Cilt: 10 Sayı:2, 2023, ss. 615-631
PAMUKKALE ÜNİVERSİTESİ
İŞLETME ARAŞTIRMALARI DERGİSİ (PIAR)
Pamukkale University Journal of Business Research
https://dergipark.org.tr/tr/pub/piar

Cybersecurity Whistleblower Protection: A Comparison of the US and the EU Approaches

Siber Güvenlik İhbarcılarının Korunması Açısından ABD ve AB Yaklaşımlarının Karşılaştırılması

Özlü DOLMA[1*]

[1] Pamukkale University, odolma@pau.edu.tr, ORCID: 0000-0002-3947-898X
* Yazışılan Yazar/Corresponding author

Makale Geliş/Received: 12.04.2023 Makale Kabul/Accepted: 23.06.2023

Araştırma Makalesi / Research Paper DOI: 10.47097/piar.1281937

Abstract

This study compares the laws in the United States and the European Union protecting cybersecurity whistleblowers from employer retaliation. Similarities and differences exist regarding the scope of laws, the definition of "retaliation," and required reporting procedures to be eligible for legal protection. In the US, no anti-retaliation federal statute directly addresses cybersecurity whistleblowing, but whistleblowers may still be protected when they disclose cybersecurity-related violations of laws falling within the scope of protected activity under the current laws. In the EU, the Directive (EU) 2019/1937 directly protects employees who report breaches falling within the scope of the EU acts, including the protection of privacy and personal data and the security of network and information systems. The two approaches also differ concerning the confidentiality of the reporting person's identity. This study provides a brief foundation for understanding how the US and EU's approaches differ in providing legal protection against retaliation for whistleblowers.

Keywords: *Whistleblowing, cybersecurity, retaliation, Directive (EU) 2019/1937, whistleblower protection.*

Jel Codes: *K24, K31, M15.*

Öz

Bu çalışma, siber güvenlik ihbarcılarını işverenlerin misilleme eylemlerine karşı koruyan Amerika Birleşik Devletleri ve Avrupa Birliği yasalarını karşılaştırmaktadır. Yasalar, kapsam, "misilleme"nin tanımı ve yasal korumaya hak kazanmak için gereken raporlama prosedürleri açısından benzerlikler ve farklılıklar göstermektedir. ABD'de hiçbir misilleme karşıtı federal yasa doğrudan siber güvenlik ihbarcılığını ele almamaktadır, ancak ihbarcılar mevcut yasalarla korunan faaliyet kapsamına giren siber güvenlikle ilgili yasa ihlallerini ifşa ettiklerinde yine de korunabilirler. AB'de, ihbarcı misillemelerine karşı yasal koruma daha az belirsizdir çünkü 2019/1937 sayılı Direktif (AB), gizlilik ve kişisel verilerin korunması ile ağ ve bilgi sistemlerinin güvenliği gibi AB yasaları kapsamında olan ihlalleri bildiren çalışanları doğrudan korumaktadır. Bu iki yaklaşım, bildirimde bulunan kişinin kimliğinin gizliliği konusunda da farklılık göstermektedir. Bu çalışma, ABD ve AB'nin genel olarak ihbarcılara ve özellikle siber güvenlik ihbarcılarına misillemeye karşı yasal koruma sağlama konusunda nasıl farklılıklar gösterdiğini ortaya koymayı hedeflemektedir.

Anahtar Kelimeler: *İhbar (bilgi uçurma), siber güvenlik, misilleme, 2019/1937 sayılı Direktif (AB), çalışanların korunması*

Jel Kodları: *K24, K31, M15.*

1. INTRODUCTION

This study aims to compare the United States and the European Union's approaches to the legal protection of corporate whistleblowers against retaliation. The similarities and differences between the regulations are discussed in terms of the following aspects; (i) the scope of laws and regulations protecting whistleblowers from retaliation, (ii) the definition of "retaliation," and (iii) required reporting procedures to qualify for legal protection. Special attention is given to whether and how cybersecurity whistleblowers are protected against retaliation under each legislation and whether the confidentiality of the reporting person's identity is assured.

As the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (hereinafter: the EU Directive) indicates, employees, working for a public or private organization and persons who are in contact with such an organization in the context of their work-related activities are most of the time the first to know about threats or harm to the public interest which can arise in that context. Accordingly, by acting as "whistleblowers" individuals who report breaches of Union law that are harmful to the public interest, such persons can significantly contribute to detecting and preventing law violations and safeguarding society's welfare.

"As individuals who escalate concerns regarding internal management of cyber risks, cyber threats, data breaches, or other cybersecurity-related information to supervisors, compliance officers, and boards of directors" (Pacella, 2016: 40), cybersecurity whistleblowers can significantly contribute to the timely detection and effective remediation of potential cybersecurity risks and incidents. In fact, the critical role of cybersecurity whistleblowers has been somehow addressed by the US Securities and Exchange Commission (SEC), the primary regulator of publicly traded companies, with the 2018 Cybersecurity Guidance (Commission Statement and Guidance on Public Company Cybersecurity Disclosures) issued as a supplement to the 2011 Guidance. In this legally non-binding guidance, the SEC emphasized the importance of appropriate and timely identification and reporting of information related to cybersecurity risks and incidents in companies operating in all industries. The Commission encouraged companies "to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure" (US Securities and Exchange Commission, 2018: 18).

