From black to white: the regulation of ethical hacking in Spain

Real, C. del; Rodriguez Mesa, M.J.

Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cict20

From black to white: the regulation of ethical hacking in Spain

Cristina Del-Real & María José Rodriguez Mesa

To cite this article: Cristina Del-Real & María José Rodriguez Mesa (2022): From black to white: the regulation of ethical hacking in Spain, Information & Communications Technology Law, DOI: 10.1080/13600834.2022.2132595

To link to this article: https://doi.org/10.1080/13600834.2022.2132595

Published online: 21 Oct 2022.

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW
https://doi.org/10.1080/13600834.2022.2132595

From black to white: the regulation of ethical hacking in Spain

Cristina Del-Real [a] and María José Rodriguez Mesa [b]

[a]Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands; [b]Department of International Public, Criminal and Procedural, University of Cadiz, Cadiz, Spain

ABSTRACT

Cyber-attacks are exponentially growing, and their impact on systems, people, and organizations increases. Among other challenges, cyber-attacks prevention must tackle the fact that many software systems are marketed with security vulnerabilities due to the companies' need to reduce time-to-market. One strategy to reduce security vulnerabilities is ethical hacking. However, while ethical hacking can bring many advantages, it also comes with many challenges. This paper introduces a comprehensive study of the possibilities and limitations of ethical hacking in Spain, both empirical and normative. On the empirical side, the paper presents the results of a Delphi study with cyber security experts in Spain on their opinions about the regulation of ethical hacking. In the normative study, the paper critically reviews the possibilities open by the International, European and Spanish law for regulating ethical hacking. The conclusions of this paper offer a roadmap for harnessing ethical hacking to improve cyber security.

KEYWORDS

White hat hacking; Delphi study; penetration test; cyber security; bug bounty programs; coordinated vulnerability disclosure

1. Introduction

Companies have a growing interest in securing their information technology systems. This interest aligns with the fact that proactive practices are increasingly being implemented.[1] However, these practices are often conflicted by the companies' need to reduce the time-to-market.[2] A strong velocity-focused approach often misses the security essentials, increasing the number of vulnerabilities[3] in a software system.[4] Consequently, many

CONTACT Cristina Del-Real c.del.real@fgga.leidenuniv.nl

[1]See e.g., Ann Cavoukian and Mark Dixon, 'Privacy and Security by Design: An Enterprise Architecture Approach' (Information and Privacy Commissioner, 2013); Anthony J Masys (ed), *Security by Design: Innovative Perspectives on Complex Problems* (Springer International Publishing, 2018) <http://link.springer.com/10.1007/978-3-319-78021-4> accessed 25 January 2022.

[2]Hiva Alahyari, Richard Berntsson Svensson and Tony Gorschek, 'A Study of Value in Agile Software Development Organizations' (2017) 125 Journal of Systems and Software 271.

[3]A vulnerability can be define as the 'occurrence of a weakness (or multiple weaknesses) within software, in which the weakness can be used by a party to cause the software to modify or access unintended data, interrupt proper execution, or perform incorrect actions that were not specifically granted to the party who uses the weakness' in Cybersecurity Unit, 'A Framework for a Vulnerability Disclosure Program for Online Systems' (US Department of Justice, 2017) Guidance 1 <https://www.justice.gov/criminal-ccips/page/file/983996/download>.

[4]Valentina Casola and others, 'A Novel Security-by-Design Methodology: Modeling and Assessing Security by SLAs with a Quantitative Approach' (2020) 163 Journal of Systems and Software 110537; Rakesh Kumar and Rinkaj Goyal, 'Modeling Continuous Security: A Conceptual Model for Automated DevSecOps Using Open-Source Software over Cloud (ADOC)' (2020) 97 Computers & Security 101967.

software systems are marketed with vulnerabilities in their code.[5] Then, reactive strategies come into play. Among the reactive strategies, one of the most popular is penetration testing. Penetration testing is a security exercise in which a cybersecurity analyst tries to find and exploit vulnerabilities in a computer system.[6] Generally, penetration testing is carried out by so-called 'ethical hackers' through bug bounty and vulnerability disclosure programs.

The discussion about ethical hacking and vulnerability disclosure is not new.[7] According to HackerOne,[8] the earliest known bug bounty program dates back to 1983 by the operating system company Hunter & Ready.[9] Since then, many large companies have initiated bug bounty and vulnerability disclosure programs. For example, Google currently has a community of Bug hunters open.[10] Examples of other companies with bug bounty programs are IBM, Twitter, and Uber.[11] Bug bounty programs for public administrations can also be found. For example, the United States launched, on April 18 2016, the program' Hack the Pentagon', a vulnerability disclosure program by the US Department of Defense.[12] Many companies and organizations are launching these programs because they have the potential to improve their cybersecurity.[13]

Spain is strongly committed to cybersecurity, as seen in the Global Cybersecurity Index by the International Telecommunication Union. According to the latest version, Spain scored fourth-best in the world and second-best in the European Union in 2020.[14] However, as can be noticed in the latest *The 2021 Hacker Report* by HackerOne,[15] Spain lags behind other countries in implementing bug bounty programs and vulnerability disclosure policies. Particularly, Spanish public administrations are the most reluctant to launch formal collaboration with ethical hackers. Only one recent example of a public administration leading a bug bounty program in Spain can be found. A popular hacker, Antonio Fernandes, together with 14 other ethical hackers, carried out the first bug bounty pilot project in Catalunya, where they were able to identify up to five vulnerabilities in the networks of the *Generalitat de Catalunya* in 2020.[16]

[5]Jeffrey R Jones, 'Estimating Software Vulnerabilities' (2007) 5 IEEE Security & Privacy Magazine 28.
[6]See, for example, B Arkin, S Stender and G McGraw, 'Software Penetration Testing' (2005) 3 IEEE Security and Privacy Magazine 84.
[7]B Smith, W Yurcik and D Doss, 'Ethical Hacking: The Security Justification Redux', *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No.02CH37293)* (IEEE, 2002) <http://ieeexplore.ieee.org/document/1013840/> accessed 3 March 2022.
[8]HackerOne is the biggest vulnerability coordination and bug bounty platform that connect companies with ethical hackers. See https://www.hackerone.com
[9]HackerOne, 'The Hacker-Powered Security Report 2017' (HackerOne, 2017) 5.
[10]Google, 'Home | Google Bug Hunters' <https://bughunters.google.com/about/rules/6625378258649088> accessed 4 March 2022.
[11]HackerOne, 'IBM – Vulnerability Disclosure Program' (*HackerOne*, 2018) <https://hackerone.com/ibm> accessed 4 March 2022; HackerOne, 'Twitter – Bug Bounty Program' (*HackerOne*, 2014) <https://hackerone.com/twitter?type=team> accessed 4 March 2022; HackerOne, 'Uber – Bug Bounty Program' (*HackerOne*, 2016) <https://hackerone.com/uber?type=team> accessed 4 March 2022.
[12]HackerOne, 'U.S. Dept of Defense – Vulnerability Disclosure Program' (*HackerOne*, 2016) <https://hackerone.com/deptofdefense?type=team> accessed 4 March 2022.
[13]Akemi Takeoka Chatfield and Christopher G Reddick, 'Crowdsourced Cybersecurity Innovation: The Case of the Pentagon's Vulnerability Reward Program' (2018) 23 Information Polity 177.
[14]International Telecommunications Union, *Global Cybersecurity Index 2020. Measuring Commitment to Cybersecurity* (International Telecommunication Union, 2021).
[15]HackerOne, 'The 2021 Hacker Report: Understanding Hacker Motivations, Development and Outlook' (HackerOne, 2021).
[16]Arantxa Herranz, 'Así fue primer bug bounty de una Administración Pública en España: 15 hackers contra la Generalitat catalana' (*Xataka*, 4 February 2021) <https://www.xataka.com/pro/asi-fue-primer-bug-bounty-administracion-publica-espana-15-hackers-generalitat-catalana> accessed 4 March 2022.

This study explores the possibilities and limitations of regulating ethical hacking in the context of Spain. The paper is structured as follows. Section 2 introduces the definition and historical evolution of ethical hacking. Section 3 describes the two models of ethical hacking that we will explore in this study: bug bounty programs and coordinated vulnerability disclosure policies. Section 4 provides a comprehensive empirical study of the possibilities of ethical hacking in the opinion of Spanish stakeholders. Then, Sections 5–7 analyze the possibilities of ethical hacking from the legal perspective. Specifically, in the international context (Section 5), in the European law (Section 6), and in Spanish Criminal Law (Section 7). This comprehensive study of the possibilities of ethical hacking allows us to propose regulation models of ethical hacking in Section 8. Finally, the study finalizes with the conclusions in Section 9.

2. What is ethical hacking?

In 2014, the Royal Spanish Academy[17] (RAE) introduced the word 'hacker' in the official dictionary, defined as 'Person who illegally accesses other people's computer systems to appropriate them or obtain secret information'.[18] The RAE had positioned itself. The hacker was, in essence, a criminal. However, if we look back to the concept's origins, they are not linked to criminal activities. The concept of 'hacker' was born in a context and a community not even related to computer science. It was within the *Tech Model Railroad Club*, a student organization of the *Massachusetts Institute of Technology* (MIT) founded between 1946 and 1947 and dedicated to the automation of scale trains. In the mid-60s, this group of students began to popularize the word 'hacker' to define those members who used their creativity to develop quick, effective –and not necessarily orthodox– solutions.[19]

As many of these students ended up using the PDP-1[20] to program their scale trains, soon the word 'hacker' was transferred and consolidated in computer science. Back then, hackers themselves considered their activities to be honest and valuable to society. However, as Leeson and Coyne claim[21], soon after, 'hackers began to realize the potential of *hacking* for personal gain'. In other words, some hackers began to use their computer skills for criminal purposes and enter into companies' and organizations' computer systems to obtain economic benefits, information and fame. These individuals were called 'crackers' to differentiate them from hackers.

However, with the popularization of 'hacker', the concept became associated with illicit intrusions into computer systems, that is, with computer crimes.[22] In turn, 'cracker'

[17]Translation of 'Real Academia Española', also known by the abbreviation, 'RAE'. RAE is the official royal institution with the mission of ensuring the stability of Spanish language. More information can be found in <https://www.rae.es/la-institucion> accessed 10 March 2022.

[18]Translated from the original version: '*Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta*'.

[19]Steven Levy, *Hackers: Heroes of the Computer Revolution* (1st ed, Anchor Press/Doubleday, 1984).

[20]The PDP-1 was the first computer developed by Digital – one of the largest computer companies in the US between 1960 and 1990 – to be used to design the first video game: *Spacewar!*

[21]Peter T Leeson and Christopher J Coyne, 'The Economics of Computer Hacking' (2005) 1 Journal of Law, Economics & Policy 511.

[22]Kyung-Shick Choi, Claire S Lee and Eric R Louderback, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime', *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Springer International Publishing, 2019) <http://link.springer.com/10.1007/978-3-319-90307-1_2-1> accessed 6 April 2020.

became less common. Given this historical evolution, it can be argued that the RAE merely embodied the most popular definition in their 2014 proposal. However, some hackers reacted to this formalized criminalization of the concept. Among them, the popular *hacker* of Telefónica,[23] Chema Alonso, launched a campaign to collect signatures with the aim of the RAE changing the definition of 'hacker'.[24] His request was accepted when, in 2017, the RAE included a new definition of the hacker as 'A person who is an expert in computers, and who deals with system security and develop improvement techniques'.[25] However, the damage had been done. For most people, the hacker was a cybercriminal.

