THE 18TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

Green Economy and
Sustainable Development

Aspects Regarding CyberSecurity Developments on SaaS Software Platforms

Andrada-Iulia State[1], Georgiana-Alexandra Moroșanu[2], Laura-Andreea Rață[3], Marius Geru[4]

Abstract: This paper explores the dynamic interplay between cybersecurity, legislation, and SaaS platforms, focusing on the current landscape, potential future threats, and emerging legal challenges. SaaS providers, acting as custodians of considerable amounts of personal data, are significantly impacted by diverse legal frameworks such as the GDPR, CCPA, HIPAA, and PCI-DSS. These frameworks mandate stringent data protection and security measures. The paper further elucidates the sector-specific regulations and discusses the complex issue of cross-border data transfers, underscoring the need for adequate safeguards. This work examines how laws deal with cybersecurity threats and emphasizes the importance of complying with them to reduce these risks. It addresses challenges and conflicts that arise when SaaS and cybersecurity laws intersect, including issues related to data ownership and protection responsibilities. This paper makes suggestions to improve legal protections through international collaboration, adapting laws to keep up with technology, and ensuring transparency in data processing. It also explores potential future threats and legal challenges, such as cyber threats powered by AI, quantum computing, privacy paradoxes, and questions about data sovereignty. Therefore, the paper stresses the necessity of staying ahead of regulatory changes and fostering a comprehensive cybersecurity strategy that blends technology, people, processes, and legislation.

Keywords: legal frameworks; protection; AI; legislation; security

1. Introduction

The world has had to find new paths away from the patterns and habits of the 20th and early 21st centuries, which were marked by prolonged conflicts, both military and political, towards more positive and constructive domains. Technology became the new preoccupation, with the defining goal of getting out of the crisis and the structuring of a society based on knowledge and technology. The opportunities that technology can offer have yet to be defined. Thus, mankind has become more focused on the

[1] Project Assistant, S.C. THECON S.R.L., Romania, Address: Calugareni street, No. 3, Galati, Romania, Tel.: +40771518864, E-mail: andradastate@thecon.ro.

[2] PhD, Faculty of Engineering, "Dunărea de Jos" University of Galați, Romania, Address: Domnească street, No. 111, 800201, Galați, Romania, Tel.: +40336130208, Fax: +40236314463, Corresponding author: alexandra.costin@ugal.ro.

[3] Marketing researcher, S.C. THECON S.R.L., Romania, Address: Calugareni street, No. 3, Galati, Romania, Tel.: +40771518864, E-mail: laurarata@thecon.ro.

[4] Project Manager, S.C. THECON S.R.L., Romania, Address: Calugareni street, No. 3, Galati, Romania, Tel.: +40771518864, E-mail: marius@thecon.ro.

development of this sector in order to ensure a living and to simplify the repetitive procedures that human resources used to perform.

The reason behind choosing this subject was the desire to represent as much as possible that the functions of technology are unlimited and that the information we gathered a year, a month, a day or an hour ago are information that has already been superseded and needs to be updated. The level of technology is developing extremely rapidly but also the ingenious ways of approaching it have become equally limitless.

In recent years, SaaS web platforms have become increasingly prevalent. These platforms leverage cloud technology, allowing businesses to access software applications and services on demand without installing and maintaining them on their own servers. This approach has many benefits, including lower costs, greater flexibility and improved scalability (Mäkilä, Tuomas et al., 2010). As businesses increasingly adopt SaaS web platforms for their software needs, it is crucial to consider the potential cybersecurity risks. These platforms come with clear benefits yet represent new challenges for IT professionals safeguarding sensitive data. Given the frequency of data breaches, taking necessary precautions to protect the company’s information is imperative.

This may involve implementing robust access controls, conducting frequent security audits and staying informed about the latest security threats and best practices. By prioritizing cybersecurity measures, anyone can ensure that the business truly benefits from the advantages of SaaS platforms without compromising the safety of the company data.

Cybercriminals increasingly target SaaS platforms due to the valuable data they store. Users must remain aware of the numerous threats that loom in today’s digital world (Tracy, Rao & Hall, 2021). In the past two years, computer system unavailability offenses have occurred in sectors such as banking, freight forwarding, healthcare and government.