Unfortunately, potential whistleblowers often do not prefer to raise their concerns or suspicions of misconduct since they can encounter retaliation in various forms, such as harassment, firing, or threats. The EU Directive highlights that potential whistleblowers are reluctant to disclose their concerns or suspicions of wrongdoings because of the fear of retaliation. Employees may become vulnerable to mistreatment by their employers in terms of termination of employment, negative impact on promotions or salary, unjustified negative performance assessment, transfer and change of workplace, harassment, or discrimination (Kaufmann et al., 2020). They may even be alienated by their co-workers, bullied, and labeled as "traitors" by their colleagues (Teichmann and Wittmann, 2022). Cybersecurity whistleblowers are no different; like all whistleblowers, they also experience retaliation for their disclosures (Pacella, 2016). Therefore, granting legal protections against retaliation and

ensuring the confidentiality of the reporting person's identity can encourage employees to report their concerns regarding law violations (European Data Protection Supervisor, 2016), including those related to cybercrime and cybersecurity vulnerabilities.

The importance of providing balanced and adequate whistleblower protection is increasingly acknowledged at the European and international levels (Directive (EU) 2019/1937). The US and the EU have enacted laws and regulations to address this issue. Nevertheless, they have significant differences in many respects, including the anti-retaliation protection for cybersecurity whistleblowers. The EU Directive stipulates minimum common standards for whistleblowing protection across the Member States' jurisdictions. It protects employees who report breaches falling within the scope of the EU acts concerning various areas, including the protection of privacy and personal data and the security of network and information systems. In contrast, in the US legislation no federal statute directly addresses cybersecurity whistleblowing and a possible protection must be interpreted from various existing federal or state laws (Pender et al., 2021).

Recognizing the importance of whistleblower protection, the US has enacted statutes with whistleblowing protection provisions for public and private company employees. These legal protections afforded to whistleblowers aim to encourage employees to disclose observed organizational wrongdoing (Exmeyer and Jeon, 2020). While laws such as the Whistleblower Protection Act (WPA) of 1989 and the Whistleblower Protection Enhancement Act (WPEA) of 2012 explicitly provide uniform protections to whistleblowers at the federal level, other federal statutes do not directly provide retaliation protection for whistleblowers. However, they may still form a basis to offer safeguards for those alleging wrongdoing. In addition to this diversity of regulations at the federal level, all the states have specific statutes to protect whistleblowers, which also vary considerably among them (Exmeyer and Jeon, 2020). Some laws and regulations compared below in detail reveal the diversity of practices.

2. US FEDERAL STATUTES PROVIDING PROTECTIONS TO CYBERSECURITY WHISTLEBLOWERS

The first and most crucial difference between the US and the EU approaches to whistleblower protections lies in the fact that in the US, various federal statutes and state laws can provide legal protections for employees who report violations of laws. However, no one principal statute protects whistleblowers against retaliation (Marcum and Young, 2020). Existing US laws protect certain employees and industries (Kohn, 2017). Moreover, no federal laws specifically protect cybersecurity whistleblowers. However, current anti-retaliation regulations may still apply to employees who raise concerns regarding security flaws or data breaches (Hammer and Bundschuh, 2016).

For instance, in 2002, the Congress passed Sarbanes-Oxley Act (SOX), which provides protections for employees of publicly traded companies who provide evidence of fraud. The SOX requires public corporations to establish and maintain proper internal control structure and procedures for financial reporting and obliges them to disclose all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls (Sarbanes-Oxley Act, 2002). Internal control structure and procedures include maintenance of records that appropriately reflect the

transactions and dispositions of the assets of the issuer to permit preparation of financial statements in accordance with generally accepted accounting principles (Sarbanes-Oxley Act, 2002). Furthermore, the act stipulates that companies may not discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment of any lawful act done by the employee in providing information that the employee reasonably believes to be a violation of specified federal law, any SEC rule or regulation, or any federal law that relates to fraud against shareholders (18 U.S.C. § 1514A, 2021). Thus, it is reasonable to conclude that employees of public corporations who report flaws in cybersecurity policies and procedures, which were designed for preventing and detecting any misuse or improper disposition of information stored in digital form, may have a statutory cause of action under this law (Hammer and Bundschuh, 2016). However, given the absence of binding cybersecurity regulations, it is still possible that their reports may fall outside the scope of "protected activity" (Pacella, 2016).

Later in 2010, the Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act, which introduced enhanced provisions to encourage and protect corporate whistleblowers (Leifer, 2014). The Dodd-Frank Act defined the term "whistleblower" as "any individual who provides, or two or more individuals acting jointly who provide, information relating to a violation of the securities laws to the SEC in a manner established, by rule or regulation, by the Commission" (15 USC § 78u–6(a)(6), 2021). As in the SOX, according to the Dodd-Frank Act, no employer may discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment because of any lawful act done by the whistleblower in (1) providing information to the SEC in accordance with the whistleblower incentive section, (2) initiating, testifying in, or assisting in any investigation or judicial or administrative action of the SEC based upon or related to such information, or (3) making disclosures that are required or protected under the Sarbanes-Oxley Act of 2002, the Securities Exchange Act of 1934, and any other law, rule, or regulation subject to the jurisdiction of the SEC (15 U.S.C. § 78u-6, 2021). Although the SEC has been taking a proactive approach to whistleblowing, and cybersecurity whistleblowing in particular (US Securities and Exchange Commission, 2018), whether cybersecurity whistleblowers can take advantage of the protection under the Dodd-Frank Act still remains as a "grey area" (Pender et al., 2021).

