Law and Vulnerability Disclosure

Project Report

University of Rennes 1

Master's Degree in Cybersecurity

Elvin Maubert, Baptiste Le Piouf, Luca Pourceau

May 16, 2025

Abstract

In a time of increasing cyber threats, responsible vulnerability disclosure plays a key role in securing digital systems. However, in France, the legal framework surrounding such disclosures remains unclear and often risky for ethical hackers acting in good faith. Through legal analysis and interviews with cybersecurity professionals, we identify significant legal gaps and propose practical recommendations. Our goal is to help establish a safer environment for researchers and companies alike, by balancing security needs with legal protection.

Contents

1 Introduction

In a world where cyber threats are growing more frequent and more sophisticated, the way we handle the disclosure of security vulnerabilities has become a critical issue. As digital systems become more central to daily life, from government services to personal data and industry infrastructure, the damage caused by an unpatched vulnerability can be severe financially, socially, and even politically.

Ethical hackers, researchers, and cybersecurity professionals play a key role in identifying and reporting these flaws before they can be exploited. Yet, in France and many other countries, the legal system still struggles to make a clear distinction between those who act with good intentions and those who do harm. Entering a system without permission remains a criminal offense, even when done to improve security. This legal uncertainty creates fear and hesitation, discouraging responsible disclosure and potentially leaving systems vulnerable.

At the same time, institutions like ANSSI and CERT-FR, along with global frameworks such as the CVE system, have created channels to help coordinate safe and responsible disclosures. Companies, too, are developing their own policies to manage these reports. However, there is still no unified or fully protective legal framework for those who report vulnerabilities especially when they do so independently or anonymously.

This topic is especially relevant today, as societies rely more than ever on digital infrastructure. Without clear protections and procedures, we risk pushing away those who help keep systems secure. This research aims to better understand the balance between cybersecurity needs and legal boundaries, and to shed light on the gaps that still need to be addressed to protect ethical hackers and the public interest.

2 Methodology

At the beginning of the project, our main objective was to explore French law more broadly in order to better understand legal texts, articles, different types of penalties, and how the legal system works in general. This step was essential to approach the rest of the project more effectively. It also revealed a genuine interest in this field, which was a refreshing change from our usual focus on computer science.

Next, our goal was to gather as much information as possible and better understand the current legal framework for vulnerability disclosure. We came across many official documents, including articles from the Defense Code. Navigating through these legal texts helped us become more comfortable with the French legal system and its logic. We also deepened our understanding of technical tools we had only briefly encountered before, such as anonymization (in the technical part) and CVEs (in the disclosure process).

However, after a certain point, our research started to become repetitive and lacked concrete results. What we were missing was field experience, input from professionals who deal with real-world situations every day. This is why we decided to meet them during cybersecurity events. These interactions not only renewed our motivation, but also helped us push our research further and even raised new and thought-provoking questions.

In the end, by constantly analyzing this incomplete legal framework, we were able to identify its limits and develop mature recommendations that could one day help reduce the legal uncertainty faced by researchers, companies, and the State.

3 Meeting Experts

One of the most valuable aspects of this project was the opportunity to meet professionals working in the field. Despite extensive online research, nothing compares to speaking with experts who deal with real-world situations on a daily basis. Most of these exchanges took place during cybersecurity events such as BreizhCTF (Rennes) and THCon (Toulouse), and they allowed us to deepen our understanding of the topic. Some of these professionals remained in contact with us after the events, showing interest in our work and helping us by answering

questions via email.

These discussions revealed a somewhat surprising fact: cybersecurity law is almost completely unknown to around 90% (to avoid overgeneralizing) of the professionals we spoke to. This lack of awareness is mostly due to the protection offered by contracts in corporate settings. During audits and penetration tests, the limits and authorizations for accessing information systems are clearly defined in the signed contract. If the contract is violated, it is typically considered a breach of labor law rather than a violation of the laws protecting information systems from unauthorized access.

Originally, our goal was simply to gather professional opinions on the topic, but our focus shifted toward the personal experiences of researchers who operate outside the scope of such contracts, and are therefore truly exposed to the legal system. In all the situations described to us, the vulnerabilities were reported directly to the affected companies, who often welcomed the reports, even when submitted anonymously. Our attempt to study legal consequences turned out to be more complicated than expected. Very few criminal procedures have been initiated over vulnerability disclosures, and some researchers tend to remain discreet about their actions. Indeed, a hacker whose activities lie on the legal borderline, or even cross it, is unlikely to share their experience publicly, for fear of being identified or facing retaliation.

In the end, these conversations were extremely valuable. Not only did they help answer some of our questions, but more importantly, they raised new important ones, thought-provoking questions from professionals who offered a fresh, expert perspective on the topic.

City	Organization	Name	Role / Position
Toulouse	Sopra Steria	Jérémie Dhune Simon Delayen Lilian Marié Olivier Rollat	Security expert and pentesters
	Orange Cyber Defense	Jean-Pascal Thomas	Vulnerability reports section
Rennes	Synacktiv	—	Security experts and pentesters
	YesWeHack	—	
	ANSSI	—	

4 Results & Recommendations

A legal protection based on judgment As explained in the white paper, ANSSI provides legal protection to individuals who report vulnerabilities, as stated in Article L.2321-4 of the Code of Defense. However, this protection is based on the authority's assessment of the researcher's good faith. This creates a sense of legal uncertainty for researchers, who take risks and may hesitate to contribute, even though this ecosystem is essential in the field of cybersecurity. In most cases, vulnerabilities are reported in a constructive and cooperative way, as long as the researcher hasn't abused the system during their investigation.

