

OBJET : Allocations Doctorales 2024 - Note - Recrutement des doctorants

Informations sur l'emploi		
	Organisation / Entreprise	Université de Caen Normandie
	Domaine de recherche	Droit
	Profil du chercheur	Doctorant
	Pays	France
	Date limite de dépôt des candidatures	Vendredi 6 juin 2025, 12 h Envoi du document unique (PDF) par mail à l'École doctorale DROIT NORMANDIE. L'accusé-réception ne fera pas foi de la recevabilité de la candidature.
	Type de contrat	Contrat doctoral
	Statut de l'emploi	Contrat à durée déterminée
	Le poste est-il financé par le programme-cadre de recherche de l'UE ?	Non
	L'emploi est-il lié à un poste de personnel au sein d'une infrastructure de recherche ?	Doctorant au sein de l'ICREJ (Institut caennais de recherche juridique) – UR 967.

Description de l'offre		La vulnérabilité numérique
	Description du poste et du projet de doctorat (fléché et financé)	Digital vulnerability <u>Version Française</u> <i>Illectronisme, désinformation, interfaces trompeuses, manipulation des émotions, voilà autant de situations qui correspondent à des situations de vulnérabilité numérique subies par une personne. La vulnérabilité numérique se manifeste sous deux formes principales, elle peut être personnelle, liée à un affaiblissement personnel physique ou intellectuel, ou contextuelle, notamment en raison d'un déséquilibre de pouvoirs ou de la complexité de l'environnement dans lequel la personne se trouve.</i> <i>Aucune étude transversale de la vulnérabilité numérique n'a été menée par la doctrine juridique française, qui s'intéresse seulement à certains de ses aspects. Parallèlement, des projets de recherche sont en cours à l'étranger portant sur la vulnérabilité numérique dans les relations entre l'administration et ses usagers.</i> <i>Le projet de thèse porte sur l'étude globale de la vulnérabilité numérique dans les relations entre personnes privées. Il vise à analyser de manière critique les dispositifs consacrés pour la prendre compte et à en dégager les insuffisances. La recherche doctorale explorera ainsi la lutte contre l'illectronisme, l'interdiction des IA manipulatrices ou la gestion des risques des techniques de reconnaissance émotionnelle. Des propositions d'évolutions législatives pourront être faites, notamment par la consécration de nouveaux droits (droit de ne pas utiliser les communications électroniques, droit à l'intégrité intellectuelle...). Le travail de recherche s'appuiera sur l'étude des initiatives législatives étrangères et sur une méthodologie de recherche adaptée qui supposera l'établissement d'un état des lieux de la vulnérabilité numérique – notamment sur la base des statistiques et études sociologiques disponibles et d'entretiens - et de dégager différentes situations typiques pour les besoins du raisonnement. Cet état des lieux nourrira les réflexions du doctorant. La thèse fera progresser l'état des savoirs en droit du numérique et de la vulnérabilité.</i>

		<u>Version Anglaise</u> <i>Illectronism, misinformation, misleading interfaces, manipulation of emotions - these are all situations that correspond to digital vulnerability experienced by an individual. Digital vulnerability manifests itself in two main forms: it can be personal, linked to a physical or intellectual personal weakness, or contextual, notably due to an imbalance of power or the complexity of the environment in which the person finds himself.</i> <i>No cross-disciplinary study of digital vulnerability has been carried out by French legal doctrine, which is only interested in certain aspects. At the same time, research projects are underway in other countries on digital vulnerability in relations between the administration and its users.</i> <i>This thesis project is concerned with the global study of digital vulnerability in relations between private individuals. The aim is to critically analyze the mechanisms in place to address this issue, and to identify their shortcomings. Doctoral research will thus explore the fight against illectronism, the prohibition of manipulative AI or the risk management of emotional recognition techniques. Proposals for legislative changes could be made, in particular by establishing new rights (right not to use electronic communications, right to intellectual integrity, etc.). The research work will be based on a study of foreign legislative initiatives and on an adapted research methodology, which will involve drawing up an inventory of digital vulnerability - notably on the basis of available statistics and sociological studies, and interviews - and identifying various typical situations for the purposes of reasoning. This inventory will provide the basis for the doctoral student's reflections. The thesis will advance the state of knowledge in digital law and vulnerability.</i>
	Placement salarial	2100-2300 € / mois.

