GOUVERNEMENT
Liberté
Égalité
Fraternité

anr agence nationale de la recherche

Financé par l'Union européenne
NextGenerationEU

FRANCE 2030

Programme et Équipement Prioritaire de Recherche

« Cybersécurité »

Appel à projets « AAP Cybersécurité »

Date de clôture : 30/09/2022 à 11h00 (heure de Paris).

Adresse de consultation de l'appel à projets : https://anr.fr/PEPR-Cyber-AAP

Résumé

La stratégie nationale d'accélération pour la cybersécurité, qui s'inscrit dans le plan d'investissement France 2030, s'articule autour de quatre axes principaux :

- Développer des solutions souveraines de cybersécurité ;
- Renforcer les liens et les synergies entre acteurs de la filière ;
- Soutenir la demande (individus, entreprises, collectivités et État), notamment en la sensibilisant mieux tout en faisant la promotion des offres nationales ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre.

Le Programme et Équipement Prioritaire de Recherche (PEPR) pour la cybersécurité, sous le pilotage du CEA, du CNRS et d'Inria, a pour vocation de soutenir des activités stratégiques de recherche fondamentale, au plus haut niveau mondial, en support aux industriels de la filière et répondant aux priorités définies dans le cadre de la stratégie nationale.

Cet appel à projets vise à financer des projets de recherche à des niveaux de TRL 1 à 4, destinés à apporter des éléments de connaissance indispensables aux développements des technologies de cybersécurité et favoriser l'émergence de ces outils et solutions avant leur transfert vers le secteur industriel. Il est doté d'un budget de 15 M€ et couvre les trois axes thématiques suivants :

- Protection des données multimédias.
- Recherche et techniques d'exploitation de vulnérabilités.
- Cryptanalyse de primitives cryptographiques.

Un seul projet sera retenu par axe thématique.

Le projet devra impliquer entre 4 et 8 unités de recherche. Un établissement (ou groupe d'établissements, conformément au règlement financier) sera identifié comme établissement coordinateur et un chercheur ou enseignant-chercheur sera identifié comme responsable scientifique du projet. Le responsable scientifique n'est pas nécessairement contractuellement lié à l'établissement coordinateur. Il ne doit pas être le responsable scientifique d'un autre projet du PEPR Cybersécurité ou d'un autre PEPR.

La durée maximale des projets est de 5 ans.

L'aide minimale demandée des projets devra être de 3,5 M€ en regard des objectifs des thématiques.

Mots-clés

Axe 1 : tatouage d'images, de sons et de vidéos (*watermarking*), traçage de traites, détection de manipulations d'informations, hypertrucage (*deepfake*), attaques et protections d'algorithmes de *machine learning* de classification d'images, biométrie et reconnaissance faciale, biométrie comportementale à des fins d'authentification.

Axe 2 : recherche de vulnérabilités et de portes dérobées, développement d'exploits, méthodologies d'attaques, apprentissage machine, automatisation, investigation numérique, analyse forensique, outils et méthodologies d'analyses sur dispositifs physiques.

Axe 3 : cryptanalyse, clef symétrique, clef asymétrique, schéma de signature, algorithme de chiffrement, chiffrement authentifié, mode de chiffrement, fonction de hachage, MAC, factorisation, logarithme discret, courbes algébriques, couplages.

Dates importantes

Clôture de l'appel à projets

Les éléments du dossier de soumission doivent être déposés sous forme électronique, y compris les documents signés par le responsable légal de chacun des partenaires, impérativement avant le :

30 septembre 2022 à 11h (heure de Paris)

sur le site :
https://france2030.agencerecherche.fr/PEPR-Cyber-AAP

Contacts ANR

Chargé de Projet Scientifique : Pierre Bonnet

Responsable de Programme : Clara Bertolissi

Il est nécessaire de lire attentivement l'ensemble du présent document et les instructions disponibles sur le site de soumission des dossiers :

https://france2030.agencerecherche.fr/PEPR-Cyber-AAP

Pour toute question : PEPR-Cyber@anr.fr

Sommaire

1.Contexte et objectifs de l'appel à projets

1.1.Contexte

La stratégie d'accélération nationale pour la cybersécurité, qui s'inscrit dans le plan d'investissement France 2030, s'articule autour de quatre axes principaux :