Unfortunately, good faith cannot be clearly defined in law, as it depends on the context and the researcher's intention. What's really needed is better communication and clearer guidance on what is acceptable during vulnerability research, especially when it involves remaining connected to a system, collecting or sending files (which could be seen as suspicious), or triggering exploitation that causes damage. These actions, even if unintentional, may appear malicious and be judged as such by both ANSSI and the affected organizations, which still have the right to report the case to the public prosecutor.

CVE overreliance on the US government funding As we looked into the CVE program, we found that while it's a key part of global cybersecurity by centralizing vulnerabilities, it also has some weaknesses, especially when it comes to funding. The program is mainly financed by

the US Department of Homeland Security, through CISA. But, during our research, a breaking news highlighted the fact that this dependence can occurs to be a real problem for the sustainability of the program. Indeed, on April 16 2025, that funding temporarily expired and wasn't renewed for several hours.

This situation showed us just how fragile the program can be. Relying on a single source of funding while not being a public institution makes it more vulnerable to political changes. And even if the program created the CVE foundation to gather fund from other sources having funding from private entity could raise some trust problems about the independence of CVE.

One point of improvement could be to establish a similar institution but on the public side. It would remain a centralized database that could bring more transparency to the system. It seems that the European Union want to develop a similar entity with the creation of the European Vulnerability Database managed by the European Union Agency for Cybersecurity (ENISA) made operational in May 2025. Having this kind of program at the European level enables them to have a greater impact.

Legal framework Our analysis of the French legal framework has revealed numerous shortcomings. Firstly, it is worth noting that this framework is neither unnecessarily strict nor non-existent, as one might have thought, but rather its main issue is somewhat more complex. It stems from the concept of authorization, which fails to consider the context in which researchers and hackers must operate when disclosing vulnerabilities. Indeed, the problem lies in the fact that the legislation does not take into account that the actions it penalizes under articles 323-1 to 323-8 of the Penal Code are essential for researchers in the process of vulnerability discovery. In practice, without the explicit authorization of the owner of an information system, a researcher is in no way legally permitted to test the security of that system and subsequently report vulnerabilities. We observed a concrete example of this issue when discussing a case judged by the Albi Criminal Court (TJ d'Albi, June 6, 2024). As explained in the white paper, the court clearly stated that the good intention claimed by the defendant was irrelevant as long as he did not have permission to access the system. Furthermore, there is also no mechanism to exempt a hacker from criminal liability, even if they manage to prove their good faith.

Mitigations One of the main obstacles to responsible vulnerability disclosure is the lack of authorization to access a system, even when the researcher's intention is ethical and focused on finding vulnerabilities. Today, the only framework that sets any limits are the internal disclosure policies defined by companies. Although these policies have no legal value by themselves, they have strong potential to be effective. If made mandatory, similar to how privacy policies are now widespread, the legal system could consider them as a formal reference when evaluating a disclosure. In such a case, protection could be automatically granted to researchers as long as they follow the stated rules, and the notion of "good faith" would no longer be necessary. This would reduce the legal uncertainty currently felt by many researchers.

We can imagine a few scenarios that would help ensure a fair and balanced framework. For example, if a company does not publish a disclosure policy, it could either be held accountable for that omission, or, if a researcher discloses a vulnerability, their actions could still be judged under the current "good faith" approach, but with greater tolerance, since the lack of guidance was the fault of the company.

This would give companies the freedom to define their own legitimate rules and could range from strict prohibitions to more open approaches allowing researchers to test their systems under certain conditions. However, this freedom should come with support, especially from ANSSI, which could help companies better understand the risks and protections associated with setting such limits. This would reduce the chance of misunderstandings or oversights that could unintentionally expose companies to more openness than they intended.

What we aim for is a mutual understanding between researchers and companies. One possible approach would be to make companies' disclosure policies apply as soon as a researcher begins vulnerability testing. But this would require defining what qualifies as vulnerability research, something difficult to pinpoint, since it can include a wide range of techniques, including physical penetration testing or phishing. Another option would be to have researchers explicitly agree to the policy before testing, like signing an agreement as a contract. However, this would require linking the researcher's identity to the agreement, which would eliminate any possibility of anonymity.

To conclude, while we are not legal experts, we believe that improvements are clearly possible. From our perspective as computer scientists, creating a stronger and more protective framework seems achievable—one that would allow researchers to work safely, and companies to regularly benefit from valuable insights to improve their system security.

5 Acknowledgment

We would like to thank our supervisor, Hermine Cappé, for her involvement in this project. Her support was extremely valuable and allowed us to explore a field in which we had no prior knowledge, but which turned out to be both interesting and enriching.

We also thank Christèle Jacq-Arnoult, Head of Ecosystem Relations at CyberSchool, for her precious help in connecting us with professionals in the field. Her support greatly contributed to the progress of our research.

We are grateful to Jérémie Dhune, as well as Olivier Rollat, Simon Delayen, and Lilian Marié from Sopra Steria, for the quality of their discussions, their insights, and the concrete examples they shared. Their interest in our topic strengthened our motivation and helped guide our work.

We would also like to thank Jean-Pascal Thomas from Orange Cyberdefense for the time he dedicated to us and his availability in answering our questions.

Many thanks as well to the teams at Synacktiv in Rennes for their technical expertise, and to YesWeHack for their valuable input on bug bounty programs and their role in the responsible disclosure ecosystem.

Finally, we thank ANSSI for the resources it made available, which significantly contributed to our reflection on the French regulatory framework.

To all of you, thank you for your valuable contribution to this research.