MEILLEURES PRATIQUES DU G7 POUR UNE RECHERCHE SÉCURITAIRE ET OUVERTE

Groupe de travail sur la sécurité et l'intégrité de l'écosystème de la recherche (SIGRE)

Ce document est une copie du document original intitulé G7 Best Practices for Secure & Open Research publié par le G7.

Février 2024

TABLE DES MATIÈRES

Énoncé de la vision

Dans le document Valeurs et principes communs du G7 sur la sécurité et l'intégrité de la recherche, les membres soutiennent :

> *La poursuite d'un système de la recherche collaborative où l'importance de tous les talents – tant au niveau national qu'international – est reconnue. L'ouverture et la sécurité ne sont pas contradictoires, mais complémentaires et se renforcent mutuellement.*

Les membres du G7 reconnaissent que le respect de la liberté de la recherche scientifique est une pierre angulaire indispensable à la démocratie et une valeur fondamentale commune pour une coopération de recherche de confiance et ouverte avec des partenaires internationaux. Les membres s'engagent à promouvoir la coopération internationale en matière de recherche et les conditions de liberté, d'indépendance, d'ouverture, de réciprocité et de transparence dans lesquelles elle s'épanouit.

Pour soutenir cette vision, les membres du G7 ont élaboré et approuvé un ensemble de principes sur la sécurité de la recherche qui sont communs aux membres du G7 et aux communautés universitaires et qui sont cohérents avec les valeurs communes établies concernant l'intégrité de la recherche. Cet ensemble de principes de la sécurité de la recherche et les valeurs communes sur l'intégrité de la recherche sont présentés dans le document Valeurs et principes communs du G7 sur la sécurité et l'intégrité de la recherche et les annexes A et B ci-dessous.

Pour soutenir la mise en œuvre des principes de la sécurité de la recherche et des valeurs communes concernant l'intégrité de la recherche susmentionnés, les membres du G7 ont dressé une liste des meilleures pratiques afin de fournir des informations de haut niveau sur les pratiques qui contribuent à la sécurité et à l'ouverture de la recherche. Reconnaissant que toutes les parties prenantes aient un rôle à jouer pour assurer la sécurité et l'intégrité de la recherche, ces meilleures pratiques sont destinées aux gouvernements, aux organisations de financement de la recherche, aux institutions de recherche et aux chercheurs, soit collectivement ou individuellement, en fonction de leur rôle au sein de la recherche. Vous trouverez à l'annexe C des exemples de meilleures pratiques qui sont mises en œuvre par différents membres du G7.

Pour compléter ce document sur les meilleures pratiques, une académie virtuelle sera également développée pour aider les parties prenantes du G7 et au-delà à mettre en œuvre des pratiques de sécurité et d'intégrité de la recherche au sein de leurs institutions. Cette académie virtuelle permettra aux utilisateurs d'explorer la manière dont chaque membre du G7 aborde la sécurité et l'intégrité de la recherche, et inclura des exemples supplémentaires de meilleures pratiques et d'études de cas à titre de référence.

Pourquoi l'intégrité et la sécurité de la recherche sont-elles importantes?

La recherche ouverte et collaborative est à la base des mesures prises au niveau national et mondiale pour répondre à certaines des questions les plus difficiles et les plus urgentes qui nous sont posées. Il est important de favoriser les collaborations scientifiques internationales. Ces collaborations accélèrent le rythme des découvertes et augmentent le dynamisme et l'ouverture de nos communautés de recherche.

L'intégrité de la recherche - c'est-à-dire le respect des valeurs, des principes et des meilleures pratiques professionnelles qui assurent la validité, la pertinence sociale, la responsabilité et la qualité de la recherche – est le principe de base qui permet aux chercheurs de collaborer dans un environnement de recherche équitable, innovant, ouvert et de confiance. L'intégrité de la recherche permet aux individus d'avoir confiance dans le développement des connaissances et dans la diffusion de ses résultats.

En même temps, les avancées scientifiques et leurs applications potentielles peuvent faire de la recherche une cible pour ceux qui cherchent à accéder sans autorisation aux connaissances de la recherche et à les transférer. Ces acteurs cherchent à faire progresser leurs propres objectifs et le font sans tenir compte ou sans en faire profiter ceux qui financent et mènent les travaux. Bien que ces activités puissent être réalisées pour divers objectifs économiques, stratégiques, géopolitiques ou militaires, les résultats finaux enfreignent les normes et les valeurs qui constituent les fondements de la recherche internationale, y compris la sécurité et l'intégrité de la recherche.

La sécurité de la recherche - comprend les actions qui protègent nos communautés de la recherche des acteurs et des comportements qui posent des risques économiques, stratégiques et/ou de sécurité nationale et internationale. Il s'agit d'un domaine émergent pour de nombreux chercheurs, institutions et gouvernements. Les gouvernements du G7 reconnaissent que notre approche individuelle et collective de la sécurité de la recherche peut évoluer au fil du temps et que, par conséquent, notre compréhension de ce qui constitue les meilleures pratiques continuera également d'évoluer. Le principe d'adaptabilité doit sous-tendre la mise en œuvre de toute meilleure pratique en matière de sécurité de la recherche, en reconnaissant que les approches peuvent devoir être adaptées pour tenir compte des risques nouveaux et émergents, et être suffisamment proportionnels et flexibles pour maintenir et soutenir l'autonomie des activités de recherche des institutions de recherche et des chercheurs, tout en préservant la qualité de la recherche.

De plus amples informations sur la relation entre l'intégrité de la recherche et les risques pour la sécurité de la recherche figurent à l'annexe B du document du G7 sur les valeurs et principes communs en matière de sécurité et d'intégrité de la recherche.

Qu'est-ce que le « risque » en matière de sécurité de la recherche??

Les gouvernements et les membres de la communauté des chercheurs font souvent référence au « risque » lorsqu'ils discutent de la sécurité de la recherche. Les meilleures pratiques présentées dans ce document sont souvent axées sur l'identification, la compréhension et l'atténuation des risques liés à la sécurité de la recherche, d'où l'importance de définir ce que l'on entend par ce terme.

En ce qui concerne la sécurité de la recherche, les risques peuvent inclure des activités illégales et/ou non transparentes, telles que :

- L'influence indue, l'interférence ou l'appropriation illicite de la recherche, y compris le vol pur et simple d'idées, de résultats de recherche et de la propriété intellectuelle par des États, des armées et leurs mandataires, ainsi que par des acteurs non étatiques et des activités criminelles organisées; et

- D'autres activités et comportements clandestins ayant des répercussions négatives sur les implications économiques, stratégique et au niveau de la sécurité nationale.

Les risques liés à la sécurité de la recherche peuvent provenir aussi bien de l'intérieur que de l'extérieur d'une équipe ou d'une institution de recherche par différents moyens. Les moyens par lesquels les acteurs peuvent influencer, interférer ou détourner la recherche comprennent l'infrastructure (tant numérique que physique), les personnes et le financement. Ces méthodes peuvent être utilisées de manière illicite comme point d'entrée pour l'exploitation, mais il est également possible d'y accéder par des moyens licites ou légaux, mais sans divulgation transparente de l'objectif visé ou de son utilisateur final, ce qui pourrait entraîner des utilisations non intentionnelles ou préjudiciables de la recherche. Les domaines de risque suivants doivent être pris en compte et évalués lors de l'élaboration d'un projet de recherche. L'application de la diligence raisonnable en matière de la sécurité de la recherche représente un élément supplémentaire dans la planification et l'évaluation d'ensemble lesquels sont nécessaires à la structuration d'un projet de recherche.

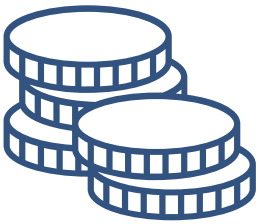
Infrastructure (numérique et physique)

- Les cybermenaces peuvent prendre la forme de cyberattaques (telles que l'hameçonnage ou les rançongiciels) qui exploitent des vulnérabilités pour accéder aux données ou aux résultats de la recherche.
- L'accès physique peut être utilisé pour acquérir des données ou des résultats de recherche dans les installations où la recherche est menée.

Personnes

- Des personnes extérieures à une équipe ou d'une institution de recherche peuvent chercher à s'associer à des chercheurs pour atteindre leurs objectifs ou pour obtenir des avantages non divulgués, ce qui a des répercussions en matière de sécurité.
- Des personnes au sein d'une équipe ou d'une institution de recherche, qui ont un accès direct ou indirect à des connaissances ou à des documents exclusifs, pourraient être motivées, soutenues ou poussées par d'autres à accéder à la recherche ou à la voler à leur profit ou au profit d'autres personnes. De mauvaises pratiques d'hygiène en matière de sécurité pourraient faciliter cet accès par d'autres personnes.