There are two other SEC regulations, namely, "Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information" and "Regulation S-ID: Identity Theft Red Flags", which may encourage employees of non-public companies for engaging in whistleblowing activities without fear of retaliation by their employer. Regulation S-P requires that every investment company and every investment adviser registered with the Commission must protect the security and confidentiality of customer records and information by adopting the necessary written policies and procedures for this purpose (17 C.F.R. § 248.30, 2013). Regulation S-ID, on the other hand, imposes that "each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account" (17 C.F.R. § 248.201(d), 2020). Given that Regulation S-P and Regulation S-ID are subject to the jurisdiction of the SEC, an employee who reports cybersecurity risks and incidents regarding

the security and confidentiality of customer records and information or an employer's failure to have an adequate identity theft program can be protected under the Dodd-Frank Act. It may protect employees of non-public companies who raise these concerns, provided they are subject to Regulations S-P and S-ID, such as registered investment companies or registered investment advisors (Ronicker and LaGarde, 2019).

A regulation that explicitly protects whistleblowers against retaliation is the Federal Acquisition Regulation (1984). It was issued as Chapter 1 of Title 48 of the Code of Federal Regulations, which is the primary regulation for use by all executive agencies in their acquisition of supplies and services with appropriated funds. It became effective in April 1984, and the Department of Defense (DoD), General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) jointly issued the FAR. In Subpart 3.9, "Whistleblower Protections for Contractor Employees," it is stated that "Government contractors shall not discharge, demote or otherwise discriminate against an employee as a reprisal for disclosing information to a Member of Congress, or an authorized official of an agency or of the Department of Justice, relating to a substantial violation of law related to a contract (including the competition for or negotiation of a contract)" (48 C.F.R. § 3.9, 2021). Furthermore, in acquiring information technology, the FAR obliges agencies to have the appropriate information technology security policies and requirements and the standard security configurations listed on the National Institute of Standards and Technology's website (48 C.F.R § 39.101(c), 2021). Any failure of agencies to adhere to these standards may lead to disclosure under the FAR. In particular, cybersecurity professionals who disclose their government-contractor employer's failure to meet these standards may therefore be granted protections against retaliation.

According to a provision issued by the US Nuclear Regulatory Commission (NRC) in 2009, under the section "Physical Protection Requirements at Fixed Sites," entitled "Protection of Digital Computer and Communications Systems and Networks," "each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks, up to and including the design basis threat as described in the general provisions of Part 73.1" (10 C.F.R § 73.54, 2022). The NRC explicitly states that "it is illegal for licensees to take discriminatory action, such as firing, reduction of pay, poor performance appraisals, or reassignment to a lower position or job, against a worker for raising safety concerns to management or the NRC" (US Nuclear Regulatory Commission (NRC), 2017: 5) Thus, any employee of an NRC licensee who raised a cybersecurity safety concern can be considered engaged in protected activity.

The US Health Insurance Portability and Accountability Act of 1996 (HIPAA) also protects whistleblowers from retaliation. The HIPAA Security Rule (2013) establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity (e.g., a health plan or a health care clearinghouse) and requires appropriate administrative, physical, and technical safeguards to ensure electronically protected health information's confidentiality, integrity, and security (US Department of Health and Human Services Office for Civil Rights, 2022). It states that "a covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for filing a

complaint based on the belief that a covered entity or business associate is not complying with the administrative simplification provisions" (HIPAA Administrative Simplification Regulation Text 45 C.F.R. § 160.316, 2013). Furthermore, the HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information (US Department of Health and Human Services Office for Civil Rights, 2013). Covered entities must have written policies and procedures regarding breach notification in place. Thus, a cybersecurity whistleblower in the healthcare field who works for an entity subject to these regulations and reports law violations by their employer may be entitled to protection against retaliation.

Retaliation protections are also under other regulations for whistleblowers reporting misconduct in various industries and administrative areas. The diversity of federal statutes that can provide legal protections for whistleblowers reveals that understanding what constitutes protected activity under each of these statutes is essential for effectively asserting a claim since cybersecurity whistleblowing is not the explicit focus of any of those laws. The anti-retaliation protections granted depend on the entity the whistleblower works for, the wrongdoing the whistleblower reports, and the procedures used to report it (i.e., internally or externally) (Ronicker and LaGarde, 2019). This diversity of federal laws in the US concerning protection against retaliation renders finding the applicable law that may protect the whistleblower a daunting task (Marcum et al., 2019). Further, the lack of a binding regulation that fully protects cybersecurity whistleblowers from retaliation will likely discourage them from reporting misconduct (Pacella, 2016).

3. THE EUROPEAN WHISTLEBLOWER PROTECTION DIRECTIVE

In the case of the EU, however, the EU Directive explicitly states that, in terms of the material scope, it applies to reports concerning defined breaches falling within the scope of the Union acts concerning various areas, including the protection of privacy and personal data, and security of network and information systems. Under the EU Directive, a whistleblower is granted protection when reporting breaches of EU laws in the areas of public procurement, financial services, products and markets, prevention of money laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, and security of network and information systems.[1] The EU Directive applies to reporting persons working in the private or public sector who acquired information on breaches in a work-related context, including employees, civil servants, persons having self-employed status, shareholders, and persons belonging to the administrative, management, or supervisory body of an undertaking, including non-executive members, volunteers, and paid or unpaid trainees, any persons working under the supervision and direction of contractors, subcontractors, and suppliers (Directive (EU) 2019/1937, Article 4, Personal Scope 1. (a)-(d)). Protecting all types of employees without making any distinction in terms of their employment status is one of the

[1] The EU Directive lists in its Annex following Union legislation on the protection of privacy and personal data and security of network and information systems: Directive on Privacy and Electronic Communications (2002), General Data Protection Regulation (2016), and Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

distinguishing characteristics of the EU Directive compared to the US federal and state statutes.

