Is the Road to Hell Paved with Good Intentions? A Criminological and Criminal Law Analysis of Prospective Regulation for Ethical Hacking in Italy and the EU*

Gaia Fiorinelli[1*] and Maria Vittoria Zucca[1,2]

[1] *Sant'Anna School of Advanced Studies, Pisa, Italy*
[2] *IMT School for Advanced Studies, Lucca, Italy*

Abstract

The article aims to contribute to the current research on regulatory frameworks and best practices for ethical hacking, from the perspective of criminology and criminal law, providing insights into the Italian legal system that may also inform EU-wide regulations in this domain. The research employs a multidisciplinary approach by: (i) conducting a historical and criminological analysis of the contemporary "renaissance" of ethical hacking, which includes analyzing the rules of engagement in BBPs and the key factors influencing hackers' choices between responsible disclosure and malicious exploitation of vulnerabilities; (ii) addressing the prevailing uncertainty about the legal qualification of ethical hacking, by assessing the criminal regime that might still be applicable to "well-intentioned" computer intrusions in Italy; (iii) providing a comparative perspective on EU legal systems that have decriminalized or otherwise incentivized ethical hacking practices as pivotal tools for enhancing a holistic notion of cybersecurity.

Keywords

Ethical hacking, Vulnerability disclosure, Cybercrime, Cybersecurity, Criminal Law, Criminology

1. Introduction

In a landscape where cyber threats are growing in both number and complexity [1], public institutions and private companies increasingly rely on "vulnerability researchers" as crucial allies in building cybersecure systems, networks, and software [2]. Nevertheless, only a few States in the EU already have a fully established national policy to tackle the legal risks arising from this activity [3]; among the various legal risks (copyright, data protection, etc.), criminal law is considered to be the most relevant barrier in establishing national policies for vulnerability research and disclosure [3, 4].

In this regard, Directive (EU) 2022/2555 (NIS 2), while encouraging ICT manufacturers and providers to implement procedures to receive vulnerability information from third parties (as mentioned in recital 58), emphasizes to Member States the importance of facilitating

ITASEC 2024: The Italian Conference on Cybersecurity

* Author contributions: G.F. and M.V.Z. jointly designed the research and the structure of the paper, and jointly wrote Section 7; G.F. wrote Sections 1, 5, 6, and M.V.Z. wrote Sections 2, 3, 4.

* Corresponding Author.
gaia.fiorinelli@santannapisa.it (G. Fiorinelli); maria.zucca@santannapisa.it (M.V. Zucca)

coordinated vulnerability disclosure by establishing a national legal framework on which all actors can rely (see article 12). As part of their national policy, Member States should address the legal challenges encountered by vulnerability researchers, and in particular their potential exposure to criminal liability, e.g. by adopting "*guidelines as regards the non-prosecution of information security researchers*" (as stated in recital 60). On the same wavelength, also the Cyber Resilience Act, in the provisional text adopted by the EU Parliament on 12 March 2024, makes explicit reference to the importance of coordinated vulnerability disclosure policies, and to the need to "*incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts*", referring to "*bug bounty programmes*" as an alternative to the sale on the "*black market*" of information on vulnerabilities (see recital 77). Also Regulation (EU) 2019/881 (Cybersecurity Act) states that Coordinated Vulnerability Disclosure programs "*could play an important role in Member States' efforts to enhance cybersecurity*" (recital 30).

Since Italy is not among the States that already have a national policy on ethical hacking, the forthcoming implementation of the NIS 2 Directive may also be the right opportunity to adopt specific rules to manage the legal risks associated with vulnerability research and disclosure. The definition of this legal regime will have to take into account several factors: on the one hand, it will have to be based on a preliminary mapping of all the criminal risks that researchers (and even entities commissioning vulnerability research) may face; on the other hand, the legislator will also have to define – within the wide range of conducts labeled "ethical hacking" – the scope of activities (and even damages) "socially acceptable" for the overall improvement of cybersecurity (e.g. only agreed or also spontaneous testing; limited or open researches, etc.) [5]. To this end, the most common rules of engagement in vulnerability disclosure or bug bounty programs could serve as a benchmark. Moreover, lawmakers must also assess the overall implications of such policies on both "well-intentioned" and malicious actors: a criminological insight into the key incentives driving hackers to either disclose vulnerabilities or exploit them for illicit purposes can shed light on how national policies themselves may deter or inadvertently encourage criminal activity [4].

To address these issues, the paper is structured as follows: Section 2 analyzes the *Renaissance* of ethical hacking, aiming to refine the understanding and definition of vulnerability research. Section 3 focuses on the most common rules of engagement in bug bounty programs, which may be considered "soft law" best practices for shaping national criminal policies. Since the "decriminalization" of ethical hacking entails the risk of attracting not only *white hat*, but also *black hat* hackers, Section 4 delves into the criminological factors that may influence hackers to opt for responsible disclosure of vulnerabilities or to exploit them. Based on this criminological framework, Sections 5 and 6 are dedicated to the prospective regulation of ethical hacking in Italian criminal law, starting from an analysis of the legal risks for vulnerability researchers (Section 5), and then delving into the national policies adopted by other EU States to exempt white hats from criminal liability (Section 6). In Section 7, we offer some concluding remarks and argue for the need for an EU-wide regulation of vulnerability research and disclosure.