Financement



- Le financement pourrait être utilisé comme une incitation à accéder ou à transférer des données, des processus et des résultats de la recherche, potentiellement sans divulgation transparente de l'objectif visé ou de l'utilisateur final.

Lorsque nous parlons de « risque » dans les meilleures pratiques ci-dessous en matière de sécurité et d'intégrité de la recherche, nous faisons référence aux risques susmentionnés. Bien que les pratiques individuelles puissent évoluer, ces catégories de risques – et les meilleures pratiques qui y correspondent – sont délibérément larges, pour pouvoir tenir compte de l'évolution de ces risques.

Meilleures pratiques du G7 en matière de sécurité et d'intégrité de la recherche

Aucune partie prenante ne détient à elle seule l'entière responsabilité de la protection de la recherche. Il s'agit d'une responsabilité partagée entre toutes les parties prenantes. C'est pourquoi le présent document est structuré en fonction des meilleures pratiques et des parties prenantes concernées par ces pratiques. La collaboration avec les membres de la communauté des chercheurs est essentielle pour assurer que les risques sont atténués de manière proportionnelle, rapidement et de façon coordonnée. En travaillant collectivement, les parties prenantes peuvent renforcer la communauté de la recherche dans son ensemble contre les risques liés à la sécurité de la recherche.

La liste suivante des meilleures pratiques a été formulée par les membres du G7, à partir d'initiatives et de programmes existants.

Nombre de ces pratiques conviennent à l'ensemble de la communauté de la recherche – **gouvernements, organisme de financement de la recherche** (y compris les organismes de financement privés, publics et gouvernementaux), **institutions de recherche** (y compris les associations qui les représentent, ainsi que les institutions de recherche gérées par le gouvernement) et **chercheurs**.

Étant donné que le contexte et la structure de l'écosystème de recherche varient d'un pays du G7 à l'autre, les meilleures pratiques peuvent être mises en œuvre différemment par chaque membre pour répondre aux besoins de leur communauté de recherche.

Aucune partie prenante ne détient à elle seule l'entière responsabilité de la protection de la recherche. Il s'agit d'une ***responsabilité partagée*** *entre toutes les parties prenantes.*

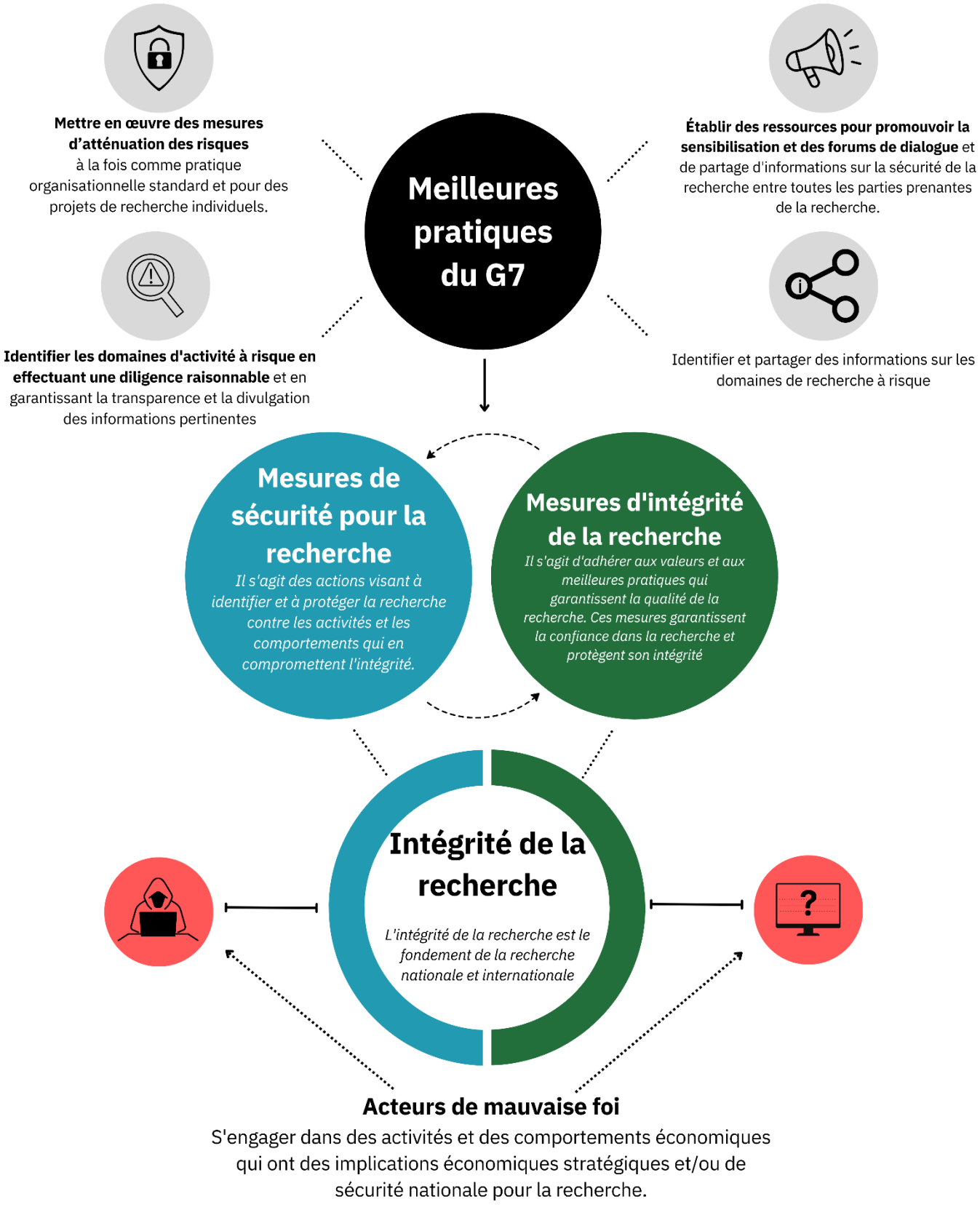


Figure 1: *Graphique illustrant la manière dont les meilleures pratiques du G7 soutiennent à la fois la sécurité et l'intégrité de la recherche.*

1. Mettre en place des ressources pour promouvoir la sensibilisation et des forums de dialogue et de partage d'informations sur la sécurité et l'intégrité de la recherche entre toutes les parties prenantes de la recherche.

La sécurité de la recherche est un nouveau domaine de préoccupation en matière de sécurité nationale et peut constituer un nouveau domaine de risque pour de nombreuses personnes et institutions. Un dialogue continu entre les parties prenantes de la communauté de la recherche, tant au niveau bilatéral que multilatéral, est important pour maintenir un partage d'informations actif et régulier et pour accroître la sensibilisation. Le partage d'informations peut se faire par la mise à disposition de ressources (bases de données en ligne, formation, etc.) et par la création d'équipes ou de groupes de travail chargés d'examiner les besoins actuels et futurs de la communauté de la recherche, sur la base d'une compréhension de la conduite générale de la recherche.

Toutes les parties prenantes, y compris les gouvernements, les organismes de financement de la recherche, les institutions de recherche et les chercheurs doivent éviter de cibler des personnes ou des communautés spécifiques lorsqu'ils mènent des activités de sensibilisation ou abordent la question des risques pour la sécurité. Le choix de la terminologie et du vocabulaire utilisés lors de ces dialogues doivent garantir l'absence de discrimination, de harcèlement et de coercition, ce qui est fondamental pour le succès de la recherche.

Les gouvernements : La mise en place de forums de dialogue et d'échange d'informations entre un gouvernement et les différentes parties prenantes de la communauté scientifique peut aider tous les partenaires à mieux comprendre l'environnement de la recherche et ses risques pour la sécurité. Ces dialogues peuvent avoir de nombreux objectifs, notamment le partage d'informations sur les risques actuels et émergents, l'identification des besoins de la communauté de la recherche pour le développement de ressources et le soutien aux politiques relatives à la sécurité et à l'intégrité de la recherche. Par exemple, un gouvernement peut être en mesure de partager des renseignements non classifiées pour informer les organismes de financement, les institutions et les chercheurs de nouveaux risques ou de nouvelles pratiques. De même, les informations peuvent provenir de la communauté de la recherche pour les gouvernements afin que ces derniers aient une connaissance suffisante de la culture et des processus de la recherche pour élaborer des renseignements et des politiques sur les risques qui sont appropriés au domaine de la recherche.