Hackers' community's alternative to this distorted view of themselves was to adopt the adjective 'white hat' as a way to decriminalize their actions.[26] Therefore, three different types of hackers can be found: black hat hackers, gray hat hackers, and white hat hackers. Black hat hackers are cybercriminals.[27] When hackers act illegally, but their intentions are not malicious, they are known as gray hat hackers. These hackers identify vulnerabilities in an organization's systems without their express permission. Sometimes, these hackers aim to reveal to organizations that their cybersecurity is weak.[28] Black hat and white hat hackers differ from white hat hackers in that the latter have some kind of authorization from organizations to perform penetration testing in the organization's network.[29] These hackers are also known as 'ethical hackers' or 'penetration testers'.

The ethical hacker can be thus defined as a cybersecurity expert specialized in performing intrusions to identify vulnerabilities in computer systems (hardware, software and networks). They aim to test and evaluate the computer systems' security.[30] Ethical hackers improve cybersecurity by performing penetration testing in an organization's networks to identify potential vulnerabilities and evaluate corporate security policies and user behavior to find potential risks.[31]

In Spain, ethical hackers play this role within private companies, working as '(cyber)security analysts'.[32] However, ethical hackers' ambitions can exceed the limits of their company's network. In the international context, the role of *bug bounty hunters* is increasingly popular among the ethical hacking community. They look for and detect vulnerabilities in organizations' computer systems in exchange for rewards. Unlike cybersecurity analysts, bug bounty hunters are not formally hired by the company or organization. Instead, the company offers a reward *ex-post* to anyone who can find vulnerabilities in their systems. The prerequisite for

[23]Telefónica is a Spanish multinational telecommunications company.
[24]Arantxa Herranz, 'Un Informático Contra El Lenguaje: El Día Que La RAE Cambió El Significado de "Hacker"' *Diario Sur* (Madrid, 17 February 2018) <https://www.diariosur.es/tecnologia/internet/informatico-lenguaje-cambio-20180217121743-ntrc.html> accessed 9 March 2022.
[25]Translation from the original in Spanish: '*Persona experta en el manejo de computadores, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora*'.
[26]Levy (n 19).
[27]Thomas Georg, Burmeister Oliver and Low Gregory, 'Issues of Implied Trust in Ethical Hacking' (2018) 2 The ORBIT Journal 1.
[28]ibid 5.
[29]Aron Laszka and others, 'The Rules of Engagement for Bug Bounty Programs' in Sarah Meiklejohn and Kazue Sako (eds), *Financial Cryptography and Data Security* (Springer 2018).
[30]Sebastian Kubitschko, 'The Role of Hackers in Countering Surveillance and Promoting Democracy' (2015) 3 Media and Communication 77.
[31]Tracey Caldwell, 'Ethical Hackers: Putting on the White Hat' (2011) 2011 Network Security 10.
[32]ibid.

this type of program to work is that the company supports this type of action through vulnerability disclosure reward programs or 'crowd-sourced security'.[33] However, the 'ethical' label does not neutralize the fact that the hacking behavior means to access a computer system by violating security measures originally established to prevent access in the first place. In other words, while the intentions of vulnerability disclosure rewards programs are legitimate, the behavior of penetrating in a computer system –where sensitive data could have been stored– is not without legal challenges.

3. Regulating ethical hacking

Three legal situations can be distinguished about the penetration of a computer system: (a) absolute prohibition of any unauthorized access (no exemptions from criminal responsibility); (b) a generic and global authorization; and (b) freedom of access as long the aim is to detect and report vulnerabilities well-intentionally. These three situations motivate, respectively, three vulnerability disclosure models. A first model in which only those who have an explicit and individualized authorization from the owner to detect vulnerabilities in the system would be exempt from any responsibility. Usually, a person is hired specifically by the company for this purpose. Secondly, the bug bounty model. And finally, the coordinated vulnerability disclosure (CVD) policy, which allows collaboration with security researchers and can be compatible with bug bounty programs. This section analyses the latter two models.

3.1. Bug bounty programs

A bug bounty program is a rewards program offered by organizations by which individuals can perform security assessments on the organizations' computer systems in exchange for compensation.[34] The bug bounty business model rewards hackers for disclosing vulnerabilities and helping customers patch their products.[35] Three factors differentiate the collaboration on which bug bounty is based from other models of engagement or outsourcing: (a) the job is requested through an open call to which any hacker can respond; (b) hackers who volunteer can be unknown to the organization, and (c) there is no minimum number of participants.[36]

There are three categories of bug bounty programs depending on the relationship between the hacker and the organization:

(a) Institutional or managed directly by software providers that establish policies and compensations (e.g. Microsoft, Google or Facebook).

[33]Omer Akgul and others, 'The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs', *The Workshop on Security Information Workers* (2020).
[34]Laszka and others (n 29); Andreas Kuehn and Milton Mueller, 'Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities' [2014] SSRN Electronic Journal <https://www.ssrn.com/abstract=2418812> accessed 2 March 2022.
[35]Ross Anderson and Tyler Moore, 'Information Security: Where Computer Science, Economics and Psychology Meet' (2009) 367 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 2717.
[36]Thomas D LaToza and Andre van der Hoek, 'Crowdsourcing in Software Engineering: Models, Motivations, and Challenges' (2016) 33 IEEE Software 74.

(b) Via platforms where there is a legitimate intermediary host of simultaneous bug bounty programs for multiple organizations. In this case, the host determines the amount of the reward.
(c) Through private intermediaries who buy vulnerabilities from hackers and then resell them. They usually offer higher rewards than the suppliers.[37]

Although there is no express authorization, launching the program implies a general and anonymous authorization aimed at anyone who can detect a vulnerability in the system and communicate it in exchange for a reward. Depending on the more or less restrictive interpretation given to the term 'unauthorized', bug bounty programs may or may not be considered a case of illicit access.

Bug bounty programs have many advantages. Following Krishnamurthy and Tripathi[38], the main advantage for companies is the reduction of costs because bug bounty programs are a cheaper option when compared to operating only with hired employees. In addition, bug bounty programs create a competitive mindset among researchers, leading to more alternatives from which the company can choose. Besides, Publicity accompanying a bug bounty program leads to increased product awareness and mindshare among developers, leading to increased interest and use of the company's products. There are also advantages for security researchers (i.e. ethical hackers). For instance, they can earn a significant amount of money. In this regard, some studies have analyzed the incentives and practices of organizations and ethical hackers who initiate and participate in these programs. For example, one study looked at Google Chrome and Mozilla bug bounty programs and found that these programs were more cost-effective compared to hiring full-time researchers for vulnerabilities disclosure.[39] Another study explored well-known bug bounty platforms like Wooyun and HackerOne and found that top contributors were important in discovering vulnerabilities and groups of white hat hackers make significant contributions.[40] Another study that analyzed 77 bug bounty programs collected through the HackerOne website found that those programs with more rules with greater content and explicit statements on duplication, disclosure, and other relevant processes were associated with more bugs resolved.[41] Another study found that bug bounty programs are effective for companies of all sizes and levels of prominence.[42] This was particularly positive for small and medium enterprises, which often lack the cachet and resources to recruit in-demand cybersecurity professionals. Therefore, the authors concluded that bug bounty programs seem to democratize access to IT talent.

[37]Suresh S Malladi and Hemang C Subramanian, 'Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations' (2020) 37 IEEE Software 31.
[38]Sandeep Krishnamurthy and Arvind K Tripathi, 'Bounty Programs in Free/Libre/Open Source Software' in Jürgen Bitzer and Philipp JH Schröder (eds), *The Economics of Open Source Software Development* (Elsevier, 2006) <https://linkinghub.elsevier.com/retrieve/pii/B9780444527691500081> accessed 24 February 2022.
[39]Matthew Finifter, Devdatta Akhawe and David Wagner, 'An Empirical Study of Vulnerability Rewards Programs', *Proceedings of the 22nd USENIX Security Symposium* (USENIX, 2013).
[40]Mingyi Zhao, Jens Grossklags and Peng Liu, 'An Empirical Study of Web Vulnerability Discovery Ecosystems', *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (ACM 2015) <https://dl.acm.org/doi/10.1145/2810103.2813704> accessed 2 March 2022.
[41]Laszka and others (n 29).
[42]Kiran Sridhar and Ming Ng, 'Hacking for Good: Leveraging HackerOne Data to Develop an Economic Model of Bug Bounties' (2021) 7 Journal of Cybersecurity 1.

However, bug bounty programs also have drawbacks. The program may not attract researchers qualified enough to detect vulnerabilities from the companies' perspective. From the ethical hackers' perspective, the main disadvantage can be the uncertainty about the amount of the reward. Although the compensation is usually high enough, sometimes it can be better to spend the time on an activity that generates secure income. In addition, annual reports of bug bounty platforms show that the outcomes can be quite inefficient sometimes.[43] For example, some platforms report that the percentage of invalid reports ranges from 35% to 55%[44], which can indicate how inefficient these programs can be. In response to this, some programs have attempted to regulate the inflow of invalid reports by adjusting the rules and incentives.[45]

3.2. Coordinated vulnerability disclosure (CVD)

A Report by CEPS Task Force on 'Software Vulnerability Disclosure in Europe'[46] –based on recommendations to States aimed at providing legal clarity to software (ISO/IEC 29147:2014 and ISO/IEC 30111)– analyzed the different models that States can follow for the implementation of a CVD. According to ISO/IEC 29147, vulnerability disclosure is defined as 'techniques and policies for vendors to receive vulnerability reports and publish remediation information'. Moreover, it is a process through which vendors and vulnerability researchers may work cooperatively to find solutions that reduce the risks associated with a vulnerability.

The authors include seven recommendations based on European law on page 81 of the CEPS Task Force Report[47], including (a) protection of security researchers so that they can continue their work without being subject to criminal prosecution, and (b) incentives for security researchers to encourage white-hat hackers to participate in CVD programs. The authors recommend amending national legislation to support CVD by using the framework introduced in the Netherlands as a model.[48]

The CVD process involves a series of steps that may or may not be followed in order. The steps can be repeated for each vulnerability detected. According to the scheme proposed by Householder et al.[49], the CVD process would include the following steps:

– *Discovery*: A researcher (hacker) discovers a vulnerability.
– *Reporting*: A vendor or a third-party coordinator receives a vulnerability report from the researcher – i.e. the individual or organization that reports the detected vulnerability to the vendor.

[43]Bugcrowd, 'The State of Bug Bounty' (Bugcrowd, 2018) Company report.
[44]Zhao, Laszka, and Grossklags, 'Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery' (2017) 7 Journal of Information Policy 372.
[45]Aron Laszka, Mingyi Zhao and Jens Grossklags, 'Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platformsç' in Ioannis Askoxylakis and others (eds), *Computer Security – ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II* (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016).
[46]Marietje Schaake and others, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges : Report of a CEPS Task Force* (Centre for European Policy Studies, 2018) <https://www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges> accessed 24 February 2022.
[47]ibid 81.
[48]ibid 82.
[49]Allen Householder and others, 'CERT® Guide to Coordinated Vulnerability Disclosure' (Carnegie Mellon University, 2017) 29 <https://kilthub.cmu.edu/articles/report/CERT_Guide_to_Coordinated_Vulnerability_Disclosure/12367340/1> accessed 24 February 2022.

– *Validation and triage*: the analyst validates the report to ensure accuracy before taking further action.
– *Remediation*: A remediation plan is developed and tested. The deployer usually carries out the remediation plan. Ideally, the remediation plan includes a software patch – but also other mechanisms.
– *Gaining public awareness*: the vulnerability and the remediation plan is disclosed to the public.
– *Promote deployment*: The remediation is applied to the systems involved.

The involvement of multiple parties requires a coordinator to orchestrate the remediation process. Coordination between a single hacker and a single vendor is relatively straightforward, but when multiple hackers are involved, or a complex process is at stake, coordination requires special attention.

4. An empirical examination of ethical hacking in Spain: A Delphi study

Our Delphi study aims to answer the following two questions: (a) how does the ethical hacking community currently contribute to cybersecurity in Spain? And (b) to what extent would a regulation allowing ethical hacking be accepted by Spanish stakeholders? This study complements the normative analysis that we will carry out later by empirically exploring the possibilities and limitations of the regulation of ethical hacking in Spain.