Exigences		
	Conditions d'admission	Après audition du (de la) candidat(e) devant un jury, le mardi 10 juin 2025, à partir de 13 h. 30, et délibération du Conseil restreint de l'ED Droit Normandie, sera admis à préparer une thèse consacrée à l'usage des armes par les forces de l'ordre, l'étudiant(e), ayant réuni les conditions d'admission suivantes : (1) Etre titulaire d'un master (grade national de master) en droit (privé ou public) au 1^{er} octobre 2025, avec mention. (2) Etre en mesure de présenter, pendant l'audition, son cursus universitaire, le bien-fondé de son analyse du sujet et le calendrier de sa recherche sur les 3 ans que dure le contrat doctoral. (3) Avoir rédigé un mémoire sur un sujet en droit du numérique sur le thématique de la vulnérabilité numérique.
	Eligibilité	Pour présenter sa candidature au projet de thèse fléché et financé par l'Université de Caen Normandie, le(la) candidat(e) doit être titulaire d'un master en droit du numérique ou être en voie de l'être au 1^{er} sept. 2025. En outre, le(la) candidat(e) doit être spécialisée par son cursus en droit du numérique, mais aussi en droit des libertés, en droit international et européen (droit de la Convention européenne des droits de l'homme en particulier). Une ouverture au droit comparé est un plus.
Applications		
		La demande doit être présentée sous la forme d'un document PDF unique, dont les pages sont numérotées. L'ensemble du document doit contenir : (1) Une lettre de motivation décrivant les intérêts du candidat à la recherche et expliquant les raisons de la candidature. (2) Un programme de recherche trimestriel sur

		3 ans. (3) Un curriculum vitae (CV). (4) Copies des relevés de notes de licence en droit et de master 1 en droit (privé ou public), de master 2 s'il a été obtenu. (5) Les coordonnées de deux personnes de référence ou en situation de recommander le(la) candidat(e) au projet de recherche doctorale fléché et financé. (6) Le mémoire de recherche soutenu ou une présentation du travail de recherche en cours pour un étudiant qui serait actuellement en master 2.
Lieu(x) de travail		Université de Caen (Normandie, France) Esplanade de la Paix. – 14032 Caen. UFR Droit (bât. D.). – ICREJ.
Où s'adresser ?		Mail de l'école doctorale : esther.camus@unicaen.fr ed98.dn@unicaen.fr penelope.cochennec@unicaen.fr droit.recherche@unicaen.fr
Contact		Mail du porteur ou directeur de thèse : Thibault.douville@unicaen.fr



UNIVERSITÉ
CAEN
NORMANDIE



A compter de la campagne 2024, les universités et écoles d'ingénieurs Normandes ont mis en place un processus **unique** de soumission et d'évaluation pour les allocations d'établissement et les allocations 100% région, accompagné d'un calendrier unique de soumission et d'évaluation.

Merci de cocher impérativement au moins une case (possibilité de cocher les deux cases en cas de double soumission)

La demande concerne :

☒ Une allocation d'établissement

☒ Une allocation régionale 100 %

(note : les demandes d'allocation INSA sont à compléter en utilisant le formulaire 50%)

Merci de remplir pour toutes les demandes la partie commune (pages 2-4). Dans le cas d'une demande d'allocation régionale (ou de double demande), remplir également la section correspondante (pages 5-8). Il n'est pas nécessaire de remplir les items suivants, qui seront complétés par l'établissement en cas de pré-sélection du dossier : « *Rattachement de l'opération à l'Accord de Partenariat Stratégique* », « *Contact administratif au sein de l'établissement porteur* » ; et « *rattachement à l'APS dans le cas où le sujet de thèse ne correspondrait à aucun domaine de la S3* ». De même, les « Documents obligatoires à joindre au dossier » seront remontés par l'établissement.

Date limite de dépôt en ligne sur la plateforme de Normandie Université : 24 Janvier 2025

PARTIE COMMUNE : à remplir dans tous les cas (soumission à l'établissement ou à la région)

INFORMATIONS GENERALES

Intitulé du projet : La vulnérabilité numérique

Acronyme du projet : Digital-vulnerability

Etablissement porteur : Université de Caen

Localisation du projet (nom du laboratoire et adresse) : Institut caennais de recherche juridique/ICREJ – Unité de recherche 967 – Université de Caen Normandie

Discipline du projet : Droit privé et sciences criminelles - 01

Coordinateur du projet dans le laboratoire d'accueil :

Nom : Douville

Prénom : Thibault

Courriel : thibault.douville@unicaen.fr

Si laboratoire sur plusieurs sites, précisez le lieu : Ville / Campus / Établissement hébergeur

Équipe de recherche (si existante) : Institut caennais de recherche juridique/ICREJ

Adresse : Esplanade de la paix

N° - Libellé de la voie :

Code postal : 14000

Commune : Caen

École doctorale de rattachement du directeur de thèse : ED Droit Normandie

Période d'exécution du projet :

Du 01/09/2025 au 31/08/2028, soit 36 mois de projet.