Les gouvernements peuvent également envisager de créer une ressource centrale permettant aux membres de la communauté de la recherche d'obtenir des renseignements et accroître la sensibilisation. Cette ressource centrale pourrait

contenir des renseignements à jour sur les risques actuels et en évolution, et constituer une source d'informations sur les ressources susceptibles de contribuer à la mise en œuvre de certaines des meilleures pratiques identifiées dans ce document.

Les organismes de financement de la recherche : Les organismes de financement de la recherche peuvent entretenir des relations régulières avec les organismes gouvernementaux responsables de définir les attentes en matière de financement et de programmes de recherche, lesquels participent à l'élaboration de politiques plus larges liées à la sécurité et à l'intégrité de la recherche. De même, l'engagement des organismes de financement de la recherche auprès des institutions de recherche et des chercheurs est essentiel pour comprendre les questions émergentes et les besoins non satisfaits. Les organismes de financement de la recherche peuvent également contribuer à la diffusion et à la promotion des ressources afin d'accroître la sensibilisation.

Institutions de recherche : Les institutions de recherche jouent un rôle essentiel dans l'identification des besoins des chercheurs. En établissant un dialogue actif avec les chercheurs d'une institution, des outils et des ressources peuvent être développés pour combler les lacunes dans la compréhension des risques et fournir des informations pertinentes et actualisées sur l'environnement actuel des risques, s'adaptant aux contextes et aux processus organisationnels spécifiques. Les institutions de recherche peuvent former et informer régulièrement leur personnel sur les domaines de risque potentiel et sur la manière de les atténuer, afin de s'assurer qu'ils restent au fait des menaces existantes. Ils peuvent diffuser des ressources pour les chercheurs afin d'accroître la sensibilisation aux risques au sein de leur communauté de recherche.

Politiques en action

En 2019, le Royaume-Uni a lancé la campagne Recherche digne de confiance (*Trusted Research*) afin d'améliorer la connaissance du secteur de la recherche et de l'innovation britannique en matière de sécurité de la recherche. Cette campagne s'inscrit dans le contexte d'une collaboration et d'une ouverture croissantes sur le monde extérieur au sein du monde universitaire britannique.

Les chercheurs : En s'engageant dans une sensibilisation et un partage d'informations efficaces, les chercheurs peuvent être en mesure de protéger leur recherche et, ce faisant, l'intégrité de leurs écosystèmes de recherche nationaux et internationaux. Les chercheurs ont également un rôle à jouer en contribuant aux dialogues à tous les niveaux pour s'assurer que leurs besoins sont bien formulés et compris, afin qu'ils puissent être pris en compte par les gouvernements, les organismes de financement de la recherche et les institutions de recherche.

2. Identifier et partager les renseignements sur les domaines de recherche à risque.

Outre le partage régulier d'informations sur la sécurité et l'intégrité de la recherche en général, il est important de fournir des informations ciblées sur les risques, c'est-à-dire d'identifier les domaines de recherche les plus susceptibles d'être ciblés et la manière dont ils le sont. L'identification des domaines de recherche les plus à risque favorise une approche de la sécurité de la recherche proportionnelle au risque, tout en continuant à soutenir la collaboration internationale et la science ouverte, mais en reconnaissant que certains domaines de recherche justifient un niveau de sécurité plus élevé que ceux qui présentent un risque moindre. Les domaines de recherche qui sont les plus susceptibles de présenter risques pour la sécurité et l'intégrité devraient être régulièrement réexaminés et mis à jour afin de rester pertinents et de répondre à l'évolution de la science et de l'environnement des risques.

Les gouvernements : Les gouvernements doivent travailler en collaboration avec les organismes de financement, les institutions et les chercheurs pour s'assurer que l'identification des domaines à risque est exacte et répond aux besoins du secteur de la recherche. Les gouvernements ont un rôle à jouer en aidant la communauté de la recherche de leur pays à comprendre les risques dans certains domaines, notamment en fournissant des informations sur les domaines à risque tels que :

- Les domaines ayant un lien évident avec le développement des capacités militaires ou de renseignement ;
- Les domaines à double usage, en ce sens qu'ils ont des applications militaires/de renseignement et civiles ;
- Les domaines qui peuvent avoir des retombées économiques importantes ;
- Les domaines avec un accès potentiel à des données personnelles sensibles ou à de grands ensembles de données qui peuvent être sensibles dans leur forme agrégée ;
- Les domaines des infrastructures critiques, y compris les processus, systèmes, installations, technologies, réseaux, biens et services essentiels à la santé, à la sécurité ou au bien-être économique des citoyens d'un pays et au bon fonctionnement du gouvernement ; et
- Les domaines qui relèvent des intérêts économiques et/ou stratégiques nationaux prioritaires.

Les organismes de financement de la recherche : Les organismes de financement de la recherche devraient mettre en œuvre les exigences en matière de sécurité et d'intégrité de la recherche de manière ciblée, en se concentrant sur les domaines de recherche présentant le risque le plus élevé. Les organismes de financement doivent également établir un dialogue avec les chercheurs pour s'assurer qu'ils ont une compréhension complète d'un projet et des risques potentiels.

Institutions de recherche : Les institutions de recherche devraient savoir quelles activités de recherche sont menées dans leurs propres installations dans les

domaines de recherche que le gouvernement considère comme sensibles. Ils peuvent à leur tour aider les chercheurs à déterminer si leurs recherches présentent un risque plus élevé et leur apporter leur soutien par le biais d'un partage d'informations.

Les chercheurs : Les chercheurs sont les mieux placés pour connaître leurs propres recherches et l'environnement dans lequel elles sont menées. Les chercheurs doivent réfléchir à la manière dont leur travail pourrait être détourné et utilisé à mauvais escient, suivre les orientations gouvernementales existantes pour déterminer si leur recherche peut être considérée comme sensible, et utiliser tous les outils fournis par les gouvernements, les organismes de financement ou les institutions de recherche pour faire preuve de diligence raisonnable sur leur recherche.

Politiques en action

En juin 2023, le Département de la défense (*Department of Defense*) des États-Unis a lancé une politique à l'échelle du Département pour l'évaluation des projets de recherche fondamentale afin d'identifier les conflits d'intérêts provenant d'une influence étrangère. Le Département appliquera ces politiques pour faire une évaluation basée sur les risques de sécurité des propositions pour les projets de recherche fondamentale afin d'atténuer les risques potentiels pour la sécurité de la recherche.

3. Identifier les domaines d'activité à risque en faisant preuve de diligence raisonnable et en assurant la transparence et la divulgation des informations pertinentes.

Les risques peuvent provenir de diverses sources et il est essentiel de déterminer d'où les menaces sont le plus susceptibles de provenir afin d'élaborer des mesures d'atténuation des risques en réponse à ces menaces. En définissant les principaux facteurs de risque, d'autres bonnes pratiques, telles que la mise en œuvre de mesures d'atténuation des risques, peuvent être mieux appliquées.

Les gouvernements : En collaboration avec leurs communautés de recherche respectives, les gouvernements devraient prendre la responsabilité d'élaborer des cadres politiques qui définissent les exigences de diligence raisonnable et de transparence pour les organisme de financement de la recherche, les institutions et les chercheurs. Ces cadres devraient équilibrer les intérêts nationaux et mondiaux, en promouvant la recherche, la science et l'innovation tout en mettant en place des mesures de protection de la recherche contre les risques identifiés.

Les gouvernements et les agences de la sécurité nationale doivent également fournir des conseils aux institutions de recherche et aux chercheurs sur les risques les plus récents pour la communauté de la recherche, en évaluant régulièrement l'environnement de la menace pour s'assurer que la communauté de la recherche puisse identifier les risques et que les cadres soient cohérents dans la protection de la recherche. Grâce à une évaluation régulière, les cadres politiques peuvent être revus afin de déterminer s'ils répondent toujours aux besoins de la communauté de la recherche et aux objectifs de sécurité et d'intégrité de la recherche. Les gouvernements ont une meilleure connaissance des tendances en matière de risque et peuvent partager ces informations pour faciliter l'identification des risques lorsque cela est possible. En outre, les gouvernements doivent veiller à ce que tout cadre politique mis en place n'ait pas de conséquences négatives involontaires, afin de préserver les libertés académiques et d'éviter la discrimination et le harcèlement.

