Caen on7 mai 2025

SUBJECT: Doctoral grants 2024 - Note - Recruitment of doctoral students

Employment information		
	Organisation / Company	University of Caen Normandy
	Area of research	Law
	Researcher profile	Doctoral student
	Country	France
	Deadline for applications	**Friday 6 June 2025, 12 noon** Send the single document (PDF) by e-mail to the DROIT NORMANDIE doctoral school. The acknowledgement of receipt will not be taken as proof of the admissibility of the application.
	Type of contract	Doctoral contract
	Employment status	Fixed-term contract
	Is the post funded by the EU Research Framework Programme?	No
	Is the job linked to a staff position within a research infrastructure?	Doctoral student at ICREJ (Institut caennais de recherche juridique) - UR 967.

Campus 1
Esplanade de la Paix - CS 14032 - 14032 Caen cedex 5
02 31 56 55 51
ufr-droit.unicaen.fr

Description of the offer		Digital vulnerability Digital vulnerability
	Description of position and doctoral project (targeted and funded)	*<u>French version</u>* *Illectronism, misinformation, misleading interfaces, manipulation of emotions - these are all situations that correspond to digital vulnerability suffered by an individual. Digital vulnerability can take two main forms: it can be personal, linked to a physical or intellectual weakness, or contextual, due in particular to an imbalance of power or the complexity of the environment in which the individual finds him or herself.* *No transversal study of digital vulnerability has been carried out by French legal doctrine, which is only interested in certain aspects of it. At the same time, research projects are underway in other countries on digital vulnerability in relations between the administration and its users.* *This thesis project is concerned with the overall study of digital vulnerability in relationships between private individuals. Its aim is to critically analyse the measures in place to address this issue and to identify their shortcomings. The doctoral research will explore the fight against e-vulnerability, the prohibition of manipulative AI and the risk management of emotional recognition techniques. Proposals for legislative changes could be made, in particular by enshrining new rights (right not to use electronic communications, right to intellectual integrity, etc.). The research will be based on a study of legislative initiatives in other countries and on an appropriate research methodology, which will involve drawing up an inventory of digital vulnerability - in particular 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 input for the doctoral student's reflections. The thesis will advance the state of knowledge in digital law and vulnerability.* *<u>English version</u>*

		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. *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.* *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.*
	Salary placement	2100-2300 € / month.
Requirements		
	Admission	After the candidate has ***appeared*** before a jury on **Tuesday 10 June 2025, from 1 pm. 30**, and ***deliberation*** by the Restricted

		Council of the ED Droit Normandie, the student who meets the following admission requirements will be admitted to prepare a thesis on the use of weapons by the forces of law and order: (1) Hold a master's degree (grade national de master) in law (private or public) on [1]October 2025, with honours. (2) Be able to present, during the ***audition***, their academic background, the rationale for their analysis of the subject and the timetable for their research over the 3 years of the doctoral contract. (3) Have written a ***dissertation on a subject in digital law on the theme of digital vulnerability.***
	Eligibility	To apply for the thesis project funded by the Université de Caen Normandie, the applicant must hold a master's degree in digital law or be in the process of doing so by [1]September 2025. In addition, candidates should have specialised training in digital law, as well as in the law of freedoms and international and European law (in particular the law of the European Convention on Human Rights). An interest in comparative law is a plus.
Applications		
		The application must be submitted in the form of a single PDF document, with numbered pages. The entire document must contain : (1) A ***covering letter*** describing the candidate's research interests and explaining the reasons for applying. (2) A quarterly research programme over 3 years. (3) A ***curriculum vitae*** (CV). (4) ***Copies of transcripts*** of marks for the bachelor's degree in law and master's degree 1 in law (private or public), and master's degree 2 if obtained.

		(5) The ***contact details*** of two referees or people in a position to recommend the candidate for the doctoral research project targeted and funded. (6) The defended ***research dissertation*** or a presentation of the research work in progress for a student who is currently doing a Master 2
Place(s) of work		University of Caen (Normandy, France) Esplanade de la Paix. - 14032 Caen. UFR Droit (bât. D.). - ICREJ.
Where to find us		Mail of the doctoral school : *esther.camus@unicaen.fr* *ed98.dn@unicaen.fr* *penelope.cochennec@unicaen.fr* *droit.recherche@unicaen.fr*
Contact		Mail of the thesis supervisor : *Thibault.douville@unicaen.fr*

As of the 2024 campaign, Normandy's universities and engineering schools have introduced a **single** submission and evaluation process for institutional grants and 100% regional grants, together with a single submission and evaluation timetable.