Résumé, vulgarisé et diffusable du projet (2000 caractères maximum espaces compris pour chacune des version) :

Description à destination d'un public non averti/novice sur le sujet. Ce paragraphe pourra être utilisé dans des documents de communication en cas de subventionnement du projet.

Version Française

Illectronisme, désinformation, interfaces trompeuses, manipulation des émotions, voilà autant de situations qui correspondent à des situations de vulnérabilité numérique subies par une personne. La vulnérabilité numérique se manifeste sous deux formes principales, elle peut être personnelle, liée à un affaiblissement personnel physique ou intellectuel, ou contextuelle, notamment en raison d'un déséquilibre de pouvoirs ou de la complexité de l'environnement dans lequel la personne se trouve.

Aucune étude transversale de la vulnérabilité numérique n'a été menée par la doctrine juridique française, qui s'intéresse seulement à certains de ses aspects. Parallèlement, des projets de recherche sont en cours à l'étranger portant sur la vulnérabilité numérique dans les relations entre l'administration et ses usagers.

Le projet de thèse porte sur l'étude d'ensemble de la vulnérabilité numérique dans les relations entre personnes privées. Il vise à analyser de manière critique les dispositifs consacrés pour la prendre compte et à dégager leurs insuffisances. La recherche doctorale explorera ainsi la lutte contre l'illectronisme, l'interdiction des IA manipulatrices ou la gestion des risques des techniques de reconnaissance émotionnelle. Des propositions d'évolutions législatives pourront être faites, notamment par la consécration de nouveaux droits (droit de ne pas utiliser les communications électroniques, droit à l'intégrité intellectuelle...). Le travail de recherche s'appuiera sur des initiatives législatives étrangères et sur une méthodologie de recherche adaptée qui supposera l'établissement d'un état des lieux de la vulnérabilité numérique à partir de quelques situations typiques. Cet état des lieux nourrira les réflexions du doctorant. La thèse contribuera à enrichir l'état des savoirs en droit du numérique mais aussi s'agissant de la maîtrise du phénomène de vulnérabilité.

Version Anglaise

Illectronism, misinformation, misleading interfaces, manipulation of emotions - these are all situations that correspond to digital vulnerability experienced by a person. Digital vulnerability manifests itself in two main forms: it can be personal, linked to a physical or intellectual personal weakness, or contextual, notably due to an imbalance of power or the complexity of the environment in which the person finds himself.

No cross-disciplinary study of digital vulnerability has been carried out by French legal doctrine, which is only interested in certain aspects. At the same time, research projects are underway in other countries on digital vulnerability in the relationship between the administration and its users.

This thesis project is concerned with the overall study of digital vulnerability in relations between private individuals. The aim is to critically analyze the mechanisms in place to address this issue, and to identify their shortcomings. Doctoral research will thus explore the fight against illectronism, the prohibition of manipulative AI or the risk management of emotional recognition techniques. Proposals for legislative changes could be made, in particular by establishing new rights (the right not to use electronic communications, the

right to intellectual integrity, etc.). The research work will be based on foreign legislative initiatives and an adapted research methodology, which will involve drawing up an inventory of digital vulnerability based on a few typical situations. This inventory will provide the basis for the doctoral student's reflections. The thesis will contribute to enriching the state of knowledge in digital law, but also in terms of mastering the phenomenon of vulnerability.