The development of technology and process automation in recent times has made electronic systems susceptible to cyber attacks. Among the most common are ransomware, viruses and botnets. At the same time, the diverse and free mode, facilitated by the online space, has pushed governments to divide their jurisdictional competences between the situations reported. The difficulty of determining the criminological dimension as well as the competence of a state to intervene in a given situation has encouraged attackers to commit such crimes through a lack of response and punishment at the expense of low-risk profits.

The paper begins by providing a comprehensive understanding of SaaS architecture, including its definition and unique characteristics. This chapter establishes the foundation for understanding the cybersecurity threats and legal implications that will be discussed later. The third chapter identifies and explains the significant cybersecurity threats SaaS platforms face. It includes real-world case studies to illustrate the potential dangers and to provide context for the subsequent discussion of legal frameworks. The paper then delves into the legal frameworks that apply to SaaS platforms. This involves an exploration of data protection laws, sector-specific regulations and cross-border data transfer rules. The chapter Legal Frameworks Relevant to SaaS Platforms includes an exploration of regulatory norms, penalties, international cooperation, and more.

The paper then moves into strategic recommendations and anticipates future directions in the SaaS sector. It provides actionable insights for SaaS providers on improving cybersecurity measures and ensuring compliance with existing and anticipated legal frameworks.

This research paper aims to deepen the understanding of the unique challenges and considerations for SaaS platforms in cybersecurity. Exploring both the technical and legal aspects offers a comprehensive viewpoint that can inform better practices and policies in the future.

2. A Deep Dive into SaaS Architecture, Definition and Distinctive Characteristics

SaaS stands for Software as a Service, a way of delivering software where a service provider hosts the applications and makes them accessible to customers through the Internet. SaaS applications are designed to hold multiple users simultaneously, which is called multi-tenant architecture and is a key feature of SaaS platforms. This structure enables efficient use of server resources and allows for the streamlined introduction of updates or improvements across all tenants simultaneously (Kang & Hur, 2011; Carraro, 2006).

Distinctive Characteristics of SaaS Architecture:

1. Multi-Tenancy - a fundamental characteristic of SaaS architecture is multi-tenancy, where a single instance of a software application serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants (Kang & Hur, 2011; Mietzner, Metzger et al., 2009);

2. Scalability - SaaS solutions must be highly scalable to accommodate various users. As more users join the system, the architecture should scale seamlessly to meet the demand. Similarly, when the number of users decreases, it should be able to scale down (Wei-Tek, Huang & Shao, 2011);

3. Availability - High availability is a critical feature of SaaS architecture, designed to ensure maximum uptime, which often requires redundancy, fault tolerance, and effective failover protocols (Su, Wenbo et al., 2014);

4. Security - Since sensitive data is often stored and managed within SaaS applications, robust security measures are critical. The security architecture of these solutions includes encryption, secure access controls, regular security audits, and compliance with various data security standards (Rath, Annanda et al., 2019; Pradnyesh, 2016);

5. Accessibility - SaaS applications are accessible over the Internet, which means they can be used anywhere and on any device with an Internet connection (Sohaib et al., 2018). Being web-based makes them incredibly flexible and convenient for users.

6. Data Integration - SaaS solutions often provide APIs allowing integration with other software systems. It is crucial because businesses typically use various software tools, and integrating them can significantly improve efficiency and workflow (Hai, Henry & Sakoda, 2008).

7. Subscription-based Pricing - SaaS typically operates on a subscription model, where users pay a regular fee for access to the software rather than purchasing the software outright. This pricing model makes high-quality software more affordable for businesses (Laatikainen, Gabriella & Ojala, 2014).

8. Automatic Updates - One of the key advantages of SaaS architecture for users is that updates and new features are added automatically, without the need for the user to install or download anything (Kuldeep, Rajpurohit & Deyannavar, 2018).

SaaS architecture aims to deliver dependable service quality and security, allowing for easy expansion as required while being accessible from any location and consistently updated. This approach provides substantial advantages to users, especially companies since it offers cost-efficient, adaptable, and easy-to-maintain software solutions.