- Développer des solutions souveraines de cybersécurité ;
- Renforcer les liens et les synergies entre acteurs de la filière ;
- Soutenir la demande (individus, entreprises, collectivités et État), notamment en la sensibilisant mieux tout en faisant la promotion des offres nationales ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre.

Le Programme et Équipement Prioritaire de Recherche (PEPR) pour la cybersécurité, sous le pilotage du CEA, du CNRS et d'Inria, a pour vocation de soutenir des activités stratégiques de recherche fondamentale, au plus haut niveau mondial, en support aux industriels de la filière et répondant aux priorités définies dans le cadre de la stratégie nationale.

Le programme comporte deux types d'actions de recherche et une action de pilotage :

- des projets ciblés dont les thématiques et les consortiums ont été identifiés avec l'objectif de répondre efficacement à des enjeux scientifiques et technologiques majeurs pour structurer des communautés de recherche, obtenir des avancées scientifiques et permettre l'émergence des technologies de ruptures bénéficiant à l'ensemble des acteurs français de la filière.
- des projets sélectionnés sur appel à projets, sur des thématiques identifiées et autour desquelles la communauté scientifique se fédère et s'organise pour répondre conjointement aux appels.
- l'action de pilotage comprend le suivi scientifique et budgétaire de tous les projets, la coordination entre eux, la vérification de leur adéquation avec le plan France 2030 et la dissémination des résultats vers la communauté scientifique, étatique et industrielle, ainsi que vers le grand public.

1.2.Objectifs de l'appel à projets

Cet appel à projets vise à financer des projets de recherche à des niveaux de TRL 1 à 4, destinés à apporter des éléments de connaissance indispensables aux développements des technologies de cybersécurité et favoriser l'émergence de ces outils et solutions avant leur transfert vers le secteur industriel. Il est doté d'un budget de 15 M€ et couvre les trois axes thématiques suivants :

- Protection des données multimédias.
- Recherche et techniques d'exploitation de vulnérabilités.
- Cryptanalyse de primitives cryptographiques.

Un seul projet sera retenu par axe thématique.

L'aide minimale demandée des projets devra être de 3,5M€ en regard des objectifs des thématiques.

1.3.Rôle des pilotes du PEPR pour cet appel à projets

Dans le cadre de cet appel à projets, les pilotes ont été en charge de la préparation du texte décrivant les objectifs, le périmètre scientifique et les thématiques de l'appel. Notamment, il s'agissait d'assurer la cohérence et la complémentarité de cet appel avec les projets ciblés d'une part et avec l'ensemble de la stratégie d'accélération nationale d'autre part.

Le deuxième rôle des pilotes sera de proposer au Secrétariat Général Pour l'Investissement, sur la base des évaluations et du classement, réalisés par un comité de sélection indépendant à dimension internationale, les projets qui pourraient être financés et le montant d'aide qui pourrait leur être définitivement attribué.

Le troisième rôle des pilotes est le suivi des projets lauréats lors de revues, en concertation avec l'ANR et le coordinateur de la stratégie d'accélération nationale. Il s'agira de discuter des avancées scientifiques et de

dissémination, mais également d'évoquer les points relatifs aux ressources humaines et aux équipements, ainsi que les difficultés rencontrées.

