Management de l'innovation - Management de la propriété intellectuelle*, décembre 2010. *http://www2.afnor.org/espace_normalisation/structure.aspx?commid=74206*
- **Ministère de la Jeunesse, de l'Éducation et de la Recherche**, **Ministère délégué Recherche et Nouvelles Technologies,** *Protection et valorisation de la recherche publique*, Septembre 2003.
- **INPI :** *L'enveloppe Soleau, tout ce qu'il faut savoir avant de déposer une enveloppe Soleau. http ://www.Inpi.fr/fileadmin/mediatheque/pdf/brochure_enveloppe_soleau.pdf*
- **CNRS/MESR,** *Le cahier de laboratoire national, Février 2010 http ://www.dgdr.cnrs.fr/mpr/pratique/guides/CLN/CLN.htm*
- **SCIE**, *Guide des bonnes pratiques en matière d'intelligence économique*, Février 2009 *http ://www.economie.gouv.fr/demarche-d-intelligence-economique*
- **CEA :** *Livret du référent : Accueil d'un collaborateur. Protection du patrimoine scientifique et technique du CEA*, Juin 2011.
- **Charte de propriété intellectuelle** *et de transfert de technologie et de connaissance des instituts Carnot, politique relative à la propriété intellectuelle http ://www.inrets.fr/fileadmin/valorisation/charte-propriete_intellectuelle*
- **Légifrance**, *Code de la Propriété intellectuelle. http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414&dateTexte=20111209*
- **MINEFI**, *La propriété industrielle. http ://www.industrie.gouv.fr/enjeux/pi/definition.htm*
- **MINEFI**, *La stratégie de protection de la propriété intellectuelle au sein des pôles de compétitivité. http ://www.industrie.gouv.fr/guidepropintel/reglementations/strategie_de_protection.htm*
- **CEA**, *La valorisation au CEA, dossier de presse, Juin 2008. http ://www.cea.fr/le_cea/actualites/cea_valorisation-7541*
- **Université de Strasbourg**, Service de Valorisation, *Guide des bonnes pratiques de valorisation, Juin 2009. http ://servalor.unistra.fr/IMG/pdf/Guide_valorisation_01_2010.pdf*
- **INPI :** *Le brevet, les 16 étapes clés. http ://www.Inpi.fr/index.php?id=2103&L=0*
- **INPI :** *Ce qui peut être breveté. Nouveauté. http ://www.Inpi.fr/fr/brevets/qu-est-ce-qu-un-brevet/ce-qui-peut-etre-brevete.html*

■ **INPI :** *Se protéger à l'étranger.*
http ://www.Inpi.fr/fr/brevets/la-vie-de-votre-brevet/se-proteger-a-l-etranger.html

■ **Recommandations** *pour l'adoption d'une charte de la propriété intellectuelle par les établissements publics d'enseignement supérieur et de recherche ; MESR ; 15/06/2001.*

■ **AUTM** *Licensing Survey.*
http ://www.autm.net/Licensing_Surveys_AUTM.htm

■ **Lettre Trésor-Eco septembre 2010** *- Le recul de l'emploi industriel en France de 1980 à 2007 : quelle est la réalité ?*
http://www.tresor.economie.gouv.fr/file/326706

■ **OMPI/WIPO Stats :** *C.1 Demandes déposées par des résidents, par office.*
http ://www.wipo.int/ipstats/fr/statistics/patents/patent_report_2007.html#P153_20554

■ **Besondere** *Nebenbestimmungen für Zuwendungen des Bundesministeriums für Bildung und Forschung zur Projektförderung auf Ausgabenbasis (BNBest-BMBF 98).*
http ://www.kp.dlr.de/profi/easy/bmvel/pdf/0330a.pdf

■ **Nebenbestimmungen** *für Zuwendungen auf Kostenbasis des Bundesministeriums für Bildung und Forschung an Unternehmen der gewerblichen Wirtschaft für Forschungs- und Entwicklungsvorhaben.*
http ://www.kp.dlr.de/profi/easy/bmbf/pdf/0348a.pdf

■ **OCDE :** *Turning science into business : patenting and licensing at public research organizations ; OECD Breakfast series; 28/05/2003.*
http ://www.science.oas.org/Doc/turning_science_into.pdf

■ **Law of the People's Republic of China** *on Progress of Science and Technology.*
http ://www.china.org.cn/china/LegislationsForm2001-2010/2011-02/11/content_21899295.htm

■ **INPI :** *Tarif des procédures.*
http ://www.Inpi.fr/fr/acces-rapide/tous-nos-tarifs.html

■ **Managing university** *Intellectual Property in the Public Interest* ; National Research Counsil ; USA ; October 2010 ; the national academies press.
http ://www.nap.edu/catalog.php?record_id=13001

■ **World Bank statistics.** *Royalties and licences fees payments. Royalties and licenses fees receipts* ; 2011.
http ://data.worldbank.org/indicator/BX.GSR.ROYL.CD

■ **Résolution du Conseil européen** 10323/08 du 30/05/2008 concernant la gestion de la propriété intellectuelle dans les activités de transfert de connaissances et un code de bonne pratique destiné aux universités et aux autres organismes de recherche publics.
http ://register.consilium.europa.eu/pdf/fr/08/st10/st10323.fr08.pdf

■ **MINEFI :** *Guide des bonnes pratiques en matière de propriété intellectuelle pour la mise en œuvre de l'Accord sur la coopération scientifique et technologique entre la France et les États-Unis en matière de sécurité, signé le 17/12/08* ; septembre 2009.

3

Politique de Sécurité des Systèmes d'Information

Introduction

La nécessité d'une politique de sécurité des systèmes d'information (PSSI) n'est plus à démontrer. Il n'est toutefois pas inutile d'y revenir régulièrement, tant les bonnes habitudes se perdent vite. La PSSI participe à la fois d'une démarche de protection des données et des processus et d'une démarche d'efficacité, donc de compétitivité.

Dans ce domaine, deux axes doivent être privilégiés :

• le réglementaire, qui répond à nombre de questions,

• les bonnes pratiques, qui correspondent souvent à du bon sens et à des pratiques d' «hygiène informatique», mais dont certaines restent à inventer et qui tiennent d'une démarche qualité.

Il est important de prendre conscience que la sécurité des systèmes d'information concerne tous les personnels dans leurs pratiques quotidiennes. Elle concerne également toutes les données et process d'une unité de recherche (son patrimoine informationnel) et pas seulement les informations classifiées de défense. Un article en cours d'écriture, un brevet en cours de rédaction, des résultats non encore publiés, des contrats industriels etc. sont autant de données précieuses pour un chercheur, un laboratoire ou un établissement. La PSSI d'un établissement doit prendre en compte les possibilités de fuites d'information (par accès indu ou par négligence), les pertes d'information, l'intégrité des données, les atteintes à l'image etc.

Les référentiels

Les services de l'État en charge de la SSI sont :

• l'ANSSI, Agence nationale de la sécurité des systèmes d'information ;

• les FSSI (fonctionnaires de sécurité des systèmes d'information) des ministères de tutelle. Au MESR, la fonction de FSSI est assurée au sein du service du HFDS ;

• le Service des technologies et des systèmes d'information de la sécurité intérieure, commun à la DGGN (direction générale de la Gendarmerie nationale) et à la DGPN (direction générale de la Police nationale). Il dépend du MIOMCTI (ministère de l'Intérieur, de l'Outre Mer, des Collectivités territoriales et de l'Immigration).

Différents référentiels existent déjà :

• **Instruction générale interministérielle n° 1300/SGDSN/PSU/PSD** du 30 novembre 2011 sur la protection du secret de la défense nationale.

Titre V : Mesures de sécurité relatives aux systèmes d'informations (articles 85 à 94).

– Champ d'application (article 85).

– Chapitre 1 : L'organisation des responsabilités relatives aux systèmes d'information (articles 86 à 89).

– Chapitre 2 : La protection des systèmes d'information (articles 90 à 94).

• Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

• **Référentiel général de sécurité (RGS)**. Publication des principes dans le décret en Conseil d'État 2010-112 (voir en particulier article 3 et article 5). Promulgation de la première version du RGS le 18 mai 2010 au JO par l'arrêté du 6 mai 2010 dit arrêté RGS.(38)

• ANSSI : recueil de mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau Diffusion restreinte. Version 1.0 du 2 mars 2011. Document issu du GT Refonte de l'II 486 Volet SSI.

• **Norme ISO/CEI 27000** : norme de sécurité de l'information publiée conjointement en mai 2009 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI).

Spécificités du monde de la recherche

Des difficultés inhérentes aux spécificités du monde académique existent.

• La multiplicité des acteurs de la PSSI et la nécessité d'établir clairement les rôles et responsabilités de chacun d'entre eux. Le monde académique doit mettre en place une meilleure organisation et identifier clairement la chaîne de décision et de remontée d'informations dans les institutions. Il est important

(38) *http ://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000021780121&dateTexte=*

de bien séparer la dimension « stratégique » et « politique » de la SSI et son application pratique.

• Les tutelles multiples des laboratoires, qui amènent les chercheurs à exercer leurs différentes activités sur un même lieu de travail, ce qui augmente la problématique de la confidentialité.

• L'indispensabilité de la coopération et les méthodes de travail en laboratoires sans murs augmentent les risques de fuite d'information, de diffusion mal contrôlée de l'information, de perte d'intégrité des données, etc.