The COVID-19 pandemic has significantly accelerated the trend towards remote work, a shift expected to persist in the post-pandemic business environment (Alhomdy et al., 2021; Tudor, 2022). SaaS applications have played a crucial role in this transition, enabling businesses to adapt and thrive despite the challenges. The sudden shift to remote work required robust solutions for collaboration and communication and SaaS applications were able to meet this need. Tools like Zoom, Microsoft Teams, Slack and Google Workspace (Parra, Otto & Granda, 2021) have enabled teams to work together effectively despite them being physically apart. These tools facilitate real-time collaboration, video conferencing, file sharing, and project management, enabling a seamless transition to remote work. Since SaaS applications are cloud-based and accessible over the Internet, employees could access their work from anywhere, anytime, and on any device with an Internet connection. With the shift to remote work, businesses are increasingly concerned about data security. However, SaaS applications offer robust security measures such as data encryption (Chinedu, 2018), user authentication (Hussein, Hassan & Khalid, 2016), and regular security updates (Banka, Ankit, et al., 2013) to ensure that sensitive company data remains secure even when accessed remotely.

The pandemic caused changes in the business landscape making SaaS applications an invaluable asset due to their scalability. Companies can adjust their software usage based on their needs and integrate new features or tools seamlessly. This flexibility enables businesses to stay responsive and agile in a rapidly changing environment. Furthermore, SaaS applications automate repetitive tasks, streamline processes, and can be integrated with other tools (Tsai, Huang & Shao, 2011; Gao et al. 2012), resulting in productivity growth. This has been particularly valuable in a remote work environment where efficiency and well-organized workflows are crucial.

SaaS eliminates the need for businesses to maintain their IT infrastructure and servers, resulting in significant cost savings. This has been especially helpful during the pandemic, when many companies sought ways to cut costs. SaaS applications have been beneficial for businesses in the post-COVID-19 world (Alhomdy et al., 2021). They make remote work and collaboration easier, ensure data security, and offer flexibility and scalability. As the business landscape changes, SaaS applications will become even more important, especially as remote and hybrid work models grow (Alhomdy et al, 2021; Tudor, 2022). While SaaS integrations can greatly improve efficiency and productivity, it’s important to approach them with a complete and strong cybersecurity strategy. By taking the time to implement and maintain strong security practices, businesses can mitigate potential risks and better protect their data and systems (George, Shaji & Sagayarajan, 2023).

3. Cybersecurity Threats to SaaS Platforms

The rapid proliferation of digital technologies, the internet, and associated cybernetic infrastructures have resulted in a significant increase in cybercrime across the globe and Romania is no exception. This contemporary criminal activity encompasses various malicious actions, from data theft and online fraud to cyberstalking and hacking.

Cybercrime is defined in the Penal Code specifically in the chapter on Article 249 “*Fraud committed by means of computer systems and electronic means of payment*” (Lupascu, 2023).

In the article on protection of data systems, entitled “*Offenses against the security and integrity of data systems and data*” (Lupascu, 2023), the following offenses are described: Article 360: Illegal access to a computer system; Article 361: Illegal interception of a computer data transmission; Article 362: Altering the integrity of computer data; Article 363: Disrupting the functioning of information systems;

Article 363: Unauthorized transfer of computer data; Article 364: Illegal operations with computer devices or software.

In addition to the rules laid down in the New Penal Code, Law 161/2003 established in Article 48 and 49 of the new law, further computer-related offenses (Legislation, 2003). Thus, the first article describes "*the act of entering, modifying or deleting computer data without right or restricting access to such data, resulting in data that is not accurate, for the purpose of being used to produce a legal consequence, shall constitute an offense and shall be punishable by 2 to 7 years' imprisonment*" (Legislation, 2003) and is supplemented by the following article of the same law, which defines as an aggravating form of the offense "*the act of causing damage to a person's property by entering, modifying or deleting computer data, restricting access to such data or preventing in any way the functioning of a computer system, with the aim of obtaining a material benefit for oneself or for another person, constitutes an offense and shall be punishable by imprisonment for a term of 3 to 12 years*" (Legislation, 2003).

Illegal access to a computer system is the typical form of manifestation of cybercrime, where the active subject of the offence may be represented by both a natural person or a legal person, who must also have a minimum level of technical knowledge to access a system. The threshold is represented by the minimum knowledge that can vary from case to case, not infrequently we have been surprised by situations where Romanian citizens have hacked into the NASA and Pentagon websites, having an educational background equivalent to 8 or 12 grades. The case of Robert Butyka, referred to as Iceman, in the cyberspace, has hacked 25 computer servers at the Jet Propulsion Laboratory (JPL) in December 2010, causing $600,000 in damage and rendering them unusable for several months. The servers belonged to NASA (Court of Appeal Cluj, 2012).