2. The *Renaissance* of Ethical Hacking

To accurately understand the evolution of vulnerability disclosure programs, it's crucial to be well-versed in the hacking landscape and its historical progression. The "hacking chronicles"

commenced in the winter of 1958-1959, thanks to the pioneering technological explorations of students at the Massachusetts Institute of Technology (MIT) in Cambridge, specifically within MIT's student model railroad club (known as "Tech Model Railroad Club"), marking the first-ever usage of the term "hacker" in history [6]. Originally, this term held an entirely positive connotation: within the club's jargon, it referred to individuals with exceptional technical and computer skills, capable of working on a tech problem in a creative manner, divergent from what's outlined in an instruction manual, ultimately pushing programs beyond their intended functions [7]. It was simply this: a cohort of brilliant and versatile students, enrolled in MIT's inaugural computer science courses, who committed themselves wholeheartedly to computing. As an instant result, the concept of "ethical hacking" emerged, accompanied by its "romantic" portrayal: hackers are driven by the imperative to understand and explore technology, without any malicious intent or desire to cause harm, whether it be to data, programs, or even systems [8].

The shift, however, will be brief towards an entirely negative perception of hackers: transitioning from being hailed as "heroes of the computer revolution" by Steven Levy, to being labeled and depicted merely as cybercriminals by mass media, public opinion, and collective imagination. During the 1980s and 1990s, fear and concern about hackers appeared to rapidly escalate worldwide: the apparent and perceived ease of committing criminal acts using a computer serves as a motivating catalyst for many individuals to engage in illicit activities [9]. As a result, the term "hacker" swiftly evolved into a synonym for "digital transgressor". These renovated individuals deviate significantly from the primeval ideals of ethical hacking, focusing solely on system-cracking to breach computer systems, inflict damage, obtain confidential data, engage in espionage, or even indulge in pure vandalism.

However, in contemporary times, we are witnessing the "Renaissance of ethical hacking", marking a return to the original and positive connotations of hackers. It's evident indeed that businesses can derive significant benefits from leveraging the expertise of ethical hackers [10]. When a business's defenses exhibit a vulnerability, ethical hackers can detect and expose it, facilitating remediation before a malicious hack occurs. Thus, companies have started implementing a variety of security programs to leverage external expertise in fortifying their systems. Foremost among these initiatives are bug bounty programs (hereinafter BBPs), which are becoming increasingly vital components of organizations' security strategies [11].

Building upon this historical background, the term "ethical hacking" will be used throughout this paper to encompass various scenarios, such as penetration testing, bug bounty programs, independent research, where IT experts "explore" or "attack" systems and networks with the goal of finding vulnerabilities or other security flaws, devoid of any malicious intent [12]. Nevertheless, as the research aims to outline a concise set of principles, that can encompass different actors and contexts of ethical hacking while ensuring legal certainty, BBPs will be examined in more detail, as a model for "spontaneous yet solicited" identification and disclosure of vulnerabilities, aligning with the paradigm outlined in NIS 2 Directive and Cyber Resilience Act.

3. The Rules of Engagement for Bug Bounty Programs

As the emphasis on digital protection intensifies, companies are exploring alternative approaches, including the implementation of specific security programs. Among these

emerging initiatives, BBPs are gaining increasing prominence. BBPs entail the organizational practice of compensating external parties with monetary reward for identifying and reporting security vulnerabilities discovered in the firm's systems or products, thereby fortifying their overall security posture [10]. These programs are crucial to uncover loopholes that internal security teams may overlook due to constraints such as personnel, time, expertise, or even cost limitations, which could potentially become prime targets for malicious attackers [13]. Nowadays, BBPs are often facilitated by bug bounty platforms such as HackerOne, BugCrowd, Cobalt, and others, serving as legitimate intermediaries that host simultaneous BBPs for multiple organizations. The reward amount is typically determined by the host, while the platforms simplify the process by managing the payment of bounties and by acting as central hubs, attracting both white hats and organizations, fostering collaboration, and enhancing overall security measures [14]. Each BBP operates under its own set of rules of engagement which dictate the interaction between white hats and organizations. These rules fulfill at least two key functions. Firstly, they outline the expected behavior of ethical hackers when engaging in vulnerability discovery on the program's platform and when submitting vulnerability reports. Secondly, they establish specific obligations for organizations, such as determining the size of bounty payments for specific types of discovered vulnerabilities and setting the expected timeframe for the prompt resolution of identified issues. Following this discussion, we aim to briefly outline a general taxonomy of the contents of BBPs' engagement rules, providing a standardized structure for program descriptions.

In-scope / Out-of-scope Areas: Statements of this nature define the scope of BBPs. Organizations typically list the specific system and product areas on which the white hats should focus their efforts. Simultaneously, each organization can explicitly outline all the domains and areas that are out of scope for white hats. Typically excluded are web applications hosted by third parties, as these are beyond the organization's control and may present lower risks [14].

Eligible / Non-eligible Vulnerabilities: This category outlines criteria for identifying vulnerabilities that organizations desire white hat hackers to uncover. Typically, organizations prioritize vulnerabilities that could pose significant threats to their security posture while certain vulnerabilities may be excluded from bug bounty rewards due to their low or negligible security risk. Clearly outlining these non-eligible vulnerabilities can streamline the report processing workflow and prevent the submission of reports that may ultimately be deemed invalid, reducing associated costs [15].

Disclosure Guidelines: Organizations may specify whether they permit white hat hackers to publicly disclose identified issues or if they require them to allow sufficient time for issue resolution before any public disclosure occurs. This concern often stems from the organization's focus on internal security.

Prohibited or Unwanted Actions: Rules in this category list instructions and boundaries to white hat hackers regarding actions they should avoid when searching for vulnerabilities. Additionally, dangerous activities such as social engineering and physical access to data centers are forbidden. Non-compliance with these rules may lead to disqualification from receiving bounty rewards or future participation in the program, potentially leading to legal consequences or exclusion from the entire bug bounty platform.