La PSSI de l'État

Une PSSI de l'État est en cours de rédaction, fin 2011, par un groupe interministériel piloté par l'ANSSI. Cette PSSIE s'appliquera à tous les ministères et, probablement, aux établissements sous tutelle. Il conviendra que les établissements prennent en compte ses recommandations dans la définition de leur PSSI. La PSSIE reprend les bonnes pratiques applicables de la norme internationale ISO 27002 et contiendra une série de directives d'application :

• directive de sécurité physique des locaux ;
• directive d'architecture et d'exploitation des SI ;
• directive de sécurité des postes de travail ;
• directive de sécurité des réseaux ;
• directive de sécurité des systèmes de l'hébergement ;
• directive de sécurité du développement et de maintenance des systèmes.

Cette nouvelle politique crée une « culture sécurité des SI » commune et une zone de confiance homogène entre tous les agents de l'État.

Éléments à intégrer dans la PSSI d'un établissement de recherche :

• Pratiques d'hygiène informatique classiques : récupération des données et suppression des comptes informatiques des stagiaires et visiteurs après leur départ, sauvegardes régulières, contrôles d'accès physiques et informatiques respectant le principe du besoin d'en connaître, y compris aux archives, authentification des personnes, gestion des mots de passe, conservation et exploitation des fichiers log pour détection et suivi des intrusions, filtrages des emails, antivirus, gestion des données conservées sur les ordinateurs lors des déplacements, signalisation des incidents, **identification rapide et claire des services informatiques en charge**, installation de logiciels contrôlée, etc. Les bonnes pratiques d'hygiène informatique doivent être appliquées tant au bureau, qu'en déplacement ou au domicile.

• Outils de veille et d'investigation sur internet : les protections nécessaires à appliquer sont déterminées par une étude des risques spécifique (décret RGS 2010-112 article 3) et gérées par une prise de responsabilité formelle de l'autorité sur l'emploi du SI (décret 2010-112 article 5). Les mesures détaillées peuvent être très restrictives et préconiser l'exploitation uniquement locale des flux RSS ou des sites web et des bases de données. Elles peuvent être plus ouvertes sur le monde extérieur tout en comportant des aspects de protection des accès :

– le recours à des services communs sûrs et vérifiés (CEDOCAR, e-Veil...) ;

– le refus d'utilisation de services hébergés dans le nuage informatique comme :

• des moteurs de recherche (e.g. Google, Bing, Yahoo...),

• du courrier électronique hébergé (e.g. GMail, Hotmail, MsLive...),

• des sites de stockage et de partage des données (*e.g.* DropBox Mediafire...) ;

• des services plus diffus (Webex, Skype) ;

– la protection de l'accès aux moyens de collecte (tunnel chiffrant, adresse IP masquée, gestion de l'empreinte du poste) ;

– l'identification, la neutralisation et le filtrage systématique de tous les traceurs tiers : Google-analytics, FaceBook, Twitter et autres. Ceci est bien sûr fonction de ce que l'on veut protéger (la sémantique et la dynamique des actions de veille et d'investigation) et ne fait que minimiser les traces laissées en cas d'accès à des sites web extérieurs.

• Contrôler et réglementer l'utilisation du *cloud computing* et l'externalisation des données du chercheur. Porter une attention particulière au stockage des données dans des « coffres-forts virtuels »). On se réfèrera au guide édité par l'ANSSI dans le domaine « sécurité de l'externalisation », qui s'intitule *Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques*[39].

(39) *ANSSI : Externalisation et sécurité des SI : un guide pour maîtriser les risques*

• Contrôler et réglementer les accès virtuels ou à distance aux centres de calculs ou aux ordinateurs des laboratoires. Gérer, notamment, le problème du contrôle des accès à distance (vérification des identités).

• Contrôler et réglementer les accès aux grilles de calcul internationales qui mettent en commun les ressources informatiques de laboratoires et de centres de calcul.

• Chiffrement et signature : protéger les échanges des données sensibles. Utiliser des outils de chiffrement robustes et vérifier leur robustesse auprès du FSSI ou de l'ANSSI.

• De faux certificats SSL circulent (Google en a été victime en août 2011) : une base de données internationale se monte. Se montrer vigilant sur ce point.

• Identifier les sites malveillants. On peut trouver des listes noires de sites malveillants sur des sites académiques, e.g. sur celui de l'université de Toulouse : *http ://cri.univ-tlse1.fr/blacklists/*. On pourra également utiliser le proxy Squid (*http ://www.squid-cache.org/*) couplé aux outils de filtrage SquidGuard (*http ://www.squidguard.org/*) (solution gratuite).

• Vérifier régulièrement l'utilisation d'images des sites de l'établissement par des sociétés comme Google street view, par exemple. Prévenir la CNIL en cas d'utilisation frauduleuse (e.g. images prises depuis des routes privées de campus).

• Définir une politique de détection, remontée et traitement des incidents (intrusions, débits incontrôlés, …)

RÈGLES D'HYGIÈNE INFORMATIQUE INDIVIDUELLE
(inspirées des recommandations de l'ANSSI)

Au bureau et/ou à la maison

1. **Vérifiez que votre logiciel antivirus est activé :** vous devez vous assurer qu'un logiciel antivirus est installé sur votre ordinateur et qu'il est activé et actualisé. Si un virus est détecté, demandez l'aide du service informatique. **À la maison**, utilisez un logiciel antivirus comprenant une fonction de mise à jour automatique des définitions de virus. Configurez votre logiciel afin qu'il analyse automatiquement, à intervalles réguliers, tous les fichiers enregistrés sur votre ordinateur.
2. **Sauvegardez vos données importantes : au bureau**, placez-les sur l'espace commun sauvegardé. **À la maison**, copiez régulièrement sur des supports externes (par exemple CD ou DVD) tous les fichiers importants que vous ne pourriez pas remplacer facilement. Conservez ces supports à un endroit distinct. Pour pouvoir récupérer rapidement vos données après une panne matérielle ou une compromission de sécurité, créez une copie de sauvegarde de l'ensemble du système (image du disque) ou des disques de récupération de la configuration de votre ordinateur.
3. **Utilisez exclusivement des supports informatiques d'origine connue et contrôlée (clés USB, disques durs externes, etc.).**
4. **Au bureau : ne modifiez jamais vous-même la configuration de votre matériel ou de vos logiciels.**
5. **Utilisez un mot de passe fort et ne le donnez à personne :** votre mot de passe est votre **clé personnelle**. Choisissez un mot de passe fort, qui soit à la fois difficile à deviner et facile à retenir, de façon à ne pas devoir l'inscrire quelque part.
6. **Ne laissez pas votre ordinateur connecté s'il n'est pas utilisé :** éteignez votre ordinateur ou fermez votre connexion à l'internet lorsque vous ne l'utilisez pas. Sinon, votre ordinateur risque d'être « détourné » et de devenir un « zombie », exécutant des commandes à votre insu. Cette précaution est essentielle pour ceux qui utilisent les connexions internet à large bande, très répandues.

7. **Protégez les informations numériques contre l'accès par des personnes non autorisées.**
8. **Utilisez la messagerie électronique à bon escient :**
   – **envoi** : veillez à toujours vérifier l'adresse des destinataires et le niveau de confidentialité d'un message à envoyer et des documents joints. Attention notamment à l'historique des échanges inclus dans le message ;
   – **réception** : n'ouvrez pas les courriels non sollicités ou d'origine inconnue, même si l'objet ou la pièce jointe semble intéressant. Méfiez-vous de toute pièce jointe à un courriel non sollicité. Désactivez les fonctions de script (par exemple Javascript, ActiveX, etc.) dans les programmes de messagerie électronique tels qu'Outlook.
9. **Utilisez l'intranet de façon judicieuse :** toutes les informations internes diffusées sur l'intranet ne sont pas nécessairement destinées à l'ensemble des agents. Il est bon de vérifier si l'intranet est le support approprié pour le partage d'informations ou si un autre support serait plus approprié pour un meilleur contrôle d'accès.
10. **Apposez une marque de propriété sur tous les documents que vous produisez.**
11. **Conservez toutes les informations importantes et/ou confidentielles en lieu sûr :** i.e. pas sur des disques durs locaux ou dans des dossiers publics d'Outlook Exchange.
12. **Ne naviguez jamais sur l'internet à partir d'un compte administrateur**. il est préférable de créer et d'utiliser des comptes avec privilèges limités.
13. **Signalez immédiatement les incidents au service compétent :** signalez sans délai tout incident, y compris la perte ou le vol d'un ordinateur ou d'une clé USB, tout signe d'intrusion, d'utilisation frauduleuse d'un ordinateur ou d'infraction de sécurité, ainsi que tout comportement inhabituel ou inattendu.
14. **À la maison, effectuez des mises à jour de votre système :** veillez à ce que votre système d'exploitation (par exemple, Windows XP, Vista, etc.) et vos applications bénéficient des correctifs les plus récents. À l'heure actuelle, la plupart des éditeurs proposent une fonction de mise à jour automatique. Si tel n'est pas le cas, vous devez vérifier périodiquement sur le site web du fabricant la disponibilité de mises à jour ou vous inscrire sur ses listes de distribution.
15. **À la maison, utilisez un pare-feu :** utilisez votre propre pare-feu ou les fonctions de pare-feu intégrées dans votre système d'exploitation ou logiciel antivirus. Apprenez à le configurer pour n'activer que les services requis (par exemple, courrier électronique, navigation web, etc.)
16. **À la maison, protégez votre réseau sans fil :** placez votre point d'accès au centre de votre habitation, loin des murs extérieurs. Modifiez le nom du réseau par défaut (Service Set Identifier , SSID) et activez les fonctions de sécurité, de préférence la fonction WPA2 (Wi-Fi Protected Access). Activez éventuellement le filtrage Media Access Control (MAC).
17. **Au bureau :** « nettoyez » les disques durs des ordinateurs personnels avant de les affecter à un autre agent (effacez toutes les données).