Les organismes de financement de la recherche : Les organismes de financement de la recherche sont responsables de la mise en œuvre des cadres politiques établis par les gouvernements pour atteindre l'objectif d'identification, d'évaluation et d'atténuation des domaines de risque dans les projets de recherche. Les demandes de financement doivent démontrer de manière transparente les activités réalisées pour faire preuve de diligence raisonnable afin d'identifier les risques et de divulguer les risques potentiels pertinents. Pour faciliter cette identification, les organismes de financement devraient utiliser les orientations et les approches établies par les gouvernements ou leurs propres orientations et approches pour que les demandeurs divulguent et identifient les risques. Ces approches devraient permettre aux chercheurs de démontrer facilement et de manière transparente leur divulgation et leur évaluation des risques. Lors de l'examen des

demandes, les organismes de financement ont la responsabilité d'évaluer les risques en fonction du mérite scientifique et des bénéfices de la proposition.

Cela peut inclure, par exemple, l'évaluation de tout partenaire d'un projet ou la divulgation de tout conflit d'intérêts ou d'affiliations. Les gouvernements étrangers, les armées, leurs mandataires et d'autres organisations peuvent chercher à faciliter le transfert non autorisé de connaissances en recourant à des partenariats, à des chercheurs ou à des membres de la communauté de la recherche pour accéder à des informations de recherche (par exemple, des données), à des connaissances de recherche, ainsi qu'à la propriété intellectuelle et à la technologie qui en résultent. Pour réduire ces risques, les organismes de financement doivent savoir qui est impliqué dans un projet de recherche et quelles sont leurs associations. Des personnes pourraient être sciemment ou non cooptées ou contraintes de faciliter un transfert de connaissances non désiré d'une manière qui pourrait nuire à la sécurité nationale.

Les organismes de financement pourraient envisager d'exiger la transparence et la divulgation des informations relatives aux conflits d'intérêts potentiels et de les uniformiser en les incluant dans les formulaires de demande de financement. Il peut s'agir de la divulgation d'informations relatives aux personnes participant à un projet (affiliations à des organisations, nominations, activités de conseil rémunérées) ou à d'autres sources de financement de la recherche (contributions en nature, en personnel ou en espèces), y compris de la part de gouvernements étrangers.

Afin de garantir le maintien du principe de la protection de la liberté de la recherche et d'éviter la discrimination et le harcèlement, les organismes de financement de la recherche doivent surveiller tout impact négatif involontaire dans la mise en œuvre des programmes de sécurité et d'intégrité de la recherche, et prendre des mesures pour assurer que la discrimination et le harcèlement ne sont pas acceptés dans le cadre de leurs programmes de financement de la recherche.

Institutions de recherche : Les institutions de recherche peuvent mettre en place des mesures pour aider leurs chercheurs à identifier et à évaluer les risques, et à assurer la transparence dans la divulgation des informations. Les institutions de recherche peuvent envisager de désigner un responsable au niveau de la haute direction pour prendre en charge les questions relatives à la sécurité et à l'intégrité de la recherche et contribuer à garantir une approche uniforme. Les risques liés à la sécurité de la recherche pourraient, par exemple, être intégrés dans le cadre ou le registre des risques d'une organisation, ou dans le cadre institutionnel sur l'intégrité de la recherche. Les risques pour la réputation, l'éthique et la sécurité nationale liés aux projets de recherche doivent faire l'objet de discussions régulières au niveau de la direction afin de permettre aux institutions de répondre et de s'adapter rapidement aux nouvelles préoccupations. Les institutions de recherche doivent s'assurer que les personnes chargées de prendre des décisions en matière de gestion des risques comprennent clairement l'étendue de leurs responsabilités et disposent d'un soutien approprié pour identifier les cas où il convient d'envisager la transmission de décisions à un échelon supérieur.

En outre, les institutions devraient être responsables de l'identification et de l'évaluation des risques institutionnels, qui peuvent s'appliquer à plusieurs projets ou disciplines de recherche. Par exemple, l'identification des risques liés à l'infrastructure – tant physique que numérique – relèverait généralement de la responsabilité de l'institution, les contrôles d'accès physique et les contrôles de cybersécurité étant souvent mis en place au niveau de l'institution, plutôt que par des chercheurs de manière individuelle pour des projets spécifiques. De plus, les institutions devraient revoir la formulation des ententes de recherche afin de s'assurer que les résultats sont documentés de manière transparente et favorables à toutes les parties.

Afin de maintenir le principe de liberté de la recherche et d'éviter la discrimination et le harcèlement, les institutions de recherche devraient surveiller tout impact négatif de la mise en œuvre des initiatives en matière de sécurité et d'intégrité de la recherche et faire part de leurs constatations aux organismes de financement de la recherche ou aux gouvernements afin que ces situations puissent être corrigées immédiatement.

Politiques en action

En juillet 2021, le gouvernement du Canada a publié les Lignes directrices sur la sécurité nationale dans les partenariats de recherche (Lignes directrices) afin d'intégrer les considérations de sécurité nationale dans le processus d'établissement, d'évaluation et de financement des partenariats de recherche. Les demandeurs qui présentent une demande aux programmes de financement de la recherche où les Lignes directrices s'appliquent doivent fournir un Formulaire d'évaluation des risques, y compris un plan d'atténuation des risques.

Les chercheurs : Comme indiqué précédemment, ce sont les chercheurs qui connaissent le mieux leur domaine de recherche et le travail qu'ils effectuent. Par conséquent, ils sont souvent les mieux placés pour identifier les domaines d'activité à risque potentiel, notamment en ce qui concerne les partenariats et les personnes, avec l'appui des renseignements sur les risques fournis par les gouvernements et d'autres sources crédibles. Pour faciliter l'identification des risques, les chercheurs doivent également s'engager à identifier, à évaluer et à atténuer les risques potentiels pour l'intégrité et la sécurité de leur recherche. Cela inclut la divulgation appropriée d'informations à leurs institutions et à leur(s) organisme(s) de financement de recherche, qui peuvent être au fait de tendances émergentes plus larges en matière de risques, lesquelles peuvent ne pas être immédiatement évidentes pour un chercheur. Cela permet aux chercheurs de demeurer au fait du contexte général des risques ou de leur évolution.

Comprendre les motivations et les intérêts des partenaires et des membres de l'équipe peut aider à identifier les domaines de risque potentielles. En faisant preuve de diligence raisonnable, on peut identifier des indicateurs de risque qui suggèrent que l'autonomie d'un individu peut être compromise; des indications de relations avec

des gouvernements étrangers, des services militaires ou de sécurité sur des domaines de recherche sensible; des informations montrant que votre partenaire opère dans des pays connus pour accéder à la propriété intellectuelle des chercheurs et/ou la voler; ou toute information suggérant un manque de transparence.

En apprenant à mieux connaître les personnes impliquées dans un projet et en comprenant leurs motivations et leurs objectifs, il sera plus facile d'identifier et d'évaluer les risques liés à l'utilisation de la technologie.

4. Mettre en œuvre des mesures d'atténuation des risques, tant dans le cadre de pratiques organisationnelles uniformisées que pour des projets de recherche individuels.

Après avoir identifié la présence d'un risque et son ampleur, les membres de la communauté scientifique sont généralement mieux placés pour y remédier et en atténuer les effets. L'atténuation des risques vise à réduire la probabilité et l'impact des risques à un niveau acceptable pour le chercheur, son institution, l'organisme de financement de la recherche et le gouvernement concerné. Les mesures d'atténuation des risques peuvent être mises en œuvre au niveau de l'organisation, en créant des normes qui doivent être respectées, et au niveau d'un projet spécifique, où une approche plus adaptée de l'atténuation des risques peut être appropriée pour les projets présentant des caractéristiques uniques susceptibles d'élever leur niveau de risque. Les mesures d'atténuation doivent être proportionnelles au niveau de risque afin de garantir une recherche à la fois sécuritaire et ouverte. Les mesures d'atténuation devront peut-être être ajustées au fil du temps en fonction de l'évolution des risques et bénéficieront d'un réexamen périodique pour déterminer si elles répondent toujours de manière appropriée aux risques actuels ou si des changements sont nécessaires pour répondre à de nouvelles préoccupations.

Les parties prenantes, telles que les organismes de financement et les institutions de recherche, peuvent également envisager de mettre en place une gouvernance des risques au niveau de l'organisation et du projet. La mise en place de politiques et de processus organisationnels permettant d'évaluer et d'atténuer les risques associés aux risques organisationnels ainsi qu'aux projets de recherche individuels est indispensable pour assurer une cohérence dans le processus décisionnel.

Les gouvernements : Les gouvernements ont un rôle important à jouer en fournissant des orientation sur l'atténuation des risques. Ils peuvent développer des ressources et des mécanismes de partage d'informations pour aider les autres membres de la communauté de la recherche à appliquer ces bonnes pratiques.