It is crucial to recognize that BBPs carry the risk of not only attracting attention from *white hat*, who report vulnerabilities to the firm, but also from *black hat* hackers. The latter may

attempt to exploit the website for malicious purposes, disclose vulnerabilities online, or sell them on underground marketplaces [10]. Hence, the paper will delve deeper into analyzing the criminological reasoning behind hackers' decisions to opt for responsible disclosure over malicious exploitation of vulnerabilities, or vice versa.

4. *Hacker's Dilemma*: Reporting Vulnerabilities vs. Criminal Exploitation

Individuals who discover vulnerabilities face four options: (1) take no action, (2) report the flaw privately to the vendor or a related security organization through security programs (as BBPs), (3) publicly disclose the flaw, or (4) keep the information private to enable potential attacks, either by the discoverer or by selling it to third parties on underground marketplaces. Over the last 30 years, public reporting on vulnerabilities has evolved, reflecting shifts in the relationship dynamics between security organizations and the hacker community, moving towards coordinated disclosure practices.

In this context, the commonly used term is coordinated vulnerability disclosure (hereinafter CVD) which refers to the practice wherein a hacker identifying a vulnerability in an IT system reports it to the system's owner, or a related security organization, who resolves the issue before any public disclosure occurs. As explored further in this article, some countries are starting to implement policies for CVD, aiming to enhance the security of IT systems and minimize the criminal exploitation of vulnerabilities. However, before delving into a comparative analysis of these frameworks, we must inquire: what are the essential requirements for an effective CVD policy, and how do they align with criminological understandings of criminal hacking? Furthermore, will a CVD policy primarily benefit white hats, or can it also serve as a deterrent for potential cyber-offenders, dissuading them from engaging in criminal activities and promoting ethical behavior instead [16]?

Hence, an initial step in understanding the criminological aspects of CVD involves exploring the motives behind both criminal exploitation of vulnerabilities and the choice to engage in CVD instead (as outlined in *Table 1*).

Table 1
Motives comparison: CVD and vulnerability exploitation

Factors beyond CVD	Factors beyond criminal hacking
Moral obligation	Curiosity/Addiction
Education policies for young hackers	Association in criminal hacking circles
Reward and recognition	Cost-Benefit analysis

The literature regarding the motivations behind reporting vulnerabilities through CVD primarily focuses on the factors driving individuals towards pursuing a career in ethical hacking [16, 17]. It reflects the portrayal of early hackers as pioneers of the computer revolution, believing in the potential of information access, technological accessibility, and computer usage for societal progress. Presently, ethical hackers appear also to be motivated by the objective to enhance cybersecurity, improve IT system security, reduce breach risk, assist individuals, and safeguard companies. In this context, informing system owners of vulnerabilities seems to be perceived as both a moral obligation and a matter of common sense [18]: just as we would alert

someone if their front door is open in the physical world, why wouldn't we do the same for a vulnerable system?

However, this inner duty is fueled by two main factors: recognition and reward. How system owners react to reported vulnerabilities can significantly impact vulnerability reporting, either encouraging or dissuading it. For instance, an organization lacking a CVD policy may face issues in managing reports, potentially ignoring or denying the presence of vulnerabilities. This may leave the reporters feeling underestimated or even subject to legal repercussions if the organization misinterprets their intentions and reports them to the authorities [19]. Particularly for "novice" ethical hackers, the response from system owners could impact their self-perception, as external validation plays a crucial role in affirming their actions and shaping their own ethical identity. Without such acknowledgment, they may feel undervalued, leading to a cessation of reporting or even a shift towards criminal hacking. Moreover, ethical hackers expect some form of rewards for their contributions, whether in monetary terms (such as through BBPs) or simply through public recognition. This acknowledgment allows them to gain social status within the white hat community, bolster their CV, and showcase their skills. A portrayal of a young hacker by Van't Hof [18] reflects these motivations: "*I ask whether the cash bounties are important to him. Not really, he tells me. He hacks for the recognition in whatever form that comes. He wants to solve the puzzle and he wants to show other people that he has done so*".

Another crucial factor to consider in maintaining a career in ethical hacking, especially for young hackers, is the impact of education policies. Young hackers may need guidance from knowledgeable individuals in their environment to address their inquiries, given the difficulty in accessing accurate information independently, since parents often lack expertise in ICT-related topics, and schools may not adequately offer information either [20]. In the Netherlands, several recent initiatives address this challenge. For instance, volunteers from the organization "Hack in the Class" visit schools to teach hacking and programming skills, providing insights into the ethical boundaries of hacking. These initiatives draw inspiration from social learning theory, originally formulated to explore the origins of criminal behavior [21], but which can be adapted to understand the motivations behind ethical hacking engagement. Associating with prosocial peers or participating in an ethical hacking community can inspire individuals to pursue and persist in ethical hacking endeavors. Indeed, interacting with other ethical hackers serves as a catalyst, facilitating the transfer of ethical hacking skills and values to younger IT enthusiasts within their social circles.

On the flip side of the coin, criminological research has identified various motives behind criminal hacking and related behaviors. These motives could offer insight into why individuals opt to exploit a vulnerability or sell it on the underground market, rather than disclosing it or taking no action [22].