L'ANSSI (*www.ssi.gouv.fr*), l'agence gouvernementale en charge de la sécurité des systèmes d'information, édite une série de guides, de règles et de recommandations applicables. L'agence a notamment publié en octobre 2011, une série de questions à se poser en matière d'hygiène informatique, intitulée « Avez-vous oublié les fondamentaux ? ». Cette check-list, destinée prioritairement aux entreprises, est une source de réflexion pour un établissement de recherche.

Avez-vous oublié les fondamentaux ?[40]

20 octobre 2011

Combien de personnes disposent du mot de passe administrateur permettant d'accéder au système central de gestion des droits ?
Il convient de réduire le nombre de titulaires de comptes disposant de privilèges élevés aux seules personnes pour lesquelles ces privilèges sont nécessaires à l'accomplissement de leur mission. Des listes doivent être tenues à jour pour tous les comptes de ce type, dont évidemment les comptes permettant d'accéder au système central de gestion des droits, qui constituent des cibles de choix pour les attaquants.

Quel mot de passe est utilisé pour installer une imprimante ? Le mot de passe permettant le contrôle total de votre système d'information, ou un autre ?
Le partage de mot de passe entre comptes doit être banni.

Chaque administrateur dispose-t-il d'un mot de passe différent ?
Afin de limiter les risques de compromission du mot de passe et de favoriser la traçabilité des actions, chaque individu doit utiliser un mot de passe personnel.

Lorsqu'un administrateur travaille à autre chose qu'à des tâches d'administration, quel type de compte utilise-t-il ?
Les comptes avec des droits d'administrateur doivent être strictement réservés à l'exécution de tâche d'administration. Des procédures doivent avoir été définies et une charte de l'administrateur établie afin de préciser ces conditions. Les administrateurs doivent utiliser un compte non privilégié lorsqu'ils effectuent des actions plus exposées, comme lire leurs courriels ou naviguer sur le web.

Quand, pour la dernière fois, quelqu'un a-t-il vérifié qui disposait des droits d'accès à la messagerie de votre PDG ou DG ?
Les accès à des ressources sensibles, comme la messagerie de dirigeants, doivent faire l'objet d'une surveillance régulière.

Qui a vérifié si, cette nuit, un fichier zip de 2 Go n'avait pas été extrait de votre système d'information ?

Quelqu'un regarde-t-il de temps en temps si les flux sortant de votre SI, la nuit par exemple, sont légitimes ? Si les adresses de destination sont normales ?

La dernière fois que vous êtes venus travailler un dimanche, quelqu'un est-il venu vous demander le lundi s'il était normal que quelqu'un se soit connecté sur votre compte dimanche ?
L'analyse des journaux d'événements permet de repérer les activités inhabituelles et de détecter d'éventuels signes d'intrusion. Les journaux d'événements doivent être activés, configurés et centralisés pour permettre cette analyse. De plus, le système utilisé doit permettre de générer des alertes simples et l'organisation doit prévoir le personnel et les procédures permettant de traiter ces alertes.

Votre propre poste de travail est-il à jour de ses correctifs de sécurité (pour l'ensemble des logiciels installés) ?
Il convient de mener un inventaire logiciel pour tous les postes de travail et d'utiliser un système centralisé de gestion des mises à jour pour corriger les vulnérabilités des logiciels inventoriés. Il ne suffit pas de mettre à jour uniquement le système d'exploitation, mais bien l'ensemble de logiciels déployés sur son parc.

Votre SI comporte-t-il encore des applications tournant sur Windows XP pack 2, voire 2000, voire même NT4 (on en voit plus souvent qu'on ne le penserait) ? Dans ce cas, quelles mesures de précaution ont été prises ?
Lorsqu'il n'est pas possible de migrer ces applications vers des systèmes maintenus par l'éditeur, il convient d'isoler de manière particulièrement restrictive et de porter une attention particulière à leurs journaux d'événements.

Quelqu'un a-t-il la cartographie de votre réseau - vraiment, pas juste une idée plus ou moins précise dans sa tête, mais un vrai schéma ?

(40) *ANSSI : Avez-vous oublié les fondamentaux ?*

Le maintien d'une cartographie à jour est indispensable pour pouvoir identifier les vulnérabilités et les corriger. Elle permet également de pouvoir réagir rapidement en cas de détection d'intrusion en limitant les risques de créer des dysfonctionnements par méconnaissance de son système d'information.

Combien d'accès internet avez-vous ? Où sont-ils ? Sont-ils tous administrés ? Surveillés ?
De trop nombreuses organisations laissent se multiplier les accès internet « sauvages », comme des lignes ADSL. Le résultat est une perte de capacité de surveillance des flux entrants et sortants et de blocage des flux illégitimes. Les accès sauvages échappent en effet aux systèmes de filtrage et de détection d'intrusion. Lorsqu'ils les identifient, des attaquants peuvent privilégier ces accès pour exfiltrer des données. Tout accès internet doit donc être recensé dans la cartographie et des règles de filtrage et de surveillance adaptées doivent y être associées. Le nombre d'accès doit être le moins élevé possible.

Combien de temps se passe-t-il entre le moment où quelqu'un quitte votre organisation et le moment où son compte est supprimé ?
Tout compte devenu inutile doit être immédiatement supprimé. Dans le cas contraire, un attaquant peut l'utiliser discrètement - qu'il s'agisse de l'ancien titulaire du compte ou d'un attaquant externe tirant profit de la situation. Une procédure adaptée doit donc être mise en place pour que le service informatique soit informé en cas de départ d'un employé et puisse supprimer ses droits d'accès. Lorsqu'une personne dispose d'un compte temporaire dans l'organisme (exemple : stagiaire, prestataire), une date d'expiration devrait être configurée dès la création du compte.

Combien avez-vous de comptes non individuels, de comptes de service ? À quoi servent-ils ?
Trop souvent les comptes partagés entre plusieurs individus ou de services possèdent des mots de passe faibles (type mot de passe = nom de compte) et qui n'expirent jamais. Or ces comptes permettent généralement d'accéder à de multiples ressources et, pour les comptes de services, disposent souvent de privilèges élevés. Pour ces raisons, ils sont l'une des premières cibles des attaquants. Il convient donc de tenir une liste de ces comptes et d'en mener une revue périodique pour en restreindre le nombre.

L'exécution automatique des supports usb est-elle désactivée ?
Les logiciels malveillants se diffusent très facilement par l'intermédiaire des supports USB lorsque l'exécution automatique de ces derniers est activée. Pour faciliter la gestion de cette fonctionnalité, vous pouvez utiliser des mécanismes de stratégie de groupe (GPO sous Windows) afin de désactiver les fonctions d'autorun et d'autoplay.

Les utilisateurs peuvent-ils installer des applications ?
Les utilisateurs ne doivent pas disposer de privilèges d'administrateurs. Par ailleurs, les stratégies de restrictions d'exécution logicielle (SRP et AppLocker sous Windows) restreignent l'exécution de logiciels malveillants et empêchent l'utilisateur de lancer un programme depuis un média amovible ou depuis son profil utilisateur. Il faut être vigilant aux environnements tels que Java, Adobe Air ou Perl, qui permettent d'exécuter des logiciels sans être contraints par les stratégies de restriction d'exécution logicielle.

Quel plan avez-vous en cas d'intrusion majeure dans votre système ?
Une intrusion d'ampleur dans un système d'information est une crise. Chaque heure qui passe peut notamment signifier la fuite d'informations stratégiques, avec dans certains cas, leur publication à des fins de déstabilisation. Des risques de suspension de l'activité de l'organisation sont aussi à prévoir. Un plan de réponse spécifique doit donc exister. Le plan de réponse doit prévoir les mesures organisationnelles et techniques permettant de délimiter au plus vite l'ampleur de la compromission et de la circonscrire. Par exemple, les documents nécessaires à la gestion de la crise, comme la cartographie du système, la liste des personnels en mesure d'intervenir sur les systèmes, les coordonnées des administrations susceptibles de porter assistance, doivent être tenus à jour et connus des personnels qui devront piloter la gestion de ce type de crise.

Que se passe-t-il quand vous découvrez un poste de travail compromis par un virus ? Le changez-vous simplement ou vérifiez-vous si par hasard l'attaquant n'aurait pas rebondi ailleurs dans votre système ?
La recherche d'éventuelles autres traces d'intrusion sur votre système est indispensable après la découverte d'une compromission. Généralement, les attaquants ne se contentent pas en effet de la compromission d'un ordinateur : ils s'ouvrent de multiples portes d'entrées dans le système afin de pouvoir revenir si d'aventure leur porte principale était refermée.

3. POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

- Effectuer une veille sur le site de l'ANSSI pour bénéficier des nouveaux guides de bonnes pratiques et de recommandations.
- La sécurité des systèmes d'information concerne tous les personnels dans leurs pratiques quotidiennes.
- Les services en charge de la sécurité des SI fonctionneront plus efficacement en réseau de façon à permettre les retours d'expérience et les échanges de bonnes pratiques entre les établissements.
- Des référentiels en matière de protection des SI existent déjà (ANSSI, RGS, norme ISO 27000…). Il est important de les appliquer.
- Etablir une démarche qualité et hygiène informatique (voir les règles et bonnes pratiques du guide). Diffuser les bonnes pratiques dans les entités.
- Contrôler et réglementer l'utilisation du « cloud computing » et les accès virtuels/à distance aux centres de calculs/ordinateurs.
- Crypter les données si besoin : clés USB, emails, ordinateurs …
- Identifier les données à protéger (résultats de recherche non publiés, contrats…).
- Protéger les échanges de données sensibles : utiliser des outils de chiffrement et de signature et vérifier leur robustesse auprès des FSSI (fonctionnaires de sécurité des systèmes d'information des ministères).
- Établir une politique réaliste des accès à distance.
- Être vigilant vis-à-vis des certificats SSL : de faux certificats circulent (Google en a été victime en août 2011).
- Diffuser les pratiques dans toutes les entités des établissements.
- Identifier clairement la chaîne de décision dans l'établissement.
- Établir une chaîne de remontée des informations sur les incidents.
- Saisir le FSSI du ministère de tutelle en cas d'incident grave ou de questionnement.

Bibliographie

- **ANSSI :** *Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques*
  http ://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html
- **ANSSI :** *Avez-vous oublié les fondamentaux ?*
  http ://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/avez-vous-oublie-les-fondamentaux.html
- **ANSSI :** *Recueil de mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau Diffusion Restreinte Version 1.0 du 2 mars 2011*
  http ://www.ssi.gouv.fr
- **Instruction générale interministérielle n°1300/SGDSN/PSU/PSD** *du 23 juillet 2010. Titre V : Mesures de sécurité relatives aux systèmes d'informations. Chapitre 1 : L'organisation des responsabilités relatives aux systèmes d'information (articles 86 à 89)*
  http ://www.ssi.gouv.fr/IMG/pdf/igi1300.pdf
- **Instruction générale interministérielle n°1300/SGDSN/PSU/PSD** *du 23 juillet 2010. Titre V : Mesures de sécurité relatives aux systèmes d'informations. Chapitre 2 : La protection des systèmes d'information (article 90 à 94)*
  http ://www.ssi.gouv.fr/IMG/pdf/igi1300.pdf
- **Norme ISO/CEI 27000** *de sécurité de l'information*
  http ://www.iso.org/iso/fr/catalogue_detail?csnumber=41933
- **RGS :** *Référentiel général de sécurité*
  http ://www.ssi.gouv.fr/rgs/

4

Développement de l'interface entre la recherche et le milieu socio-économique

Introduction

Le MESR a élaboré une stratégie nationale de recherche et d'innovation (SNRI[41]). Cet exercice de prospective scientifique inédit en France, a permis de définir cinq principes directeurs et trois axes prioritaires de recherche pour la période 2009-2012.

« Totalement insérée dans un système mondial de compétition et de collaboration, la recherche française doit répondre, dans un cadre européen, aux principes suivants :

• la recherche fondamentale doit être promue dans toutes ses dimensions, en particulier dans le cadre des très grandes infrastructures de recherche ;

• **une recherche ouverte à la société et à l'économie est le gage de la croissance et de l'emploi. Cette vision globale implique de promouvoir une société innovante, dans laquelle l'innovation est générée et portée par l'ensemble des citoyens ;**

• une meilleure maîtrise des risques et un renforcement de la sécurité sont particulièrement importants dans notre société ; ils doivent donc être des dimensions privilégiées de l'innovation sociale et culturelle autant que technologique ;

• les sciences humaines et sociales doivent avoir un rôle majeur au sein de tous les axes prioritaires notamment pour la construction des interfaces interdisciplinaires ;

• la pluridisciplinarité est indispensable pour permettre les approches les plus innovantes et les plus adaptées aux enjeux de notre société. »

La politique de valorisation des établissements se basera sur une politique de partenariat recherche-industrie bien comprise. Pour que le projet de partenariat soit pleinement efficace, il est essentiel qu'il soit bien partagé par les deux parties, ce qui implique une définition conjointe du projet acceptée par tous. Pour un fonctionnement optimal, il importe que chaque partie comprenne et prenne en compte les besoins et spécificités de son partenaire :

• différences d'objectifs : production et diffusion de savoirs et de connaissances pour l'un ; obtention d'une solution pratique directement valorisable pour l'autre ;

• différences en termes de contraintes de temps : nécessité d'un temps suffisant pour procéder à une approche rigoureuse (observation, modélisation, validation) dans la recherche d'une solution scientifiquement reconnue pour l'un ; nécessité pour l'autre d'obtenir rapidement une solution efficace mais non nécessairement originale pour se positionner efficacement face à la concurrence ;

• différences en termes d'exploitation des résultats : objectifs en termes de publication et de reconnaissance scientifique pour l'un ; impératif de confidentialité et de prise de protection industrielle pour l'autre.

Afin de favoriser cette compréhension mutuelle et d'optimiser les chances de réussite des transferts et collaborations, il semble nécessaire de créer les conditions d'échanges constructifs, soit au sein de l'établissement, soit à l'extérieur. Il s'agit avant tout de mettre clairement en avant les objectifs définis à travers le plan stratégique de l'établissement, et d'opérer un travail précis d'identification des entreprises (groupes industriels, PME…) ou des pôles de compétitivité les plus à même de valoriser les projets mis en avant par la politique de l'établissement. Différents types de mesures à des niveaux et des échelles différents peuvent être envisagés afin d'aménager la mise en relation de ces deux milieux.

Les modes de coopération recherche-industrie

La coopération entre industriels et établissements de recherche se fait selon plusieurs modes. Quelle que soit la forme de coopération choisie, une contractualisation avant les travaux sera toujours préférée. Les clauses de publication et le partage des droits de PI résultant devront toujours être discutés avant le début des travaux :

• la coopération de recherche dans le cadre des programmes institutionnels nationaux (ANR, FUI, pôles de compétitivité, programmes des « investissements d'avenir », etc.) ou européens (PCRD). Il n'y a, en règle générale, pas de flux financiers entre les partenaires. La PI est encadrée par un accord de consortium respectant les conditions générales de l'agence de financement du programme. Les résultats sont suivis par l'État au travers des structures de tutelle, d'accompagnement ou d'évaluation, ou par la commission européenne ;

• la coopération scientifique bilatérale, entre un ou plusieurs établissements de recherche et

(41) MESR - *SNRI*

une entreprise (ou un groupe). Généralement, il existe un flux financier entre l'entreprise et les partenaires académiques. Plusieurs types de contrats sont envisageables :

– l'accord-cadre, préféré en cas de coopération régulière, qui prévoit le partage de la PI, le règlement des droits de PI, le partage des droits d'exploitation et des royalties, pour l'ensemble des projets co-développés ;

– la convention de partenariat sur un projet défini ;

• la réponse à des appels d'offres internationaux non encadrés dans des programmes ;

• les coopérations de transfert de technologies du monde académique vers l'industrie, qui consistent à industrialiser un savoir-faire nouveau développé par le monde académique et auront vocation à s'effectuer dans le cadre des sociétés d'accélération du transfert de technologies une fois celles-ci mises en place. Ces opérations s'accompagnent ou non de cession ou licences de brevets ;

• la consultance : un chercheur est rémunéré par l'entreprise pour effectuer des activités de conseil dans le domaine de la recherche. Les résultats appartiennent à l'entreprise. Les activités de consultance doivent concerner la recherche et non pas la production ou l'exploitation. L'accord de l'établissement est nécessaire. Il est conseillé aux établissements de suivre ces activités de consultance et de veiller à ce qu'elles ne soient pas en contradiction avec des accords passés avec d'autres industriels ou avec l'intérêt public ;

• la prestation de services par un laboratoire à une entreprise, souvent basée sur des savoirs et savoir-faire existants du laboratoire. Les résultats appartiennent alors à l'industriel ;

• la cession de matériels ou de produits par une entreprise à un laboratoire. La question de la responsabilité de l'établissement doit être posée et les droits de dépôt de brevets doivent être étudiés en amont ;

• la cession de brevets, la vente de licences de brevets ;

• l'équipe-conseil : activité d'expertise ; savoir et savoir-faire existants du laboratoire ; les résultats appartiennent généralement à l'entreprise.

La phase de contractualisation est importante, elle est souvent décisive pour la suite de la collaboration et la réussite de l'opération. L'aide de services spécialisés est nécessaire. Le contrat CIFRE est un outil efficace dans le cadre de coopérations recherche-industrie. **Les fédérations professionnelles** sont souvent d'excellents points d'entrée dans la recherche d'un partenaire industriel. On privilégiera l'ensemencement du tissu industriel national ou communautaire, porteur d'emplois locaux.

Risques d'une mauvaise phase de contractualisation :

• manque à gagner financier ;

• contraintes sur la liberté à publier ou à entreprendre librement des recherches ;

• perte des droits de propriété intellectuelle (y compris dans le cas de la création d'une entreprise issue de la recherche publique. La législation en la matière est souvent avantageuse pour l'inventeur-entrepreneur, réduisant du même coup les retombées positives pour la recherche publique et l'intérêt général) ;

• fuite des idées vers la concurrence ;

• exploitation abusive des résultats.

L'accompagnement des industriels à l'international devient une pratique de plus en plus courante. Il participe à la stratégie d'influence nationale et à sa politique économique. Le transfert de technologies issues de la recherche publique à l'international (hors UE) doit être fait avec circonspection et ne pas entraver l'action des industriels français ou européens dans le pays cible. C'est pourquoi une action commune est souvent préférable.