Les organismes de financement de la recherche : Les organismes de financement de la recherche pourraient envisager de mettre en œuvre des exigences spécifiques portant sur la sécurité et l'intégrité de la recherche dans leur processus de demande de financement. Ils pourraient aussi envisager d'établir des politiques ou des conditions selon lesquelles le financement exige que certaines mesures atténuation des risques soient obligatoires. Les organismes de financement pourraient envisager d'encourager ou d'exiger des candidats qu'ils veillent à ce que les participants à un programme spécifique répondent à certaines exigences de formation concernant la sécurisation de leur recherche, qu'ils disposent de plans de cybersécurité et de mesures de contrôle pour la gestion des données, conformément aux meilleures pratiques existantes et en cours d'évolution de la communauté de la recherche. En outre, du fait qu'ils reçoivent les propositions de recherche présentées par les candidats, les organismes de financement de la recherche sont probablement en mesure d'identifier et de développer les meilleures pratiques générales en matière

d'atténuation des risques. À leur tour, ils peuvent diffuser des orientations sur les mesures d'atténuation des risques à l'ensemble de la communauté de la recherche (en collaboration avec les gouvernements).

Institutions de recherche : Les institutions de recherche peuvent envisager de mettre en œuvre diverses mesures pour se protéger et protéger leurs chercheurs. Par exemple, les Institutions peuvent envisager de recourir à des pratiques appropriées de cybersécurité, des contrôles d'accès physiques, de veiller au respect des obligations juridiques pertinentes de leur pays et de mettre en place des mesures de protection de la propriété intellectuelle.

Pour encourager des pratiques rigoureuses en matière de sécurité et d'intégrité de la recherche, une institution de recherche peut également établir un code de conduite sur la sécurité et l'intégrité de la recherche à l'intention de ses chercheurs. Un code de conduite peut identifier des normes générales pour les chercheurs au sein de l'institution. Il peut également définir les attentes quant à la manière dont les chercheurs doivent réagir lorsqu'ils sont confrontés à des cas d'accès non autorisé, d'interférence malveillante ou de coercition. La mise en place de politiques et de procédures appropriées permettant au personnel de signaler des problèmes ou des préoccupations et favorisera le partage d'informations et l'identification et l'atténuation des risques.

Politiques en action

Plus de 120 institutions de recherche, organisations et sociétés professionnelles en Allemagne ont mis en place des Comités d'éthique pour la recherche en lien à la sécurité (*Committees for Ethics in Security-Relevant Research*) locaux pour fournir des conseils aux chercheurs et aux institutions de recherche sur les aspects liés à la sécurité de leurs recherches. Ces Comités ont été créés sur la base des Recommandations pour le fonctionnement de la recherche en lien à la sécurité (*Recommendations for Handling of Security-Relevant Research*) présentées en 2014 par l'Académie nationale allemande des sciences Leopoldina (*German National Academy of Science Leopoldina*) et la Fondation pour la recherche allemande (*German Research Foundation*), et mises à jour en 2022.

Les institutions peuvent également envisager d'offrir une formation sur les normes pour les bonnes pratiques en matière de cybersécurité et de sécurité physique. Si le personnel voyage ou partage des renseignements au niveau international, il doit être informé, formé et équipé pour savoir comment assurer leur propre sécurité et celle de leurs renseignements sensibles.

Les chercheurs : Pour mettre en œuvre des mesures d'atténuation des risques, les chercheurs peuvent élaborer des plans d'atténuation des risques comportant des étapes claires pour réduire des risques. Idéalement, les plans d'atténuation des risques devraient être élaborés avec le soutien de l'institution et/ou de l'organisme de financement du chercheur afin de gérer les risques identifiés lors d'un examen

préalable des domaines de préoccupation potentiels. La stratégie d'atténuation des risques choisie par le chercheur doit équilibrer les avantages et les risques et ne pas entraver sa capacité à collaborer, à attirer des talents internationaux ou à obtenir un financement durable. Les plans d'atténuation des risques doivent être aussi précis que possible et leur contenu peut varier en fonction des types de risques identifiés.

Ces mesures d'atténuation des risques peuvent être intégrées aux pratiques d'hygiène de la recherche existantes, avec des mesures et des procédures documentées et communes à tous les membres d'un projet de recherche, et mises en œuvre et surveillées pour s'assurer qu'elles sont respectées. Les membres doivent se familiariser avec les contrôles mis en place. Des procédures de formation et d'intégration doivent être mises en place pour s'assurer que les risques sont gérés de manière appropriée, tant au début que pour toute la durée du projet. Ces pratiques en matière de sécurité et d'intégrité de la recherche sont plus efficaces lorsqu'elles sont intégrées dans les pratiques générales de la recherche.

Conclusion

La recherche ouverte et collaborative nous permet de répondre à certaines des questions les plus difficiles au monde. L'intégrité de la recherche est la base à partir de laquelle les chercheurs peuvent opérer dans notre environnement de recherche mondial. Pour soutenir l'intégrité de la recherche, les meilleures pratiques ci-dessus ont pour but d'aider les communautés de la recherche à mettre en place et à améliorer les processus et les efforts visant à protéger leurs recherches respectives et à permettre le fonctionnement et la poursuite d'un système collaboratif de la recherche fondé sur la confiance réciproque. Ces pratiques ont été élaborées pour soutenir la recherche en respectant de nombreux principes clés de l'intégrité de la recherche, tels que la liberté académique, la science ouverte, la transparence, la divulgation et l'honnêteté, l'absence de discrimination, de harcèlement et de coercition, le renforcement de la confiance du public et l'autonomie institutionnelle.

La sécurité de la recherche reste un domaine émergent pour les communautés de la recherche dans le monde entier et c'est donc un concept qui continuera d'évoluer au fil du temps. Ces pratiques doivent continuer à être adaptées pour faire face aux risques nouveaux et émergents afin que les mesures prises soient proportionnelles et appropriées.

Annexe A – Valeurs communes en matière d'intégrité de la recherche

Liberté académique : La liberté d'enseigner, de mener et de publier des recherches dans un environnement universitaire où l'accent est mis sur la participation de tous est un principe fondamental de la recherche. Elle fait partie intégrante du mandat des institutions de recherche, qui est de poursuivre la vérité, d'éduquer les étudiants et de diffuser la connaissance et la compréhension. La liberté académique exige un environnement où les chercheurs bénéficient d'une autonomie et d'une sécurité d'emploi, et sont libres de toute influence extérieure indue ou de toute limitation à la recherche académique

Absence de discrimination, de harcèlement et de coercition : L'absence de discrimination, de harcèlement et de coercition est une valeur fondamentale pour le succès de la recherche. Tous les membres de la communauté de la recherche doivent être à l'abri de la discrimination, du harcèlement, de l'intimidation, de la coercition ou des menaces pour leur sécurité personnelle ou celle de leur famille. La discrimination, le harcèlement et la coercition peuvent être le fait d'un individu, d'un groupe, d'une institution ou d'un gouvernement. Il s'agit notamment de cas où des entités peuvent contraindre et harceler des individus pour qu'ils agissent de manière contraire à l'éthique et malhonnête – contre leur volonté ou leur intérêt – afin de soutenir les objectifs, les intérêts et les instructions d'une entité.

Équité, diversité et inclusion : L'équité, la diversité et l'inclusion (EDI) consistent à promouvoir activement les principes d'accès, de diversité et de non-discrimination dans toutes les activités de recherche, y compris les processus de recrutement et les perspectives de carrière. Ces principes sont nécessaires pour tous les aspects de la recherche. L'EDI contribue à la diversité des identités et de la pensée, en laissant place à une variété d'idées, de cultures et de points de vue. Veiller à ce que chacun puisse participer librement à la communauté de la recherche, à l'écosystème ou à l'entreprise permettra de contribuer à la construction d'un monde innovant, prospère et inclusif.

Autonomie institutionnelle : Les institutions de recherche ne peuvent remplir leurs missions envers les étudiants, le corps enseignant, le personnel et la société que si elles sont libres de poursuivre et de diffuser des connaissances fondées sur des preuves, des données et une évaluation par les pairs. Les institutions doivent être libres de poursuivre leurs propres missions. Ces missions peuvent être basées sur la supervision et l'orientation de leur gouvernance, ou peuvent être destinées à répondre aux besoins de la communauté et aux besoins locaux. Quoi qu'il en soit, l'autonomie institutionnelle nécessite un environnement sûr et sécuritaire dans lequel tous les individus et les institutions sont libres et protégés de toute influence extérieure indésirable.