4.1. Method

The Delphi method aims to obtain the consensus of experts on a certain topic.[50] Consensus is obtained through a structured and iterative process in which experts give their opinions anonymously over several rounds. In this study, we followed the broadly defined characteristics of Delphi studies: anonymous responses, iteration, controlled feedback, and group statistical response.[51] In other words, the opinions of the expert panel members are obtained from a self-administered questionnaire, through several rounds in which participants receive feedback on the experts' responses to previous rounds, and the final result is the degree of consensus measured with a statistical value.

4.1.1. Delphi design

The study was structured into three rounds; an introductory first round (R1), a second-round with closed questions (R2), and a final round of feedback and consensus among experts (R3). R1 was designed as an open, introductory questionnaire. It explored the extent to which ethical hackers were perceived as a relevant actor for cybersecurity in Spain. The experts had to answer two questions. First, 'do you consider ethical hackers to be relevant actors for cybersecurity in Spain?', with two answer options (1 = 'Yes', 2 = 'No'). Second, participants had to answer which activities, out of a list of six, ethical

[50]Theodore J Gordon and Olaf Helmer, 'Report on a Long-Range Forecasting Study' (RAND Corporation, 1964); Olaf Helmer, 'Analysis of the Future: The Delphi Method' (RAND Corporation, 1967).
[51]Gene Rowe and George Wright, 'The Delphi Technique as a Forecasting Tool: Issues and Analysis' (1999) 15 International Journal of Forecasting 353.

hackers usually perform in Spain. This question was multiple-choice and included the following activities:

(a) Intrusion into computer systems to detect flaws in their protocols and applications in order to improve the cybersecurity of a company or organization,
(b) Assisting companies or organizations to respond to serious cyber-incidents,
(c) Tools and software applications development to improve the cybersecurity of a company or organization,
(d) Detection and reporting to the police of serious cybercrimes such as trafficking in child pornography,
(e) Forensic investigations of serious cyber-incidents, and
(f) Training for companies and organizations to improve their cybersecurity.

In addition, an open response option (i.e. 'other activities') was included where experts could include additional activities that, to their knowledge, were carried out by ethical hackers not covered by the questionnaire.

Once understood, through the R1 results, the role of ethical hackers in Spain, R2 and R3 aimed to obtain the consensus of experts regarding the suitability of a law that would regulate the activity of white hat hackers. Delphi experts were asked to explain they agreed with the statement 'There should be a law that regulates ethical hacking, so that hackers are allowed to analyze the cybersecurity of a company or organization without being hired by it', measured through a Likert-5 scale in which 1 = 'completely disagree' and 5 = 'completely agree.'

After R2, statistical analyses of the results were carried out to measure the consensus obtained. The statistical analysis between rounds in a Delphi study consists of obtaining the scores that indicate whether or not there is consensus among the experts regarding the questions asked. In case there is no consensus, in the next round, the experts are asked the same question again, this time offering them, in an anonymized form, the distribution of the answers given by the entire panel of experts. This study used the interquartile range (IQR) as an indicator to measure consensus. The IQR is a descriptive statistical dispersion measure that measures the difference between the scores obtained in the first and third quartile ($IQR = Q_3 - Q_1$). It is the dispersion measure for the median and consists of the mean 50% of the observations. [52] A small IQR means that the data are more pooled and, therefore, there is less dispersion in the distribution of responses (i.e. a greater consensus).

The range of the IQR depends on the number of answer options. The more points the scale has, the higher the minimum expected IQR. For this study, we established that the IQR should be ≤ 1,[53] which means that more than 50% of all opinions are within a point of difference on the scale.[54] As no consensus was obtained for the R2 question (IQR > 1), the question was again included in Round 3 for a second assessment. R1 was implemented

[52]Uma Sekaran and Roger Bougie, *Research Methods for Business: A Skill-Building Approach* (Seventh edition, Wiley, 2016).
[53]Miriam S Raskin, 'The Delphi Study in Field Instruction Revisited: Expert Consensus on Issues and Research Priorities' (1994) 30 Journal of Social Work Education 75; Mary Kay Rayens and Ellen J Hahn, 'Building Consensus Using the Policy Delphi Method' (2000) 1 Policy, Politics, & Nursing 308.
[54]E De Vet, 'Determinants of Forward Stage Transitions: A Delphi Study' (2004) 20 Health Education Research 195.

between July 1 and August 31, 2020. The R2, between September 14 and October 13, 2020. And the R3, between November 10 and 30, 2020.

4.1.2. Participants

Participants' selection began with a list of relevant experts in the cybersecurity field in Spain. Most of these names were identified through conferences the researchers attended in 2019 and 2020. Others through snowball sampling of the previous researchers' contacts. In this regard, we followed well-stablished practices of access to fieldwork, including the identification of gatekeepers, obtaining credentials, and building rapport with potential participants.[55] Experts received an invitation email to participate in a Delphi study.[56] Some contacts on this list replied affirmatively, while others referred to other contacts who they felt might be more appropriate for this research. In total, 275 experts were invited to participate, including both the initial contacts on the list and new contacts suggested by the experts.

Of the 275 people invited, 129 answered the R1 questionnaire,[57] which represents a response rate of 46.9%, the usual one in this type of study.[58] This sample size is larger than the sample of ten experts recommended in the literature as the minimum number of participants.[59] Moreover, the sample size of our Delphi is well above that handled by 83% of Delphi studies, which use less than 50 experts (61% of the total) or between 51 and 100 experts (22% of the total).[60] R2 was completed by 110 experts, with an attrition rate of 14.7%. Round 3 by 104, with an attrition rate of 0.5% compared to the previous one. Both attrition figures are consistent with that of other studies with a similar sample size of the expert panel.[61]

Of the 129 experts who responded to R1, a total of 104 were men (80.6%) and 25 women (19.4%), a proportion that we managed to maintain throughout the three rounds (see Table 1).[62] The mean age of the R1 participants was 44.1 years (Min. = 22, Mode = 43, SD = 9.1 Max. = 66). 72.9% ($n = 94$) had held managerial positions in the field of cybersecurity, while 27.1% ($n = 35$) had not held any managerial position at the time of R1. Participants had worked for a mean of 11.4 years in the field of cybersecurity (Mo = 10; SD = 7.6). Table 1 summarizes the distribution of the socio-demographic and professional characteristics of the participants throughout the three rounds.

4.1.3. Post-Delphi interviews

In R3, we asked participants if they would be available for an interview. 34 of the experts participating in the Delphi study agreed to be interviewed. We interviewed six experts

[55] Antonio M Díaz Fernández, *La investigación de temas sensibles en criminología y seguridad* (1st edn, Tecnos, 2019).
[56] See the email in app.
[57] We sent the invitation email twice.
[58] Susan C Slade and others, 'Consensus on Exercise Reporting Template (CERT): Modified Delphi Study' (2016) 96 Physical Therapy 1514.
[59] Y Camara and others, 'Stakeholder Involvement in Cattle-Breeding Program in Developing Countries: A Delphi Survey' (2019) 228 Livestock Science 127.
[60] Elizabeth Gargon and others, 'Higher Number of Items Associated with Significantly Lower Response Rates in COS Delphi Surveys' (2019) 108 Journal of Clinical Epidemiology 110.
[61] ibid.
[62] In order to keep the female participants engaged in the research –and thus maintain the gender proportion– we specifically addressed women who were not responding to the questionnaire with emails where we express our interest in getting their opinions. We could control their participation because experts had to provide an email account that was used to match their responses across rounds.

Table 1. Socio-demographic and occupational distribution of the Delphi expert panel.

	R1 ($N = 129$)		R2 ($N = 110$)		R3 ($N = 104$)	
	n	%	*n*	%	*n*	%
Sex						
Male	104	80.6	90	81.8	84	80.8
Female	25	19.4	20	18.2	20	19.2
Age						
25 or less	3	2.3	2	1.8	2	1.9
26–35	18	14.0	13	11.8	13	12.5
36–45	51	39.5	45	40.9	43	41.3
46–55	42	32.6	35	31.8	33	31.7
56 or more	15	11.6	15	13.6	13	12.5
Education level						
Secondary education	4	3.1	3	2.7	3	2.9
Some college/professional degree	10	7.8	8	7.3	6	5.8
Bachelor	27	20.9	25	22.7	24	23.1
Masters	61	47.3	51	46.4	50	48.1
PhD	27	20.9	23	20.9	21	20.2
Sector						
Police and Armed Forces	24	18.6	21	19.1	20	19.2
Tech companies	26	20.2	24	21.8	21	20.2
Private companies	39	30.2	30	27.2	29	27.9
Public sector	20	15.5	19	17.3	18	17.3
Academia	20	15.5	16	14.5	16	15.4
Cybersecurity experience						
Less than 5 years	38	29.5	32	29.1	31	29.8
6–10 years	32	24.8	30	27.3	27	26.0
11–20 years	46	35.7	36	32.7	35	33.7
More than 20 years	13	10.1	12	10.9	11	10.6

from the public sector, eight members of police organizations and the military, eleven technology company executives, eight CISOs, and one academic. The interviews were conducted between December 17 2020, and February 5 2021, with an average duration of 48 min. During the interviews, participants were able to extend their answers on the reasons for their support or rejection of the regulation of ethical hacking in Spain.

4.2. The hacking community in Spain

81.4% ($n = 105$) of the experts answered that ethical hackers are relevant actors in cybersecurity in Spain. Figure 1 shows that, in the opinion of experts, hackers mostly perform intrusions into computer systems to detect vulnerabilities. While systems intrusion is the main activity performed by ethical hackers – explained extensively in the literature[63]– we obtained that ethical hackers are involved in other activities such as training companies and organizations, the development of cybersecurity tools, and disseminating cybersecurity culture.

On the other hand, the experts identified neither helping companies nor organizations to respond to serious cyber-incidents nor reporting of cybercrimes as defining activities of the ethical hacking community to the same extent as the three previous ones. Perhaps helping organizations and reporting cybercrimes imply a certain voluntariness of

[63]See, e.g., Ajinkya A Farsole, Amruta G Kashikar and Apurva Zunzunwala, 'Ethical Hacking' (2010) 1 International Journal of Computer Applications 14; Georg, Oliver and Gregory (n 27); Sonali Patil and others, 'Ethical Hacking: The Need for Cyber Security', *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* (2017); Sharif Rezazadehsaber, 'When is Hacking Ethical?' (Master's Thesis, State University of New York 2015).

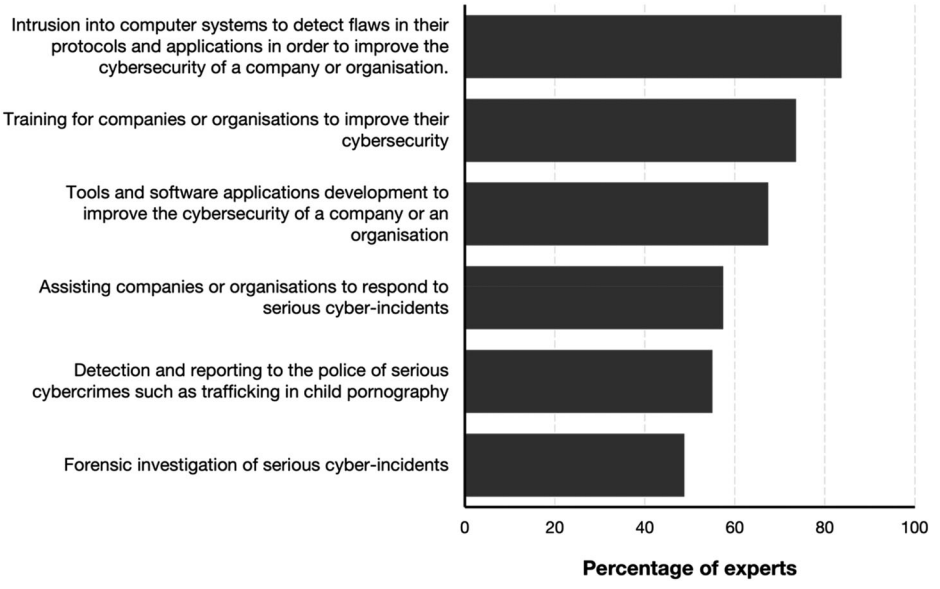

Figure 1. Expert responses to the Delphi Round 1 question about the activities of the ethical *hacker* community (N = 129).

ethical hackers to perform a function that would neither bring them an economic benefit –as it is an aid– nor fall within the functions for which they were hired. In addition, as we will discuss later in this paper, an ethical hacker must either be employed by the company or be a government official to help a company or organization respond to cyber incidents (see Section 7). Therefore, those cases in which the ethical hacker finds a vulnerability in an organizations' system that has not given its consent for the intrusion – for example, by hiring the ethical hacker to carry out such activity– would be committing a crime. Finally, less than half of experts reported that ethical hackers conduct forensic investigations in Spain.