In contrast to the US approach, the EU Directive expressly states that "the respect for privacy and protection of personal data is considered crucial as fundamental rights in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union are the areas in which whistleblowers can help to disclose breaches, which can harm the public interest" (Directive (EU) 2019/1937: 20). Furthermore, it is indicated that "whistleblowers can also help disclose breaches of Directive (EU) 2016/1148, which introduces a requirement to provide notification of incidents, including those that do not compromise personal data, and security requirements for entities providing essential services across many sectors" (Directive (EU) 2019/1937: 20). Moreover, the EU Directive emphasizes the importance of ensuring the continuity of services essential for the functioning of the internal market and the well-being of society. Accordingly, whistleblowers' reporting in this area is considered crucial since it can help the prevention of security incidents which would have an impact on key economic and social activities and widely used digital services and the prevention of any infringement of EU data protection rules.

4. THE DEFINITION OF "RETALIATION" IN US AND EU WHISTLEBLOWING LAWS

Although there are some similarities in terms of what constitutes an "adverse treatment" or a "retaliation" suffered by the reporting person under the EU Directive and the US federal statutes and state laws, compared to the US approach, the EU Directive has a more comprehensive and precise definition of retaliation. In Article 5, the EU Directive defines retaliation as "any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or public disclosure, and which causes or may cause unjustified detriment to the reporting person." Unlike the US federal statutes and state laws, the EU Directive provides a clear and comprehensive list of forms of retaliation, including threats of retaliation and attempts of retaliation, against reporting persons. Some forms of retaliation for which Member States need to take the necessary measures to prohibit are suspension, lay-off, dismissal or equivalent measures, demotion or withholding of promotion, change of location of the place of work, reduction in wages, change in working hours, withholding of training, a negative performance assessment or employment reference, imposition or administering of any disciplinary measure, reprimand or other penalties, including a financial penalty, discrimination, disadvantageous or unfair treatment (Directive (EU) 2019/1937, Article 19).

In the US, on the other hand, each federal statute that may provide legal protections to a whistleblower explains what constitutes a "retaliation" or an "adverse action" in its unique way. For instance, according to both Dodd-Frank and SOX, "no employer may discharge, demote, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the whistleblower" in providing information to the SEC; in participating in any SEC investigation or action based on such information; or "in making disclosures that are required or protected under the Sarbanes-Oxley Act of 2002," other specified federal law or SEC law, rule, or regulation (15 USC § 78u–6(h)(1)(A), 2021).

Conversely, specific personnel actions can constitute an "adverse action" in other US laws. For instance, the Whistleblower Protection Act (WPA) of 1989 and the Whistleblower Protection Enhancement Act (WPEA) of 2012 provide protections to federal government employees who disclose information that they reasonably believe provides evidence of (1) any violation of any law, rule, or regulation; or (2) gross mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to public health or safety (Whistleblower Protection Enhancement Act, 2012).

The Merit Systems Protection Board (MSPB), which is an independent, quasi-judicial federal agency that, among other functions, receives and adjudicates whistleblower retaliation claims under the WPA (Office of the Whistleblower Ombuds, 2022), defines the term "adverse consequences" as "a personnel action that is taken as well as a personnel action that is not taken and even one that is threatened as a result of such a disclosure" (US Merit Systems Protection Board, n.d.). The MSPB lists prohibited personnel practices by referring to 5 U.S.C. § 2302 (2021). Some of the actions that are specified in this list are, for instance, a reinstatement, a decision concerning pay, benefits, or awards, an order for psychiatric testing or examination, any other significant change in duties, responsibilities, or working conditions (US Merit Systems Protection Board, n.d.). The US Office of Inspector General, on the other hand, defines "whistleblower retaliation" in a straightforward way: "It is an adverse action in response to a protected disclosure of information and includes almost any personnel action, failure to take a personnel action, or the threat to take or fail to take a personnel action, which adversely affects the whistleblower." (Office of Inspector General, n.d.).

5. REPORTING PROCEDURES TO BE FOLLOWED FOR RETALIATION PROTECTION

The EU and the US also differ in how the reporting of breaches should be carried out procedurally. To be protected under US laws, the person must verify whether internal or external reporting is required before blowing the whistle. For instance, a whistleblower is entitled to SOX protections provided that she makes such a report to a federal regulatory or law enforcement agency, any Member of Congress or any committee of Congress, a person with supervisory authority over the employee, or such another person working for the employer who has the authority to investigate, discover, or terminate misconduct (Sarbanes-Oxley Act, 2002). Accordingly, both internal and external whistleblowers are protected under SOX.

In case of pursuing a retaliation claim under Dodd-Frank, the SEC explicates that "an individual is required to have reported information about possible securities laws violations to the Commission in writing before experiencing the retaliation" (US Securities and Exchange Commission, 2023). If the individual chooses to report internally to the company, he or she is required to report that information directly to the SEC, either before or at the same time as reporting internally. If the person has already reported to the company, the person still needs to report to the Commission (US Securities and Exchange Commission, 2023). So, the whistleblowers who only report their concerns internally cannot pursue a retaliation claim under Dodd-Frank.

Under the WPA, on the other hand, protected disclosures can be made either internally to others within the agency or externally, with exceptions for sensitive material. The WPA protects public disclosures as long as the underlying information is not restricted from release

by executive order or specifically prohibited by statute. When a public disclosure is not protected by the WPA, the law still protects disclosures to federal inspectors general, the Office of Special Counsel, and individuals within the whistleblower's agency who are authorized to receive the information. The WPA protects disclosures of classified information to properly cleared recipients in Congress if the information being disclosed was classified by the head of a non-intelligence element agency and if the disclosure does not reveal intelligence sources and methods (Office of the Whistleblower Ombuds, 2022).