Firstly, criminal hacking often arises from the challenge of breaking into a system, curiosity, desire to learn, and notably, feelings of addiction and empowerment [16, 23]. Indeed, the sense of omnipotence derived from the relationship with computers, the awareness of being capable of controlling technology, and leveraging it to achieve any objectives, fosters among hackers the belief of belonging to an elite group. In the words of Bruce Sterling [24]: "*when you are a hacker, it is the inner conviction of belonging to an elite that authorizes you to violate the rules, or rather to transcend them*". Driven by these inner motivations, hackers, upon gaining access to a system, may develop curiosity about the data stored and proceed to download it, acting

disproportionately and violating most of CVD policies. A well-known case described in Van't Hof [18] exemplifies this, where a hacker breached into a hospital's computer systems. Although the defendant claimed to have ethical motives, he admitted that "*curiosity drove him to access the server on more than one occasion*" leading him to access patient records of specific celebrities.

Secondly, criminal behavior can be learned and replicated through social interaction and modeling, especially when individuals associate with deviant peers who provide deviant definitions through social learning processes [21, 25]. The decision to mimic such behavior depends on the prevailing values within the community, e.g. the hacker community, which determines whether the acquired skills are employed for constructive or malicious purposes. Notably, certain black hat hackers' communities reject collaboration with government or even large companies, leading members to refrain from reporting vulnerabilities as doing so may jeopardize their reputations [16]. Additionally, in some criminal hacking circles, successfully breaching a system can elevate one's social status and reputation, while identifying an unknown vulnerability and either selling it or utilizing it in personal malicious hacks would showcase significant skills [23]. Conversely, as previously mentioned, within the white hat community, reporting vulnerabilities through legitimate channels can elevate an individual's social status. Thus, a hacker's community affiliation can significantly influence their own response and shape their actions upon discovering vulnerabilities [18].

Ultimately, in line with one of the core criminological theories, the rational choice perspective, individuals assess the potential costs and benefits of engaging in illicit activities when presented with opportunities to do so, aiming to minimize risks and maximize profits. For criminal activities, the primary costs associated with offending typically arise from the perceived risks of adverse social consequences, including detection, prosecution, and punishments [26]. However, for many cybercrimes, involving unauthorized access to computer systems, detection rates remain remarkably low [9, 22], potentially increasing the likelihood of offending in cyberspace. Additionally, the persistent risk of facing legal action following a CVD program, alongside with the presence of complex rules or time-consuming disclosure processes, may constitute further significant costs in the cost-benefit analysis.

Furthermore, many contemporary criminal hackers are motivated by the pursuit of financial gain [27, 28]. This dynamic can influence vulnerability reporting in two different ways: individuals may opt to sell vulnerabilities on the underground market or report them to BBPs for monetary reward. In this context, some researchers have conducted cost-benefit analyses comparing BBPs with underground markets. Allodi [29] investigated a Russian cybercrime forum and discovered that prices in the underground marketplace are either equal to or higher than those in BBPs or other legitimate markets. However, vulnerabilities can be sold multiple times in the underground market, whereas they typically fetch only a single sale in the legitimate one. Additionally, as previously mentioned, in most criminal hacking cultures, collaborating with governments or large companies is not accepted [23, 30]. Therefore, even if bounty rewards are substantial, the decision to report vulnerabilities may be deterred by further social costs associated with an individual's reputation, thus increasing the likelihood of choosing the malicious criminal path.

5. Risks and Rewards for White Hats: *Ethical* but still *Illegal* in (Italian) Criminal Law

While ethical hacking is experiencing its *Renaissance* in the cybersecurity landscape, in Italy there is still widespread uncertainty about its *legal* qualification [5, 31]. As Italy does not yet have a national framework for the research and disclosure of security vulnerabilities [3, 32], those who engage in "ethical" IT research, intrusions, or attacks (and even those who commission them) risk falling within the scope of the relevant criminal provisions, without being able to claim any special exemption. This is especially true when *white hats* operate as independent actors; nonetheless, even BBPs or penetration testing agreements may not be always sufficient to protect well-intentioned cyber-intruders from criminal liability, much less when they act disproportionately or inadvertently cause damage or interruption/disruption of services.

Before analyzing in detail Italy's relevant legislation, it is worth making a preliminary remark: the *legal* meaning of hackers' (good) intentions is, in hindsight, not neglected in the international and European legal framework on cybercrime [12]. For instance, the Council of Europe Budapest Convention on Cybercrime (2001) states that Parties may include additional requirements in the definition of the offense of "*Illegal access*" (Art. 2: "*the access to the whole or any part of a computer system without right*"), for instance requiring the offense be committed "*with the intent of obtaining computer data or other dishonest intent*". Also in Art. 6 (*Misuse of devices*) criminal liability is excluded when the production, possession, etc., of devices designed or adapted primarily for the purpose of committing cybercrimes (as defined by the Convention) is "*not for the purpose of committing an offense*", but instead e.g., "*for the authorized testing or protection of a computer system*". Accordingly, Directive 2013/40/EU on attacks against information systems states, in Recital 16, that testing "*the reliability of information technology products or the security of information systems*" can be considered a legitimate purpose for producing or selling tools that can be used to commit attacks against IT-systems and suggests Member States require *direct intent* (i.e. malicious purpose), rather than only *general intent* (intent to commit the act). Art. 7 (*Misuse of devices*) therefore states that production, sale, etc. of tools to be used for committing computer crimes are punishable only if committed "*with the intention that it be used to commit any of the offences referred to in Articles 3 to 6*".

Both the Budapest Convention and Directive 2013/40/EU seem to implicitly recognize the permissibility of "ethical" attacks [12], and to this end, they mostly rely on the notion of *intent* (*dishonest intent, direct intent*), rather than on merely objective elements (e.g., a prior agreement between the parties), to make "good intentions" legally relevant. The exemption of acts of ethical hacking from criminal liability would not, therefore, put Italy at risk of being in breach of positive criminalization obligations.