The danger of cybercrime is the cross-border aspect it creates, analysed from the point of view of the ability of states to act, identify and punish the perpetrator, but also from the point of view of mitigating the impact of the crime on the information system. The variability of actions against the information system is difficult to understand, so authorities need to act quickly and have the necessary equipment to optimise the time of action. The passive subject in this crime is the owner of the hosting servers that can be both an individual and a legal entity, which most of the time, especially in public institutions are the same as the site owners.

The legal rule aims to protect data systems and ensure security and their inviolability and constitutes the legal object of the offence. Cybersecurity threats continue to pose significant challenges in today's digital landscape. From phishing attacks and API vulnerabilities to insider threats and ransomware incidents, organisations must remain vigilant to protect their sensitive data and infrastructure. This chapter will provide an overview of some prominent cybersecurity threats, emphasising the need for proactive security measures:

1. Phishing is an insidious tactic attackers use to deceive and extract sensitive information from unsuspecting users through social engineering. These attackers are cunning and may pose as a reputable company or bank, sending emails, messages, or websites that appear authentic and trustworthy. They then demand personal details such as usernames, passwords, credit card numbers, or social security numbers. The consequences of a successful phishing scam are dire, leading to identity theft, financial loss, or unauthorised access to confidential data (Basit, Abdul, et al., 2021). It's crucial to stay vigilant and remain cautious while conducting any online activities to avoid falling victim to these malicious attacks.

2. API (*Application Programming Interfaces*) allow different software applications to communicate, and SaaS applications commonly use them for integration with other software solutions. However, if

APIs are not secured properly, they can become a significant cybersecurity threat. Attackers can exploit API vulnerabilities to gain unauthorised access, manipulate data, cause denial of service, or even take over servers (Dharitri, Gohil & Halabi, 2020). Common API vulnerabilities include weak authentication, lack of encryption, and inadequate access control.

3. Insider Threats refer to cybersecurity threats that originate from within the organization. An employee, contractor, or any other individual authorized to access the organization's systems could start this type of vulnerability (Miltiadis, Virvilis & Gritzalis, 2011; Alhanahnah et al. 2016). Insider threats can be intentional (for example, an employee selling sensitive information to a competitor) or unintentional (for example, an employee accidentally downloading malware). Insider threats can be particularly challenging to mitigate due to the level of access these individuals have.

4. Ransomware is a type of malware that encrypts the victim's files as defined earlier in the chapter. The attacker then demands a ransom from the victim to restore access to the data upon payment. Failure to pay the ransom often leads to permanent loss or unauthorized disclosure of the data. Phishing emails, malicious advertisements, or visiting infected websites serve as means of spreading ransomware. Ransomware attacks, which have been witnessing an upward trend in recent years, target individuals and large organizations, resulting in substantial financial losses and significant downtime (Hou, Shifu, et al., 2016).

5. DDoS Attacks (*Distributed Denial of Service*) manifest themselves by attackers sending large packets of data to targeted systems of institutions, companies or home users, in order to block them or make it difficult for them to operate for long periods of time. This is a coordinated attack by cyber criminals on targets, and this attack leads to the unavailability of the entire system or data networks. In the period generated by COVID-19, the number of such cases reported in 2020 reached 10 million attacks, 1.6 million more than in 2019 (Lopez & Buscetta, 2021). These attacks originated from multiple directions and from multiple infected computers, which became zombielike sources acting as a transmitter, without the respective users being aware that their devices were infected. To combat these threats, SaaS providers and users should employ strong cybersecurity measures, including data encryption, robust access controls, secure APIs, regular security audits, and employee training (Darwish et al., 2013; Dhiyanesh & Sakthivel, 2016). Businesses should also ensure they choose SaaS providers who prioritize security and comply with relevant data privacy regulations.

6. Data Breaches take center stage as they involve the unauthorized acquisition of sensitive data stored within the SaaS platform. This data comprises extensive information, spanning customer data, financial records, intellectual property, and other sensitive data susceptible to exploitation for financial gain or malicious purposes (Mozumder, Prasead et al., 2017; Barona & Mary Anita, 2017).

7. Account Hijacking is compromising a user's login credentials through phishing or other illicit methods which enable an attacker to seize control of the account, facilitating unauthorized access to sensitive data and further disseminating malware. These compromised accounts (bots) serve as instruments for engaging in espionage activities, encompassing the surveillance of communications, tracking user behaviors, and gathering sensitive information about individuals, organizations, or governmental entities. Moreover, the attacker can manipulate the data, introducing misinformation and influencing decision-making by leveraging falsified information on social media platforms (Guillén et al., 2020).