La valorisation des applications dormantes

Les nouvelles idées développées par un laboratoire ne trouvent pas toujours de débouchés industriels et sont pourtant souvent de véritables opportunités technologiques dormantes. Diverses raisons peuvent être à l'origine de cette situation :

– l'invention est arrivée trop tôt sur un marché pas encore prêt à l'absorber ;

– le procédé est trop en amont et des applications industrielles sont difficiles à imaginer ;

– de nouvelles idées amont ne sont déclinées que dans un nombre restreint de domaines industriels ou n'ont pas encore été poussées jusqu'à l'application industrielle ;

– le manque d'information sur les besoins du monde de l'entreprise n'a pas permis d'aboutir ;

– le manque d'information de l'offre faite par le

monde de la recherche n'a pas permis d'aboutir ;

– …

L'identification de ces technologies innovantes dormantes doit être une priorité des établissements, même si certaines opportunités sont moins visibles, par exemple, parce qu'elles ne se situent pas dans le champ contractuel ou d'expertise du laboratoire. Le rôle de l'établissement est alors évident. Une politique de détection est indispensable dans le plan stratégique de l'établissement.

Le dialogue doit être renforcé avec le monde de l'industrie, selon des modalités à mettre en place par chaque établissement, pour tirer parti au maximum de ces opportunités et accélérer le transfert vers l'industrie du réservoir d'innovations du monde académique. Pour mettre en relation l'offre (du monde académique) et la demande (du monde industriel) il existe des outils : forums technologiques, colloques et séminaires recherche-industrie, programmes communs de R&D bilatéraux ou multilatéraux (accords de R&D bilatéraux, projets institutionnels en consortium financés par des agences de financement publiques, laboratoires communs...), dialogue avec les fédérations professionnelles, pratiques de veille, sites internet de description des compétences et savoir-faire des laboratoires. La tentation est forte de mettre en ligne sur internet l'ensemble des savoir-faire des laboratoires pour une communication large. Cette pratique a des limites évidentes de confidentialité, qu'il convient de prendre en compte (par sites sécurisés à accès protégé ou par limitation des détails dans le contenu, par exemple). Ce dernier mode, on le voit, possède ses limites : la difficulté de l'exercice de communication, qui consiste à dévoiler suffisamment d'informations pour être compris et attractif, sans dévoiler l'information stratégique.

Les bourses CIFRE et l'embauche par le monde industriel d'anciens doctorants connaissant bien les laboratoires sont des aides précieuses pour la mise en relation des deux mondes.

Il est nécessaire de privilégier une politique commune et coordonnée inter-établissements et interdisciplinaire pour gagner en efficacité, tout en respectant l'autonomie et la responsabilité de chaque partenaire.

4. DÉVELOPPEMENT DE L'INTERFACE ENTRE LA RECHERCHE ET LE MILIEU SOCIO-ÉCONOMIQUE

- Contractualiser systématiquement avant le lancement des travaux de R&D prévu dans une collaboration (clauses de publications, partage et exploitation des droits de PI…).
- Disposer ou avoir accès à des compétences professionnelles : juridiques, propriété intellectuelle, financières, technico-commerciales.
- Opérer un travail précis d'identification des entreprises (groupes industriels, PME…) ou des pôles de compétitivité les plus à même de valoriser les projets mis en avant par la politique de l'établissement.
- Renforcer le dialogue avec le monde de l'industrie : forums technologiques, colloques et séminaires recherche-industrie, programmes de R&D bilatéraux ou multilatéraux, dialogue avec les fédérations professionnelles, pratiques de veille, sites internet sécurisés de description des compétences et savoir-faire des laboratoires…
- Il peut être risqué de mettre en ligne tous les savoir-faire des laboratoires. Ce mode de communication a donc des limites : il est difficile de dévoiler suffisamment d'informations pour être compris et attractif sans dévoiler d'informations stratégiques.
- Suivre l'activité de consultance des chercheurs et veiller à ce qu'elles ne soient pas en contradiction avec des accords passés avec d'autres industriels ou avec l'intérêt général.
- Identifier les technologies innovantes « dormantes » (qui n'ont pas encore trouvé de débouchés industriels).
- Établir une politique claire de licences / harmoniser les pratiques internes.
- Privilégier l'ensemencement du tissu industriel national ou communautaire, pour le transfert de technologies universitaires vers l'industrie.
- Préciser les modalités d'une politique d'essaimage.
- Développer une politique de contrats CIFRE.
- Privilégier une politique interdisciplinaire.
- Privilégier une politique inter-établissements.
- …

Bibliographie

- **MESR-SNRI** *(stratégie nationale de la recherche et de l'innovation) http ://www.enseignementsup-recherche.gouv.fr/pid24538/strategie-nationale-recherche-innovation-i.html*

5

Politique internationale

Introduction

La recherche française se doit d'assurer sa présence, sa visibilité et la démonstration de sa qualité sur la scène internationale. Les coopérations scientifiques internationales sont non seulement des éléments de prestige mais aussi des possibilités d'élargir les champs de recherche et d'augmenter la qualité des travaux. Elles permettent en effet, en fédérant les efforts et les connaissances et en s'ouvrant à d'autres méthodes et idées, d'accroître la créativité et les compétences scientifiques et de mieux prendre conscience des nouveaux défis globaux que la recherche sera amenée à relever.

Il existe plusieurs types d'échanges et de partenariats internationaux, allant de l'accueil de stagiaires aux collaborations de recherche avec des entreprises ou laboratoires, en passant par des missions à l'étranger, scientifiques ou de consultance, de chercheurs français. Il conviendra donc de tenir compte de ce contexte et de ces objectifs et d'intégrer dans la politique internationale de l'établissement, de façon cohérente et lisible, des concepts d'intelligence économique. Les coopérations internationales présentent un certain nombre de risques spécifiques dans le domaine de la protection du patrimoine scientifique, auxquels il convient d'apporter une vigilance accrue par la mondialisation.

La politique d'IE de l'établissement possèdera donc un volet « stratégie internationale », qui déclinera ces concepts, que ce soit en termes d'image de l'établissement, de renforcement de ses compétences techniques et scientifiques, mais aussi de sensibilisation du personnel aux comportements à adopter en mission à l'étranger ainsi que de choix des partenaires et de modes de contractualisation avec eux.

Les échanges internationaux peuvent revêtir plusieurs formes. Toutes doivent être envisagées :

• les coopérations scientifiques et techniques contractualisées avec un ou plusieurs organismes soit étrangers, soit internationaux, de durées plus ou moins longues. Ces coopérations donnent lieu à des séjours de chercheurs et d'étudiants dans les deux sens ;

• des contacts scientifiques spontanés, non contractualisés par les établissements ; ils sont souvent suivis de contractualisation ; ils donnent lieu à des séjours dans les deux sens ;

• des séjours de toute durée, effectués en délégation ou à titre individuel dans les organismes et les entreprises du secteur public ou privé ;

• des transferts de technologies, développées en coopération ou vendues ou licenciées ;

• des opérations de consultance effectuées par des chercheurs de laboratoires français pour des entreprises étrangères ;

• l'emploi temporaire de chercheurs étrangers dans les laboratoires français (post-doc, chercheurs ou enseignants-chercheurs invités …) ;

• des coopérations universitaires contractualisées entre établissements et donnant lieu à des séjours de quelques mois (master) à quelques années (doctorat) dans les laboratoires français ;

• l'accueil d'étudiants en stage ou en doctorat dans les laboratoires sous contrat individuel ;

• l'activité des français à l'étranger à l'occasion de missions d'ordre économique, scientifique et technologique (conférences, séjours dans des laboratoires étrangers, enseignement, sélection d'étudiants …).

Stratégie internationale

Définition de la stratégie internationale

Une stratégie d'établissement à l'international est un plan cohérent, dans le temps, dans l'espace scientifique et dans ses financements, fait dans un objectif précisé, de choix de sujets de recherche, de partenaires et de modes de coopérations. La stratégie internationale doit accompagner la stratégie scientifique et celle de valorisation et non pas les précéder, même s'il est bon de saisir quelques opportunités, quand elles se présentent.

S'il est vrai que les chercheurs et les laboratoires ont une grande liberté dans la façon de mener leur stratégie scientifique et, transitivement, leur stratégie de coopération internationale, tous les établissements se dotent d'une politique d'établissement en la matière, i.e. d'un ensemble de directives et de recommandations dans les choix précités. De même les décisions de financement des coopérations sont généralement du ressort de l'établissement, voire de l'institut dans le cas des très gros établissements.

Rôle des ministères : Les établissements d'enseignement supérieur et de recherche se dotent, individuellement ou collectivement (exemple Agreenium), d'une stratégie d'action à l'international compatible avec les orientations affichées par leur ministère de

tutelle. Le rôle du ministère des Affaires étrangères et européennes (MAEE) est important dans le dispositif par les financements qu'il apporte aux doctorats en cotutelle, aux coopérations scientifiques ou à l'organisation de colloques et par les différentes actions de mise en relation des chercheurs français avec des chercheurs étrangers qu'il met en place dans les services culturels et scientifiques de ses ambassades. Le MAEE met également à disposition des scientifiques des bulletins d'information et de veille en collaboration avec l'ADIT ainsi que des recommandations, mises à jour en temps réel, pour les visiteurs de pays à risques (hygiène, santé, politique, terrorisme, risques climatiques …).