To map the risks for white hats under Italian criminal law, reference should be made first to Art. 615-*ter* Penal Code (*Illegal access*), according to which anyone who "illegally" ("*abusivamente*" - without right) enters a computer or telematic system protected by security measures is punished [33]. The offense requires general intent and is punishable upon complaint by the rightsholder, unless e.g. (i) if committed against computers or telematic systems of public interest, or (ii) if it results in the destruction or damage of the system, or interruption of its functioning, or the destruction or damage of the data, information or programs contained therein. In these latter cases, public prosecutors proceed *ex officio*.

Interpretive solutions exist to limit how the provision applies to ethical hacking, but none of them provide legal certainty:

1. *Prosecution by complaint*: some authors highlight that hackers operating under penetration test agreements, BBPs, etc. can trust that the target organization will not pursue criminal charges against them [31]; however, the (in)existence of the conditions that trigger *ex officio* prosecution cannot be easily planned and managed in advance (e.g., not causing an interruption in the functioning of the system or any damage). Moreover, the prosecution *ex officio* if the target organization is "of public interest" excludes ethical attacks in the public sector from the regime of prosecution *by complaint*.
2. *"Without right" clause*: hackers could also claim that they are not "illegally" accessing the computer system when fulfilling an agreement or following a set of rules established by the target organization (BBPs, CVDs). To this end, reference can be made to case law on Art. 615-*ter* Penal Code, that links the (il)legality of the access to the "breach of the conditions and limits resulting from the set of prescriptions issued by the owner of the system" and to "reasons ontologically unrelated to those for which the right of access is granted to him" [34]. However, in the absence of an express provision, a sufficient degree of legal certainty is again not achieved. Moreover, this exemption does not apply to those who find and report vulnerabilities spontaneously, without prior authorization.
3. *Consent*: other authors propose that the legality of ethical hacking might find its basis in the general defense of "consent of the rightsholder" as outlined in Art. 50 of the Penal Code, even in the form of "presumed" or "supposed" consent [5, 35]; these forms of consent are, however, debated and the defense of "Consent" is applicable only when "private" interests are at stake. As for defenses, reference has been made also to *necessity* [36].
4. *Ex-post exemption in case of responsible disclosure:* the only court decision that can be found in Italy about ethical hacking ruled, in 2019, for the lawfulness of the activity of the white hat, since it was carried out with the methodology of "responsible disclosure", as the defendant immediately and repeatedly reported to the company the vulnerability he found [5, 31]. However, this decision does not recall a clear legal basis and relies on an *ex-post* assessment: this would not guarantee that the same conclusion can be reached in all similar cases.

In addition to the offence of *Illegal access*, vulnerability researchers could potentially fall under Art. 635-*bis* Penal Code (*Data interference*, in case of damaging, deletion, etc.), Art. 635-*quater* Penal Code (*System interference*, in case of hindering the functioning of a computer system), or even Art. 340 Penal Code (*Interruption of public services*, if the attack results in the disruption of a public service). None of these provisions require, in fact, a direct or dishonest intent underlying the action of the offender. On the contrary, in the various offences related to the paradigm of "misuse of devices" we can find the requirement of direct intent (*profit, harm, illicit damage or hindering*) and therefore no *white hat* will be punishable for possession, dissemination, installation, etc., of devices or programs exploitable (also) for malicious purposes, when instead acting for legitimate purposes.

To date there is only one case in Italy where hacking is not punishable, based on a specific legal provision: according to Art. 2-*bis* of Law Decree 105/2023, which amended the legal

framework on undercover operations, police officers are exempted from criminal liability for illegal access, data interference, system interference, and preliminary or instrumental actions, when these acts are committed in the framework of police undercover operations for preventing and combating terrorism or cybercrime against criminal infrastructures.

This quick overview of the Italian legal system allows us to draw three provisional conclusions: (i) the national policy on ethical hacking must take into account all the various applicable offences, as well as the conditions that, under Italian law, make certain crimes more serious or prosecutable *ex officio* (damage, public interest); (ii) following *responsible disclosure/CVD stages* may be a useful benchmark to which an exemption can be linked, but this solution currently lacks a legal basis; (iii) the requirement of direct/dishonest intent can also help differentiate legal consequences for malicious cases and well-intentioned attacks (and could be potentially linked with *responsible disclosure guidelines*, which could be an *ex-post* test of the subject's intentions, but based on criteria established *ex-ante*).

6. A Comparative Analysis of the Regulation of Ethical Hacking in the EU

As a comprehensive ENISA report shows [3], unlike Italy other States in the EU have instead adopted specific legal frameworks for ethical hacking or coordinated vulnerability disclosure, which may offer useful insights for this paper. For the purpose of the research, the different legal solutions will be sorted and discussed into some macro-categories, having a common legal rationale.