Please tick at least one box (you may tick both boxes if you are making two submissions).
The request concerns :

X An establishment allowance X

A regional allowance 100

(note: applications for INSA allowances must be completed using the 50% form)

Please complete the common section (pages 2-4) for all applications. In the case of an application for a regional allowance (or a double application), also complete the corresponding section (pages 5-8). It is not necessary to complete the following items, which will be completed by the institution if the application is pre-selected*: "Attachment of the operation to the Strategic Partnership Agreement", "Administrative contact at the supporting institution"; and "Attachment to the SPA if the thesis subject does not correspond to any area of the S3".* Similarly, the "Mandatory documents to be attached to the application" will be sent by the institution.

Deadline for online submission on the Normandie Université platform: 24 January 2025

COMMON PART: to be completed in all cases (submission to the establishment or region)

GENERAL INFORMATION

Project title: Digital vulnerability

Project acronym: Digital-vulnerability

Supporting institution: University of Caen

Project location (name of laboratory and address): Institut caennais de recherche juridique/ICREJ - Unité de recherche 967 - Université de Caen Normandie

Project discipline: Private Law and Criminal Sciences - 01

Project coordinator in the host laboratory :

Last name: Douville

First name: Thibault

Email thibault.douville@unicaen.fr

If laboratory on several sites, specify location: City / Campus / Hosting institution Research team (if any): Institut caennais de recherche juridique/ICREJ Address: Esplanade de la paix

N° - Street name :

Postcode: 14000

Town: Caen

Doctoral school to which the thesis supervisor belongs: *ED Droit Normandie*

Project implementation :

From *01/09/2025 to 31/08/2028*, i.e. a 36-month project.

PROJECT SUMMARY

A summary of the project (maximum 2000 characters including spaces for each version):
Description intended an uninformed/new audience on the subject. This paragraph may be used in communication documents if the project receives funding.
French version

Illectronism, misinformation, misleading interfaces, manipulation of emotions - these are all situations that correspond to digital vulnerability suffered by an individual. Digital vulnerability can take two main forms: it can be personal, linked to a physical or intellectual weakness, or contextual, due in particular to an imbalance of power or the complexity of the environment in which the individual finds him or herself.

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

The thesis project involves an overall study of digital vulnerability in relationships between private individuals. It aims to critically analyse the measures in place to address this issue and to identify their shortcomings. The doctoral research will explore the fight against e-vulnerability, the prohibition of manipulative AI and the risk management of emotional recognition techniques. Proposals for legislative changes could be made, in particular by enshrining new rights (right not to use electronic communications, right to intellectual integrity, etc.). The research work will be based on foreign legislative initiatives and on an appropriate research methodology, which will involve drawing up an inventory of digital vulnerability based on a number of typical situations. This inventory will provide input for the doctoral student's reflections. The thesis will contribute to the state of knowledge in digital law, but also in terms of controlling the phenomenon of vulnerability.

English version

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.

Keywords related to the project (5 words maximum) :
Vulnerability, Artificial intelligence, Illectronism, Disinformation. Individual autonomy

PRESENTATION OF THE PROJECT :

Context and objectives (maximum 2 pages): specify whether the research is incremental (continuation, reinforcement of an existing theme) or innovative (new subject), local-national-international positioning, bibliography.

The issue of digital vulnerability has not been the subject of much research in French legal doctrine, even though there are many manifestations of it in the digital environment. In Europe, research is underway, particularly in Belgium (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) and the Netherlands (Pr. Sofia Ranchordas, Tilburg University, research project devoted to the theme: Vulnerability in the Digital Administrative State) on vulnerabilities in relations between administrations and users. The proposed approach, on the other hand, looks at vulnerability in relations between private individuals.

The two forms of vulnerability identified for individuals can be found in the digital environment. Vulnerability may be personal, where the person is unable to exercise the attributes of their personality due to a personal impairment (physical or intellectual) such as a disability; vulnerability may also be circumstantial, linked to the context in which they find themselves due to an imbalance of power with a third party or the complexity of the environment in which they find themselves (on these two approaches to vulnerability: X. Largarde, "Foreword", 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). It can take the form of an inability to access the internet, to use digital tools, to perceive the veracity of information or to understand it.