Application de la stratégie internationale

L'établissement de recherche définit sa stratégie en fonction, tout d'abord, de ses choix et objectifs scientifiques, puis des recommandations des ministères de tutelle (MESR, MEFI, MAAPRAT, etc.) et du MAEE.

Pour l'application en son sein, l'établissement définit des règles applicables aux différentes entités qui le composent :

- sur le périmètre de ce qui est du ressort décisionnel de l'établissement, des instituts, des laboratoires et des chercheurs, en termes de coopération internationale ;
- sur les modes de contractualisation. La définition de critères de choix devra être privilégiée ;
- sur les sujets de recherche et sur les priorités thématiques – scientifiques. L'établissement devra définir les thèmes qu'il est possible d'ouvrir et ceux sur lesquels il s'agira d'être vigilant en termes de propriété intellectuelle, notamment si ces sujets font l'objet d'accords de partenariats industriels ou de partenariats avec la défense ;
- sur la sélection des stagiaires ;
- sur le suivi des stagiaires durant leur période de stage et sur la suite de leur parcours ;
- sur le suivi des résultats des coopérations, notamment en termes d'apports ou de retour sur investissement pour l'établissement. Une vigilance particulière est attendue sur les recherches donnant lieu à un développement industriel. Dans les conventions de coopération, il est indispensable d'évaluer à la bonne hauteur l'apport initial de connaissances de chaque partenaire et la répartition des résultats ;
- sur le suivi des visites et stages dans les laboratoires sensibles ;
- sur les règles inter-établissements pour harmoniser les politiques et stratégies des tutelles des équipes mixtes ;
- sur la stratégie « pays » de l'établissement (i.e. la sélection des partenaires de coopération; la stratégie de valorisation dans le pays, la stratégie de coopérations universitaires), qui doit être en cohérence avec la SNRI (stratégie nationale de recherche et d'innovation) du MESR ou sur la politique équivalente des ministères de tutelle (MAAPRAT, MEFI, etc.)
- sur la politique de consultance de l'établissement. Un suivi des activités de consultance des chercheurs et enseignants-chercheurs est nécessaire. Elle ne doit pas générer de conflits d'intérêts industriels avec les conventions industrielles de l'établissement (ou de ses partenaires en cas de tutelle multiple des laboratoires), ni d'atteinte à l'intérêt public. En application de la politique publique d'IE, il s'agit de favoriser, dans un monde économique où l'innovation est le moteur de la croissance, **le transfert des technologies issues du monde universitaire et de la recherche prioritairement vers l'industrie nationale ou communautaire.**

Le dispositif réglementaire de protection du potentiel scientifique et technique en vigueur encadre les coopérations, il doit être pris en compte.

Les bonnes pratiques d'une stratégie internationale

La stratégie internationale d'un établissement de recherche doit répondre à quelques critères de qualité, pour s'intégrer dans la politique d'IE. Elle doit, notamment :
- veiller à préserver l'image de la France à l'international ;
- favoriser la conservation sur le territoire français ou communautaire des technologies innovantes développées sur des crédits nationaux ou communautaires ;
- veiller à ce que les résultats de la recherche financée par la France lui soient bien attribués au prorata de sa participation, dans les indicateurs internationaux (brevets, articles scientifiques, …) notamment dans les comptes fractionnaires ;
- concilier l'intérêt général national et les intérêts particuliers du chercheur et de l'établissement.

Pour ce faire, quelques règles simples de bonnes pratiques peuvent être appliquées :

- décliner une politique de présence active dans les conférences scientifiques ;
- se définir des objectifs en termes de publications (quantité et qualité des revues) ;
- décliner une politique de présence active dans les instances décisionnelles scientifiques internationales (expertise à la commission européenne, notamment) ;
- laboratoires conjoints :

• une adresse en France pour les laboratoires internationaux permet l'attribution à la France d'une partie des articles scientifiques produits par le laboratoire[42] ,

• privilégier pour ce type de structure, les coopérations qui ont déjà prouvé leur intérêt ;

- dans les articles scientifiques écrits en co-publication, vérifier que la part qui va revenir à la France dans les comptes fractionnaires reflète bien sa participation. De même, dans les articles co-publiés par les partenaires étrangers, vérifier qu'une part reviendra à la France (par application d'une adresse en France) ;
- favoriser les coopérations d'intérêt scientifique véritable et mesurable pour la recherche française ;
- veiller à ce que les brevets issus de recherche conjointe et publiés dans un pays étranger mentionnent l'institution de tutelle nationale ;
- préférer les coopérations contractualisées aux coopérations spontanées non couvertes par une convention, notamment sur les points du partage de la PI ;
- choix des partenaires : s'assurer de la qualité des travaux du partenaire pressenti et s'assurer de sa tutelle (académique, industrielle…) ;
- dans les accords de coopération bien délimiter les champs de recherche couverts ;
- préférer le financement des coopérations à parité plutôt qu'à réciprocité de services ;
- accueil d'étudiants étrangers, non européens : privilégier la qualité des candidats à leur mode de financement ;
- harmoniser les politiques inter-établissements pour l'application aux laboratoires à tutelles multiples ;
- sensibiliser les laboratoires à ces pratiques, notamment à la protection du patrimoine scientifique et technique (PPST) et à la sécurité des systèmes d'information (SSI) ;
- établir une charte du comportement des chercheurs à l'étranger (éviter la diffusion mal maîtrisée de résultats non protégés, la signature d'accords sans avis de la tutelle…).

Le chercheur français à l'international – conseils pratiques

Missions de chercheur français à l'étranger (hors UE)

Conseils pratiques pour un chercheur ou un enseignant-chercheur se rendant en mission à l'étranger.

AVANT DE PARTIR

• Les formalités

- Consultez les recommandations spécifiques au pays de destination sur le site web du MAEE : *http ://www.diplomatie.gouv.fr* onglet « conseils aux voyageurs » ou sur celui du CNRS : *https ://dri-dae.cnrs-dir.fr* onglet « vous êtes en France - partir à l'étranger »
- Munissez-vous d'un visa en règle couvrant **l'intégralité** de la période de séjour et l'intégralité des activités que vous allez y mener.
- Notez les numéros d'urgence dont vous pourriez avoir besoin pendant votre séjour, notamment ceux des services diplomatiques français sur place.

• Les documents

- Munissez-vous uniquement des documents techniques indispensables au déplacement, à l'exclusion de tous autres, tels que carnets d'adresses, notes, article ou brevet en cours de rédaction, susceptibles d'être reproduits.
- Si vous emportez un ordinateur portable,

(42) OST, *Note méthodologique B5 – rapport annuel 2010* : « Les articles scientifiques étant souvent cosignés par plusieurs auteurs et plusieurs institutions, plusieurs options de comptage existent. Dans une logique de "contribution" à la science mondiale, chaque article est fractionné au prorata du nombre d'adresses différentes indiquées par ses auteurs, de manière à ce que la somme des adresses soit de 100 %. Ce principe est également appliqué aux articles d'un journal scientifique appartenant à plusieurs spécialités. Ce type de compte, dit "fractionnaire", où chaque article a un poids unitaire, est additif à toutes les échelles et bien adapté à la macroanalyse.»

effacez efficacement les fichiers non strictement nécessaires à la mission. Notamment, n'emportez pas votre boîte aux lettres, ni votre carnet d'adresse électronique, ni des résultats de recherche non protégés : votre disque dur peut être copié, directement ou lors d'une connexion de votre ordinateur au réseau de l'hôtel. Prendre en compte les dispositifs spécifiques du pays visité en matière de chiffrement.

- Expédiez si besoin les documents confidentiels par le moyen de la valise diplomatique (en s'assurant au préalable de son accord et des délais).

- Attention : pour l'envoi d'un colis, prendre d'abord l'attache du service scientifique de l'ambassade du pays de destination, lui transmettre toutes les informations concernant le contenu, le volume et le poids du colis. Le service scientifique s'assurera de l'accord du service de la valise et indiquera les démarches à effectuer. Les liquides, CD et DVD ne sont pas transportés par la valise diplomatique. Le prix d'envoi des colis est un prix proportionnel à leur poids.

• Le matériel

- Observez strictement les formalités d'entrée et de séjour, en évitant notamment toute atteinte à la réglementation sur l'importation et l'exportation :

• des devises ;

• des denrées alimentaires (fruits, légumes, charcuterie, fromage…) ;

• des plantes ou des semences ;

• du matériel de détection GPS ;

• des échantillons radioactifs…

À l'ambassade de France, un attaché des douanes peut vous renseigner pour les questions particulières.

- Mettez-vous en règle avec votre institution française si vous désirez exporter vers un pays étranger des échantillons ou des produits résultats de vos recherches.

■ PENDANT LE SÉJOUR

• La communication

- Évitez d'exposer des résultats de recherche non encore exploités ou protégés.

- Ne laissez jamais des documents de travail importants dans des bagages sans surveillance. Gardez avec vous les documents et supports magnétiques ou électroniques sensibles ou conservez-les dans une mallette fermée à clé. Il vous est de plus recommandé de chiffrer les documents ou supports transportant des informations sensibles.

- Évitez d'avoir des conversations importantes ou confidentielles dans une chambre d'hôtel ou chez un particulier. Les locaux d'hébergement ne garantissent pas contre les indiscrétions.

- En téléphonant ou en écrivant un message électronique, exprimez-vous en considérant que la transmission a des chances d'être interceptée. Évitez les sujets sensibles aux yeux des autorités du pays de destination.