1. *Intent and intentions* (e.g. Germany, Portugal). According to the *BSI CVD guideline for security researchers* in force in Germany [37], researchers reporting a vulnerability in one of the German Government's systems in compliance with the guideline will not be charged with any criminal offence, unless "*if recognizable criminal intentions have been or are being pursued*" [37]. In Portugal, the prospective reform will establish a national policy to be also used as a framework to check the "good intentions" of hackers for the purposes of applying criminal offences, alongside other factors (means used, logs, etc.) [3]. In both cases, *intentions* are used to draw the line between good and bad hackers, and objective elements seem to be just considered as evidence of intentions, while no objective defense or exemption is provided.
2. *"Whistleblowing" between decriminalization and exemption from reporting* (e.g. Belgium, France). Belgium can be considered one of the most relevant examples, as it introduced a special legal regime for ethical hacking in 2023 in the new "whistleblower" law [38]. The new *Klokkenluiderswet* explicitly decriminalizes cases of ethical hacking, irrespective of the consent of the target, if the conditions set out by art. 62/1 and 62/2 of the law of 7 April 2019 on cybersecurity are fulfilled. In particular, Art. 62/2 states that, within the framework of the reporting procedure set out in Art. 62/1 (report to the national CSIRT, CCB), the authors of an alert do not commit an offence as for the facts required for the alert, provided that the following conditions are met: (1) no fraudulent intent, or intent to cause harm; (2) timely information on the vulnerability to the "target", at the latest at the time of reporting to the national CSIRT; (3) no act beyond what was necessary and proportionate to verify the existence of a vulnerability; (4) no public

disclosure of the vulnerability, without the agreement of the national CSIRT. Article 62/2 also exempts whistleblowers to CSIRT from prosecution for offences punishing breach of confidentiality (professional secrecy). The criminal exemption is built around the two pillars of necessity-proportionality and compliance with the reporting procedure (time and form requirements); intentions are relevant, but only as a negative requirement of a broader assessment, that grants an objective – even if not automatic [38] – exemption from criminal liability. In France, instead, Article 47/L 2321-4 *Code de la défense* excludes the obligation of the ANSSI to report to the prosecutor researchers who disclose cyber-vulnerabilities, upon conditions that (i) they are acting in good faith (*personne de bonne foi*) and (ii) the vulnerability is reported to the ANSSI exclusively; the ANSSI keeps the identity of the reporter confidential (so it is compared here to whistleblowing), but no general exemption from criminal liability is provided [32].

3. *CVD as an Objective safe harbor* (e.g. Lithuania, Latvia). Lithuania can be regarded as a pioneering [39] and insightful example, since, after a specific reform in 2021, national law provides a "safe harbor" for ethical hackers, whose acts are legal if they meet the list of purely objective requirements set by law [3, 40, 41]: (i) *integrity*, i.e. data and systems may not be compromised, no attempt to violate passwords should be made: (ii) *necessity*, i.e. when the vulnerability is found, the search needs to be stopped, and no unnecessary activities are performed; (iii) *reporting*, within 24 hours, either to the national authority or the organization concerned; and (iv) *confidentiality*. The "intentions" of the hacker are not mentioned. Latvia also drafted a statutory RD procedure paired with an amendment of the relevant criminal law, providing a liability waiver [32, 42].
4. *CVD as a "Subjective" waiver* (e.g. Denmark). While in Denmark's 2022-2024 National Strategy for Cyber and Information Security, reference is made to a pilot of a government CVD, as a "*framework for government agencies to allow private individuals ("helpful hackers") to identify and report vulnerabilities in ICT systems*" [43], the Ministry of Justice of Denmark reported to ENISA that CVD policies could be regarded in Denmark as a "*statement from the vulnerability owner that it will not pursue a legal proceeding if the security researcher acts within the framework of the published policy*" [3]. This waiver is referred to as "subjective" in that it depends on the general "consent" of the rightsholders, but is relevant on an "objective" level in that it acts independently of any disagreement of the vulnerability owner in the single case (since the final decision is up to a court; a similar approach can be found in Switzerland [44]).
5. *Safe harbor for IT professionals.* ENISA [3] recommends Members States, for instance, to draft some criteria for the qualification of "*professional ethical hacker*" (e.g. referring to education, publications, and experiences), to be regarded as a prerequisite for legal protection, as the distinction between black and white hats may otherwise be blurred.
6. *Prosecutorial discretion* (Netherlands). In the Netherlands, researchers are protected since 2013 through the coordination of a national CVD policy [45] and a "policy letter" of the Public Prosecution Service, that identifies the relevant factors guiding prosecutorial discretion in investigating cases of ethical hacking: (i) the interest of society; (ii) proportionality; (iii) subsidiarity; (iv) compliance with CVD [3, 32].
7. *Freedom of research and right to science* (Greece): Greece reported to ENISA that freedom of research and academic expression is the constitutional basis under which researchers are being protected [3]; also, some scholars argue that under the right to science and

freedom of research, enshrined in Art. 15 of the Int. UN Covenant of 1976 and in Art. 13 of the EU Charter, States have a positive obligation to protect information security researchers [46].

Beyond the single legal solutions chosen by each State, we need to consider a series of cross-cutting factors that each legal solution more or less prioritizes: (i) as regards *hackers*, different regimes turn up exempting from liability all "well-intentioned" cyberintruders, or only those acting under specific policies/arrangements, or only professionals; (ii) as regards *acts* exempted, different legal solutions cover different ranges of conducts, irrespective of the subject committing them (only cybercrime, or also professional secrecy offence, or even all acts necessary to discover the vulnerability); (iii) as for *legal certainty*, it is clear that some regulations prioritize the need for precision, even at the cost of narrowing the scope of the "safe space", while others sacrifice certainty in favor of a case-by-case assessment and a wider allowance for ethical hacking; (iv) also, some States regulate vulnerability disclosure in a *strictly public dimension* (e.g. safeguards are conditional on the reporting of the vulnerability to the national CSIRT, and not just to the owner), while others consider also *private* agreements, policies and disclosures procedures (but the consent of the target is hardly ever decisive or relevant); (v) interestingly, no regulations encourage the *financial compensation* or *reward* of white hats.

