OFFRE DE CONTRAT DOCTORAL EN DROIT DU NUMERIQUE

« LA CYBERSECURITE DES SYSTEMES D'INTELLIGENCE ARTIFICIELLE (APPROCHE JURIDIQUE) »

Date du contrat : 1/11/2024 au 31/10/2027

Section CNU : 01-Droit privé et sciences criminelles

Rattachement : Institut caennais de recherche juridique (Université de Caen) / École doctorale Droit-Normandie.

Contexte : cette offre de contrat doctoral s'inscrit dans le cadre du projet CYRCE (cybersécurité) porté par l'Université de Caen Normandie (AMI Métiers d'avenir – ANR/France 2030/Région Normandie).

Sujet : La cybersécurité des systèmes d'intelligence artificielle (approche juridique)

Direction : Thibault DOUVILLE, professeur des universités en droit privé et sciences criminelles, Université de Caen Normandie

Résumé :

Le déploiement des systèmes d'intelligence artificielle – générative ou non – rend le fonctionnement de la société dépendante de ces systèmes faisant naître des risques systémiques. Pensons pêle-mêle au référencement de contenus sur des moteurs de recherche, à la hiérarchisation et à la modération des contenus sur les plateformes en ligne, aux diagnostics médicaux, aux décisions administratives automatisées, aux véhicules autonomes ou à la maintenance des systèmes industriels.

Si l'intelligence artificielle peut être mise au service de la cybersécurité, notamment pour la détection de flux anormaux de données ou le filtrage des spams, ou au contraire pour faciliter les atteintes de sécurité – par le développement de l'ingénierie sociale, en facilitant le hacking ou en permettant les deepfakes – le projet de thèse proposé se concentre sur la question de la cybersécurité des systèmes d'IA.

La sécurité des systèmes d'IA se pose de la même manière que pour tout système d'information. Elle présente néanmoins de nombreuses spécificités en raison de la conception des systèmes d'IA (entraînement d'un modèle à partir d'un ensemble de données, ce qui pose incidemment la question de la sécurité des données et de l'intégrité du modèle), du détournement possible de l'usage des systèmes d'intelligence artificielle ou d'une utilisation malveillante qui peut en être faite (spécialement s'agissant des intelligences artificielles génératives ou à usage général) ou de l'influence que leur environnement de fonctionnement peut avoir sur elles.

Un cadre juridique émerge progressivement pour encadrer les systèmes d'IA en général, mais aussi, plus particulièrement pour garantir leur cybersécurité. Ainsi, le règlement européen sur l'intelligence artificielle, comme le droit européen des données ou de la cybersécurité s'attachent à la cybersécurité de ces systèmes. Dans le même temps, des normes techniques se développent sur la question de cybersécurité des systèmes d'IA sur lesquelles les règles juridiques s'appuient et qui ne peuvent pas

être ignorées. Corrélativement, la complexité des chaînes d'approvisionnement des systèmes d'IA (concepteurs, utilisateurs, prestataires de services…) pose la question du partage de la responsabilité entre les acteurs concernés et celle de la mise en œuvre de l'exigence de conformité en matière de cybersécurité. La thèse proposée aura pour objet d'aborder tous ces aspects.

Profil : étudiant diplômé d'un master droit du numérique (ou d'un autre master en droit ou d'un IEP (avec une forte dominante en droit) avec un excellent parcours universitaire) et ayant soutenu un mémoire en master ; aptitude à travailler en langue anglaise.

Pièces à fournir :

- CV
- Relevés de notes (L1 au M2) et attestation de réussite du master
- Lettre de motivation
- Mémoire de master

Modalités de candidature : Candidature ouverte jusqu'au 6 septembre 2024 à communiquer à Thibault DOUVILLE (thibault.douville(@)unicaen.fr) en mettant impérativement en copie Pénélope COCHENNEC (penelope.cochennec(@)unicaen.fr).

Modalités de sélection :

- audition (deuxième quinzaine du mois de septembre) ;
- sous réserve de la validation du financement par l'établissement (mi-octobre).