The issue of digital vulnerability is all the more relevant given that technological developments are encouraging the development of deceptive digital environments (for example, through the deployment of deceptive interfaces designed on the basis of research carried out in the behavioural sciences) and, more recently, the deployment of artificial intelligence systems, in particular generative artificial intelligence, which give rise to the risk of misinformation, while systems capable of manipulating emotions by playing on stimuli are also being developed.

are developed. That said, digital tools can also be a response to people's vulnerability by helping them to do things online or better understand the information they are given. One example is the crucial role played by voice assistants.

In this context, the thesis adopts a global approach. Its first aim will be to take stock of all the mechanisms ensuring the protection of people in vulnerable situations in the digital environment and to study them critically. Think, for example, of the regime for combating illiteracy, which is limited in scope and could be generalised in the Civil Code. Another example is the ban on AI systems that use subliminal techniques below the threshold of a person's consciousness or deliberately manipulative or deceptive techniques, which raises the question of the boundary between these techniques and those used in the digital environment.
"We should also bear in mind the use of emotion recognition techniques, the aim of which is to profile the people concerned. Another example is the use of emotion recognition techniques, the aim of which is to profile the individuals concerned. Some of these techniques classed as high-risk intelligence , while others are subject to a transparency regime. Finally, there is the transparency requirement for artificial intelligence systems interacting with individuals, the scope of which is open to question. Beyond these specific provisions, the question of how to take account of the consequences of exploiting people's vulnerabilities in civil law arises, for example through the obligation provide pre-contractual information, the integrity consent and, more generally, the protection of people's dignity.

The thesis will also look at the protection of personal vulnerability from a forward-looking perspective in the light of announced developments in technology and usage. The 'dematerialisation' of the relationship between man and machine through the announced deployment of voice assistants based on artificial intelligence systems raises questions about the loyalty of these systems, the protection of consent and the quality of output, for example. In this respect, the relationship with time, due to the instantaneity of digital systems, which is an element of protection against certain vulnerabilities, such as the evolution of protective formalisms, will be raised.

New types of response to digital vulnerabilities will need to be devised, such as equivalence of effectiveness (and not functional equivalence of formalisms), justification of the information offered or of the treatment of one person in relation to another placed in a comparable situation. More generally, the usefulness of enshrining a right not to use electronic communications (i.e. a right to an alternative to digital communications) as well a right to digital integrity or dignity (along the lines of certain initiatives such as those in some Swiss cantons) could form the basis of the treatment of digital vulnerability. Beyond the legal treatment of vulnerability in the digital environment, the thesis will contribute to the reflection on the relationship between man and machine as well as the general theory of vulnerability, whether in terms of its foundations, its characteristics or its regime.

Selected bibliography :

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 and S. Mauclair (eds.), Intelligence artificielle & droits fondamentaux, Editions L'Epitoge, coll. L'Unité du Droit, 2022

A. Boujeka and M. Roccati (eds.), 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 seq.

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... 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 and M. Nihoul (eds.), 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 and 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 seq.

J. Rochfeld and C. Zolynski, "La valeur des émotions : quel régime pour le "capitalisme mental" ?", Mélanges en l'honneur de Pierre Sirinelli, Dalloz, 2022, p. 749 et seq.

R. H. Thaler & C. R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness, Penguin, 2009.

C. Zolynski, M. Le Roy and F. Levin, "L'économie de l'attention. Plaidoyer pour un droit à la protection de l'attention", Dalloz IP/IT, 2019, p. 614 et seq.

CNIL, The shape of choices, Personal data, design and desirable frictions, Cahiers IP Innovation & Prospective, n° 6, 2019

Detailed project (scientific details on the subject, questions or issues addressed, programme and planned timetable) and prospects for the team/laboratory (3 pages maximum) :

I-Scientific details

The subject of the proposed thesis is innovative. As mentioned above, the issue of digital vulnerability has not been the subject of many comprehensive studies in France and Europe. The proposed approach is to look at digital vulnerability as a whole, in terms of the use of digital tools and the understanding of this environment. It adopts the prism of individuals, which differs from the angle of analysis generally adopted for certain systems, for example the legal framework for combating disinformation (for example by means of generative AI systems) or misleading interfaces, which are considered through the practices of platforms. The proposed topic will therefore contribute to state of knowledge on the issue of vulnerability in the digital environment.