7. Final Remarks: Paving the Way to the Decriminalization of Ethical Hacking

In the absence of a specific legal framework, the label "*ethical*" has therefore no precise *legal* significance and hackers searching for vulnerabilities undoubtedly expose themselves to the risk of criminal charges, even if acting with "good intentions". The analysis conducted thus far indicates the necessity of regulating ethical hacking and offers insights into potential provisions for such regulation.

Drawing from the criminological insights discussed earlier, it's evident that there are strategies to enhance current and future CVD policies, that can be summarized as follows: (i) facilitating compliance with CVDs policies, by offering clear rules and instructions, helping individuals understand reporting procedures, and urging organizations to respond promptly; (ii) maintaining open communication with the discloser throughout the disclosure process, inviting them to test potential patches or conduct additional (paid) research for the organization, or even utilizing the disclosure process as a recruitment tool; (iii) promoting successful CVD initiatives to the general media, to raise awareness of CVDs, eliminate excuses for not reporting vulnerabilities through legitimate channels, encourage large companies or governments to recognize the value of vulnerability reporting, and implement educational programs for young hackers to foster ethical behavior.

This means that the forthcoming regulation should both (i) ensure *ex-ante* legal certainty and (ii) encompass an elastic notion of ethical hacking (i.e., not just police undercover operations, or pre-agreed security tests). In light of the various legal solutions analyzed, we can argue that a national policy regulating vulnerability research and reporting is the first necessary step to ensure certainty while imposing on researchers the reasonable burden of complying with a set of clear rules; the policy can list all the "rules of engagement" (as BBPs) and serve as

a code of conduct (permitted areas, actions, vulnerabilities, disclosure). The comparative analysis suggests that this policy should be coupled with a specific amendment in criminal law: e.g. (i) an objective waiver/defense for those who comply with the policy; or (ii) the *direct intent* requirement in the relevant offences (to be interpreted in light of the CVD policy).

Looking ahead, we can doubt whether such a reform, however necessary, would be sufficient [2].

On the one hand, while general cybersecurity and cybercrime policy is developed at EU level, due to the transnational nature of digital technologies and cyberspace, ethical hacking activities can be negatively affected by legal fragmentation and differences between Member States, especially in cross-border cases. Therefore, a sound CVD policy, with implications on the criminal liability of white hats, should perhaps be better adopted at European level, rather than at national level. On the other hand, while national policies are mainly inspired by the objective of protecting researchers and selecting hackers who deserve this "special" protection, criminological research suggests that a CVD policy should be developed with the different objective of *incentivizing* reporting [2, 32], including through education and awareness campaigns but also rewards, prizes or public recognition, if needed to draw (malicious) hackers on the "good" side.

In the end, States should perhaps distinguish white from black *acts*, rather than *hats*, by looking at the benefit to society that comes from "helpful hackers".

Acknowledgements

The research was developed within the NRRP MUR (Italian Ministry of University and Research) Project SERICS - SEcurity and RIghts in the Cyber Space, Spoke 1 – CybeRights (CUP J53C22003110001), funded by the European Union - Next Generation EU (G.F.).

References

[1] ENISA, ENISA Threat Landscape 2023, 2023. URL: http://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[2] ENISA, Developing National Vulnerabilities Programmes, 2023. URL: http://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes.

[3] ENISA, Coordinated Vulnerability Disclosure Policies in the EU, 2022. URL: http://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.

[4] OECD, Encouraging vulnerability treatment. Overview for policy makers, 2021. URL: http://www.oecd.org/digital/encouraging-vulnerability-treatment-0e2615ba-en.htm.

[5] P.P. Casale, Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento", Archivio Penale 2 (2021) 1-18.

[6] S. Levy, Hackers: Heroes of the Computer Revolution, 1st. ed., Doubleday Books, New York, 1984.

[7] I. Corradini, C. Di Fede, Hacker e internet crime, in: G. Marotta (Ed.), Tecnologie dell'informazione e comportamenti devianti, Edizioni Universitarie di Lettere Economia Diritto, Milan, 2004, pp. 183-196.

[8] G. Pomante, Hacker e computer crimes, Edizioni Simone, Naples, 2000.
[9] D. Wall, Cybercrime: the transformation of crime in the digital age, 1st. ed., Polity, Cambridge, 2007.
[10] A. Aaltonen, Y. Gao, Does the Outsider Help? The Impact of Bug Bounty Programs on Data Breaches, Fox School of Business Research Paper, 2021.
[11] S. S. Malladi, H. C. Subramanian, Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations, IEEE Softw. 37.1 (2020) 31–39. doi:10.1109/ms.2018.2880508.
[12] C. Del-Real, M. J. Rodriguez Mesa, From black to white: the regulation of ethical hacking in Spain, Inf. & Commun. Technol. Law 32(2) (2022) 1–33. doi:10.1080/13600834.2022.2132595.
[13] A. Kuehn, M. Mueller, Analyzing bug bounty programs: an institutional perspective on the economics of software vulnerabilities, 2014 TPRC Conference Paper, 2014.
[14] A. Laszka, M. Zhao, A. Malbari, J. Grossklags, The Rules of Engagement for Bug Bounty Programs, in: Financial Cryptography and Data Security, 22nd International Conference, FC 2018, Springer Berlin Heidelberg, 2018, pp. 138–159. doi:10.1007/978-3-662-58387-6_8.
[15] A. Laszka, M. Zhao, J. Grossklags, Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms, in: Computer Security – ESORICS 2016, Springer International Publishing, Cham, 2016, pp. 161–178. doi:10.1007/978-3-319-45741-3_9.
[16] M. Weulen Kranenbarg, T. J. Holt, J. van der Ham, Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure, Crime Sci. 7:16 (2018). doi:10.1186/s40163-018-0090-8.
[17] B. Fox, T. J. Holt, Use of a Multitheoretic Model to Understand and Classify Juvenile Computer Hacking Behavior, Crim. Justice Behav. 48(7) (2020) 943-963. doi:10.1177/0093854820969754.
[18] C. van't Hof, Helpful hackers: How the Dutch do responsible disclosure, Tek Tok, Rotterdam, 2016.
[19] NTIA, Vulnerability disclosure attitudes and actions: A research report, 2016. URL: http://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf
[20] R. Udris, Cyber deviance among adolescents and the role of family, school, and neighborhood: A crossnational study, International Journal of Cyber Criminology 10(2) (2016) 127–146. doi:10.5281/zenodo.163393.
[21] R. L. Akers, Social learning and social structure: A general theory of crime and deviance, 1st. ed., Northeastern University Press, Boston, 1998.
[22] T. J. Holt, A. M. Bossler, Cybercrime in Progress: Theory and prevention of technology-enabled offenses, 1st. ed., Routledge, New York, 2016.
[23] T. J. Holt, Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures, Deviant Behav. 28(2) (2007) 171–198. doi:10.1080/01639620601131065.
[24] B. Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, 1st. ed., Bantam Books, New York, 1992.
[25] E. H. Sutherland, Principles of criminology, 4th. ed., J.B. Lippincott Co., Chicago, 1947.
[26] T. C. Pratt, F. T. Cullen, K. R. Blevins, L. E. Daigle, T. D. Madensen, The Empirical Status of Deterrence Theory: A Meta-Analysis, in: F. T. Cullen, J. P. Wright, K. R. Blevins (Eds.),