Science ouverte et accès à la recherche : Tous les membres de la communauté de la recherche devraient soutenir activement le partage et l'échange des résultats, des

données, des méthodes et des apports de la recherche, tout en préservant les mesures d'incitation à l'innovation. La science ouverte – qui consiste à mettre à la disposition de tous, avec un minimum de restrictions, les apports, les résultats et les processus de la science et de la recherche – doit être pratiquée dans le plein respect de la vie privée, de la sécurité et des considérations éthiques, ainsi que de la protection appropriée des idées, des résultats de la recherche et de la propriété intellectuelle. En permettant à tous les membres de la société de s'appuyer sur des recherches déjà validées, la science ouverte contribue à accélérer le rythme des nouvelles découvertes, à améliorer la vie des autres et de nos sociétés et à contribuer à la qualité de la recherche.

Favoriser la confiance du public : Mener et poursuivre des recherches en préservant la confiance du public et de toutes les personnes impliquées dans la recherche est essentiel pour que les efforts en matière de science et de recherche continuent d'être couronnés de succès. En tant que contributeurs à l'intégrité, toutes les parties engagées dans des activités scientifiques et de recherche doivent s'efforcer de démontrer qu'elles peuvent répondre aux attentes en matière de confiance lorsqu'elles accèdent à des données ou à des travaux de recherche sensible. Pour ce faire, tous les partenaires doivent avoir une compréhension commune, claire et délibérée de l'objectif, de l'utilisation et de la propriété des résultats de la recherche. Cette compréhension doit être maintenue et respectée à tous les stades de la recherche et dans toutes les juridictions.

Maintenir la confiance du public nécessite également une bonne intendance, ce qui implique une surveillance et une gestion adéquates à tous les niveaux. Les gouvernements et les organismes de financement ont des responsabilités de gestion en ce qui concerne leurs décisions et leurs relations avec les institutions postsecondaires et les institutions de recherche. Les institutions postsecondaires et les institutions de recherche ont des responsabilités de gestion dans leurs relations avec leurs employés et leurs étudiants, ainsi que dans leurs communications avec leurs bailleurs de fonds.

Transparence, divulgation et honnêteté : Le partage totalement transparent et réciproque des méthodes, des données et des résultats de la recherche non classifiée – tout en maintenant la confidentialité le cas échéant – est essentiel à la collaboration en matière de recherche, à l'intégrité et à la libre circulation des idées et des renseignements. La transparence dans la divulgation des affiliations des chercheurs, des intérêts concurrents ou conflictuels et des sources de financement est également importante pour garantir l'intégrité de la recherche en cours. La transparence exige de l'honnêteté. En tant que valeur complémentaire, l'honnêteté implique d'être franc et exempt de fraude et de supercherie lors de la proposition, de l'élaboration, de la réalisation, de l'évaluation, de l'établissement de rapports et de la communication des travaux de recherche. Elle s'étend à tous les aspects de la recherche et comprend la reconnaissance du travail d'autrui et la formulation d'affirmations justifiables ou d'interprétations sensées sur la base des résultats de la recherche.

Annexe B – Principes du G7 sur la sécurité de la recherche

Équilibrer les intérêts nationaux et mondiaux : Le financement des partenariats scientifiques et de recherche doit continuer à être guidé principalement par l'évaluation de la valeur scientifique et de l'excellence, et prendre en considération et atténuer de manière appropriée et proportionnelle les risques pour la sécurité nationale et/ou économique, le cas échéant.

Maintenir l'ouverture et la sécurité de la recherche : La science ouverte ne doit pas être un choix après coup et les gouvernements doivent s'engager à rendre la recherche accessible lorsque rien ne justifie qu'elle reste fermée. Il est reconnu que l'ouverture doit avoir des limites et ne peut pas passer outre l'obligation de maintenir des protections sur la recherche dont la diffusion pourrait avoir des implications éthiques, géopolitiques ou de sécurité nationale négatives.

Collaboration et dialogue : Toutes les parties impliquées dans la recherche doivent s'efforcer de se soutenir et de collaborer les unes avec les autres afin de créer une communauté qui allie sécurité et ouverture. Les gouvernements devraient s'engager à partager des informations pertinentes sur la nature des risques, dans le but de gérer les risques communs avec les chercheurs et de bénéficier d'approches communes.

Efforts proactifs : Les gouvernements doivent s'efforcer de prendre des mesures proactives et de prévention pour gérer et réduire les risques liés à la sécurité et à l'intégrité de la recherche en s'appuyant sur les leçons apprises et les meilleures pratiques.

Proportionnalité des risques : La gestion des risques doit être proportionnelle et adéquatement modulée. Les réponses appropriées au risque en matière de sécurité de la recherche doivent tenir compte, entre autres, des possibilités d'utilisation abusive de la recherche et du niveau global de risque.

Responsabilités partagées : Pour gérer les risques dynamiques et changeants liés à la recherche, tous les membres de la communauté des chercheurs doivent reconnaître et comprendre leurs rôles et responsabilités distincts en ce qui concerne le traitement et la gestion des risques pour la sécurité et l'intégrité de la recherche.

Imputabilité et responsabilité : Les individus et les organisations doivent être tenus responsables de toutes leurs actions, y compris lorsque leur comportement s'écarte des normes acceptées.

Adaptabilité : Il convient de s'engager en faveur de mesures de sécurité de la recherche qui sont dynamiques, en reconnaissant que des approches trop rigides risquent de différer des recherches bénéfiques. Les approches statiques et rigides peuvent avoir un effet dissuasif important sur la recherche et ne tiennent pas compte des risques nouveaux et émergents.

Annexe C : Exemples de meilleures pratiques

Commission européenne – Procédures opérationnelles normalisées pour l'intégrité de la recherche (*Standard Operating Procedures for Research Integrity*)

Chacun des exemples sur les Procédures opérationnelles normalisées de l'UE pour l'intégrité de la recherche démontre l'une des meilleures pratiques décrites ci-dessus.

1. Le projet SOPs4RI (*Standard Operating Procedures for Research Integrity*) est un projet comprenant multiple partenaires pour une période de quatre ans (2019-2022) et est financé par la Commission européenne. SOPs4RI vise à encourager les processus de transformation au sein des organismes de recherche (OR) et des organismes de financement de la recherche (OFR) européens.

2. SOPs4RI offrira une boîte à outils en ligne, accessible gratuitement et facile à utiliser, qui peut aider les OR et les OFR à cultiver l'intégrité de la recherche et à réduire les pratiques préjudiciables. SOPs4RI établira un inventaire de procédures opérationnelles normalisées (PON) et des lignes directrices que les OR et les OFR pourront utiliser lorsqu'ils élaborent des ententes de gouvernance visant à favoriser la mise ne place de solides cultures d'intégrité en matière de recherche.

3. La Commission européenne a constaté que les violations graves de bonnes pratiques de recherche, telles que la falsification, la fabrication et le plagiat (FFP), sont relativement rares puisqu'on estime que de 1 à 2 % des scientifiques adoptent de telles pratiques. En revanche, les violations moins graves, connues sous le nom de Pratiques de recherche douteuses (PRD), telles qu'une mauvaise élaboration de la recherche, une mauvaise méthodologie et de mauvaises analyses, sont beaucoup plus fréquentes. Par conséquent, le développement de guides intuitifs permettant aux chercheurs de mieux structurer leurs recherches fait partie intégrante de l'approche de la Commission européenne visant à garantir un environnement de recherche sain.

4. Des études menées dans différents domaines disciplinaires ont montré qu'il est souvent difficile de reproduire les résultats d'études antérieures. Les comptes rendus partiels, la description inadéquate des méthodes et d'autres pratiques, telle que la PRD, sont souvent considérés comme la cause des difficultés de reproductibilité. Les problèmes de reproductibilité et les environnements de recherche inefficaces peuvent non seulement ralentir la recherche, mais aussi embrouiller le processus et mobiliser les ressources ou distraire ceux, comme les autorités de contrôle, qui travaillent dans d'autres domaines du réseau de recherche. Cette situation peut créer des brèches et des angles morts qui peuvent être exploitées pour compromettre la sécurité de la recherche.

Royaume-Uni – Portail pour la recherche digne de confiance

(1) Mettre en place des ressources pour promouvoir la sensibilisation et des forums de dialogue et de partage d'information sur la sécurité et l'intégrité de la recherche pour toutes les parties prenantes de la recherche.

Le Royaume-Uni possède un secteur de la recherche et de l'innovation florissant qui attire des investissements du monde entier. Plus de la moitié de la recherche britannique repose sur des partenariats internationaux. La campagne Recherche digne de confiance (*Trusted Research*) de l'Autorité nationale de sécurité en matière de protection (*National Protective Security Authority*, NPSA) et du Centre national de cybersécurité (*National Cyber Security Centre*, NCSC) a été lancée en 2019 afin d'améliorer la connaissance du secteur de la recherche et de l'innovation britannique sur la sécurité de la recherche. Cette campagne s'inscrit dans le contexte d'une collaboration et d'une ouverture croissantes sur le monde extérieur au sein du monde universitaire britannique.