Mots clés liés au projet (5 mots maximum) :

Vulnérabilité, Intelligence artificielle, Illectronisme, Désinformation. Autonomie individuelle

PRÉSENTATION DU PROJET :

Contexte et Objectifs (2 pages maximum) : précisez s'il s'agit d'une recherche incrémentale (poursuite, renforcement d'un thème existant) ou innovante (nouveau sujet), positionnement local-national-international, bibliographie

La question de la vulnérabilité numérique n'a pas fait l'objet de travaux de recherche nombreux dans la doctrine juridique française alors que ses manifestations sont nombreuses dans l'environnement numérique. En Europe, des travaux de recherche sont en cours, en particulier en Belgique (Pr. Elise Degrave, Université de Namur : L'État numérique et les droits humains, Académie Royale de Belgique L'Académie en poche, 25/09/2024, 146 pages) et aux Pays-Bas (Pr. Sofia Ranchordas, Tilburg University, projet de recherche consacré au thème : Vulnerability in the Digital Administrative State) sur les vulnérabilités dans les relations entre les administrations et les usagers. L'approche proposée envisage au contraire la vulnérabilité dans les relations entre personnes privées.

Les deux formes identifiées de vulnérabilités des personnes se retrouvent dans l'environnement numérique. La vulnérabilité peut être personnelle, la personne n'étant pas d'exercer les attributs de sa personnalité en raison d'un affaiblissement personnel (physique ou intellectuel) comme un handicap ; la vulnérabilité peut aussi être circonstancielle, liée au contexte dans lequel elle se trouve en raison du déséquilibre de pouvoirs avec un tiers ou de la complexité de l'environnement dans lequel elle se trouve (sur ces deux approches de la vulnérabilité : X. Lagarde, « Avant-propos », in Cour de cassation, Rapport annuel 2009. Les personnes vulnérables dans la jurisprudence de la Cour de cassation, Paris, La Documentation française, 2009, p. 58). Elle peut se traduire par l'impossibilité d'accéder à internet, à utiliser les outils numériques, à percevoir la véracité d'une information ou à la comprendre.

La question de la vulnérabilité numérique se pose avec d'autant plus d'intérêt que l'évolution technologique favorise le développement d'environnements numériques trompeurs (par exemple par le déploiement d'interfaces trompeuses conçues à partir du fruit des travaux de recherche menés concernant les sciences du comportement) et plus récemment le déploiement de systèmes d'intelligence artificielle, en particulier des intelligences artificielles génératives, qui font naître des risques de désinformation, tandis que des systèmes capables de manipuler les émotions en jouant sur les stimuli

émotionnels sont développés. Cela dit, les outils numériques peuvent aussi être une réponse à la situation de vulnérabilité des personnes en permettant de les assister dans leurs démarches en ligne ou de mieux comprendre les informations qui leur sont communiquées. Pensons à cet égard au rôle crucial joué par les assistants vocaux.

Dans ce contexte, la thèse adopte une approche globale. Elle aura d'abord pour objet de recenser l'ensemble des mécanismes assurant la protection des personnes en situation de vulnérabilité dans l'environnement numérique et de les étudier de manière critique. Pensons par exemple au régime de lutte contre l'illectronisme, dont le champ d'application est limité et pourrait faire l'objet d'une généralisation dans le code civil. Pensons aussi à l'interdiction des systèmes d'IA recourant à des techniques subliminales au-dessous du seuil de conscience d'une personne ou à des techniques délibérément manipulatrices ou trompeuses, qui pose notamment les questions de la frontière entre les techniques « délibérément » trompeuses et celles qui ne le sont, de la preuve de ce caractère intentionnel ou des techniques qui sans être délibérément trompeuses le sont concrètement. Pensons également à l'utilisation des techniques de reconnaissance des émotions, dont l'objectif est de réaliser un profilage des personnes concernées et qui sont pour certaines qualifiées de systèmes d'intelligence à haut risques et pour d'autres relèvent d'un régime de transparence. Pensons enfin à l'exigence de transparence des systèmes d'intelligence artificielle interagissant avec les personnes physiques, dont on peut s'interroger sur la portée. Au-delà de ces dispositions particulières, la question de la prise en compte des conséquences de l'exploitation des vulnérabilités des personnes en droit civil se pose, par exemple à travers l'obligation d'information précontractuelle, l'intégrité du consentement et plus généralement la protection de la dignité des personnes.

La thèse aura aussi pour objet de s'interroger d'un point de vue prospectif sur la protection de la vulnérabilité des personnes au regard de l'évolution annoncée des technologies et des usages. La « dématérialisation » des relations entre l'homme et la machine par le déploiement annoncé des assistants vocaux reposant sur des systèmes d'intelligence artificielle interroge par exemple sur la loyauté de ces systèmes, la protection du consentement ou la qualité des sorties. À cet égard, le rapport au temps en raison de l'instantanéité des systèmes numériques, qui est un élément de protection contre certaines vulnérabilités, comme l'évolution des formalismes protecteurs, se posera.