The EU approach to reporting differs from that of the US mainly in terms of its emphasis on the importance of internal reporting. The EU Directive defines "internal reporting" as "the oral or written communication of information on breaches within a legal entity in the private or public sector" (Directive (EU) 2019/1937, Article 5). It specifically states that "for the effective detection and prevention of breaches of Union law, it is vital that the relevant information reaches swiftly those closest to the source of the problem, most able to investigate and with powers to remedy it, where possible" (Directive (EU) 2019/1937: 25). The EU Directive further asserts that internally reporting persons will contribute significantly to self-correction and excellence within the organization. Based on this principle, the EU Directive indicates that "reporting persons should be encouraged to first use internal reporting channels and report to their employer if such channels are available to them and can reasonably be expected to work" (Directive (EU) 2019/1937: 25). Thus, if the reporting persons believe that the breach can be effectively addressed within the relevant organization and that there is no risk of retaliation, the EU Directive suggests reporting first internally. As a consequence, the EU Directive requires Member States to ensure that legal entities in the private and public sectors establish channels and procedures for internal reporting and for follow-up[2], following consultation and in agreement with the social partners where provided for by national law. The EU Directive further indicates that the channels and procedures should be available for the entity's workers and also for other persons, who are in contact with the entity in the context of their work-related activities, to be able to report information on breaches. This rule applies to legal entities in the private sector with 50 or more workers. However, this threshold rule regarding the company size does not apply to the entities falling within the scope of Union acts of financial services, products and markets, and prevention of money laundering and terrorist financing (Directive (EU) 2019/1937, Article 8 and Parts I.B and II of the Annex). Moreover, "taking into account the nature of the activities of the entities and the ensuing level of risk, Member States may require legal entities in the private sector with fewer than 50 workers to establish internal reporting channels and procedures" (Directive (EU) 2019/1937, Article 8: 38).

A similar approach can be observed in the 2018 Cybersecurity Guidance of the SEC. This guidance stated that "cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management" (US Securities and Exchange Commission, 2018: 18). Accordingly, the Commission encouraged companies to "adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly" and to "have sufficient disclosure controls and procedures in place to ensure that relevant

[2] The EU Directive defines a follow-up as any action taken by the recipient of a report or any competent authority to assess the accuracy of the allegations made in the report and, where relevant, to address the breach reported, including through actions such as an internal inquiry, an investigation, prosecution, an action for recovery of funds, or the closure of the procedure.

information about cybersecurity risks and incidents is communicated to the appropriate personnel and the top management" so that they can make informed disclosure decisions and certifications (US Securities and Exchange Commission, 2018: 18). However, the Commission only encouraged companies to have sufficient internal control mechanisms and procedures but did not enforce them.

Besides internal reporting, the EU Directive defines two other types of reporting, namely; (i) external reporting, which refers to the oral or written communication of information on breaches to the competent authorities, and (ii) public disclosure, which refers to making of information on breaches available in the public domain. As is the case for internal reporting, the EU Directive also grants protection concerning external reporting: It requires Member States "to designate the authorities competent to receive information on breaches falling within the scope of the Directive and give appropriate follow-up to the reports" (Directive (EU) 2019/1937: 27). The EU Directive lists the following entities as the competent authorities: Judicial authorities, regulatory or supervisory bodies competent in the specific areas concerned, authorities of a more general competence at a central level within a Member State, law enforcement agencies, anti-corruption bodies, or ombudsmen (Directive (EU) 2019/1937: 27).

Under the EU Directive, persons making a public disclosure, on the other hand, are qualified for protection under the following conditions:

> "(1) If the breach remains unaddressed, despite their internal and external reporting (e.g., if the breach was not appropriately assessed or investigated, or no appropriate remedial action was taken);
>
> (2) If the person has reasonable grounds to believe that: (i) the breach may constitute an imminent or manifest danger to the public interest, such as where there is an emergency situation or a risk of irreversible damage; or (ii) in the case of external reporting, there is a risk of retaliation, or there is a low prospect of the breach being effectively addressed, due to the particular circumstances of the case, such as those where evidence may be concealed or destroyed or where authority may be in collusion with the perpetrator of the breach or involved in the breach" (Directive (EU) 2019/1937: 29).

6. THE CONFIDENTIALITY OF THE WHISTLEBLOWER IDENTITY

Although persons who disclose an unlawful activity by their employer are protected against retaliation under regulations, their personal and professional reputations are still vulnerable to certain risks (Marcum and Young, 2020). In fact, besides retaliation, another critical concern of individuals is the release of their identity after blowing the whistle (Marcum et al., 2019). Negative consequences of whistleblowing may persist in future work. For instance, job applicants may struggle to find a new job after blowing the whistle (Overhuls, 2012). Prospective employees may be reluctant to hire applicants who have a whistleblowing history based on a perception that they were disloyal to their former employers (Eisenstadt and Pacella, 2018). Therefore, the protection of reporting person's identity can serve as a safeguard for whistleblowers to come forward to report unlawful conduct without the fear of damaging future employment prospects.

The EU Directive defines clear rules for the protection of personal data in whistleblowing cases. For the US, the protection of reporting person's identity depends on the law under which the reporting person files a whistleblower claim. Thus, whistleblowers who want to ensure that their identity is kept anonymous and confidential must file a claim under a law that provides solid legal protection for confidentiality.

According to the EU Directive protecting the confidentiality of the reporting person's identity during the reporting process and the investigations associated with the report is a crucial prevention measure against retaliation. Under Article 16 of "Duty of Confidentiality," the EU Directive requires Member States to ensure that "the identity of the reporting person is not disclosed to anyone beyond the authorized staff members competent to receive or follow up on reports, without the explicit consent of that person."