- Évitez de prendre des notes ou des enregistrements sonores ou photographiques en dehors de l'objet de la mission au cours de visites d'établissements scientifiques ou industriels ; cette pratique attire très fréquemment l'attention des services de sécurité.

• La sécurité

- En cas d'accident lors d'un déplacement, informez-en immédiatement nos services diplomatiques. Dans certains pays, si vous comptez vous éloigner des villes les plus fréquentées, prévenez l'ambassade de votre ou de vos destinations.

- N'acceptez jamais les services de faux taxis, qui sévissent surtout dans les aéroports, préférez toujours la file d'attente officielle. Les taxis officiels ont un compteur bien visible, qui délivre automatiquement un reçu.

- Ne stationnez pas à proximité des casernes, installations militaires ou assimilables, ceci peut être interprété comme tentative d'espionnage. Dans le même souci d'éviter des incidents, l'utilisation d'appareils photographiques est déconseillée sur ce type de lieu.

- En toute circonstance faites preuve de maîtrise de soi : réagir avec trop de nervosité devant une provocation ne facilite pas l'intervention des autorités consulaires ou diplomatiques. La règle impérative à suivre en cas d'incident est de rendre compte immédiatement à l'ambassade.

• Les relations humaines

- Soyez prudent dans vos relations d'apparence amicales ou affectives qui pourraient se nouer à l'occasion de vos voyages ; les services spécialisés ne répugnent pas à utiliser de tels moyens d'approche. De même, les guides et interprètes sont généralement en contact avec ceux-ci auxquels ils sont souvent contraints de prêter leur concours.

- N'acceptez pas de transporter des lettres ou des paquets à titre de « service amical » car cela peut motiver une inculpation pour espionnage ou activité subversive. De même, n'acceptez pas de

cadeau d'inconnus ou de personnes dont vous n'êtes pas totalement sûr. Ces demandes de service ou ces cadeaux peuvent être effectués dans une intention de compromission.

- Accueillez avec circonspection les confidences de personnes se disant opposées au régime ou à la politique de leur gouvernement ; elles peuvent n'être que provocation.

Au retour, rapportez à votre hiérarchie ou à votre fonctionnaire de sécurité de défense (FSD) tout élément notable relatif à la sécurité, qu'il vous ait concerné ou qu'il concerne des collègues.

Coopération scientifique franco-étrangère (hors UE)

Vous souhaitez signer un accord de coopération avec un laboratoire étranger, ne versez ni dans la paranoïa, ni dans la naïveté. Soyez conscient que certains pays ont grand besoin de développer leur système d'innovation technologique et que leur recherche est très orientée vers le développement industriel. Le monde académique (universités et académies scientifiques) est un acteur clef de ce développement de l'innovation industrielle. Quelques règles permettront un modus vivendi profitable pour les deux parties. (La plupart de ces recommandations s'appliquent à la consultance.)

PRÉPARATION DE L'ACCORD

• Vérifiez, avant toute coopération scientifique, même spontanée, qu'elle est couverte par un accord ou une convention. En cas d'absence d'accord-cadre, préparez une convention spécifique. Prenez en compte les obligations règlementaires vis-à-vis des institutions de tutelle.

• Prévoyez dans le contrat de coopération des clauses de propriété intellectuelle et des règles de co-publication, voire, le cas échant, de développement industriel, de dépôt et d'exploitation de brevets. Assurez-vous de l'accord des directions des affaires internationales et des affaires industrielles de votre institution, qui pourront vous conseiller utilement ou vous fournir des contrats-types.

• Définissez précisément le champ d'action et le domaine de recherche couverts par la convention. En cas d'extension, signez un avenant. Cette précaution prémunit contre d'éventuels litiges futurs sur des domaines connexes.

• Ne signez jamais sur place d'engagement, qui n'ait été lu et approuvé par les directions des affaires internationales et des affaires juridiques de votre institution française de rattachement. Si un texte vous a été soumis avant votre départ, vérifiez avant de signer, sur place, que le texte n'a pas été modifié (paragraphe retiré ou ajouté, par exemple).

• Faites bien apparaître, dans l'accord, le nom de l'institution de rattachement du laboratoire partenaire (université, académie scientifique, entreprise d'état ou entreprise privée).

• Renseignez-vous bien sur l'institution de rattachement du laboratoire partenaire :

- certains appartiennent au complexe militaro-industriel de leur pays. Dans ce cas, l'utilisation des résultats de recherche conjoints à des fins autres que celles que vous envisagiez est possible ;

- certains laboratoires appartenant à des grandes entreprises d'état s'affichent comme laboratoires académiques (quelques-uns ont même le droit de délivrer des doctorats). Dans ce cas, suivez de près l'exploitation industrielle des résultats ;

- dans certains pays, toutes les universités et académies possèdent ou créent à volonté des entreprises pour développer les résultats de leur recherche. Certains laboratoires académiques sont donc, de fait, des entreprises publiques. Les règles de financement de leur participation à des contrats européens s'en trouvent donc modifiées.

• Signez les accords au bon niveau : il est toujours préférable de faire signer les institutions de tutelle plutôt que les laboratoires, qui n'ont, en règle générale, pas légitimité à engager leur institution. Ne pas accepter un décalage de niveau entre les signataires : une université ou un organisme de recherche français ne doit pas signer avec un laboratoire étranger, qui n'a, en règle générale, pas non plus légitimité à engager son institution.

• Financement : préférez un cofinancement à parité, où chaque partie prend en charge les salaires et frais de mission de ses agents, à un financement par réciprocité de service.

• Tous les organismes universitaires et de recherche n'ont pas le même niveau d'excellence. En cas de doute sur le niveau d'un partenaire académique, contactez le service scientifique de l'ambassade de France, qui vous fournira quelques indicateurs nationaux.

• Vérifiez toujours la bibliographie de votre correspondant et de son laboratoire.

• Dans l'accord, séparez les échanges de doctorants et les échanges de post-doctorants, qui, en

France, ont des statuts très différents. Si l'accord implique une délivrance de diplôme (doctorat, par exemple), assurez-vous que les signataires sont bien habilités à les délivrer.

EXÉCUTION DE L'ACCORD

• N'hésitez pas à signaler une dérive ou un non-respect de l'accord : nouveaux partenaires imposés (notamment des partenaires industriels non prévus), extension du domaine de recherche…

• Ne citez pas, dans vos articles, d'auteur, ni de nom de laboratoire, qui n'ait pas concrètement participé aux travaux.

• N'hésitez pas à signaler à l'ambassade (service scientifique) et à votre institution, tout plagiat de vos résultats de recherche et de vos publications soupçonné ou constaté.

• Brevets déposés dans un pays étranger : n'acceptez pas que votre nom soit mentionné dans un brevet domestique à l'étranger sans que votre institution de rattachement soit l'un des déposants ou qu'elle ait clairement laissé tout le bénéfice des résultats à la partie partenaire ; vous vous mettriez en position d'illégalité. Signalez dès que possible la découverte de brevets déposés dans son pays par le laboratoire partenaire sur les résultats de la coopération.

Coopération universitaire avec un pays étranger

Vous souhaitez monter une coopération universitaire avec un pays étranger. Quelles sont les bonnes questions à se poser pour une coopération fructueuse ?

• Vérifiez l'équivalence des diplômes entre les deux pays, notamment en cas de délivrance de doubles diplômes

• Vérifiez la tutelle de l'université ou de l'établissement partenaire (civile, défense ou militaire, nationale ou régionale, publique ou privée…).

• Vérifiez le niveau et la visibilité de l'université partenaire dans les domaines de coopération souhaités.

• Choisissez une université partenaire qui offre le même cursus que la vôtre (LMD).

• Préférez les partenariats au niveau master, doctorat ou diplôme d'ingénieur au détriment des partenariats au niveau de la première année d'université.

• Préférez les partenariats de type « échanges d'étudiants » aux partenariats de type « accueil d'étudiants étrangers », l'implication de l'université partenaire sera d'autant plus grande et les étudiants mieux sélectionnés.

• Assurez-vous que les étudiants envoyés à l'étranger sont bien couverts par une assurance responsabilité civile, une assurance rapatriement et bénéficient d'une couverture médicale.

• Assurez-vous que les étudiants reçus sont bien couverts par une assurance responsabilité civile, une assurance rapatriement et bénéficient d'une couverture médicale pendant **l'intégralité** de leur séjour en France.

• Prenez en compte les obligations règlementaires vis-à-vis des institutions de tutelle.

Stagiaires et visiteurs étrangers

ATTENTION : les visiteurs et stagiaires étrangers (y compris les ressortissants des pays de l'UE) au sein des ZRR (laboratoires sensibles) sont soumis aux dispositions d'autorisation et d'avis fixés par le 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.

VISITEURS

Vous êtes sollicités pour recevoir une délégation officielle étrangère (hors UE).

• Signalez toujours les demandes de visites au FSD.

• N'hésitez pas à refuser une visite qui vous semble incongrue (délégation d'une institution politique non académique) ou à faire recevoir la délégation par d'autres services ou par une autre administration.

• Refusez de répondre aux questions qui ont trait à un autre service que le vôtre ou qui sont d'un niveau politique qui ne vous correspond pas.

STAGIAIRES

Vous recevez des stagiaires dans votre laboratoire, dans le cadre d'une coopération scientifique, d'une formation universitaire ou d'une demande spontanée d'un organisme étranger.