De nouveaux types de réponse aux vulnérabilités numériques auront vocation à être imaginés, comme l'équivalence d'efficacité (et non l'équivalence fonctionnelle des formalismes), la justification des informations proposées ou du traitement d'une personne par rapport à une autre placée dans une situation comparable. Plus généralement, l'utilité de consacrer un droit de ne pas utiliser les communications électroniques (c'est-à-dire un droit à l'alternative au numérique) ainsi qu'un droit à l'intégrité ou à la dignité numérique (à l'image de certaines initiatives comme dans certains cantons Suisse) pourrait constituer le fondement du traitement de la vulnérabilité numérique. Au-delà du traitement juridique de la vulnérabilité dans l'environnement numérique, la thèse contribuera à nourrir la réflexion sur les relations entre l'homme et la machine ainsi que la théorie générale de la vulnérabilité, qu'il s'agisse de ses fondements, de ses caractères ou de son régime.

Bibliographie sélective :

La vulnérabilité, Journées québécoises, Association Henri Capitant des amis de la culture juridique française, Bruylant, Coll. Travaux de l'Association Henri Capitant, 2020.

Les cahiers de la justice, 2019 N°4, dossier « Vulnérabilités », Dalloz, 2020.

- V. Barbé et S. Mauclair (dir.), *Intelligence artificielle & droits fondamentaux*, Editions L'Epitoge, coll. L'Unité du Droit, 2022
- A. Boujeka et M. Roccati (dir.), *La vulnérabilité en droit international, européen et comparé*, Presses universitaires de Paris Nanterre, coll. Sciences juridiques et politiques, 2022.
- C. Castets-Renard, J. Eynard, *Un droit de l'intelligence artificielle. Entre règles sectorielles et régime général, perspectives comparées*, Bruylant, 2023
- Y. Citton, *L'économie de l'attention. Nouvel horizon du capitalisme ?*, La découverte, 2014
- E. Dégrave, « Justice sociale et services publics numériques : pour le droit fondamental d'utiliser – ou non – internet », *Revue belge de droit constitutionnel*, 2023-3, p. 211 et s.
- T. Douville, *Droit des données à caractère personnel*, Montchrestien, coll. Domat, 2023.
- T. Douville, « Quelle protection contre l'illectronisme ? », in *Le renouvellement du droit civil sous l'influence du numérique*, Dalloz, 2024, p.
- J. Dugne, *La vulnérabilité de la personne majeure. Essai en droit privé*, Dalloz, Nouvelle Bibliothèque de Thèses, 2022
- L. Devillers, *Les robots émotionnels : santé, surveillance, sexualité... : et l'éthique dans tout ça ?*, Éd. de l'Observatoire, 2020
- R. Fassi-Fihri, *Les droits et libertés du numérique : des droits fondamentaux en voie d'élaboration*, LGDJ, coll. Thèses, 2022
- H. Jacquemin et de M. Nihoul (dir.), *Vulnérabilités et droits dans l'environnement numérique*, Larcier, Collection de la Faculté de droit de l'UNamur, 2018
- N. de Marcellis-Warin, F. Marty, E. Thelisson, T. Warin, « Intelligence artificielle et manipulations des comportements de marché : l'évaluation ex ante dans l'arsenal du régulateur », *RIDE*, 2020/2, t. XXXIV, p. 203
- M. Mercat-Bruns, « Le concept d'inclusion : genèse et continuation », *Dr. Soc.*, 2023, p. 1001 et 2024, p. 81.
- S. Lequette, *Droit du numérique*, Montchrestien, coll. Domat, 2024
- L. Pignatel, *L'émergence d'un neurodroit. Contribution à l'étude de la relation entre les neurosciences et le droit*, Dalloz, Coll. Nouvelle Bibliothèque de Thèses, 2021
- J. Rochfeld, « Les émotions du salarié. Traitement et décisions : quelles limites ? », *Mélanges en l'honneur de Pierre-Yves Verkindt*, LGDJ, 2022, p. 393 et s.
- J. Rochfeld et C. Zolynski, « La valeur des émotions : quel régime pour le “capitalisme mental” ? », *Mélanges en l'honneur de Pierre Sirinelli*, Dalloz, 2022, p. 749 et s.
- R. H. Thaler & C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Penguin, 2009.
- C. Zolynski, M. Le Roy et F. Levin, « L'économie de l'attention. Plaidoyer pour un droit à la protection de l'attention », *Dalloz IP/IT*, 2019, p. 614 et s.