We decided to offer the experts an open response option so that they could propose additional activities that had not been contemplated in the questionnaire. In total, of the 129 experts participating in R1, 25 of them suggested additional activities. The most popular was participation in 'information forums', 'public events' or 'congresses, community and dissemination', which were re-coded as 'dissemination of the culture of cybersecurity through the organization and participation of events'. This activity was suggested by the greatest number of experts ($n = 12$).

An opportunity is observed here for the future regulation of ethical hackers, as they are currently organized as a community with close ties with companies, public administrations and society, whose role as disseminators of the cybersecurity culture is well known. For instance, the hacker community participates in the *Cybersecurity Summer Bootcamp*, the *Congreso de Seguridad Digital y Ciberinteligencia – CyberWall*, and the *STIC CCN-CERT Conference*, the largest cybersecurity event nationwide. Public institutions organize these forums – the *Cybersecurity Summer Bootcamp* by the National Institute of Cybersecurity (INCIBE), the *CyberWall* by the National Police School and the *STIC CCN-CERT Conference* by the National Cryptological Center (CCN)– which proactively encourage the

hacker community to get involved and participate. For example, up to 34 ethical Spanish hacking communities participated in the organization of the 2nd *CyberWall*, among which were some of the largest hacker communities in Spain, such as *Mundo Hacker*, *Hackplayers*, and *Hack Madrid*. This may prove that the hacker community is integrated into the Spanish cybersecurity governance networks.

The rest of the activities included –each of them indicated by a single expert– were: (a) 'joint action with police organizations for the preservation of systems or avoid the loss of data', (b) 'search for transversal solutions in companies', (c) 'communication of critical vulnerabilities (in a disinterested way)', (d) 'against intelligence and covert actions', (e) 'detection of security breaches, *backdoors* or similar with the aim of solving them', (f) 'detection of *zero-day* vulnerabilities',[64] (g) 'organizational inclusion in companies dedicated to cybersecurity', (h) 'intermediation between cybercriminals and a company (e.g. for a ransomware)', (i) 'investigation of commercial products to improve their security and discover vulnerabilities', (j) 'investigation of new vulnerabilities, new *malware*, new attack vectors, etc.', (k) publication of research articles', and (l) 'talent selection to collaborate with agencies'.

4.3. Opinions about ethical hacking programs in Spain

60% of the experts' agreed' that ethical hackers should be legally regulated and allowed to audit an organization's cybersecurity without being employed legally. 18.2% 'neither agreed nor disagreed', and 21.8% of the experts in the R2 panel 'disagreed' with the regulation. Such regulation would open the door to companies developing bug bounty programs or CVD policies in Spain without ethical hackers facing the risk of being reported for carrying out intrusions to disclose vulnerabilities. Figure 2 shows the distribution of responses in R1 according to the experts' sex, cybersecurity experience and professional sector. As can be observed, their responses were homogeneous across all three variables. No statistical differences were found in any of the three variables; $t_{sex}(108) = -0.234$, $p = 0.816$; $F_{experience}(3,\ 106) = 0.067$, $p = 0.977$; $F_{sector}(4,\ 105) = 0.086$, $p = 0.987$. Despite this homogeneity across these three variables, an IQR of less than 1 was not obtained (IQR = 2), suggesting that the experts did not fully agree on their responses. As a result, this question was asked again in R3 of the Delphi study.

The consensus was reached among the experts in R3 (IQR = 1). 81.8% responded 'agree' that there should be a law to regulate ethical hackers. Only 7.7% 'disagreed' and 18.3% 'neither agreed nor disagreed' in R3. Consistent with these results, the mean increased by 7.8%, and the standard deviation decreased by 44.9%. These findings lead to the conclusion that, in general, the cybersecurity experts participating would be in favor of regulating ethical hackers. To delve deeper into the experts' responses, they were allowed to include open text responses during R3. A total of 15 entries were obtained with additional comments that fall into three groups: supporting arguments, opposing arguments, and nuances on the question.[65]

[64]Zero-day, 0-day, or zeroday vulnerabilities are a type of software vulnerabilities that are unknown, or for which no patches or fixes exist yet, and which may be being exploited for malicious purposes. For further information see Anil Lamba, Satinderjeet Singh and Balvinder Singh, 'Mitigating Zero-Day Attacks in IoT Using a Strategic Framework' [2016] SSRN Electronic Journal <https://www.ssrn.com/abstract=3492684> accessed 14 March 2022.

[65]Not all the experts responded the open-ended questions because they were not labelled as mandatory in the questionnaire.

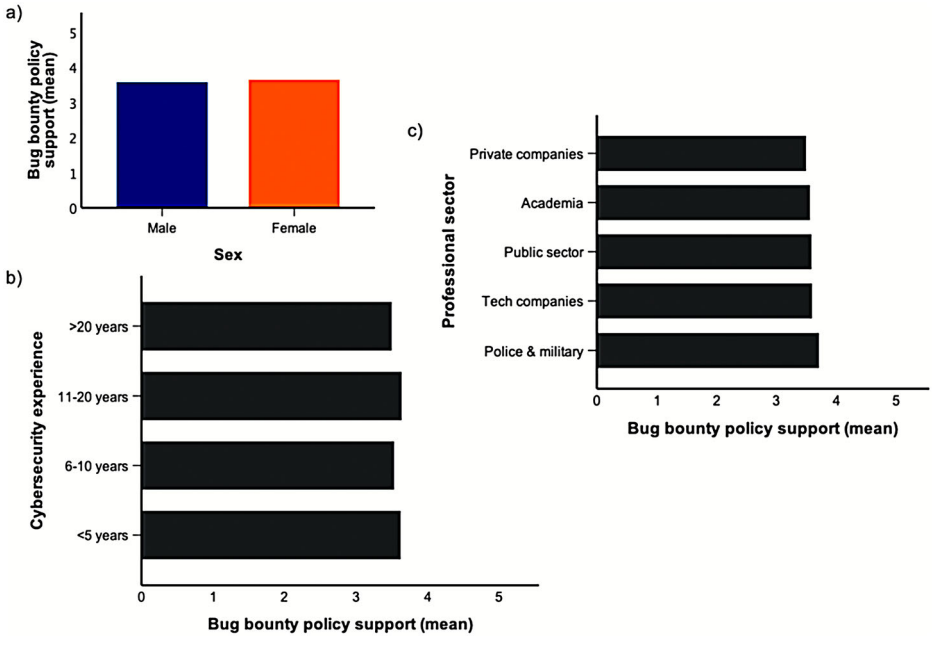

Figure 2. Experts support for ethical hacking policies in Round 1 according to a) sex, b) experience in the cybersecurity domain, and c) professional sector.

4.3.1. Supporting arguments for ethical hacking regulation

Firstly, comments in favor of regulation argue that ethical hackers are already well-established in the governance of cybersecurity in Spain, so it would be appropriate to provide them with a legal framework regulating their activity. Experts say this would be nothing more than a legalization of the already existing *de facto* laws on bug bounty programs in other countries. Other expert from the private sector proposed regulating collaborations with companies by statute to protect the latter from misuse by ethical hackers. This regulation would reduce the likelihood of ethical hackers engaging in malpractice. As one expert explains: 'A market associated with the concept of cybersecurity is being created that only seeks quick money and taking advantage of the fact that the term is fashionable. Immediate regulation is urgently needed to put an end to the proliferation of money-grabbing cliques' (male, private sector). This future law should include, among others, regulation on reporting mechanisms, legal protection for both companies and hackers and a clear remuneration system.

4.3.2. Opposing arguments for ethical hacking regulation

Five experts included comments arguing against regulation. Three of them stated that it would be unnecessary to have such a regulation. For the first expert, '[it] would imply giving legitimacy to an activity that is always on the edge of the legal/moral. The hacker's "ethical" activity is already legitimized. There is no need for further regulation' (male, private sector). Freelance hackers offer themselves to companies to carry out penetration testing. Besides, a law would violate the laws on intellectual property, data protection, and computer crimes in the Criminal Code:

> Intellectual and industrial property laws and the crime of damage, including computer damage, are well defined in the Criminal Code. Any allegedly 'ethical' action that alters a public or private entity is governed by the rest of the laws that the legal system contemplates for all citizens. I do not believe in a specific law for ethical hacking. (male, tech company)

Two other experts disagreed because they considered that a law could be potentially detrimental in the long run. Thus, a regulatory policy of ethical hacking could allow predatory practices among cybersecurity companies:

> No way. Considering that there is no real sense of the use of cybersecurity within the framework of national security in our country, it would give rise to the use of these profiles against the competition as a pitched battle of who is better or worse protected. We would encourage the hacker community to launch a 'witch hunt', sometimes paid for by third parties who only seek to harm and damage a company's reputation. (female, public sector)

During the interviews, some police officers offered further arguments against a law regulating ethical hacking. In their view, compliance with the Criminal Code should prevail over the potential benefits of regulating ethical hacking. For example, 'Computer crimes should be criminalized. It's so ridiculous. "As you had a good intention, shall we decriminalize?" Suppose we apply it to other crimes; what would be next? "Ethical" bank robberies to show that the facility's security is inadequate? (…) in the end, legalizing the intrusions would be contrary to democratic values' (male, chief police officer).

4.3.3. Nuances on the question

The activities of ethical hackers are thought to be more on the limits of what is legal, although it should not be considered a criminal activity. At this point, it is worth noting that the activity of ethical hackers differs from that of cybercriminals in that the latter take advantage of the vulnerabilities they find. In other words, the difference between a hacker and a cybercriminal would lie in whether they exploit the vulnerability or not. The controversy arises because hackers often must conduct parallel research, following similar procedures, to those of cybercriminals if they wish to find vulnerabilities. Otherwise, ethical hackers would find it extremely difficult to understand the procedures of cybercriminals. For ethical hackers, understanding and reproducing cybercriminals' behavior is the only way to combat cybercrime effectively. Consequently, in the opinion of the ethical hackers interviewed, the Spanish law should make some concessions to the activity of computer systems intrusion.