1.4.Principales caractéristiques des projets

Conformément au règlement financier des PEPR, les « bénéficiaires des aides sont des établissements d'enseignement supérieur et/ou de recherche ou des groupements de ces établissements. Les établissements privés contribuant aux missions de service public de l'enseignement supérieur et de la recherche, relevant de l'article L.732-1 du Code de l'Éducation, pourront être financés après analyse de l'ANR, avis du MESRI et validation par le SGPI. Les entreprises pourront avoir le statut d'établissement partenaire dans les projets mais ne bénéficieront pas de financement au titre de cette participation. »

Le projet devra impliquer entre 4 et 8 unités de recherche. Un établissement (ou groupe d'établissements, conformément au règlement financier) sera identifié comme établissement coordinateur et un chercheur ou enseignant-chercheur sera identifié comme responsable scientifique du projet. Le responsable scientifique n'est pas nécessairement contractuellement lié à l'établissement coordinateur. Il ne doit pas être le responsable scientifique d'un autre projet du PEPR Cybersécurité ou d'un autre PEPR.

La durée maximale des projets est de 5 ans.

Il est important que les thématiques considérées n'empiètent pas sur les sujets couverts par d'autres projets issus des PEPR. Les sujets suivants ne sont, a priori, pas visés par cet appel à projets (liste non-exhaustive) : protocoles cryptographiques, preuves de sécurité et vérification formelle, cryptanalyse des implémentations logicielles et matérielles, cryptographie post-quantique, cryptanalyse à base d'ordinateurs quantiques, chiffrement homomorphe et fonctionnel.

2.Thématiques de l'appel et projets attendus

Cet appel à projet comporte trois axes thématiques :

- Axe 1. Protection des données multimédias
- Axe 2. Recherche et techniques d'exploitation de vulnérabilités
- Axe 3. Cryptanalyse de primitives cryptographiques

En cas de doute sur l'éligibilité d'une thématique il est recommandé de contacter le responsable de programme ANR (voir coordonnées de contact en page 3).

Chaque projet doit choisir un seul axe thématique.

2.1.Axe 1 : Protection des données multimédias

Cet axe vise à soutenir des travaux de recherche amont, permettant de prospecter de nouvelles idées et méthodes et d'étudier des concepts en rupture afin de sécuriser les données multimédias. Avec des perspectives d'application à moyen et long terme, cet axe a pour ambition de mobiliser largement et transposer à ce domaine des connaissances fondamentales, des méthodes et des outils issus des disciplines des sciences de l'ingénieur et du numérique, et à susciter des projets de recherche rassemblant des compétences issues d'un large spectre de communautés scientifiques.

L'information par l'image, le texte et le son, et plus généralement à travers le multimédia, est une réalité qui s'est particulièrement accentuée avec le développement des réseaux sociaux et, plus récemment, des activités de télétravail liées à la crise sanitaire. Dans ce cadre, c'est aussi la biométrie, et en particulier la reconnaissance faciale à des fins d'authentification, qui a pris de l'ampleur.

Il est urgent de développer les compétences dans ce domaine pour protéger les informations multimédias et détecter leur falsification. Ce dernier point devient particulièrement critique avec le déploiement de modèles d'IA d'analyses d'images reposant sur la classification d'images et la détection d'objets pour prendre des décisions, par

exemple dans le domaine des véhicules autonomes. Cette problématique se retrouve pour le son. De tels usages renforcent les besoins de déployer des algorithmes d'IA sécurisées à la fois contre les attaques algorithmiques et les attaques physiques (lorsque ces applications tournent sur des systèmes embarqués).

Ainsi, l'image, le texte et le son sont devenus les principaux vecteurs de communication entre les personnes. Les travaux dans ce domaine ont été fortement portés par le besoin de garantir la propriété intellectuelle et/ou commerciale de produits, comme des photos ou des films. Protéger la propriété est en effet une dimension de ce domaine mais l'évolution des technologies et des usages impose aujourd'hui de protéger les informations et les communications, non seulement pour des raisons de propriété, mais aussi pour garantir la confidentialité des informations, qui peuvent parfois être à caractère personnel, par exemple dans le cadre de la visioconférence ou de l'authentification biométrique (voix et visage). Protéger la société des risques de désinformation, en particulier à travers l'hypertrucage (*deepfake*) d'images et de discours est également un enjeu majeur de cette discipline. Cette problématique s'étend à la sécurité des IA, dont leur intégrité (tromper un modèle en injectant des perturbations sur les capteurs), leur confidentialité (autant des modèles que des données d'entraînement) et leur disponibilité (allongement du temps de réponse ou désactivation) peuvent être compromises. Enfin, il faut souligner l'importance du sujet dans les domaines critiques (*manufacturing*, santé, mobilité) et à fort enjeu économique tels que les jeux vidéo, où la dématérialisation totale amplifie le problème du piratage.