Projet détaillé (détails scientifiques sur le sujet, questions ou verrous abordés, programme et déroulement prévu) et perspectives pour l'équipe/le laboratoire (3 pages maximum) :

I-Détails scientifiques

Le sujet de thèse proposé est novateur. Comme il a été indiqué précédemment, la question de la vulnérabilité numérique n'a pas fait l'objet d'études nombreuses et globales en France et en Europe. L'approche proposée consiste à aborder la vulnérabilité numérique comme un tout, qu'il s'agisse de l'utilisation des outils numériques ou de la compréhension de cet environnement. Elle adopte le prisme des personnes physiques, ce qui diffère de l'angle d'analyse généralement retenu de certains dispositifs, par exemple du cadre juridique de la lutte contre la désinformation (par exemple au moyen de systèmes d'IA générative) ou des interfaces trompeuses qui sont envisagés à travers les pratiques des plateformes en ligne. Le sujet proposé contribuera donc à enrichir l'état des connaissances sur la question de la vulnérabilité dans l'environnement numérique.

Le sujet est un sujet d'actualité et sa portée sociale est certaine. Il pose en effet la question du respect de l'égalité des personnes et de leur inclusion, mais aussi celle du bon fonctionnement démocratique de nos sociétés. À cet égard, rappelons qu'en 2021 (, selon l'INSEE (Insee Première, n° 1953, Juin 2023), 15 % des personnes de plus de 15 ans résidant en France étaient en situation d'illectronisme en 2021 à défaut d'avoir utilisé Internet (13,9%) ou de disposer de compétences numériques suffisantes (1,5%). Les plus touchés sont les plus de 75 ans mais le niveau de diplôme, de vie, la situation sociale en particulier l'isolement, et la profession sont également déterminants.

L'approche retenue est théorique et pratique. Théorique, elle consiste à envisager la vulnérabilité numérique à partir de la personne humaine et non à partir des plateformes numériques, des systèmes d'intelligence artificielle ou des obligations pesant sur les professionnels. Elle propose d'adopter une approche globale de la vulnérabilité numérique entendue à la fois comme la capacité à utiliser les outils numériques et à comprendre l'environnement numérique. Elle conduit à s'attacher à différentes valeurs qui pourraient constituer les fondements de la prise en compte de la vulnérabilité numérique, à savoir la protection de l'égalité des personnes, de leur dignité, de leur autonomie individuelle et décisionnelle mais aussi de la confiance qu'ils peuvent avoir dans l'environnement numérique. Ce questionnement sur les valeurs protégées fait directement écho à la position du Conseil de l'Europe dans sa Convention-cadre sur l'intelligence artificielle du 17 mai 2024, qui rattache le respect de l'autonomie personnelle à la dignité humaine : « Chaque Partie adopte ou maintient des mesures pour le respect de la dignité humaine et de l'autonomie personnelle en ce qui concerne les activités menées dans le cadre du cycle de vie des systèmes d'intelligence artificielle » (article 7). Le rapport explicatif qui l'accompagne précise en ce sens que « L'autonomie personnelle est un aspect important de la dignité humaine, et renvoie à la capacité d'autodétermination des individus, c'est-à-dire leur capacité à faire des choix et à prendre des décisions, y compris sans subir de coercition, et à vivre leur vie librement », ce qui comprend, dans le contexte de l'intelligence artificielle, « que les individus aient le contrôle sur l'utilisation et l'impact des technologies

d'intelligence artificielle dans leur vie et que leur capacité d'action et leur autonomie ne soient pas diminuées pour autant » (Conseil de l'Europe, Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, 133e Session du Comité des Ministres (Strasbourg, 17 mai 2024), Rapport explicatif, pt. 55). La thèse proposée conduira à formuler des propositions d'évolutions législatives pour adapter le droit à l'objectif poursuivi de protection des personnes. Des propositions de textes pourront être formulés, et en particulier l'introduction dans le code civil de dispositions générales concernant la vulnérabilité numérique, pour lesquelles il faudra s'interroger sur leur emplacement dans le code. Plus généralement, la pertinence de consacrer des droits fondamentaux (à l'intégrité numérique ou à disposer d'une alternative au numérique) seront discutés.