Tacking Stock: The Status of Criminological Theory, 1st. ed., Transaction Publishers, New Brunswick, 2006, pp. 367–395.
[27] D. Chan, D. Wang, Profiling cybercrime perpetrators in China and its policy countermeasures, in: R. G. Smith, R.-C. Cheung, L. Y. Lau (Eds.), Cybercrime risks and responses: Eastern and western perspectives, Palgrave, London, 2015, pp. 206–221. doi:10.1057/9781137474162_14.
[28] P. N. Grabosky, The evolution of cybercrime, 2006–2016, in: T. J. Holt (Ed.), Cybercrime through an interdisciplinary lens, 1st. ed., Routledge, London, 2017, pp. 15-36. https://doi.org/10.4324/9781315618456.
[29] L. Allodi, Economic Factors of Vulnerability Trade and Exploitation, in: CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York, NY, USA, 2017. doi:10.1145/3133956.3133960.
[30] P. Taylor, Hackers: Crime in the Digital Sublime, 1st. ed., Routledge, New York, 1999.
[31] R. Flor, Il diritto penale alla prova dell'hands-on dell'ethical hacking, Diritto di Internet 1 (2020) 165-169.
[32] A. Pupillo, A. Ferreira, G. Varisco, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges, Report of a CEPS Task Force, 2018. URL: https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/.
[33] R. Flor, Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto, Diritto penale e processo 1 (2008) 106-112.
[34] N. Bussolati, Accesso abusivo a un sistema informatico o telematico ex art. 615- ter c.p.: il nodo dell'abusività, Studium Iuris 4 (2018) 428-436.
[35] M. Dobrinoiu, The Consent of the Victim as Legal Defence in Cybercrime cases, Challenges of the Knowledge Society (2017), 174-176.
[36] M. Isler, O. Kunz, G. Moll, Strafbarkeit von Ethical Hacking, 2023. URL: http://www.ntc.swiss/news/rechtsgutachten-strafbarkeit-von-ethical-hacking.
[37] BSI, BSI CVD guideline for security researchers, 2022. URL: http://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html.
[38] C. Somers, K. Vranckaert, L. Drechsler, Belgium legalises ethical hacking: a threat or an opportunity for cybersecurity?, 2023. URL: http://www.law.kuleuven.be/citip/blog/belgium-legalises-ethical-hacking-a-threat-or-an-opportunity-for-cybersecurity/.
[39] M. Bada, C. Weisser Harris, Cybersecurity Capacity Review Republic of Lithuania. Global Cyber Security Capacity Center, 2017. URL: http://api.nrdcs.lt/wp-content/uploads/2022/12/oxford-cmm-lithuania-report-10-8-2017-final.pdf.
[40] Ministry of National Defence of the Republic of Lithuania, Key trends and statistics of the national cybersecurity status of Lithuania 2021-2022, 2022. URL http://www.nksc.lt/doc/en/Key-trends-and-statistics-2021-q1-2022.pdf.
[41] D. Teplõhh, M.-L. Orav, A. Stivriņa, M. Beniušis, Ethical hacking in the Baltics: Comparative legal map, 2022. URL: https://www.tgsbaltic.com/en/publications/ethical-hacking-in-the-baltics-comparative-legal-map/.
[42] U. Ķinis, From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach, Comput. Law & Secur. Rev. 34(3) (2018) 508–522. doi:10.1016/j.clsr.2017.11.003.

[43] The Danish Government, The Danish National Strategy for Cyber and Information Security 2022-2024, 2021. URL: http://en.digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf.
[44] Le Conseil fédéral, La promotion du piratage éthique en Suisse, 2023. URL: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/br-bericht-ethisches-hacking.html.
[45] NCSC, Coordinated Vulnerability Disclosure: The Guideline, 2018. URL: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.
[46] O. van Daalen, In defense of offense: information security research under the right to science, Comput. Law & Secur. Rev. 46 (2022). doi:10.1016/j.clsr.2022.105706.