De manière non-exhaustive, les sujets suivants peuvent d'être abordés :

- Tatouage d'images, de sons et de vidéos
- Traçage de traites
- Détection de manipulations d'images et de son (incluant la voix), hypertrucage (*deepfake*)
- Caractérisation d'attaques et développement de protections d'algorithmes de *machine learning*
- Biométrie et reconnaissance faciale, biométrie comportementale, à des fins d'authentification
- Détection d'usurpation de voix et contre-mesure.

Mots-clés associés : Tatouage d'images, de sons et de vidéos (*watermarking*), traçage de traites, détection de manipulations d'informations, hypertrucage (*deepfake*), attaques et protections d'algorithmes de *machine learning* de classification d'images, biométrie et reconnaissance faciale, biométrie comportementale à des fins d'authentification.

2.2.Axe 2 : Recherche et techniques d'exploitation de vulnérabilités

La recherche et l'exploitation de vulnérabilités dans les systèmes numériques nécessitent de nouveaux outils de criminalistiques (matériels, logiciels) pour identifier les vulnérabilités, notamment les portes dérobées. Les travaux sur la recherche et les techniques d'exploitation de vulnérabilités permettront de combler le retard de la France dans ce domaine, avec des applications opérationnelles à court terme. En effet, la disponibilité de technologies numériques de plus en plus sécurisées commence à poser de sérieux problèmes aux acteurs en charge des missions régaliennes de la justice et du respect des lois. En outre, l'offre souveraine est limitée, ce qui conduit les autorités à parfois adopter des solutions étrangères. Ce projet permettra également de mettre en place un réseau d'acteurs académiques qui a besoin à ce jour de gagner en force.

Plusieurs verrous scientifiques sont à lever. Les techniques utilisées pour chercher des modèles d'attaque dans les systèmes sont aujourd'hui limitées par la compréhension de leurs comportements. L'élaboration de modèles sémantiques dysfonctionnels (à tous les niveaux de la pile matérielle / logicielle / protocoles / systèmes / services) serait une étape clé de l'élaboration et de l'automatisation de ces techniques. De nouveaux outils d'analyse et d'attaque, combinant du matériel et du logiciel (à base de techniques de rétro-ingénieries ou d'analyses à base d'IA par exemple), sont également à développer, en particulier pour faire face aux contre-mesures présentes ou pour gérer des situations particulières comme la nécessité d'extraire des informations d'un équipement endommagé (pour lequel seules des approches physiques sont envisageables). Enfin la complexité des systèmes analysés dans le cadre des activités de lutte contre la cybercriminalité nécessite de développer des algorithmes d'analyse d'impact passant à l'échelle de ces systèmes, et de les accompagner de techniques de visualisation et de navigation interactives.

Mieux comprendre les vulnérabilités des systèmes et améliorer les techniques de recherche de vulnérabilités, en particulier les techniques automatisées, est primordial pour renforcer la sécurité des systèmes numériques. Ce

projet prend également sa source dans le fait que les systèmes informatiques sont de plus en plus sécurisés, permettant ainsi de fournir un haut niveau de sécurité face aux attaques toujours plus nombreuses. Ce niveau de sécurité pose toutefois de sérieux problèmes aux acteurs étatiques en charge des missions d'investigation légale. La recherche et l'exploitation de vulnérabilités sur ces nouveaux systèmes numériques devient souvent nécessaire pour faire face à des usages criminels qui se développent. Notons enfin que dans le cadre des cas d'usages criminalistiques, les « preuves » récupérées, que ce soit sur la valeur de la preuve elle-même et sur la manière dont elle a été récupérée, doivent être acceptables d'un point de vue juridique. Dans cette optique, les impacts légaux des techniques développées doivent être pris en compte.