L'approche retenue sera également pratique. Elle le sera par la méthode de recherche, qui impliquera une recherche *in situ* auprès de groupes de personnes vulnérables en raison de leur âge (mineurs ou personnes âgées) ou de leur situation personnelle au moyen d'entretiens sur la maîtrise et la compréhension de l'environnement numérique. Des échanges devront également intervenir avec les régulateurs compétents mais aussi le défenseur des droits, qui porte une grande attention à la désinformation et à la lutte contre l'illectronisme. Pour cela, le doctorant s'appuiera sur le réseau de recherche et les partenaires de l'ICREJ.

Pour réaliser ces travaux, au-delà des aspects sociaux du début de thèse, une méthode de recherche classique sera suivie. Elle pourra utilement être nourrie par une approche comparative dans l'hypothèse où des législations de pays tiers ont consacré des dispositions plus protectrices que les nôtres.

La thèse se déroulera donc en quatre étapes :

- 1/ Établissement d'un état des lieux de la vulnérabilité dans l'environnement numérique (6 mois)
- 2/ Étude générale du droit positif de la vulnérabilité dans l'environnement numérique (6 mois)
- 3/ Approche critique et dépassement du droit positif (6 mois)
- 4/ Établissement d'un plan de restitution des travaux et rédaction de la thèse (18 mois).

II-Perspectives pour l'équipe de recherche

Le projet de thèse contribuera à renforcer les recherches menées dans le cadre de l'ICREJ en droit du numérique et en matière de vulnérabilités.

Il s'inscrit pleinement dans la politique de recherche de l'établissement portant sur le numérique, et plus particulièrement sur l'intelligence artificielle (projet Normanthia).

Le projet de thèse fait par ailleurs directement écho aux travaux de recherche menés par le laboratoire GREYC de l'Université de Caen en intelligence artificielle et plus spécialement au rapport entre l'homme et la machine, ainsi qu'aux travaux en neurosciences menés à l'Université de Caen, ce qui permettra d'initier des travaux pluridisciplinaires dans le prolongement du projet de thèse.

En résumé, le projet de thèse présente donc une grande cohérence par rapport aux travaux de l'Unité de recherche et à la politique de recherche de l'Université de Caen. Il

permettra de soutenir et de contribuer à des recherches pluridisciplinaires en matière d'intelligence artificielle et de protection des vulnérabilités.

Principales actions et calendrier détaillés de mise en œuvre :

Du 1/09/2025 au 27/02/2026 : Réalisation d'un état des lieux de la vulnérabilité numérique (entretiens avec des groupes de personnes vulnérables quant à l'accès au numérique, son utilisation et sa compréhension et avec les régulateurs compétents en matière de numérique).

Du 01/03/2026 au 31/08/2026 : Réalisation d'une présentation globale du droit positif (interne et européen) sur la vulnérabilité numérique.

Du 01/09/2026 au 26/02/2027 : Étude critique du droit positif : adaptation des concepts, adaptation du régime (champ d'application, nature des mécanismes protecteurs...), approche de droit comparé.

Du 01/03/2027 au 31/09/2028 : Élaboration de la problématique générale, établissement puis validation d'un plan de restitution des travaux, puis rédaction.

Moyens humains, matériels, financiers ... mis en œuvre et demandés pour atteindre les objectifs :

Pour atteindre les objectifs déterminés ce sont essentiellement des moyens financiers qui devront être employés par l'Institut caennais de recherche juridique pour soutenir le travail de thèse, en particulier le financement des déplacements du doctorant pour la réalisation des entretiens et de l'étude observationnelle. Le financement d'un séjour de recherche à l'étranger devra également être envisagé.

Au-delà, les moyens classiques disponibles dans l'établissement, en particulier la documentation et le PEB seront mobilisés.

Diffusion et capitalisation des résultats :

Résultats scientifiques, publications, valorisation, démarche d'enseignement ou de formation, public visé (le cas échéant)

- Contribution aux travaux de recherche de l'ICREJ (axe numérique et vulnérabilités et droits fondamentaux) notamment aux projets de recherche menés en matière de droit de l'intelligence artificielle et en matière de protection des mineurs et des majeurs.
- Le doctorant contribuera à nourrir les échanges internationaux de l'ICREJ sur les questions de vulnérabilités et de numérique (partenariats avec l'Université de Laval, Québec ; Université de Neuchâtel, Suisse).
- La valorisation des résultats scientifiques pourra être opérée par la publication d'un rapport sur l'état des lieux en matière de vulnérabilité, puis par la présentation des travaux de recherche du doctorant à la fois au sein de l'ICREJ (journée annuelle des doctorants), au sein de la MRSH (pôle vulnérabilité), mais aussi à destination de la

communauté des juristes (publications scientifiques) et du grand public (Fête de la science, fête du droit).