Under this perspective, regarding the procedures for internal reporting and also for follow-up, the EU Directive indicates that "channels for receiving the reports should be designed, established, and operated securely, ensuring the confidentiality of the identity of the reporting person and any third party mentioned in the report and the access of non-authorized staff members should be prevented" (Directive (EU) 2019/1937, Article 9). Similarly, regarding external reporting procedures, the EU Directive specifies that external reporting channels should be "designed, established and operated in a manner that ensures the completeness, integrity, and confidentiality of the information, and the access of non-authorized staff members of the competent authority should be prevented" (Directive (EU) 2019/1937, Article 12). Furthermore, according to the EU Directive, competent authorities are required to ensure that if a report is received through channels other than the reporting channels referred to in the EU Directive or by staff members other than those responsible for handling reports, those persons who receive it are prohibited from disclosing any information that might identify the reporting person or the person concerned, and that they promptly forward the report without modification to the staff members responsible for handling reports (Directive (EU) 2019/1937, Article 12).

Regarding the processing of personal data, the EU Directive indicates that any processing of personal data carried out, including the exchange or transmission of it by the competent authorities, has to be conducted following the General Data Protection Regulation (GDPR) and the Directive (EU) 2016/680. It is also stated that "any exchange or transmission of information by Union institutions, bodies, offices, or agencies has to be conducted in accordance with Regulation (EU) 2018/1725" (Directive (EU) 2019/1937: 30). Article 17 of the EU Directive further states that personal data that are irrelevant for handling a specific report may not be collected. If it is collected accidentally, it should be deleted immediately. Furthermore, these rules apply not only to the protection of the identity of reporting persons but also to the protection of the identity of persons concerned. The EU Directive requires Member States to apply appropriate penalties to natural or legal persons that breach the duty of maintaining the confidentiality of the reporting persons' identities (Directive (EU) 2019/1937, Article 23).

In the US, the first step towards confidentiality was taken with the False Claims Act (31 U.S.C. § 3729, 2021), which enabled filing the initial whistleblower disclosure in federal court under "seal." However, the confidentiality provision of this law was not enduring, meaning that if the government decides to prosecute the company, the whistleblower's complaint could be

taken out of the seal and become a matter of public record. Although the whistleblower could request the continuity of confidentiality to the court, it was not enforced by law. It was at the discretion of the federal judge to continue with the secrecy (Kohn, 2017).

In 2010, the Congress enacted the Dodd-Frank Act, which amended the Securities Exchange Act of 1934 to add a new section, Section 21, entitled "Securities Whistleblower Incentives and Protection." The Dodd-Frank Act's amendments addressed the problem with the confidentiality provision. Section 21 directs the SEC not to disclose information that could reasonably be expected to reveal the identity of a whistleblower provided that the whistleblower has submitted information utilizing the processes specified in the act (17 CFR § 240.21F-7(a)(1)-(3), 2022). The SEC states that although it is committed to protecting the identity of the individuals, it may still have to disclose the whistleblower's identity in certain circumstances to outside persons or entities. They exemplify such identity disclosure instances: For instance, in an administrative or court proceeding, they may be required to produce documents or other information that would reveal the whistleblower's identity. They also declare that, in appropriate circumstances, they may provide information, subject to confidentiality requirements, to other governmental or regulatory entities (US Securities and Exchange Commission, 2023).

According to the WPA, however, the identity of any individual who makes a disclosure may not be disclosed by the Special Counsel (The Office of Special Counsel (OSC) enforces the WPA) without such individual's consent unless the Special Counsel determines that the disclosure of the individual's identity is necessary because of imminent danger to public health or safety or imminent violation of any criminal law (Office of the Whistleblower Ombuds, 2022).

The Inspector General Act of 1978 (IG Act) is another law protecting government employees from whistleblower retaliation. The IG Act establishes an Inspector General's responsibilities and duties and grants the Office of Inspector General (OIG) the authority to receive employee complaints (Office of Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau, n.d.). In particular, the IG Act states the following scope in Section 7: "The Inspector General may receive and investigate complaints or information from an employee of the establishment concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety" (5 U.S.C. § 7, 2011).

In the same section, the confidentiality provision indicates that: "The Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the investigation" (5 U.S.C. § 7, 2011).

The Taxpayer First Act of 2019 (TFA) also takes the protection of whistleblower identity very seriously. The TFA is a law that made significant reforms to the Internal Revenue Service (IRS), revised provisions relating to the IRS, its customer service, enforcement procedures, cybersecurity, and identity protection, management of information technology, and use of electronic systems (Taxpayer First Act, 2019). It includes law changes related to the notification process to whistleblowers and made available protection for whistleblowers against retaliation

(Internal Revenue Service, 2022a). The IRS must also protect the confidentiality of whistleblowers to the fullest extent permitted under law (Internal Revenue Service, 2022b).

7. CONCLUSION

This study aimed at understanding how cybersecurity whistleblowing may fall within the scope of some federal laws in the US to be protected against retaliation by analyzing the possible relationships between the coverage of discussed regulations and cybersecurity issues. Some existing laws were compared with the EU Directive regarding their legal coverage, the definition of "retaliation," and required reporting procedures to qualify for legal protection.

In the US, since no anti-retaliation statute specifically covers cybersecurity whistleblowers, they can be protected under laws if cybersecurity issues fall within the scope of the anti-retaliation laws (Hammer, 2016). Given the diversity of US federal statutes providing legal protection, potential whistleblowers must be knowledgeable about what constitutes protected activity under the various statutes to assert a claim effectively. An omnibus whistleblower retaliation law aimed directly at cybersecurity whistleblowers who are employed in any organization from all industrial areas would be more likely to encourage blowing the whistle on wrongful conduct in this area. Also, the transformation of the SEC's Cybersecurity Guidance into binding regulations could lead to the inclusion of cybersecurity-related disclosures, an apparent category of protected whistleblower activity under both the SOX and Dodd-Frank Acts (Pacella, 2016).