Despite the consensus among experts on the need to regulate ethical hacking, it does not appear to be an easily solvable issue, according to the experts interviewed after the Delphi. The lack of regulation means that Spain would not be taking full advantage of the opportunity for cybersecurity experts to collaborate in identifying vulnerabilities without ethical hackers risking being denounced for committing a crime. Experts say that there are more than a few cases in which a hacker has reported a vulnerability and was subsequently denounced:

> A person detected that there was a vulnerability in the Valencia metro cards. (…) Instead of thanking that person, they reported them. Many times [*public organizations*] don't listen to [*ethical hackers*]. Companies don't listen either. [*In Spain*] it is not widespread, but there are bug bounty programs in other countries. I consider that this regulation would be basic for Spain because right now, the regulation is very ambiguous. The result is that people

> find [*vulnerabilities*] but don't disclose them. I'm just giving a little bit of information, but don't give all the information because you can get into big trouble. (female, private sector)

Moreover, the lack of regulations and policies does not prevent ethical hackers from collaborating with companies or public bodies to disclose vulnerabilities (and even detect crimes). The four police officers interviewed assured that several ethical hackers collaborate with the police regularly out of a willingness to serve and not for economic benefit since they cannot pay their services because there is no flexible legal framework for these collaborations. Therefore, ethical hackers' collaborations with the police are carried out informally, unofficially. This conclusion is reflected in the testimony of one member of the Spanish police forces:

> When we detect an ethical hacker […] we want them to collaborate with us because it is their field of business. They know very well the good techniques when a new vulnerability is detected they try to prevent others from taking advantage of it. They give us information, advice … In this sense, we have detected the best computer engineering universities […]. In the end, it is all about personal relationships. I am very close friends with a senior hacker from [X] who collaborates with us in four or six campaigns a year. He does it out of friendship. Those who try to do it to make money, in the end, don't collaborate because [*the police*] can't pay them. Hackers do it altruistically, just because they trust you, because they like you because you have done them a favor, etc. There are many people, for example, who collaborate to help us discover pedophile communities. […] [*In the police*] to get an ethical hacker to collaborate, you need a year of meetings and a lot of coffees. (male, chief National Police officer)

The laws do not prevent some hackers from taking risks and reporting to the police when they find a cybersecurity breach. But, according to the experts interviewed, the hacker would face a problem if the company claims the researcher's name to the police. The police are then obliged to provide the information, which puts the hacker at risk of being reported by the company. To avoid this, hackers would be resorting to the intermediation of third parties, informing the police through their lawyers, who, due to client confidentiality, cannot reveal the hacker's name.[66]

From the experts' responses, it is clear that three steps are necessary before regulating the activity of ethical hackers. First, it would be advisable to define what an ethical hacker is and what defines their behavior. This derives from the very concept of the hacker, which, as discussed in the introduction, is socially related to that of cybercrime. Hacking education should start at universities. For example, as this hacker states during the interview: 'In Spain, there is no good definition of hacking. Consequently, a lot of potential is lost as it is a figure and a professional field that is not worked from the universities. In Spain, there is still fear of hackers; they are considered criminals. I think universities should teach the right way to do ethical hacking' (male, tech company). Therefore, the first step to regulate the activity of ethical hacking in Spain should be to provide a clear and agreed definition of 'ethical hacking'.

Second, experts regret that there is no regulatory path to becoming an ethical *hacker*. As a consequence, the public does not trust hackers. As a military officer express: 'I do not

[66] Article 5.2 of the *Código Deontológico de la Abogacía Española*, according to which 'The duty and right to professional secrecy includes all the confidences and proposals of the client, those of the adverse party, those of colleagues, as well as all the facts and documents of which he/she has had notice or has sent or received by reason of any of the modalities of his/her professional performance.'

trust them in terms of the training and the itinerary that has led them to be an ethical hacker. Specifically from the point of view of their training and what have been the motivations that have led him to acquire those abilities. Before hackers were ethical, were they cybercriminals?' (male, military). Thus, an appropriate way to legitimize the activity of ethical hackers should be implemented through talent programs. Both public organizations and private companies could drive these programs. An expert agrees with this opinion:

> Cybercriminals move overwhelming amounts of money. Cybercrime is their job; imagine a company that works 24/7, without rest. Since they have a lot of money, they attract many people who have not been called from the 'light side' up to that point. This is why I think talent programs are very important. (…) if we can attract talent and take hackers to the ethical side, we're taking them away from the cybercrime path. (female, private sector)

In the last step, a regulation defining ethical hacking activities and promoting *bug bounty* programs should be developed. According to the opinions gathered in our Delphi study, such regulation in Spain would have broad support among cybersecurity experts. However, as much as Spanish stakeholders could support regulation, legal requirements in the international, European and Spanish Law must be addressed.

5. Possibilities in the international law

Technological progress and the increasing dependence of critical infrastructures on the correct functioning of the network and IT systems is a growing concern. This concern has been reflected in various international organizations aimed at cybercrime prevention and control. The United Nations International Telecommunication Union (ITU) and the OECD The Seoul Declaration for the Future of the Internet Economy[67] can be found among these organisations. The latter includes, among other measures, the reduction of cybercrime through the strengthening of national and international cooperation between governments and authorities responsible for implementing legislation.[68]

In 1989, the Committee of Ministers of the Council of Europe adopted Recommendation No. (89) 9 on computer-related crime.[69] Recommendation (89)9 lists several deliberate acts that must be criminalized regardless and other acts that should be criminalized only at the discretion of the Member States. The former includes unauthorized access. While unauthorized access can be useful to discover vulnerabilities, it is considered generally dangerous because it can lead to system errors, crashes, and even data being destroyed due to negligence or a security deficiency. The hacking activity, on the other hand, provides access to confidential data that the hacker can use for their benefit. As it is an intrusion in the privacy of computer systems and, therefore, in the right to privacy, the activity must be punished.[70]

[67]Committee for Information, Computer and Communications Policy, Directorate for Science, Technology and Industry, 'The Seoul Declaration for the Future of the Internet Economy' (Organisation for Economic Co-Operation and Development, 2008) Ministerial Session <https://www.oecd.org/sti/40839436.pdf> accessed 14 March 2022.
[68]María José Rodríguez Mesa, *Los Delitos de Daños: Capítulo IX Del Título XIII Del CP Tras La Reforma de La LO 1/2015*, vol 138 (Tirant lo Blanch, 2017).
[69]Council of Europe (ed), *Computer-Related Crime: Recommendation No. R. (89) 9 on Computer-Related Crime and Final Report of the European Committee on Crime Problems* (Council of Europe, Publishing and Documentation Service, 1990).
[70]ibid.

Based on the above considerations, Recommendation (89) 9 urges member states to punish the access to a computer system or network without rights by violating security measures. Security of the computer system is the interest being protected. This prohibition is in addition to that of computer sabotage. As stated in the European Committee on Crime problems, [71] criminalization of unauthorized access is capable of providing protection, at an early and indirect stage, against damage resulting from the manipulation and damage of computer systems, as well as from computer espionage. In Recommendation (89) 9 an actor acting without authorization is required. Like any unauthorized activity, it is only punishable if it is committed deliberately or intentionally. In any case, national legislation is free to increase the requirements for the application of illicit access.

Given the shortcomings identified and the need to create a more relevant instrument than a Recommendation, the Council of Europe adopted the Budapest Convention on Cybercrime.[72] The Budapest Convention was the first international treaty that aimed to fight against cybercrime by harmonizing the laws of States, improving investigative techniques, and increasing cooperation. As set out in the Preamble, its main objective is to achieve a common criminal policy aimed at protecting society against cybercrime, particularly through the adoption of appropriate legislation and the promotion of international cooperation.

Article 2 of the Budapest Convention establishes the international precedent for criminal punishment of hacking, urging the parties to adopt legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.'[73]

The Budapest Convention requires member states to criminalize illegal access when it is deliberate and without permission. *A sensu contrario,* there is no obligation to criminalize authorized or non-malicious access. Illegal –or unauthorized– access implies an access that is carried out in an illegitimate manner. The behavior may be legal or justified when there are principles or interests whose weighing makes it advisable to exclude criminal liability. In that sense, according to the Explanatory Report to the Budapest Convention, the term 'illegitimate' has to be interpreted in the context in which it is being used. It may refer to conduct undertaken without authority to do so (e.g. without the authorization of the system owner) or to such behavior that is not covered by the justifications, excuses and legal defenses provided for in the domestic law of each State. Illegal access, in addition to potentially posing a danger to the security of the system, can lead to access to sensitive data, including passwords and information related to the systems to be accessed and secrets regarding the use of the system.

Although the Budapest Convention chooses to criminalize mere illegal access –malicious and unauthorized hacking– it allows States Parties to both broad and narrow criminalization of behavior. Hence, it allows States to impose additional conditions such as breaching security measures or the presence of subjective elements beyond the

[71]ibid.
[72]Convention on Cybercrime 2001.
[73]ibid 3.

generic wilful misconduct[74], such as the intent to obtain data or other criminal intent. Accordingly, the Budapest Convention does not require signatory states to criminalize ethical hacktivism. An element other than generic wilful misconduct is sufficient for unauthorized access to be legal from the standpoint of criminal law.

An example of comprehensive regulation is the proposal of the Chilean bill of 2020 implementing the Budapest Convention. Among its innovations is the incorporation of rules aimed at the legal protection of the search and notification of vulnerabilities in networks. The project contemplated, at first, an express provision that exempted from criminal liability cybersecurity analysts who, having found a vulnerability, immediately notify the responsible entity, and eventually, the competent public authority. If this law is approved, Chile would be a pioneer in the legal promotion of ethical hacking. However, after its approval by the Chamber, and pending the decision of a mixed commission appointed for this purpose, the exemption from criminal liability is limited to cases in which access to a computer system is carried out in the context of academic research, which reduces the possibilities of ethical hacking as originally envisaged.

On the basis of the flexibility provided for in the Budapest Convention, both at the European and international level, it is possible to differentiate countries with a more or less broad meaning of ethical hacking. For example, France and the Netherlands are already implementing active CVD policies that include the protection of the researcher. In France, in the event that a researcher reports a suspected vulnerability to the *Agence nationale de la sécurité des systèmes d'information* (ANSSI), article 47 L. 2321–4 exempts persons who, in good faith, report to ANSSI information about the existence of a vulnerability relating to the security of an automated data processing system from the obligation under Article 40 of the *Code de procédure*. In addition, the authority shall maintain the confidentiality of the researcher's identity at the origin of the transmission, as well as the conditions under which it took place. However, the protection of the researcher is partial since formal requirements must be met for the person to be exonerated and protected.

The Netherlands also has implemented a CVD policy with positive results and includes the full protection of the researcher. In this country, the *Coordinated Vulnerability Disclosure: the Guideline* has been implemented, which contains advice for organizations, researchers and disseminators.[75] In relation to the disseminators, the Dutch National Cyber Security Center published a framework for dealing with ethical hacking involved in responsible disclosure.[76] The law does not establish a specific ground that exempts from criminal responsibility a disseminator who acts for ideological or ethical reasons. But even if the law does not foresee it, it does not mean that ethical motives cannot play a role in assessing the criminal liability of the offender's actions. Basically, no criminal investigation will be initiated in case of legal enablement between the discloser and the company concerned. However, if there are indications that the discloser went beyond

[74]In civil law, 'wilful misconduct' refers to actions done with intent. It does not include negligent acts. Translation from the original concept '*dolo*' in Spanish.

[75]Nationaal Cyber Security Centrum, 'Coordinated Vulnerability Disclosure: The Guideline' (Ministry of Justice and Security, 2018) Policy report <https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline> accessed 14 March 2022.

[76]Nationaal Cyber Security Centrum, 'Leidraad in Te Jineb Tot Een Praktijk van Responsible Disclosure' (Ministerie van Binnenlandse Zaken er Koninkrijksrelaties, 2013) <https://kennisopenbaarbestuur.nl/rapporten-publicaties/leidraad-om-te-komen-tot-een-praktijk-van-responsible-disclosure/>.

what was necessary to discover the vulnerability, then the case will be examined thoroughly and may give rise to criminal liability.[77]

Although most EU members have not yet implemented a CVD policy, several countries are in the process. Lithuania –among the most progressive countries in this regard, according to the 2017 report of the Global Cyber Security Capacity Centre (GCSCC)[78]– is in the process of developing its own cybersecurity strategy in which the CVD would be incorporated by establishing processes to receive and disseminate vulnerability information. To date, Spain is one of the countries that has not carried out any action that would give a glimpse of a CVD policy.