De manière non exhaustive, les sujets suivants peuvent d'être abordés :

- Recherche de vulnérabilités et de portes dérobées (*fuzzing* de binaires en environnements sécurisés de confiance, canaux auxiliaires) sur des systèmes déployés
- Recherche de failles dans les noyaux de systèmes d'exploitation
- Analyse et désassemblage de codes machines exécutés non extractibles (racine de confiance par canaux auxiliaires)
- Vulnérabilités spécifiques au web
- Développement d'exploits sur systèmes sécurisés
- Méthodologies d'attaques utilisant de l'apprentissage machine
- Automatisation de la recherche de vulnérabilités et d'exploitation
- Investigation de failles matérielles pouvant être exploitées par logiciel
- Analyse forensique d'images systèmes et de mémoires de systèmes embarqués
- Menace persistante avancée
- Sécurité des téléphones mobiles
- Outils et méthodologies d'analyses sur dispositifs physiques
- Impact/évolution du cadre légal associé aux techniques criminalistiques étudiées.

Mots-clés associés : Recherche de vulnérabilités et de portes dérobées, développement d'exploits, méthodologies d'attaques, apprentissage machine, automatisation, investigation numérique, analyse forensique, outils et méthodologies d'analyses sur dispositifs physiques.

2.3.Axe 3 : Cryptanalyse de primitives cryptographiques

La cryptanalyse est une branche de la cryptologie qui consiste à étudier la sécurité des primitives cryptographiques. Elle vise aussi bien à prouver la sécurité qu'à montrer que la sécurité visée n'est pas atteinte, ce qui peut se faire par le biais d'une analyse théorique ou de l'exploitation d'une faille dans des conditions réelles ou de laboratoire.

La communauté scientifique française se situe, dans le domaine de la cryptanalyse, au tout premier plan sur la scène internationale. L'objectif de cet axe « Cryptanalyse de primitives cryptographiques » et de renforcer ce positionnement, d'essaimer les compétences au niveau national et de les transférer vers les acteurs privés et étatiques de la filière.

L'axe thématique porte sur les deux volets suivants, qui devront être tous les deux couverts par le projet retenu :

- Cryptanalyse de primitives cryptographiques à clef symétrique,
- Cryptanalyse de primitives cryptographiques à clef asymétrique.

Cryptographie à clef symétrique. Le premier volet portera sur la cryptanalyse d'algorithmes de chiffrement (par bloc ou par flot), de chiffrement authentifié, de modes de chiffrement, de fonctions de hachage, de MAC et de générateurs pseudo-aléatoires. Les travaux viseront à la fois la proposition de nouvelles techniques de cryptanalyse, l'amélioration de techniques existantes, et la cryptanalyse de primitives existantes. Concernant les primitives existantes, pourront être considérées les cryptanalyses de primitives issues des efforts de standardisation récents, mais aussi des primitives plus anciennes pour déterminer si leur dépréciation est devenue nécessaire. Le projet pourra également s'intéresser à la sécurité issue de la composition de plusieurs primitives cryptographiques et à la conception de méthodes automatiques de cryptanalyse ou d'aide à la cryptanalyse.

Cryptographie à clef asymétrique. Le second volet portera sur la cryptanalyse d'algorithmes de chiffrement, de schémas de signature, et de générateurs pseudo-aléatoires, reposant sur la difficulté de la factorisation et du logarithme discret (et plus généralement sur les problèmes mathématiques qui ne sont pas étudiés dans le cadre du PEPR Technologies Quantiques), ainsi que sur la cryptanalyse de primitives cryptographiques reposant sur des courbes algébriques ou des couplages. Les travaux viseront à la fois la proposition de nouvelles techniques de

cryptanalyse, l'amélioration de techniques existantes, et la cryptanalyse de primitives existantes, y compris les problèmes mathématiques sous-jacents.