The release of their identity to the employer discourages employees from disclosing what they reasonably believe to be misconduct. Thus, whistleblowers who want to ensure that their identity is kept confidential need to know if the law provides solid legal protection for confidentiality. Furthermore, each law has unique procedural requirements for asserting a claim, which must be followed so that the whistleblower can qualify for the protections. The whistleblower has to know whether internal or external reporting is protected under a particular law. "Depending on the steps the whistleblower has taken in the process of disclosing the wrongdoing, some statutes may not even protect a whistleblower" (Bishara et al., 2013, as cited in Marcum and Young, 2020: 4).

As indicated in the Framework for Improving Critical Infrastructure Cybersecurity (2018) issued by the National Institute of Standards and Technology (NIST), cybersecurity can be an essential and amplifying component of an organization's overall risk management. The Framework further stated that cybersecurity risk governance in organizations could be accomplished when "individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained" and "process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements" (NIST, 2018: 19). Thus, it is of crucial importance that the legal context encourages employees to report cybersecurity flaws and problems without fear of retaliation and without the potential difficulties that can arise due to legal procedures and technicalities.

The EU's approach to providing legal protection for whistleblowers in general and cybersecurity whistleblowers in particular and applying cybersecurity rules for whistleblowing practices is more univocal, comprehensive, and precise than that of the US.

The importance that the EU puts in whistleblowing is clearly stated in the EU Directive; by acting as "whistleblowers," who report breaches of Union law that are harmful to the public interest, such persons can have a significant contribution to the detection and prevention of the breaches of law and safeguarding the welfare of society (Directive (EU) 2019/1937). Accordingly, to encourage whistleblowing, the EU Directive clearly defines the rules and procedures and emphasizes the importance of protecting the confidentiality of the reporting person's identity during the reporting process and the investigations associated with the report and treats this protection as a crucial prevention measure against retaliation.

REFERENCES

Bishara N. D., Callahan E. S., & Dworkin T. M. (2013). The mouth of truth. New York University Journal of Law & Business, 10, 37-43.

Directive (EU) 2016/680. On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680.

Directive (EU) 2019/1937. On the protection of persons who report breaches of Union law. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937&from=en.

Eisenstadt, L. F. and Pacella, J. M. (2018). Whistleblowers need not apply. American Business Law Journal, 55(4), 665-719.

European Data Protection Supervisor. (2016, July 18). Guidelines on Processing Personal Information within a Whistleblowing Procedure. URL:https://edps.europa.eu/sites/default/files/publication/16-07-18_whistleblowing_guidelines_en.pdf, (Retrieval: 15.01.2023).

Exmeyer, P. C., & Jeon, S. H. (2022). Trends in state whistleblowing laws following the Whistleblower Protection Enhancement Act of 2012. Review of Public Personnel Administration, 42(2), 287-311.

Hammer, D. and Bundschuh, E. (29 December 2016). "The Rise of Cybersecurity Whistleblowing", Compliance & Enforcement. URL: https://wp.nyu.edu/compliance_enforcement/2016/12/29/the-rise-of-cybersecurity-whistleblowing/. (Retrieval: 13.01.2023).

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996). URL:https://www.govinfo.gov/app/details/PLAW-104publ191.

Internal Revenue Service. (2022-a, October 13). Whistleblower Reforms Under the Taxpayer First Act. URL:https://www.irs.gov/compliance/whistleblower-reforms-under-the-taxpayer-first-act, (Retrieval: 20.01.2023).

Internal Revenue Service. (2022-b, July 21). The IRS Whistleblower Office. URL:https://www.irs.gov/about-irs/the-irs-whistleblower-office#:~:text=Protecting%20Whistleblower%20and%20Taxpayer%20Information&text=We%20protect%20against%20the%20disclosure,a%20law%20passed%20in%202019, (Retrieval: 15.01.2023).

Kaufmann, J., Häferer, K., & Grimhardt, K. (2020). The new EU whistleblowing directive: Considerations from a German employment and data protection law perspective. Computer Law Review International, 21(1), 14-17.

Kohn, S. M. (2017). The New Whistleblower's Handbook: A Step-By-Step Guide to Doing What's Right and Protecting Yourself, 3.rd. Ed., United States of America: Lyons Press.

Leifer, S. C. (2014). Protecting Whistleblower protections in the Dodd–Frank Act. Michigan Law Review, 113(1), 121-149.

Marcum, T. M. and Young, J. A. (2020). Defining the whistleblower: The Digital Realty case and proposed legislation. Richmond Journal of Law & Technology, 26(3), 1-23.

Marcum, T. M., Young, J., & Kirner, E. T. (2019). Blowing the whistle in the digital age: Are you really anonymous? The Perils and pitfalls of anonymity in whistleblowing law. DePaul Business & Commercial Law Journal, 17(1), 1-38.

National Institute of Standards and Technology. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. (Version 1.1). URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf, (Retrieval: 20.01.2023).

Office of Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau. (n.d). Inspector General Act. URL:https://oig.federalreserve.gov/inspector-general-act.htm, (Retrieval: 04.02.2023).

Office of the Whistleblower Ombuds. (2022, March). Whistleblower protection act. URL:https://whistleblower.house.gov/sites/whistleblower.house.gov/files/Whistleblower_Protection_Act_Fact_Sheet.pdf, (Retrieval: 04.02.2023).