Recherche digne de confiance (*Trusted Research*) vise à promouvoir l'intégrité du système de collaboration internationale en matière de recherche, ce qui est essentiel au succès continu du secteur de la recherche et de l'innovation au Royaume-Uni. Cette initiative est particulièrement utile pour les chercheurs dans les domaines de la science, de la technologie, de l'ingénierie et des mathématiques (STIM), des technologies à double usage, des technologies émergentes et des domaines de recherche sensible sur le plan commercial. Les conseils ont été élaborés en consultation avec la communauté des chercheurs et des universités et sont destinés à aider le secteur britannique de la recherche et de l'innovation, qui est un chef de file en la matière, à tirer le meilleur parti de la collaboration scientifique internationale tout en protégeant la propriété intellectuelle, les recherches sensibles et les informations personnelles.

Recherche digne de confiance (*Trusted Research*) :

- Décrit les risques potentiels pour la recherche et l'innovation au Royaume-Uni.
- Aide les chercheurs, les universités britanniques et les partenaires industriels à avoir confiance dans la collaboration internationale et à prendre des décisions éclairées concernant ces risques potentiels.
- Explique comment protéger la recherche et le personnel contre les risques de vol, d'abus ou d'exploitation.

En plus du guide Recherche digne de confiance pour le monde universitaire (*Trusted Research for Academia*), le Royaume-Uni a réalisé les guides Recherches dignes de confiance pour les hauts dirigeants (*Trusted Research for Senior Leaders*) qui présente certaines considérations clés pour les responsables universitaires, et Recherche digne de confiance – Pays et conférences (*Trusted Research Countries & Conferences*) qui fournit des informations sur les menaces et des mesures d'atténuation concrètes à mettre en œuvre lors des voyages à l'étranger, ainsi qu'une liste de contrôle sur la Recherche digne de confiance (*Trusted Research)* que les chercheurs peuvent utiliser dès le début d'une collaboration.

États-Unis – Lutte contre l'influence étrangère indésirable dans la recherche menée par les établissements d'enseignement supérieur et financée par le Département

(2) Identifier et partager des informations sur les domaines de recherche à risque

En juin 2023, le Département de la défense (*Department of Defense*, DoD) des États-Unis a lancé une politique à l'échelle du Département pour l'évaluation des projets de recherche fondamentale afin d'identifier les conflits d'intérêts provenant d'une influence étrangère. Cette politique est accompagnée de deux documents :

- La Matrice décisionnelle pour informer les décisions sur l'atténuation des propositions de recherche fondamentale (*Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions*), et
- Les Listes pour l'année fiscale 2022 publiées en vertu de la section 1286 de la Loi d'autorisation de la défense nationale John S. McCain pour l'année fiscale 2019 (*Fiscal Year 2022 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019)*, telle qu'amendée.
    - Comprend des listes qui identifient les institutions étrangères dont il a été confirmé qu'elles mènent des activités problématiques, et les programmes de talent étranger dont il a été confirmé qu'ils posent une menace pour les intérêts à la sécurité nationale des États-Unis.

Le Département de la défense appliquera ces politiques pour mener une évaluation basée sur les risques de sécurité des propositions de projets de recherche fondamentale afin d'atténuer les risques potentiels pour la sécurité de la recherche. Les objectifs du Département pour l'évaluation basée sur les risques de sécurité pour les propositions de projets de recherche fondamentale sont les suivants :

- Assurer la sécurité de la recherche fondamentale financée par le Département de la défense,
- Veiller à ce que les personnes désignées divulguent pleinement les informations susceptibles de révéler des conflits d'intérêts et des conflits au niveau des engagements potentiels, et
- Transmettre un message clair à ceux qui mènent des recherches fondamentales sur les comportements acceptables et encouragés, ainsi que sur les activités qui peuvent d'entraver l'obtention d'un financement de la recherche du Département de la défense.

Des évaluation basées sur les risques de sécurité seront effectués, au minimum, pour toutes les propositions de projets de recherche fondamentale qui sont retenues pour le financement sur la base du mérite technique.

France – Protection du potentiel scientifique et technique de la nation

(2) Identifier et partager des informations sur les domaines de recherche à risque

Le potentiel scientifique et technique de la nation est constitué de l'ensemble des biens matériels et immatériels propres à l'activité scientifique (fondamentale ou appliquée) et au développement technologique. Les éléments essentiels du potentiel font partie intégrante des intérêts fondamentaux de la nation, tels qu'ils sont définis à l'article 410-1 du code pénal français.

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) vise à protéger les savoirs, les expertises et les technologies les plus « sensibles » des établissements publics et privés (laboratoires de recherches, entreprises, etc.) localisés sur le territoire national, dont le détournement ou la captation pourraient :

- porter atteinte aux intérêts économiques de la nation,
- renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense françaises,
- contribuer à la prolifération des armes de destruction massive et de leurs vecteurs,
- être utilisés à des fins terroristes en France ou à l'étranger.

Ce dispositif est fondé sur l'article 413-7 du code pénal français et s'organise principalement autour de trois textes d'application :

- le décret n° 2011-1425 du 2 novembre 2011,
- l'arrêté du Premier ministre du 3 juillet 2012,
- une circulaire interministérielle datée du 7 novembre 2012.

Concrètement, le PPST offre une protection juridique et administrative aux entités couvertes et permet :

- de contrôler les accès physique et logique de certaines zones, appelées « zones à régime restrictif » (ZRR), en sollicitant l'avis du ministère concerné,
- de protéger juridiquement contre les actes malveillants ayant des conséquences sur l'honorabilité et la compétitivité de l'entité (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information, etc.),
- de bénéficier d'un accompagnement étatique dans une démarche d'élévation du niveau de sécurité de l'entité,
- de constituer une équipe de travail responsable et sensibilisée aux enjeux de protection,
- d'appartenir à une communauté de confiance favorable aux partenariats de recherche et industriels.

La PPST est un dispositif vivant qui s'adapte aux préoccupations contemporaines. Deux décrets, publiés en mars 2022, viennent encore optimiser le traitement des demandes d'accès en ZRR afin de réduire les délais d'instruction des avis relatifs aux demandes d'accès sans compromettre la vigilance nécessaire.

Ainsi, la PPST concourt à la protection des intérêts fondamentaux de la nation, et constitue aussi un outil au service des établissements concernés, pour protéger leurs connaissances, savoirs et savoir-faire sensibles.

Canada – Les lignes directrices sur la sécurité nationale pour les partenariats de recherche

(3) Identifier les domaines d'activité à risque en faisant preuve de diligence raisonnable et en favorisant la transparence et la divulgation des informations pertinentes.

En juillet 2021, le gouvernement du Canada a publié les Lignes directrices sur la sécurité nationale pour les partenariats de recherche (Lignes directrices) afin d'intégrer les considérations de sécurité nationale dans le processus d'établissement, d'évaluation et de financement des partenariats de recherche. Les Lignes directrices ont été élaborées en consultation avec des représentants des universités et permettent à la communauté de la recherche de mener une diligence raisonnable cohérente et ciblée sur les risques pour la sécurité de la recherche.

Les demandeurs aux programmes de financement de la recherche auxquels s'appliquent les Lignes directrices doivent présenter un Formulaire d'évaluation des risques qui comprend un plan d'atténuation des risques. Les demandeurs doivent faire preuve de transparence en évaluant si :

- leur domaine de recherche peut avoir des applications militaires et civiles (c'est-à-dire, s'il est à double usage) ou s'il peut être ciblé par des gouvernements étrangers, des organisations militaires, leurs représentants ou d'autres acteurs pour promouvoir leurs capacités et leurs intérêts de sécurité nationale, et
- le partenaire de recherche proposé pose un risque pour la sécurité nationale.

Les risques pour la sécurité nationale peuvent être définis comme, sans s'y limiter, des circonstances dans lesquelles pourraient survenir des cas potentiels d'interférence étrangère, d'espionnage, de vol de propriété intellectuelle ou de transfert de connaissances non autorisé qui :

- contribuent à l'avancement des capacités militaires, en matière de sécurité et de renseignement d'États ou de groupes qui posent une menace pour le Canada, ou
- perturbent le développement de la recherche et de l'innovation canadiennes, diminuent la résilience des infrastructures essentielles ou compromettent la protection de données sensibles des Canadiens.