Outside the EU, the cases of the US and Japan stand out. In the US, it was clear from the outset that the protection of security against vulnerabilities in computer systems required organized coordination. Thus, as early as the 1980s, the Defense Advanced Research Projects Agency (DARPA) performed, among other functions, that of facilitating communication between the incipient community of security researchers and a small number of software distributors. After a period in the 1990s when, under the US anti-hacking statute, it was possible to impose criminal and civil penalties on those who accessed a computer without authorization, the collaboration between vendors –who are beginning to appreciate more and more the role played by external researchers– and security researchers began to recover in 2010. In this context, the idea of bug bounty emerged and spread as an emerging business practice. In 2016, alongside bug bounties programs, the Department of Defense announced a CVD policy for systems open to the public.[79]

In Japan, on the other hand, the recommended process for CVD is that provided for in the 'Vulnerability disclosure' guide, in line with ISO/IEC 29147:2014. The guide envisages that researchers' reports will be sent to a specific agency that conducts an initial analysis. Subsequently, the report is sent to another center from which they coordinate with the product supplier. Once the vulnerability is known to vendors, an announcement is posted in the Japan Vulnerability Notes[80] along with a distributor announcement. Thanks to this system, the number of vulnerability reports has increased significantly in recent years. Among the reasons that explain this increase is the fact that the number of researchers looking for vulnerabilities has increased, as well as the number of products subject to a potential violation.[81]

To the best of our knowledge, no previous research on ethical hacking in Spain has been carried out. It remains unknown, for instance, how the ethical hacking community contributes to ensuring cybersecurity in Spain and to what extent stakeholders would accept further regulation of ethical hacking. This paper answers these two questions by carrying out an extensive Delphi study with key Spanish cybersecurity experts.

[77] Schaake and others (n 46).

[78] Maria Bada and Carolin Weisser, 'Cybersecurity Capacity Review: Republic of Lithuania' (Global Cyber Security Centre, University of Oxford, 2017) <https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf>.

[79] Marleen Weulen Kranenbarg, Thomas J Holt and Jeroen van der Ham, 'Don't Shoot the Messenger! A Criminological and Computer Science Perspective on Coordinated Vulnerability Disclosure' (2018) 7 Crime Science 16.

[80] Japan Vulnerability Notes is Japan's national vulnerability database maintained by the the Japan Computer Emergency Response Team Coordination Center and the Japanese government's Information-Technology Promotion Agency. Online available in < https://jvn.jp/en/> accessed 14 March 2022.

[81] Ichiro Mizukoshi and Aki Nakanishi, 'Subscription; Remedy for Cyber Debris!?', *2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM)* (IEEE, 2019) <https://ieeexplore.ieee.org/document/8910190/> accessed 24 February 2022.

6. Possibilities in the European law

The possibility of serious consequences of a cyber-attack on information systems –particularly on critical infrastructures– motivated the Council of Europe to adopt the Council Framework Decision 2005/222/JHA of February 24 2005, on attacks against information systems. The Framework Decision recommends the criminalization of some Budapest Convention acts. The Council's main concern was to ensure the security of information systems in their connection with national security. The Framework Decision calls on the Member States to protect information systems and computer data from illicit access and interference. In this regard, Article 2 of the Framework Decision urges States to criminalize intentional access without right to the whole or any part of an information system. As with the Budapest Convention, the Framework Decision allows the States to decide whether or not to criminalize less serious cases and the fact that a behavior is illicit when it entails the violation of security measures.

In response to the need to further strengthen the security and proper functioning of information systems, the European Parliament and the Council adopted Directive 2013/40/EU of August 12 on attacks against information systems, which replaces Framework Decision 2005/222/JHA. The Directive requires the Member States to define minimum rules with regard to the criminal offence elements, providing for effective, proportionate and dissuasive penalties for attacks against information systems.

By 'information system', Article 2 of the Directive means 'a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance'. As regards' computer data', the Directive provides a broad concept, defined as 'a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function'. In order to protect both information systems and computer data, the Directive urges States to criminalize illegal access to information systems (Article 3), illegal systems interference (Article 4), illegal data interference (Article 5), and illegal interception (Article 6).

With regard to the offence of illegal access to information systems, Article 3 of the Directive takes a step further than the Budapest Convention and the Framework Decision, given that the violation of security measures is no longer considered an additional element that may be required by the Member States, but rather part of the criminal offence itself, as a negative element of the criminal offense. Thus, the Directive's requirement is limited to intentional, unauthorized access in breach of security measures. Moreover, as in the Convention and the Framework Decision, Member States are allowed to decide whether or not to criminalize less serious offences.

Regarding the determination of cases of lesser seriousness, the 11th Preamble of the Directive allows the Member States the option to determine which cases are of minor seriousness in accordance with their national law and practice. One of the examples of minor seriousness given by the Directive itself is precisely 'the offence and the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability'.

The Directive not only leaves the door open to the absence and the exemption from criminal liability when there is no danger to the security of computer systems or data, but also, in the 12th Preamble, expressly defends the provision of incentives to report security weaknesses as a means of prevention and effective response to vulnerabilities in information systems. In this regard, Member States are urged to commit to providing opportunities for the lawful detection and reporting of security weaknesses. Through this Preamble, the Directive leaves the door open to both bug bounty programs and CVD.

In line with the conduct of abuse of devices provided for in Article 6 of the Budapest Convention, Article 7 of the Directive requires the Member States to take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution, or otherwise making available of tools without right and with the intention that it be used to commit any of the offences referred in the Directive. As Rodríguez Mesa[82] points out, Article 7 makes it possible to harmonize a criminal law response to the use of botnets or 'zombie computers' to commit the offences provided for. Within the scope of the Directive, it includes conduct related to the establishment of remote controls over computers to spread viruses, generate spam, launch DDoS attacks or commit other types of fraud on the Internet.

By means of the Law No. 1/2015 of March 30, 2015 (hereby LO 1/2015), Spain fulfils its obligation to transpose the Directive. The Law 1/2015 includes the cases of computer damage and interference in information systems or computer sabotage among the crimes of damage; while the conducts of illicit access are typified in Title X of the Criminal Code, specifically among the crimes of discovery and disclosure of secrets (articles 197 bis and 197 ter).

7. Possibilities in the Spanish criminal law

Responding to Framework Decision 2005/222, the Law No. 5/2010 of June 22, 2010, on amendments to the Criminal Code, modifies article 197 of the Criminal Code and includes in number three the criminalization of unauthorized access to data or computer programs, or the maintenance thereof against the will of the person who has the legitimate right to exclude it. The transposition of the Directive by Law 1/2015 led the legislator to eliminate the cases of computer intrusion from the 'discovery and revelation of secrets' and to regulate it in two new precepts. Specifically, articles 197 bis and 197 ter. Article 197a criminalizes two different types of conduct in each of its paragraphs: (a) illegal access to computer systems and data, and (b) interception of non-public transmissions of computer data, the latter conduct being provided for in Article 6 of Directive 2013/40/EU. For the purposes of this study, we focus on illegal access to computer systems and data, as the interception of computer data falls outside the scope of the activity carried out by ethical hackers.

Article 197 bis of the Criminal Code establishes a prison sentence of six months to two years to 'Whoever, by any means or procedure and in breach of the security measures established to prevent it, and without being duly authorized, accesses or provides another with access to a computer system or part thereof, or who remains within it

[82]Rodríguez Mesa (n 68).

against the will of whoever has the lawful right to exclude him'.[83] Article 197 ter establishes a prison sentence of six months to two years or a three to eighteen month fine for 'Whoever, without being duly authorized, produces, acquires for use, imports or, in any way, with the intention of facilitating the perpetration of any of the criminal offences outlined in Sections 1 and 2 of Article 197 or Article 197 bis, provides third parties with:

(a) A computer programme, designed or adapted primarily for the purpose of committing such criminal offences, or;
(b) A computer password, an access code or similar data enabling access to all or part of an information system, shall be punished with a prison sentence of six months to two years or a fine of three to eighteen months.'

As can be observed, the Spanish legislator transcribes almost literally Articles 3 and 7 of Directive 2013/40/EU. However, among the possibilities offered by the Directive, the Spanish Criminal Code opts for the most restrictive approach, by criminalizing all conducts regardless of their greater or lesser seriousness, as well as by not providing for any type of exemption or reduction of the penalty based on the purpose of the perpetrator or the risk to the protected legal asset.

7.1. The crime of computer access or intrusion (197 bis 1)

Article 197 bis 1 includes a common offence. The offender can be any legal person, including both natural and juridical persons – although in practice will be a natural person with computer skills. The lack of authorization implies that the conduct was carried out 'without right', thus determining its unlawfulness. Article 2 of Directive 2013/40/EU defines as 'without right' any conduct 'which is not authorized by the owner or by another right holder of the system or of part of it, or not permitted under national law.' Therefore, authorization must be understood as including both classical consent and the cases covered by laws and contractual agreements between the parties.[84] The person entitled to authorize is the owner of the computer system, whether a natural or juridical person.[85]

Authorization by the owner of the computer system must be examined in the case of employees and contracted persons – whose functions include penetration testing. The Spanish Supreme Court requires judicial authorization for the employer to access the content of the computer tools made available to the employee.[86] The offense also requires that the intrusion was carried out in violation of security measures that had been implemented to prevent an intrusion. In other words, the perpetrator must carry out the intrusion with the aim of neutralizing security measures. Where no security measures are in place (e.g. the computer system is publicly accessible or no security

[83]Ministerio de Justicia, Organic Act 10/1995, dated 23rd November, on the Criminal Code 2015 107.
[84]Rodríguez Mesa (n 68).
[85]María del Mar Carrasco Andrino, 'El Delito de Acceso Ilícito a Los Sistemas Informáticos (Arts. 197 y 201)' in Francisco Javier Álvarez García and José Luis González Cussac (eds), *Comentarios a la Reforma Penal de 2010* (Tirant lo Blanch, 2010).
[86]Jesús David García Sánchez and Marta García Bel, 'El Poder de Control Del Empresario Sobre El Correo Electrónico de Sus Trabajadores. A Propósito de La Sentencia de La Sala de Lo Penal Del Tribunal Supremo de 16 de Junio de 2014' [2015] Actualidad Jurídica Uría Menéndez 117.

measures are in place), the conduct is not a crime. Furthermore, in the authors' opinion, the conduct is not criminal when the security measures are inadequate and therefore allow access to the data in the system.

The offense does not require any specific intent to harm or obtain an economic benefit. Therefore, as expressly highlighted by Carrasco Andrino,[87] ethical hacking would also be a crime because it is consummated with a single access to a computer system. In other words, illegal access is a conduct crime. It does not require the copying of the data, its alteration, breaking or disabling of the computer system – which would fall under the computer crimes provided for among the crimes of damage in Title XII of the Spanish Criminal Code.

Unlike the offenses of unlawful interference with data (article 264 Criminal Code) and unlawful interference with information systems (article 264 bis Criminal Code), the offense of unlawful access or intrusion does not require it to be particularly serious. In this sense, Directive 2013/40/EU only obliges States to punish serious acts. Therefore, taking into account the European requirements –and in coherence with the principles of minimum intervention and opportunity– it would be perfectly legitimate for the Spanish legislator to decide to punish only serious acts. Since we are dealing with a conduct crime, it seems obvious that the seriousness cannot refer to the result but to the action. This lesser seriousness could be assessed according to the intention of the perpetrator in carrying out the unauthorized access. For example, it could be assessed that the perpetrator communicates the vulnerability detected according to a certain protocol in order to assess the intent.

This interpretation will depend to a large extent on the legal right to be protected in the criminal precepts. If the legal right refers to intimacy and privacy, the unauthorized access alone would already harm the protected legal right. However, a different conclusion would be reached if it is considered that the protected legal right affects the security of information systems. In other words, possibilities for regulating ethical hacking in Spain depend on what the protected legal right by the 197 bis Criminal Code is.