Actions prévues dans le cadre de la diffusion de la Culture Scientifique, Technique et Industrielle (CSTI) en supplément des actions Fêtes de la Science (1 page maximum) :

Participation à la nuit du droit et aux actions pour la science et la société déployés par l'ICREJ.

IMPACTS DU PROJET

Impacts sur l'équipe :

Retombées attendues (équipe, établissement ou organisme d'accueil)

Renforcement des axes de recherche « Numérique » et « Vulnérabilités » et droits fondamentaux par le traitement d'un sujet inexploré en France sous le prime adopté. Contribution à faire de Caen l'un des centres de recherche reconnu sur ceux deux thématiques, ce qui se traduit à la fois par une notoriété internationale (nombreuses invitations des chercheurs à l'étranger) et par la sollicitation des pouvoirs publics pour des missions d'expertise sur ces deux thématiques.

La thèse s'inscrit plus généralement dans la dynamique de l'établissement qui est porteur d'un projet de déploiement des formations et de projets de recherche en matière d'intelligence artificielle (Normantheia) auquel la faculté de droit et l'ICREJ sont parties.

Impacts sur le territoire :

Retombées attendues (liens sociaux-économiques, rayonnement, CSTI...)

Les résultats du travail de recherche bénéficieront directement aux décideurs publics et aux acteurs économiques régionaux qui pourront s'appuyer sur eux comme élément de définition de politiques de gestion des vulnérabilités numériques.

AVIS DE LA DIRECTION DU PROJET

Directeur de thèse

Nom et Prénom : DOUVILLE Thibault, professeur des universités

Etablissement / Organisme de rattachement :

Avis motivé du directeur de thèse sur la recherche envisagée en ce qui concerne les objectifs scientifiques et technologiques poursuivis et leur place dans les orientations de recherche du laboratoire d'accueil :

Avis totalement favorable. Le projet est novateur, inexploré, il permettra d'enrichir l'état des connaissances concernant la prise en compte par le droit des situations de vulnérabilité. La méthodologie de recherche s'appuie sur une étude de terrain pour en tirer des

enseignements critiques quant à l'état du droit et les évolutions nécessaires de celui-ci. Le projet s'inscrit en outre dans la stratégie et les axes de recherche de l'ICREJ et de l'Université de Caen Normandie. Il permettra de renforcer l'équipe de recherche de l'Université de Caen travaillant sur la régulation du numérique.

Date : 20/01/2025

Nom, Prénom : Professeur Thibault DOUVILLE

Information sur les derniers doctorants encadrés (maximum 5 derniers doctorants):

Lucile Dutat, La cybersécurité des systèmes d'intelligence artificielle, début 01/01/2025 (contrat doctoral ANR)

Tristan Quilès, Le devoir de vigilance en matière de cybersécurité : étude à propos des chaînes de sous-traitance, début 20/11/2023 (financement CIFRE)

Sarah Porcher, L'assurance du cyber risque, codirection avec le Professeur Pierre-Grégoire Marly, début : 10/09/2019 (soutenance prévue en 2025)

Sarah Markiewicz, Le document électronique, début : 28/11/2018 (soutenance 2025).

Le directeur du laboratoire indiquera l'adéquation de ce projet avec la stratégie du laboratoire d'accueil :

Projet en total adéquation avec les axes stratégiques du laboratoire, il s'inscrit en effet à la fois dans l'axe numérique et l'axe vulnérabilités et droits fondamentaux. En outre, ce projet renforce l'équipe en cours de constitution en droit du numérique à l'Université de Caen Normandie. Avis fortement favorable de la direction du laboratoire.

Date : 21/01/2025

Nom, Prénom : Professeur Eléonora BOTTINI



Le directeur du laboratoire devra fournir **au plus tard le 10 mars** (de façon séparée du dossier) **un interclassement (avec justification) des demandes du laboratoire** incluant les allocations établissement et 100% région (1 classement par site pour les Unités multisites) *validé par son conseil d'Unité. Merci de ne pas indiquer d'interclassement dans ce document de soumission*