Mots-clés associés : cryptanalyse, clef symétrique, clef asymétrique, schéma de signature, algorithme de chiffrement, chiffrement authentifié, mode de chiffrement, fonction de hachage, MAC, factorisation, logarithme discret, courbes algébriques, couplages.

3.Examen des projets proposés

3.1.Procédure de sélection

Les projets recevables (cf. § 3.21.4) seront évalués par un comité de sélection indépendant à dimension internationale. Ce comité pourra recourir, le cas échéant, à des expertises externes et pourra procéder à une audition des porteurs des projets.

À l'issue de ses travaux, le comité de sélection remettra aux pilotes du PEPR Cybersécurité un rapport comprenant :

1) les notes attribuées aux projets évalués selon les critères indiqués au §3.3 par axe thématique;
2) la liste des projets par axe thématique que le comité recommande pour financement en raison de leur qualité, évaluée sur la base des critères indiqués au § 3.3**Erreur ! Source du renvoi introuvable.** ;
3) la liste des projets que le comité propose de ne pas financer.

Chaque projet évalué fera l'objet d'un argumentaire justifiant de sa position sur l'une des deux listes. Le comité pourra formuler un avis sur le montant des financements demandés.

Les pilotes du PEPR proposeront au Secrétariat Général Pour l'Investissement la désignation des projets qui pourraient être financés et le montant d'aide qui pourrait leur être définitivement attribué. Le Premier ministre, après avis du SGPI, arrêtera la décision concernant les bénéficiaires et les montants accordés. Chaque projet fera l'objet d'un contrat entre l'ANR et l'établissement coordinateur du projet, détaillant les obligations réciproques des parties.

Les membres du comité de sélection ainsi que les éventuels experts externes sollicités s'engagent à respecter les règles de déontologie et d'intégrité scientifique établies par l'ANR. La charte de déontologie de l'ANR est disponible sur son site internet. L'ANR s'assurera du strict respect des règles de confidentialité, de l'absence de liens d'intérêt entre les membres du comité ou experts externes et les porteurs et partenaires des projets, ainsi que de l'absence de conflits d'intérêts pour les membres du comité et experts externes. En cas de manquement dûment constaté, l'ANR se réserve le droit de prendre toute mesure qu'elle juge nécessaire pour y remédier. La composition du comité de sélection sera affichée sur le site de publication de l'appel à projets à l'issue de la procédure de sélection.

3.2.Critères de recevabilité

IMPORTANT

Les dossiers ne satisfaisant pas aux critères de recevabilité ne seront pas soumis au jury et ne pourront en aucun cas faire l'objet d'un financement.

1) Le dossier de soumission doit être déposé complet sur le site de soumission de l'ANR avant la date et l'heure de clôture de l'appel à projets, indiquées en page 3 de ce document. De plus, le document administratif et financier doit être déposé sur le site de soumission de l'ANR avant la date et l'heure indiquées en page 3.
2) Le document scientifique du projet doit impérativement suivre le modèle disponible sur le site internet de l'appel à projets et être déposé au format PDF non protégé. Il ne doit pas dépasser 20 pages.
3) Satisfaire les conditions décrites au § 1.4.

4) Sont exclus également les projets qui causeraient un préjudice important du point de vue de l'environnement (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie.

3.3.Critères d'évaluation

Les experts externes et les membres du comité de sélection sont appelés à examiner les propositions de projet selon les critères d'évaluation ci-dessous, regroupés en trois catégories.

1) **Excellence et ambition scientifique :**

- Clarté des objectifs et des hypothèses de recherche ;
- Caractère novateur, ambition, originalité, rupture méthodologique ou conceptuelle du projet par rapport à l'état de l'art ;
- Pertinence de la méthodologie.