7.2. Interpretations of the protected legal right

7.2.1. Intimacy

The crimes of discovery and disclosure of secrets have 'privacy' as a protected legal right. Among them is the crime of computer intrusion. Privacy is a fundamental right recognized in article 18 of the Spanish Constitution. Its criminal legal protection implies, according to the Spanish Supreme Court, the existence of a sphere of privacy that can be considered secret. This means that the person can decide to exclude third parties. Privacy can be understood in two different facets: as a physical space; or –for the purposes of this article– as an ideal information space.

However, there are differences between articles 197 and 197 bis Criminal Code that may allow different interpretations of the protected legal right. This difference was introduced by the Law 1/2015, which separated the crime of discovery and disclosure of secrets (article 197 Criminal Code) from the crime of computer intrusion (art. 197 bis Criminal Code). In article 197 Criminal Code, a concept of personal privacy of an individual

[87]Carrasco Andrino (n 85).

nature is handled. It is understood as an area of personal privacy from which third parties are excluded. The Constitutional Court grants the holder the power to exclude others from a sphere that he considers closed, personal and his own. However, due to the proliferation of databases that store personal data, this legal right acquires positive content. In other words, it is considered that 'the protection of the right to privacy must also include the right to control one's own personal data contained in automated databases so that the individual can decide and be guaranteed who knows and for what purpose he knows and uses such personal data'.[88]

From this double definition of the protected legal right, the intrusion into the whole or part of computer systems in which personal data of third parties are stored would damage personal privacy. This interpretation of article 197 bis of the Criminal Code poses a problem. Authorization is not required from the third parties –whose data is stored in the computer system– but from the owner of the computer system. Consequently, personal privacy is not the legal right protected in the offense of article 197 Criminal Code. Instead, personal privacy is protected in number 2 of article 197 of the Criminal Code, which punishes anyone who 'without being authorized, seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in the computer, electronic or telematic files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without being authorized, accesses these by any means, and whoever alters or uses them to the detriment of the data subject or a third party'. These conducts, as can be seen, go beyond the illicit access to a computer system typified in article 197 bis Criminal Code.

In addition, after the 2015 reform, the mere access to the computer system or part of it, rather than access to the data or programs contained in the computer system, became punishable. This reveals that the crime does not protect personal data or data relating to personal intimacy, but computer systems. Therefore, the protected legal right of this figure would be completely dissociated from the intimacy.[89]

7.2.2. Informational self-determination as a third-generation fundamental right

In the United States, privacy is a fundamental right enshrined in the 4th Amendment to the Constitution. In Spain, the Supreme Court has been expanding its content since it was recognized. It currently ranges from the immaterial sphere of the individual in everything they wish to keep private, to the right not to have one's opinions or behavior known or investigated.[90] We are referring to informational privacy. Informational privacy is the exercise of control or limitation of access to one's personal information. It affects personal data that is stored and communicated between different computer databases, and through social networks.[91] From the moral dimension of privacy, some philosophers configure

[88]Luz María Puente Aba, 'Delitos Contra La Intimidad y Nuevas Tecnologías' [2007] Eguzkilore: Cuaderno del Instituto Vasco de Criminología 163, 165.

[89]M Asunción Colás Turégano, 'Nuevas Conductas Delictivas Contra La Intimidad (Arts. 197, 197 Bis, 197 Ter)' in José Luis González Cussac, Elena Górriz Royo and Ángela Matallín Evangelio (eds), *Comentarios a la Reforma del Código Penal de 2015* (Tirant lo Blanch, 2015).

[90]Antonio Orti Vallejo, 'El Nuevo Derecho Fundamental (y de La Personalidad) a La Libertad Informática (A Propósito de La STC 254/1993, de 20 de Julio)' [1994] Derecho privado y Constitución 305.

[91]Herman T Tavani, 'Informational Privacy: Concepts, Theories, and Controversies' in Kenneth Einar Himma and Herman T Tavani (eds), *The Handbook of Information and Computer Ethics* (John Wiley & Sons, Inc, 2008) <https://onlinelibrary.wiley.com/doi/10.1002/9780470281819.ch6> accessed 24 February 2022.

the right to privacy as an absolute and indisputable right. The right to privacy, for these authors, acquires the status of Human Rights.[92]

In Spain, Supreme Court Decision 254/1993, of June 20, 1993, outlines the possibility of creating a new fundamental right, integrated among the rights related to the personality. Specifically, in Article 18.4 of the Spanish Constitution, on the subject of computer files containing personal data. This line is developed, among others, by Pérez Luño.[93] The author argues that the new right should be recognized as a third-generation fundamental right. The author argues that it should not be relegated to a mere appendix of other constitutional values or rights. Pérez Luño insists on this need when he states that, in computerized societies, power rests on the use of information. This information makes it possible to influence and control the behavior of citizens. Therefore, the protection of personal data 'constitutes an important criterion for the political legitimization of technologically developed democratic systems'.

Regardless of the interpretation, the conduct of access and knowledge of both personal data and data that form part of the most intimate core of individuals would be violating the essential content of the right to privacy. In cases of 'police hacking', in which law enforcement agencies access a computer system with the intention of discovering breaches in the system and illegal content (i.e. remote access to the computer system, acoustic and audiovisual surveillance, tracking and tracing), the Spanish Criminal Procedure Act[94] enables the State to use spyware programs for investigative purposes. The use of spyware to detect vulnerabilities or security breaches in a computer system by the State means that the authorities use the same techniques as hackers, though with a different purpose; that of discovering the commission of a crime and the person suspected of committing it. In this case, the intrusion requires judicial authorization and is directed against a specific person; the suspect.[95]

While some European Union countries allow remote search measures of computer systems as security and crime prevention measures –for example, in Germany, they exist in intelligence (*Verfassungsschutz*) and security forces (*Polizeirecht*)– Spain does not allow investigative measures restricting fundamental rights.[96] Even so, the 'remote search' provided for in article 588 *septies* of the Spanish Civil Procedure Law[97] –i.e. remote access that allows both access to the contents of the computer and real-time monitoring of the activity carried out without the user's knowledge– is a controversial measure due to its high degree of intrusion in the sphere of privacy, both due to the lack of knowledge of the subject and its extension in time.[98] In order to prevent the intrusion from affecting the essential core of the right to privacy, article 588 bis of the Criminal Procedure Act incorporates a series of 'guiding principles' common to all these technological research measures. It establishes that they must satisfy the principles of specialty,

[92]See e.g., Lee Andrew Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247.
[93]Antonio Enrique Pérez Luño, *Los derechos humanos en la sociedad tecnológica* (Universitas, 2012).
[94]Royal Decree of 14 September 1882 approving the Law of Criminal Procedure, amended by Law 13/2015.
[95]Hernán Blanco, 'El Hackeo Con Orden Judicial En La Legislación Procesal Española a Partir de La Ley Orgánica 13/2015 Del 5 de Octubre' [2021] InDret 431.
[96]Lorena Bachmaier Winter, 'Registro Remoto de Equipos Informáticos y Principio de Proporcionalidad En La Ley Orgánica 13/2015' (2017) 71 Boletín del Ministerio de Justicia 1, 8.
[97]Law 1/2000, of 7 January, on Civil Procedure.
[98]Bachmaier Winter (n 96).

suitability, exceptionality, necessity and proportionality, the concurrence of which must be sufficiently justified in the enabling judicial resolution.[99]

However, even if privacy were accepted as a third-generation fundamental right susceptible to criminal protection, its content is not far from that of personal intimacy. Therefore, it poses the same problems when trying to configure it as the protected legal right in the crime of computer intrusion.

7.2.3. The security of information systems

When faced with the problem of the legal right protected in cybercrime, we recommend taking a relativist position in line with other authors.[100] This position argues that, when the novelty of the computer crime lies in the means employed, the legal right protected shall be that which corresponds to the nature of the offense committed. For example, cyber-enabled crimes, such as fraud. In these crimes, computer systems are used only as a tool to perpetrate the fraud.[101] Therefore, the protected legal right is patrimony. On the other hand, when the crime damages the integrity of the computer system (i.e. hardware, software system, applications, or data), a new legal right appears that gives these crimes their own autonomy. In other words, in cyber-dependent crimes, the legal property protected is new and specific to this type of crime.[102]

The location of computer crimes in the Criminal Code, between crimes against privacy (i.e. unlawful access) and crimes of damage (i.e. unlawful interference with computer data and systems), makes it difficult to consider them as autonomous crimes in which a legal right other than intimacy and privacy –in the first case– and the property of others –in the second– are protected. However, Budapest Convention expresses in this sense when it states that 'the legal interest protected here is the integrity and proper functioning or use of stored data and software'. According to ISO/IEC 17799:2000, the content of information security is the preservation of confidentiality, integrity and availability of information. This conception could lead to understanding that both the crimes typified as computer damages, as well as those typified in article 197 bis Criminal Code, respond to the guarantee of the information stored, processed and transmitted in a computer system.

The discussion revolves around whether information security meets the necessary requirements to be guaranteed legally and autonomously through criminal law.[103] The European Commission is particularly concerned about the proper functioning and security of computer systems in order to ensure a secure information society free from cyber-attacks. From this perspective, we can state that, through criminal law protection of the integrity and availability of the information contained in computer networks and media, the security of computer information systems is guaranteed.[104]

[99]Blanco (n 95) 44.
[100]For example, see Francisco Bueno Arús, 'El Delito Informático' [1994] Actualidad Informática Aranzadi 2.
[101]Mike McGuire and Samantha Dowling, 'Chapter 2: Cyber-Enabled Crimes -Fraud and Theft' (Home Office, 2013) Research report 75 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf> accessed 7 April 2020.
[102]David Maimon and Eric R Louderback, 'Cyber-Dependent Crimes: An Interdisciplinary Review' (2019) 2 Annual Review of Criminology 191.
[103]Rodriguez Mesa (n 43) 64.
[104]Carmen Tomás-Valiente Lanuza, 'Articles 197–201 of the Discovery and Revelation of Secrets' in Manuel Gómez Tomillo (and), *Practical comments on the Criminal Code*, theft 2 (1st Edition, Aranzadi Thomson Reuters, 2015); Carrasco Andrino (n 66); Colás Keep us (n 70); Jorge Alexandre González Hurtado, 'Security in Information Systems as an Autonomous

Furthermore, as Rodriguez Mesa states,[105] the increasing quantitative and qualitative importance of the information contained in the computer media of an increasingly digitized society 'fully justifies the creation of a legal asset that responds to a new basic need of people and of the processes of social relations'. As for the content of this new legal right, it would take the form of the confidentiality, availability and integrity of data and computer systems.

While article 197 bis would protect the confidentiality of computer systems, such confidentiality must be placed in the context of security. Security is understood as the absence of vulnerabilities that allow access to systems and data by third parties. But, as Mayer Lux emphasizes,[106] the mere reference to computer security fails to fully explain the wrongfulness of computer crimes involving the use of computer networks because the idea of security only refers to the absence of risk in the use of computer systems. According to the author,[107] 'before being secure, computer systems must be efficient and effective, that is, capable of (adequately) performing the operations of storage, processing or transfer of data'. From this reflection derives the idea that computer security only contributes to explaining the wrongfulness of computer crimes using computer networks 'to the extent that it acts as a quality of an efficient and effective computer system'.

8. Regulatory models of ethical hacking in Spain

The regulation of ethical hacking programs depends on three factors: (a) the legal right protected, (b) the subject granting authorization, and (c) the type of organization. Ethical hacking would be excluded from the Spanish legal system if the protected legal right was considered to be personal intimacy. Consequently, the authorization of third parties shall be required to access the computer system which contains their personal data.

Under the interpretation of a violation of personal privacy, the owners of the data –and not the owner of the system– will have to provide the authorization. Today, this problem is largely blurred by generic data protection clauses. In these clauses, the company is authorized in advance to access the data. Consequently, the authorization for the company to authorize access to the computer system by a third party is also transferred. Under this interpretation, no criminal conflict would exist when a person who has been hired and authorized to detect vulnerabilities accesses a system. However, bug bounty programs, and especially the CVD model, do pose criminal legal conflicts.