Les organismes de financements procèdent à une validation administrative des risques en utilisant des renseignements de source ouverte pour s'assurer de l'exactitude de la demande et partagent les demandes avec les ministères et les agences responsables de sécurité nationale pour une évaluation des risques et des conseils, le cas échéant. Reconnaissant que les risques de sécurité évoluent et peuvent provenir de n'importe où dans le monde, les Lignes directrices ne visent aucun pays ou aucune entreprise en particulier. L'évaluation des risques est effectuée au cas par cas.

Les Lignes directrices visent à garantir que la recherche canadienne est aussi ouverte que possible et aussi sécuritaire que nécessaire. Les Lignes directrices reconnaissent la responsabilité partagée entre les chercheurs, les institutions de recherche, les organismes de financement et le gouvernement afin de faire preuve de diligence raisonnable. Les demandes de partenariat de recherche qui sont évaluées comme présentant un risque inacceptable pour la sécurité nationale ou qui comportent des risques qui ne peuvent pas être atténués de façon appropriée ne sont pas financées.

Japon – Liste de contrôle des nouveaux risques liés à l'internationalisation et à l'ouverture croissantes de la recherche

(3) Identifier les domaines d'activité à risque en faisant preuve de diligence raisonnable et en favorisant la transparence et la divulgation des informations pertinentes.

Depuis quelques années, on s'inquiète de la dégradation des valeurs, telles que l'ouverture et la transparence, qui sont à la base de l'environnement de la recherche, et du danger pour les chercheurs de se retrouver involontairement en situation de conflit d'intérêts et d'engagement en raison des nouveaux risques liés à l'internationalisation et à l'ouverture croissantes des activités de recherche. Dans ces circonstances, les Orientations de politiques visant à garantir l'intégrité de la recherche en réponse aux nouveaux risques associés à l'internationalisation et à l'ouverture croissantes des activités de recherche (*Policy Directions for Ensuring Research Integrity in Response to New Risks Associated with Increasing Internationalization and Openness of Research Activities*) ont été publiées lors du Conseil de promotion de la stratégie d'innovation intégrée (*Integrated Innovation Strategy Promotion Council*) le 27 avril 2021. Elles constituent des mesures gouvernementales visant à garantir l'intégrité de la recherche.

Sur la base des Orientations de politiques, le Bureau du Conseil des ministres (*Cabinet Office*) a créé, en décembre 2021, un modèle de Liste de contrôle pour les chercheurs et un modèle de Liste de contrôle pour les universités et les institutions de recherche, qui peuvent être utilisés pour la formation et à d'autres fins pour sensibiliser les chercheurs, les universités et les institutions de recherche.

Les modèles de Liste de contrôle comprennent des questions qui permettent de gérer les éléments suivants, du point de vue des chercheurs, des universités et des institutions de recherche :

- Les risques, y compris la mauvaise gestion des conflits d'intérêt et d'engagement, les risques entraînant des fuites de technologies et d'informations, et la dégradation de la confiance,
- Les procédures de collaboration et d'accord avec des organisations ou des universités étrangères et l'offre de dédommagements et de biens en provenance de pays étrangers, et
- Les risques liés aux homologues des collaborations et des accords avec des organisations ou des universités étrangères.

Le modèle de Liste de contrôle pour les universités et les institutions de recherche a été révisé en juin 2023, après un incident de violation présumée de la Loi sur la prévention de la concurrence déloyale (*Unfair Competition Prevention Act*).

Les universités et les institutions de recherche sont encouragées à utiliser ces modèles pour créer leur propre liste de contrôle adaptée à leurs exigences et à leur situation spécifiques.

Italie – Programme national de recherche : Plan national pour la science ouverte

(4) Mettre en œuvre des mesures d'atténuation des risques, tant dans le cadre des pratiques organisationnelles courantes que pour les projets de recherche individuels.

En juin 2022, le gouvernement italien a publié le Plan national pour la science ouverte (*Piano Nazionale Scienza Aperta*), un document de référence qui soutient les efforts déployés par la communauté scientifique italienne dans ce domaine au cours des dernières années, notamment :

- Plusieurs universités italiennes rejoignent la Coalition pour l'avancement de l'évaluation de la recherche (*Coalition for Advancing Research Assessment*, CoARA). L'Accord sur la réforme de l'évaluation de la recherche (*Agreement on Reforming Research Assessment*) présente une orientation commune pour l'évolution des pratiques d'évaluation de la recherche, des chercheurs et des organismes de recherche. L'objectif principal est de maximiser la qualité et l'impact de la recherche.
- CoARA – Des groupes de discussion ont été lancés par la conférence permanente des directeurs d'universités italiennes.
- Le Réseau italien de reproductibilité (*Italian Reproducibility Network*) a été lancé au début de 2023. Cette organisation à but non lucratif a pour objectif de promouvoir, soutenir et protéger les pratiques de la science ouverte par le biais d'un certain nombre d'activités de sensibilisation et d'éducation.

Le Plan national pour la science ouverte comprend plusieurs composantes de l'approche de la science ouverte, telles que :

- l'accès gratuit aux articles universitaires,
- des données et des codes accessibles,
- un système d'évaluation des universités italiennes, et
- l'assurance de la sécurité et de l'intégrité de l'écosystème de la recherche.

Le document donne une orientation claire, tout en laissant à la communauté la possibilité de concevoir des systèmes de règles et de mesures d'incitation compatibles avec l'approche. De ce point de vue, le Plan national n'est qu'une première étape. Il reste encore beaucoup à faire pour promouvoir et mettre en œuvre les changements nécessaires pour une communauté de recherche transparente, digne de confiance et équitable.

Allemagne

(4) Mettre en œuvre des mesures d'atténuation des risques, tant dans le cadre des pratiques organisationnelles courantes que pour les projets de recherche individuels.

Plus de 120 institutions de recherche, organisations et sociétés professionnelles en Allemagne ont mis en place des Comités d'éthique pour la recherche en lien à la sécurité (*Committees for Ethics in Security-Relevant Research*, KEF) locaux afin de donner des conseils aux chercheurs et aux institutions de recherche sur les aspects de leur recherche qui touchent à la sécurité. Ces comités ont été créés sur la base des Recommandations pour le traitement de la recherche liée à la sécurité (*Recommendations for Handling of Security-Relevant Research*) présentées en 2014 par l'Académie nationale allemande des sciences Leopoldina (*German National Academy of Science Leopoldina*) et la Fondation pour la recherche allemande (*German Research Foundation*, DFG), et mises à jour en 2022. Ces recommandations visent à accroître la sensibilisation du secteur universitaire et renforcer l'autogestion des enjeux relatifs à la science et à la sécurité de la recherche. Selon ces recommandations, la recherche liée à la sécurité comprend les travaux scientifiques susceptibles de produire des connaissances, des produits ou des technologies pouvant être utilisés par des parties tierces pour porter atteinte à la dignité humaine, à la vie, à la santé, à la liberté, à la propriété, à l'environnement ou à la coexistence pacifique. Ce type de recherche est qualifié de « préoccupante » si sa mauvaise utilisation peut être immédiate et si les dommages potentiels sont importants.

Les KEF sont généralement interdisciplinaires. Ils apportent une expertise pertinente, notamment en matière d'éthique, de droit et de sciences humaines pour évaluer les risques et les avantages des recherches liées à la sécurité. Ils sensibilisent les chercheurs aux aspects de leur travail liés à la sécurité, par exemple en leur offrant des conseils et en organisant régulièrement des événements sur les domaines de recherche présentant un risque de mauvaise utilisation. Ils constituent un instrument important pour renforcer la responsabilité des chercheurs face aux risques d'abus dans leur recherche et pour atténuer ces risques, par exemple par le biais de conseils et du renforcement des compétences. En outre, ils aident à contextualiser les projets de recherche d'un point de vue éthique et contribuent ainsi à une meilleure évaluation des demandes de financement dans les domaines de recherche particulièrement exposés au risque d'abus. De plus, les KEF peuvent légitimer la recherche liée à la sécurité par au moyen d'évaluations éthiques dans le cadre de leurs consultations. En assurant la transparence et en promouvant la réflexion éthique, les KEF contribuent également à renforcer la confiance du public dans la recherche.

La création et le travail des KEF sont soutenus par le Comité conjoint sur le traitement de la recherche liée à la sécurité (*Joint Committee on the Handling of Security-Relevant Research*), un organe consultatif établi par la DFG et la Leopoldina en 2015. Le Comité conjoint organise régulièrement des événements pour promouvoir les échanges entre les KEF, renforcer leurs compétences et les sensibiliser aux domaines de recherche actuels présentant un risque élevé.