Overhuls, C. H. (2012). Unfinished Business: Dodd-Frank's Whistleblower Anti-Retaliation Protections Fall Short for Private Companies and Their Employees. The Journal of Business, Entrepreneurship & the Law, 6(1), 1-22.

Pacella, J. M. (2016). The cybersecurity threat: Compliance and the role of whistleblowers. Brooklyn Journal of Corporate, Financial & Commercial Law, 11, 38-70.

Pender, K., Cherasova, S., & Yamaoka-Enkerlin, A. (2021). Compliance and whistleblowing: How technology will replace, empower and change whistleblowers. In J. Madir (Ed.), FinTech (pp. 365-394). UK: Edward Elgar Publishing.

Regulation (EU) 2016/679. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

95/46/EC (General Data Protection Regulation). URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Regulation (EU) 2018/1725. On the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN.

Ronicker, A. and LaGarde, M. (March 2019). "Cybersecurity Whistleblower Protections: An Overview of the Protections and Rewards Available to Cybersecurity Whistleblowers Under Federal and State Law". URL:https://katzbanks.com/sites/default/files/cybersecurity-whistleblower-protection-guide.pdf. (Retrieval: 20.01.2023).

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204 (2002). URL:https://www.govinfo.gov/app/details/PLAW-107publ204.

Taxpayer First Act, Pub. L. No. 116-25 (2019). URL:https://www.govinfo.gov/app/details/PLAW-116publ25.

Teichmann, F.M. and Wittmann, C. (2022). Whistleblowing: Procedural and dogmatic problems in the implementation of directive (EU) 2019/1937. Journal of Financial Regulation and Compliance, 30(5), 553-566.

US Department of Health and Human Services Office for Civil Rights. (2013, July 13). Breach Notification Rule. URL:https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, (Retrieval: 01.02.2023).

US Department of Health and Human Services Office for Civil Rights. (2013, March 26). HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162, and 164. URL:https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf, (Retrieval: 01.02.2023).

US Department of Health and Human Services Office for Civil Rights. (2022, October 20). The Security Rule. URL:https://www.hhs.gov/hipaa/for-professionals/security/index.html, (Retrieval: 01.02.2023).

US Merit Systems Protection Board. (n.d.). Prohibited Personnel Practice 8: Whistleblower Protection. URL:https://www.mspb.gov/ppp/8ppp.htm, (Retrieval: 18.01.2023).

US Nuclear Regulatory Commission (NRC). (2017, August). Reporting Safety Concerns to the NRC (NUREG/BR-0240, Revision 8) [Brochure]. URL:https://www.nrc.gov/docs/ML1720/ML17208A272.pdf, (Retrieval: 08.02.2023).

US Office of Inspector General. (n.d.). OIG Whistleblower Protection Coordinator. URL:https://www.oig.dol.gov/whistleblower-coordinator.htm#:~:text=Whistleblower%20retaliation%20is%20an%20adverse,which%20adversely%20affects%20the%20whistleblower, (Retrieval: 26.01.2023).

US Securities and Exchange Commission (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. URL:https://www.sec.gov/rules/interp/2018/33-10459.pdf, (Retrieval: 16.01.2023).

US Securities and Exchange Commission. (2023, February 3). Office of the Whistleblower: Whistleblower Protections. URL:https://www.sec.gov/whistleblower/retaliation, (Retrieval: 15.01.2023).

Whistleblower Protection Act of 1989, Pub. L. No. 101-12 (1989). URL:https://www.govinfo.gov/content/pkg/STATUTE-103/pdf/STATUTE-103-Pg16.pdf.

Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199 (2012). URL: https://www.govinfo.gov/app/details/PLAW-112publ199.

10 C.F.R. § 73 (2022). URL:https://www.govinfo.gov/app/details/CFR-2022-title10-vol2/CFR-2022-title10-vol2-part73.

15 U.S.C. § 78u-6 (2021). URL:https://www.govinfo.gov/app/details/USCODE-2021-title15/USCODE-2021-title15-chap2B-sec78u-6.

17 C.F.R. § 240.21F-7 (2022). URL:https://www.govinfo.gov/app/details/CFR-2022-title17-vol4/CFR-2022-title17-vol4-sec240-21F-7.

17 C.F.R. § 248.201 (2020). URL:https://www.govinfo.gov/app/details/CFR-2020-title17-vol4/CFR-2020-title17-vol4-sec248-201.

17 C.F.R. § 248.30 (2013). URL:https://www.govinfo.gov/app/details/CFR-2013-title17-vol3/CFR-2013-title17-vol3-sec248-30.

18 U.S.C. § 1514A (2021). URL:https://www.govinfo.gov/app/details/USCODE-2021-title18/USCODE-2021-title18-partI-chap73-sec1514A.

31 U.S.C. § 3729 (2021). URL:https://www.govinfo.gov/app/details/USCODE-2021-title31/USCODE-2021-title31-subtitleIII-chap37-subchapIII-sec3729.

48 C.F.R. § 3.9 (2021). URL:https://www.govinfo.gov/app/details/CFR-2021-title48-vol1/CFR-2021-title48-vol1-part3-subpart3-9.

48 C.F.R. § 39.101 (2021). URL:https://www.govinfo.gov/app/details/CFR-2021-title48-vol1/CFR-2021-title48-vol1-sec39-101.

5 U.S.C. § 7 (2011). URL:https://www.govinfo.gov/app/details/USCODE-2011-title5/USCODE-2011-title5-app-inspector-sec7.

5 U.S.C. § 2302 (2021). URL:https://www.govinfo.gov/app/details/USCODE-2021-title5/USCODE-2021-title5-partIII-subpartA-chap23-sec2302.