The subject is a topical one, and its social significance is clear. It raises the question of respect for the equality of individuals and their inclusion, but also that of the proper democratic functioning of our societies. In this respect, it should be remembered that in 2021 (according to INSEE (Insee Première, No. 1953, June 2023)), 15% of people aged 15 and over living in France were in a situation of "illectronisme" because they had not used the Internet (13.9%) or had insufficient digital skills (1.5%). The people most affected are the over-75s, but the level of education, standard of living, social situation (particularly isolation) and occupation are also decisive factors.

The approach adopted is both theoretical and practical. Theoretically, it consists of considering digital vulnerability from the point of view of the human being and not from the point of view of digital platforms, artificial intelligence systems or obligations on professionals. It adopting a global approach to digital vulnerability, understood as both the ability to use digital tools and to understand the digital environment. It leads us to focus on the various values that could form the basis for taking digital vulnerability into account, namely the protection of people's equality, dignity, individual autonomy and decision-making, as well as the trust they may have in the digital environment. This questioning of the values protected directly echoes the position of the Council of Europe in its Framework Convention on Artificial Intelligence of 17 May 2024, which links respect for personal autonomy to human dignity:
"Each Party shall adopt or maintain measures for the respect of human dignity and personal autonomy with regard to activities carried out in the context of the life cycle of artificial intelligence systems" (Article 7). The accompanying explanatory report specifies that "personal autonomy is an important aspect of human dignity, and refers to the capacity for self-determination of individuals, i.e. their ability to make choices and decisions, including without coercion, and to live their lives freely", which includes, in the context artificial intelligence, "that individuals have control over the use and impact of technologies

(Council of Europe, Council Europe Framework Convention Artificial Intelligence and Human Rights, Democracy and the Rule of , 133rd Session of the Committee of Ministers (Strasbourg, 17 May 2024), Explanatory Report, pt.
55). The proposed thesis will lead to proposals legislative changes adapt the law to the objective of protecting individuals. Proposals for texts could be formulated, and in particular the introduction into the civil code of general provisions concerning digital vulnerability, for which it will be necessary to consider their location in the code. More generally, the relevance of enshrining fundamental rights (to digital integrity or to have an alternative to digital technology) will be discussed.

The approach adopted will also be practical. This will be reflected in the research method, which will involve *on-site* research with groups of people who are vulnerable because of their age (minors or the elderly) or their personal situation, by means of interviews on their mastery and understanding of the digital environment. Discussions will also need to take place with the relevant regulators, as well as with the Défenseur des droits, which pays a great deal of attention to misinformation and the fight against illiteracy. To achieve this, the doctoral student will draw on ICREJ's research network and partners.

In order to carry out this work, over and above the social aspects at the start of the thesis, a traditional research method will be followed. It could usefully be supplemented by a comparative approach in the event that legislation in third countries has enshrined more protective provisions than our own.

The thesis will therefore be carried out in four stages:

1/ Drawing up an inventory of vulnerabilities in the digital environment (6 months)

2/ General study of positive law on vulnerability in digital environment (6 months)

3/ A critical approach to positive law (6 months)

4/ Drawing up a plan for presenting the work and writing the thesis (18 months).

II- Prospects for the research team

The thesis project will help to strengthen the research carried out ICREJ on digital law and vulnerabilities.

It fully in line with the institution's research policy on digital technology, and more specifically on artificial intelligence (Normanthiia project).

The thesis project also directly echoes the research work carried out by the GREYC laboratory at the University of Caen on artificial intelligence, and more specifically on the relationship between man and machine, as well as the neuroscience work carried out at the University of Caen, which will enable multidisciplinary work to be initiated as an extension of the thesis project.

In summary, the thesis project is highly consistent with the work of Research Unit and the research policy of the University of Caen. It

will support and contribute to multi-disciplinary research into artificial intelligence and vulnerability protection.

Main actions and detailed timetable for implementation :

From 1/09/2025 to 27/02/2026: Carrying out an assessment of digital vulnerability (interviews with groups of people who are vulnerable terms of digital access, use and understanding, and with the regulators responsible for digital issues).

From 01/03/2026 to 31/08/2026: Production of a comprehensive presentation of positive law (domestic and European) on digital vulnerability.

From 01/09/2026 to 26/02/2027: Critical study of positive law: adaptation of concepts, adaptation of the system (scope, nature of protective mechanisms, etc.), comparative law approach.