2) **Qualité du consortium, moyens mobilisés et gouvernance :**

- Compétence, expertise et implication du responsable scientifique du projet : capacité à coordonner des consortiums pluridisciplinaires et ambitieux, parcours scientifique, reconnaissance internationale ;
- Qualité et complémentarité du consortium scientifique au regard des objectifs du projet ;
- Adéquation entre les moyens humains et financiers mobilisés (y compris ceux demandés dans le cadre du projet) par rapport aux objectifs visés ;
- Pertinence du calendrier, gestion des risques scientifiques et solutions alternatives, crédibilité des jalons proposés ;
- Pertinence et efficacité de la gouvernance du projet (pilotage, organisation, animation, mise en place de comités consultatifs, etc.).

3) **Impact et retombées du projet :**

- Capacité du projet à répondre aux enjeux de recherche de l'axe thématique choisi ;
- Impacts économiques et sociétaux, contribution au développement de solutions en réponse aux enjeux des domaines prioritaires de la stratégie d'accélération nationale ;
- Stratégie de diffusion (*in itinere* et *ex post*) et de valorisation des résultats, adhésion aux principes FAIR, Open Science et promotion de la culture scientifique.

4.Dispositions générales pour le financement

4.1.Financement

Les appels financés au titre du PEPR présentent un caractère exceptionnel et se distingue du financement récurrent des établissements universitaires ou de recherche.

Les financements alloués représentent des moyens supplémentaires destinés à des actions nouvelles. Ils pourront permettre le lancement de projets de recherche innovants, et financer, par exemple, l'achat d'équipements ainsi que des dépenses de personnel affecté spécifiquement à ces projets et de fonctionnement associé.

Les dépenses éligibles sont précisées dans le règlement financier relatif aux modalités d'attribution des aides de l'action PEPR. Le soutien financier sera apporté sous la forme d'une dotation, dont le décaissement est effectué par l'ANR pour l'établissement coordinateur du projet, selon l'échéancier prévu dans le contrat, sur la durée du projet.

Cet appel à projets sera présenté à la Commission européenne pour faire partie du plan de relance national dans le cadre de la facilité de relance et résilience (FRR).

4.2.Accords de consortium

Les projets financés conduits en partenariat devront établir un accord de consortium (dans les 12 mois suivant la communication de l'accord de financement) précisant les droits et obligations de chaque établissement partenaire

du projet. Cet accord précisera :

- la répartition de la dotation financière, des tâches et des livrables entre les différents partenaires, ainsi que les moyens humains et financiers mobilisés en propre par ces derniers ;
- les modalités scientifiques, techniques et financières d'accès aux ressources partagées entre les partenaires ;
- les modalités de valorisation des résultats obtenus à l'issue des recherches et de partage de leur propriété intellectuelle et industrielle.

4.3.Science ouverte

Dans le cadre de la contribution de l'ANR à la promotion et à la mise en œuvre de la science ouverte, et en lien avec le Plan national pour la science ouverte au niveau français (PNSO) et le Plan S au niveau international, L'ANR encourage les bénéficiaires de la subvention France 2030 à déposer les pré-prints dans des plateformes ouvertes ou archives ouvertes et à privilégier des identifiants pérennes ou uniques (DOI ou HAL Id, par exemple). Par ailleurs, l'ANR recommande de privilégier la publication dans des revues ou ouvrages nativement en accès ouvert[1].

L'ensemble du consortium devra appliquer les mentions obligatoires de se référer à France 2030 et au PEPR Cybersécurité et ce, dans tous les actions et livrables émanant du programme.

Enfin, l'Établissement coordinateur s'engage à fournir dans les 6 mois qui suivent le démarrage du projet, une première version du Plan de Gestion des Données (PGD) selon les modalités indiquées dans le contrat attributif d'aide.