• Assurez-vous que le stagiaire ait un visa en règle : soit un visa de scientifique pour un chercheur invité, soit un visa d'étudiant avec une convention

de stage ou une inscription dans une université française.

• Faites signer une clause de confidentialité avant l'entrée au laboratoire et assurez-vous que le stagiaire a bien compris à quoi cette clause l'engage ; notez que les étudiants n'étant pas tenus par la réglementation s'appliquant aux personnels (d'une entreprise ou d'une institution), une clause décrivant le partage en cas de dépôt de brevet d'invention est indispensable.

• Signalez au responsable SSI rapidement tout flux de données informatiques important ou répété à destination du pays d'origine.

• Si l'un de vos visiteurs apporte des échantillons, vérifiez qu'il soit en règle avec les lois de son pays sur l'exportation de produits et de résultats de recherche.

• S'il s'agit d'une demande de stage spontanée non liée à une coopération scientifique ou universitaire, renseignez-vous auprès de l'ambassade de France sur l'organisme d'appartenance du demandeur.

• S'il s'agit d'une visite dans une zone à régime restrictif, assurez-vous d'être en adéquation avec la réglementation en vigueur.

5. POLITIQUE INTERNATIONALE

■ Sensibiliser les laboratoires, les chercheurs et, globalement, l'ensemble du personnel aux bonnes pratiques en matière de protection du patrimoine scientifique et technique et de sécurité des systèmes d'information dans le cadre des coopérations internationales.

■ Faire valider les projets de recherche avec des partenaires étrangers par les instances ad-hoc.

■ Définir des règles applicables aux différentes entités de l'établissement en ce qui concerne :

- le périmètre de ce qui est du ressort décisionnel de l'établissement, des laboratoires ou des chercheurs en matière de coopération internationale ;
- les modes de contractualisation à privilégier pour les coopérations internationales ;
- la sélection et le suivi des stagiaires dans la cadre des coopérations internationales (notamment dans les laboratoires sensibles) ;
- le suivi des visites de délégations étrangères (ou autres) dans les laboratoires sensibles et les administrations des établissements (prévenir systématiquement les instances ad-hoc) ;
- le suivi des résultats des coopérations internationales, notamment en termes d'apports ou de retour sur investissement pour l'établissement ;
- la stratégie « pays » de l'établissement (sélection des partenaires de coopération, stratégie de valorisation et de coopérations universitaires dans le pays…) ;
- la politique de consultance de l'établissement (suivi des activités de consultance).

■ Faire signer une clause de confidentialité aux stagiaires et aux visiteurs avant l'entrée dans le laboratoire.

■ Définir les thématiques qu'il est possible d'ouvrir et celles sur lesquelles il s'agira d'être vigilant en termes de PI.

■ Décliner une politique de présence active dans les conférences scientifiques.

■ Définir une stratégie en termes de publications (quantité et qualité des revues).

■ Vérifier que la part des co-publications internationales qui va revenir à la France dans les comptes fractionnaires bibliométriques reflète bien la participation de l'établissement français.

■ Pour les laboratoires internationaux conjoints, une adresse en France permet l'attribution à la France d'une partie des articles scientifiques produits par ces laboratoires.

■ Veiller à ce que les brevets issus de recherche conjointe et publiés dans un pays étranger mentionnent l'institution de tutelle nationale.

- Vérifier les conditions de financement des agences nationales des pays étrangers (certaines peuvent préempter la PI issue du projet financé) ainsi que la législation relative à la propriété intellectuelle afin de s'assurer que l'établissement demeure propriétaire de sa PI et pourra librement l'exploiter.
- Ne jamais se rendre dans une institution étrangère sans un ordre de mission et une convention d'accueil qui règlera les questions de responsabilité en cas de dommage ainsi que de partage de la PI sur les résultats éventuels et de confidentialité des informations échangées.
- Préférer les coopérations contractualisées aux coopérations spontanées non couvertes par une convention, notamment sur les points du partage de la PI.
- Ne jamais signer sur place (à l'étranger) d'engagement qui n'ait été lu par les directions des affaires internationales et des affaires juridiques de l'institution française de rattachement.
- Établir une charte du comportement des chercheurs à l'étranger : éviter les ordinateurs portables emportés contenant des informations sensibles inutiles pour la mission en cours, la signature d'accord sans avis de tutelle…
- À l'étranger, se munir uniquement des documents techniques indispensables au déplacement.
- N'emporter un ordinateur portable que si cela est réellement nécessaire : souvent, les documents indispensables à la mission, transportés sur un support électronique, peuvent être suffisants.
- Utiliser le réseau des ambassades pour les missions à l'étranger : prise de contact avec les attachés et les conseillers scientifiques. Cela peut renseigner les chercheurs en déplacement à l'étranger sur les risques potentiels dans le cadre de leur mission, et peut également permettre aux ambassades de capitaliser l'expérience de ces chercheurs et de la mettre au profit d'autres missions. Cette recommandation concerne aussi les personnels administratifs en mission à l'étranger.
- En cas d'incident lors de missions à l'étranger, la règle impérative est de rendre compte immédiatement à l'ambassade.
- Au retour de missions internationales, signaler à la hiérarchie ainsi qu'au service ad-hoc tout incident, élément notable relatif à la sécurité, qu'il vous ait concerné ou qu'il concerne des collègues.

Bibliographie

- **OST,** *note méthodologique B5 – rapport annuel 2010 http ://www.obs-ost.fr/fr/le-savoir-faire/etudes-en-ligne/travaux-2010/rapport-biennal-edition-2010.html*

Sigles et acronymes

AERES	Agence d'évaluation de la recherche et de l'enseignement supérieur
AFNOR	Association française de normalisation
CEI	Commission électrotechnique internationale
CEN	Comité européen de normalisation (European Committee for Standardization)
CENELEC	Comité européen de normalisation électrotechnique (European Committee for Electrotechnical Standardization)
CRIE	Chargé de mission régionale en matière d'intelligence économique
DDRI	Direction départementale du renseignement intérieur
DGGN	Direction générale de la Gendarmerie nationale
DGPN	Direction générale de la Police nationale
D2IE	Délégation interministérielle à l'intelligence économique
DIRECCTE	Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi
DPI	Droits de propriété intellectuelle
ETSI	European Telecommunications Standards Institute
FRAND	Fair, Reasonable And Non Discriminatory
FSD	Fonctionnaire de sécurité et de défense
FSSI	Fonctionnaires de sécurité des systèmes d'information
GPO	Group Policy Object
HFDS	Haut-fonctionnaire de défense et de sécurité
INPI	Institut national de la propriété industrielle
ISO	International Organization for Standardization (Organisation internationale de normalisation)
l'ANSSI	Agence nationale de la sécurité des systèmes d'information
MAC	Media Access Control
MAEE	Ministère des Affaires étrangères et européennes
MESR	Ministère de l'enseignement supérieur et de la recherche
MIOMCTI	Ministère de l'Intérieur, de l'Outre-Mer, des Collectivités territoriales et de l'Immigration
OCDE	Organisation de coopération et de développement économiques
OECD	Organisation for Economic Co-operation and Development
OMPI	Organisation mondiale de la propriété intellectuelle (cf. WIPO)
PI	Propriété intellectuelle
PPIE	Politique publique d'intelligence économique
R&D	Recherche et développement
RGS	Référentiel général de sécurité
SATT	Société d'accélération du transfert de technologies
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SNRI	Stratégie nationale de recherche et d'innovation
SSID	Service Set Identifier
UE	Union européenne
UIT	Union internationale des télécommunications
USB	Universal serial bus
WIPO	World Intellectual Property Organization (cf. OMPI)
WPA/WPA2	WiFi Protected Access
ZRR	Zone à régime restrictif

GUIDE DE L'INTELLIGENCE ÉCONOMIQUE POUR LA RECHERCHE

L'élaboration de ce guide s'est effectuée dans le souci de concertation et collaboration avec les principaux acteurs concernés. Ont participé des établissements de recherche publique (organismes de recherche, écoles et universités), ministères et institutions publiques et autres institutions dont l'expertise est susceptible d'aider à la protection et à la valorisation des résultats de la recherche publique.
Le guide ne prétend pas inventer ni soumettre de nouvelles règles ou une stratégie nouvelle en matière de transfert de technologies ou de gestion d'établissement. De nombreux documents déjà évoqués existent en la matière. Le guide s'attache à répertorier les plus pertinents d'entre eux et à les mettre en perspective avec la problématique de l'intelligence économique.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCOLOGIE, DU DÉVELOPPEMENT DURABLE, DES TRANSPORTS ET DU LOGEMENT

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE MER, DES COLLECTIVITÉS TERRITORIALES ET DE L'IMMIGRATION

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE L'INDUSTRIE

MINISTÈRE DU BUDGET, DES COMPTES PUBLICS ET DE LA RÉFORME DE L'ÉTAT

MINISTÈRE DE L'AGRICULTURE, DE L'ALIMENTATION, DE LA PÊCHE, DE LA RURALITÉ ET DE L'AMÉNAGEMENT DU TERRITOIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

ANSSI · SGDSN · Gendarmerie nationale · DCRI · Service de coordination à l'intelligence économique · afnor NORMALISATION · cea · cnrs · Conférence des présidents d'université

FIST · IFP Energies nouvelles · inpi INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE · INSA LYON · Instituts thématiques Inserm Institut national de la santé et de la recherche médicale · InsermTransfert · oséo · UPMC SORBONNE UNIVERSITÉ