From 01/03/2027 to 31/09/2028: Drawing up the general problem, establishing and validating a plan for reporting the work, then writing the report.

Human, material and financial resources used and requested to achieve objectives :

To achieve the objectives setthe Caen Institute for Legal Research will essentially have to use financial resources to support the thesis work, in particular to fund the doctoral student's travel to conduct interviews and carry out the observational study. Funding for a research trip abroad should also be considered.
Beyond that, the traditional resources available in the institution, in particular documentation and ILL, will be mobilised.

Dissemination and capitalisation of results :
Scientific results, publications, promotion, teaching or training approach, target audience (if applicable)

- Contribution to ICREJ's research work (digital vulnerability and fundamental rights), in particular to research projects on artificial intelligence law and the protection of minors and adults.
- The PhD student will contribute to ICREJ's international exchanges on vulnerability and digital issues (partnerships Université de Laval, Quebec; Université de Neuchâtel, Switzerland).
- The scientific results could be used to publish a report on the state of the art in terms of vulnerability, and then to present the doctoral student's research work both within ICREJ (annual doctoral students' day) and within the MRSH (vulnerability unit), as well as for the general public.

the legal community (scientific publications) and the general public (Fête de la science, Fête du droit).

Actions planned as part of the dissemination of Scientific, Technical and Industrial Culture (STIC) in addition to the Fêtes de la Science actions (1 page maximum) :

Participation in ICREJ's law night and actions for science and society.

PROJECT IMPACTS

Impact on the team :
Expected spin-offs (team, host institution or organisation)

Strengthening of the 'Digital' and 'Vulnerabilities' and fundamental rights research areas by tackling a subject unexplored in France under the prime adopted. Helping to make Caen one of the world's leading research centres in these two areas, which is reflected both in its international reputation (numerous invitations to researchers abroad) and in the fact that it is called upon by public authorities to provide expertise in these two areas.

More generally, the thesis is part of the institution's dynamic, which is behind a project to roll out training and research projects in artificial intelligence (Normanthiia), to which the Faculty of Law and ICREJ are party.

Impact on the region :
Expected spin-offs (social and economic links, outreach, CSTI, etc.)

The results of the research work will be of direct benefit to public decision-makers and regional economic players, who will be able to use them as a basis for defining policies for managing digital vulnerabilities.

OPINION OF THE PROJECT MANAGEMENT

Thesis supervisor

Surname and First Name: DOUVILLE Thibault, University Professor Affiliated

Institution/Organisation :

A reasoned opinion from the thesis supervisor on the proposed research, with regard to the scientific and technological objectives pursued and their place in the research guidelines the host laboratory:

Totally favourable opinion. The project is innovative and unexplored, and enhance knowledge of how the law takes account of situations of vulnerability. The research methodology is based on a field study, from which the following conclusions can be drawn

critical lessons about the state of the law and the changes that need to be made. The project is also in line with the strategy and research priorities of ICREJ and the University of Caen Normandie. It will strengthen the research team at the University of Caen working on digital regulation.

Date: 20/01/2025
Full name: Professor Thibault DOUVILLE

Information on the last doctoral students supervised (maximum 5 last doctoral students):

Lucile Dutat, Cybersecurity of artificial intelligence , start 01/01/2025 (ANR doctoral contract)
Tristan Quilès, Le devoir de vigilance en matière de cybersécurité : étude à propos des chaines de sous-traitance, début 20/11/2023 (CIFRE funding)
Sarah Porcher, L'assurance du cyber risque, co-directed with Professor Pierre-Grégoire Marly, start date: 10/09/2019 (defence expected in 2025)
Sarah Markiewicz, The electronic document, start: 28/11/2018 (defence 2025).

The laboratory director will indicate the project fits in with the host laboratory's strategy:

The project is fully in line with the laboratory's strategic priorities, as it is part of both the digital axis and the vulnerabilities and fundamental rights axis.
In addition, this project will strengthen the team currently being set up in digital law at the Université de Caen Normandie. Strongly favourable opinion from the laboratory management.

Date: 21/01/2025
Full name: Professor Eléonora BOTTINI

By 10 March at the latest, the laboratory director must provide (separately from the application) **an inter-ranking (with justification) of the laboratory's applications,** including establishment and 100% regional ~~allocations (1 ranking per~~ site for multi-site units), *validated by the Unit Council. Please do not indicate any inter-ranking in this submission document.*