4.4.Aide d'État

Les aides versées dans le cadre du présent appel à projets sont soumises à la réglementation européenne relative aux aides d'État (articles 107, 108 et 109 du Traité sur le fonctionnement de l'Union européenne et textes dérivés), dès lors qu'elle est qualifiable d'aide d'État. Ainsi, ce financement doit respecter les règles européennes relatives aux aides d'État et s'inscrire dans le cadre du Règlement (UE) n°651/2014 de la Commission du 17 juin 2014 déclarant certaines catégories d'aides compatibles avec le marché intérieur en application des articles 107 et 108 du traité.

5.Modalités de soumission

5.1.Contenu du dossier de soumission

Le dossier de soumission devra comporter l'ensemble des éléments nécessaires à l'évaluation scientifique et technique du projet. Il devra être déposé avant la clôture de l'appel à projets, dont la date et l'heure sont indiquées en page 3.

IMPORTANT

Aucun élément complémentaire ne pourra être accepté après la clôture de l'appel à projets dont la date et l'heure sont indiquées page 3.

Les documents devront être déposés sur le site de soumission dont l'adresse est mentionnée page 3. Afin d'accéder à ce service, il est indispensable d'obtenir au préalable l'ouverture d'un compte (identifiant et mot de passe). Pour obtenir ces éléments, il est recommandé de s'inscrire le plus tôt possible.

Le dossier de soumission complet est constitué de deux documents intégralement renseignés :

[1] Le site DOAJ (https://doaj.org/) répertorie les revues scientifiques dont les articles sont évalués par les pairs et en libre accès. Le site DOAB (https://www.doabooks.org/) fait de même pour les monographies.

1) Le « document scientifique », d'une longueur maximum de 20 pages, rédigé en français, comprenant une description du projet envisagé, selon le format fourni, avec en annexe des éléments biographiques sur les chercheurs et enseignants-chercheurs responsables de lots dans le projet et une liste de leurs principales publications scientifiques dans l'axe thématique ;

2) Le « document administratif et financier », qui comprend la description administrative et budgétaire du projet.

Les éléments du dossier de soumission (document administratif et financier au format Excel et modèle de document scientifique) seront accessibles à partir de la page web de publication du présent appel à projets (voir adresse en page 3).

5.2.Procédure de soumission

Les documents du dossier de soumission devront être transmis par le responsable scientifique du projet, sous forme électronique impérativement :

- avant la date de clôture indiquée 3 page 3 du présent appel à projets,
- sur le site web de soumission selon les recommandations du § 5.3**Erreur ! Source du renvoi introuvable.**.

L'inscription préalable sur le site de soumission est nécessaire pour pouvoir soumettre un projet.

Seule la version électronique des documents de soumission présente sur le site de soumission à la clôture de l'appel à projets est prise en compte pour l'évaluation.

Un accusé de réception, sous forme électronique, sera envoyé au responsable du projet lors du dépôt des documents.

5.3.Conseils pour la soumission

Il est fortement conseillé :

- d'ouvrir un compte sur le site de soumission au plus tôt ;
- de ne pas attendre la date limite d'envoi des projets pour la saisie des données en ligne et le téléchargement des fichiers (attention : le respect de l'heure limite de soumission est impératif) ;
- de vérifier que les documents déposés dans les espaces dédiés des rubriques « documents de soumission » et « documents signés » sont complets et correspondent aux éléments attendus. Le dossier de soumission et le dépôt des documents signés ne pourra être validés par le responsable du projet que si l'ensemble des documents a été téléchargé ;
- de consulter régulièrement le site internet dédié au programme, à l'adresse indiquée en page 33, qui comporte des informations actualisées concernant son déroulement ;
- de contacter, si besoin, les correspondants par courrier électronique, à l'adresse mentionnée en page 3 du présent document.

GOUVERNEMENT

Contacts

Les renseignements concernant le processus administratif (constitution du dossier, démarches en ligne, taux d'aide) pourront être obtenus auprès de l'ANR par courriel :

PEPR-Cyber@anr.fr