Regarding bug bounty programs in Spain, there are a few platforms. For example, one of the first bug bounty platforms in Spanish is *Epic Bounties*. *Epic Bounties* is a service that mediates between security researchers and companies that decide to launch their bounty program. The platform exclusively fulfils a mediation service since the contract is signed between the company or organization and a community of ethical hackers so that they can detect possible vulnerabilities in the company's systems and networks. Once a vulnerability has been detected, it is reported to the companies so that they can take the

Legal Asset. European and Spanish Perspective' [2016] Revista Penal México 59; Norberto Javier de la Mata Barranco, 'Crimes Against the Integrity and Availability of Data and Computer Systems After THE LO 1/2015' in Silvina Bacigalupo and others (eds), *Criminal Law Studies: tribute to Professor Miguel Bajo* (Editorial Universitaria Ramón Areces, 2016).

[105]Rodríguez Mesa (n 68) 65.

[106]Laura Mayer Lux, 'El Bien Jurídico Protegido En Los Delitos Informáticos' (2017) 44 Revista chilena de derecho 261, 234.

[107]ibid 235.

necessary measures to avoid attacks in the future. The value of the reward will depend on the severity of the vulnerability found.

Accepting that access must be authorized by the company or organization that owns the information system –and not by the third-party data owners– the company's contract with the ethical hackers is already sufficient authorization for the conduct not to be a crime. This is a model compatible with the current regulation.

The viability of ethical hacking programs in Spanish Public Administrations is not as simple. Unlike other countries, the Spanish Public Administration does not resort to ethical hacking programs. Vulnerabilities in Public Administration computer systems can only be discovered by employees or officials. As we mentioned earlier in the paper, only one pilot experience can be found in Spain. The *Generalitat de Catalunya* invited 15 hackers to carry out the first bug bounty of a public administration in Spain. The purpose of this pilot experience –in addition to identifying vulnerabilities in information systems to prevent future cyber-attacks– was to assess the possibilities and risks of this type of program in the public sector. Despite the success of the program, there are many obstacles –mainly administrative– that would have to be regulated so that bug bounty programs could become a viable alternative in the Public Administration.

Among the biggest limitations is the rigidity of the regulations on contracting in the Public Administration (i.e. public offer, delimitation of tasks, salary, determination of the contractor, etc.). These regulations, strongly anchored in administrative law, are incompatible with the flexibility required by bug bounty programs. For example, the need for administrative law to foresee all assumptions in advance clashes with the fact that the amount of the hacker's reward for detecting a vulnerability will depend on the detected vulnerability seriousness. On the one hand, it would be necessary to design a specific administrative contract that includes the particularities of bug bounty programs. On the other hand, a series of limits, commitments and prohibitions should be established for hackers participating in the program. In this sense, it must not be forgotten that ethical hackers are being given access to public computer systems with sensitive and confidential data – and even to critical infrastructures computer systems.

Finally, with regard to CVD programs, Spain has not even considered its implementation. Considering the current wording of article 197 bis Criminal Code, in which mere unauthorized access is a crime, the communication of a serious vulnerability by an ethical hacker to a company or public body would be proof of illicit access and, therefore, of the crime commission. This fact explains why vulnerabilities detected by ethical hackers are not usually communicated –or the communication anonymous– as the experts pointed out during the Delphi study (see Section 4).

The implementation of a CVD model in Spain –as in The Netherlands, the United States and Japan– would require a modification of the current typification that would exempt from criminal responsibility ethical hackers who communicate the vulnerability detected. As we discussed above, both the Budapest Convention and Directive 2014/40/EU allow this approach. Before analyzing the possible models of criminal exemption, it should be noted that CVD programs are possible only if the legal right protected is the security of computer systems – and not personal intimacy or privacy. Otherwise, both personal intimacy and privacy would be subject to injury with mere unauthorized access, regardless of cybercriminal intention. However, if the approach of defining the protected legal right as the security of computer systems is taken – specified in the case of article 197 bis

CP in the confidentiality of computer systems– those behaviors that are aimed at enhancing the security of the whole or part of a computer system –through vulnerabilities detection and communication– would not harm the protected legal right, but contribute to its protection. In other words, ethical hackers would rather help to improve the security of computer systems by protecting their confidentiality against potential illegal intrusions.

There are two alternatives to exempt from criminal liability the ethical hacker acting under a CVD policy – only if the security of computer systems is the legal right protected. On the one hand, it can be demanded that the intrusion be carried out with criminal intention. On the other hand, a clause of exemption from criminal responsibility in cases in which the vulnerability is communicated in accordance with previously established protocols can be included. Of these two alternatives, the former does not require a prior regulation of a CVD policy since the absence of the subjective element –i.e. criminal intention– prevents the behavior from being a crime. However, despite being a simpler solution in coherence with the Budapest Convention and the Directive, it would decriminalize electronic snooping. The latter alternative requires having a CVD protocol in advance and would only exempt from criminal responsibility those who detect and disclose the vulnerability in accordance with the established protocol. The exemption, which would have to be configured as a blank criminal rule with respect to the CVD protocol, would find its basis in the absence of harm of the protected legal right – i.e. the security of computer systems.

The adoption of a CVD policy would increase the security of organizations. However, the organization shall be able to respond to the vulnerability detected. Once the CVD policy is implemented in a State, any organization can receive a vulnerability report. However, when there is no CVD policy, vulnerability researchers are unclear about how the organization will respond. Researchers are at risk that they, however well-intentioned, are prosecuted as criminals. Thus, the possibility of an unexpected reaction by the organization may deter potential researchers. An organization not supported by a CVD policy may, for instance, not know how to respond or not understand the vulnerability and, therefore, might decide to ignore it or deny the existence of the vulnerability. As we analyzed above in the Delphi study, it may even be the case that the company misinterprets the intentions of the researcher and reports it to the police.[108] In this context, regulations must be adapted to new cybersecurity needs. Spain should take advantage of the resources available by offering legal certainty to both companies and ethical hackers.

9. Conclusions

This paper analyzed the possibilities of the regulation of ethical hacking in the context of Spain. Two possible models of ethical hacking were analyzed: bug bounty programs and coordinated vulnerability disclosure policies. We carried out an extensive study, both empirical and normative. First, this paper offers the results of an extensive Delphi study on the current role of ethical hackers and stakeholders' acceptance of a regulation that allows intrusion into computer systems without the organization's direct hiring of a security analyst. Second, we studied the international, European, and national regulations to

[108]Weulen Kranenbarg, Holt and van der Ham (n 79).

understand the possibilities of a regulation of ethical hacking. The results of these comprehensive studies allow us to formulate the following conclusions.

Firstly, according to the results of the Delphi study, cybersecurity experts agreed that ethical hackers are relevant actors in the cybersecurity governance landscape in Spain. They contribute to cybersecurity by disclosing the vulnerabilities in computer systems through penetration tests in order to prevent future cybercrimes. However, due to the limitations of current regulations, the possibilities of performing penetration tests in Spain are limited to when there is a contract between the company and the security analyst. In the Delphi study, however, we obtained that a regulation that facilitates bug bounty programs and CVD policies would be widely accepted by stakeholders in Spain, regardless of their professional sector.

Secondly, the Budapest Convention allows for an interpretation of intrusions into computer systems that is compatible with bug bounty programs and CVD policies. Perhaps this is the reason why we could find experiences of several countries that have either participated in bug bounty programs or have approved CVD policies.

Thirdly, European law also offers possibilities for the regulation of ethical hacking programs. Directive 2013/40/UE leaves the interpretation of the offence of intrusion into computer systems to the discretion of the Member States. Moreover, we highlight how preamble 12 offers an opportunity to develop bug bounty programs or CVD policies by expressly supporting actions that encourage the disclosure of vulnerabilities in computer systems.

Fourthly, we analyzed the possibilities offered by the Spanish criminal law with respect to a regulation of bug bounty programs or CVD policies. According to our analysis, the feasibility of ethical hacking policies depends on the legal right protected, the subject granting authorization, and the type of organization. According to our analysis, the most important element is the definition of the legal right protected. If it is understood that article 197 bis Criminal Code protects either personal intimacy or privacy, the computer systems intrusion shall be considered a conduct crime. However, if the legal right protected is the security of computer systems, then both bug bounty programs and CVD policies would be contributing to protecting the legal right. Under the latter interpretation, computer systems intrusion under ethical hacking programs would not be a crime.

In this paper, we support the second interpretation. However, an implementation of this policy must be carried out gradually. We recommend starting by precisely defining ethical hackers and their missions, as well as establishing mechanisms to differentiate their activity from that of cybercriminals. These mechanisms must be able to identify when hackers are acting ethically.[109] There are already some mechanisms, such as ethical hacking certifications – e.g. the Certified Ethical Hacker, CEH, by the International Council of Electronic Commerce Consultants. In addition, it would be advisable to guarantee the ethics of hackers' conduct through scrupulous and transparent action protocols. For instance, the communication of the vulnerability should be carried out immediately, both to the company and to the police.

[109]Danish Jamil and Muhammad Numan Ali Khan, 'Is Ethical Hacking Ethical?' (2011) 3 International Journal of Engineering Science and Technology 3758.

F. Scott Fitzgerald wrote, 'So we beat on, boats against the current, borne back ceaselessly into the past'.[110] When we think of ethical hackers, bug bounty programs, and CVD policies, Fitzgerald's words make sense in an unexpected realm. After all, neither the bug bounty programs nor the figure of bounty hunters is new. One could envision in today's ethical hackers an evolution of the former bounty hunters, reformed criminals who protected the population in exchange for economic rewards and who were regulated by the Highwayman Act in England in 1692. These bounty hunters ended up being the germ of the London Metropolitan Police. Today's ethical hackers may be but the germ of the police of the future.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Authors' statement

Cristina Del-Real: Conceptualization, Methodology, Validation, Formal Analysis, Investigation, Resources, Data curation, Writing – Original Draft (Sections 1, 2, 4 and 9), Writing – Review & Editing, Visualization, Project administration. María José Rodríguez Mesa: Validation, Formal Analysis, Investigation, Resources, Writing – Original Draft (Sections 3, 5, 6, 7 and 8), Writing – Review & Editing, Supervision.

Acknowledgements

This work is part of the doctoral thesis 'La gobernanza de la ciberseguridad en España: Un estudio empírico de los actores, redes de colaboración y prospectiva desde las teorías de la seguridad plural', defended on 10th September 2021 in Jerez de la Frontera (Cádiz, Spain). The authors want to thank Dr. Antonio M. Díaz Fernández (University of Cádiz) for his comments on previous versions of this article.

ORCID

Cristina Del-Real http://orcid.org/0000-0003-3069-4974
María José Rodriguez Mesa http://orcid.org/0000-0003-4977-9978

Appendix. Invitation email to the Delphi study.

Hello [Name of person],

I am delighted to contact you. I am a PhD candidate in criminology at the University of Cadiz, where I am writing a thesis on the cybersecurity governance in Spain.

I would like to invite you to participate in the panel of experts of the Delphi study I am conducting

[110]F Scott Fitzgerald, *The Great Gatsby* (Alma Classics, 1925).

for my thesis. This type of study seeks to obtain the consensus opinion of experts on a topic. Your participation would be anonymous, and your opinions will never represent any organization.

The procedure is very simple and will not take much time from you. The survey is structured in three Rounds, each lasting about 7 min. In the following link [LINK] you can find the questionnaire to Round 1.

I will send you the link to Round 2 in September, and to Round 3 in October. If you decide to participate, your response to all three Rounds is very important for me to be able to use the data.

At the end, I will send you a report with a summary of the main results, in case they are of interest to you.

If you have any questions, please do not hesitate to contact me.

Best regards and, again, my sincere thanks in advance,

Cristina.