8. A Man-in-the-Middle Attack (*MitM*) is when the attacker covertly intercepts and potentially modifies the communication between two parties under the false pretense that they are engaging in direct communication. By intercepting and manipulating the communication, attackers can purloin sensitive data or introduce malicious content (Mallik, 2019).

9. Zero-Day Exploits denote software vulnerabilities that remain undisclosed to the relevant parties responsible for addressing them, including the software vendor. If the vulnerability remains unmitigated, malicious hackers can exploit it to impact computer programs, data, or networks adversely (Yaman, 2021).

All of these cybersecurity threats require robust security measures to prevent. These threats include maintaining up-to-date software and systems, implementing strong access control and authentication measures, providing regular security training to employees, and implementing a comprehensive security strategy.

The following are two case studies that showcase major cyber attacks that targeted SaaS platforms. In 2018, a major cyber attack, Salesforce Data Leak, a leading SaaS platform provider, compromised sensitive customer information. Attackers exploited a vulnerability in the Salesforce API, allowing them to access and extract customer data, including names, addresses, phone numbers, and social security numbers (Suryateja, 2018; Chinedu, Paschal, & Nwankwo, 2018). The incident affected thousands of Salesforce customers, raising concerns about data privacy and security on SaaS platforms. Salesforce took immediate action to address the issue, patch the vulnerability and enhance security measures to prevent similar attacks in the future.

And the second case study is the 2019 Capital One Breach, a prominent financial institution that fell victim to a significant cyber attack targeting its SaaS infrastructure. The attacker exploited a misconfigured web application firewall (*WAF*) on the AWS cloud platform, leading to unauthorised access to sensitive customer data (Novaes Neto, Nelson et al., 2020). The breach compromised the personal information of over 100 million Capital One customers, including names, addresses, credit scores, and social security numbers. The incident highlighted the importance of proper configuration and security practices when deploying SaaS applications on cloud platforms. Capital One promptly addressed the issue, implemented additional security measures, and cooperated with authorities to investigate the breach.

These real-life examples illustrate the serious consequences of cyber attacks on SaaS platforms, emphasising the importance of strong security measures. Cybersecurity threats can lead to substantial financial losses for businesses and individuals. Ransomware attacks, for example, can result in hefty ransom payments or the costs associated with recovering from a data breach. Companies may also face regulatory penalties, lawsuits, and reputational damage, all of which can have long-term financial implications.

In 2018, an extensive investigation was launched after Romanian, German and French authorities reported ransomware attacks on the data systems of several hospitals. Given the scale of this phenomenon and the large number of reports of the national D.I.I.C.O.T., support was requested and the Special Intervention Brigade for Combating Organised Crime in Constanța. At international level, a joint investigation team has been set up with the support of Europol, Eurojust and Interpol, involving more than 17 law enforcement officers. Operation Gold Dust, as it was called by investigators who conducted massive investigations that also led to the arrests of three other South Koreans, one person from the United States and a fifth person was arrested by Kuwaiti authorities. All individuals have been found responsible for creating and providing an optimal format for running these Ransomware and Service programs to produce damage and extortion by the REevil and GrandCrab organization groups (Minister of Interior Affairs of Romania, 2021).

This type of attack materialises from the creation by members of the more ransomware-type programs and the distribution of this infrastructure with the aim of selling them on and causing damage to companies and target institutions. In a document published by the European Court of Auditors on "*Challenges for an effective EU cyber security policy*" of March 2019 (European Court of Auditors, 2019), a statistic was highlighted according to which: these infrastructure provision services attackers end up costing an average of €15 and the damage caused by the use of this software amounts to thousands and hundreds of thousands of euros, depending on the targets. Most of the time, the aim is to attack the institutions of countries that have a legal system developed in this sector or which have no infrastructure to combat this phenomenon.

The message received by the victims of the ransomware attack on the affected computer systems directed them to access a page on a search engine called TOR, which ensures anonymity on internet platforms. The page where the victims of the attack were directed led to a payment platform to generate decryption code, along with the instructions necessary to complete the payment.

4. Legal Frameworks Relevant to SaaS Platforms

The offence, as defined by the dictionary of the Romanian language, is "a socially dangerous act, consisting in the violation of a criminal law, in the guilty commission of an offence" (Dexonline, 2023). From the point of view of the New Criminal Code, Article 15 paragraph (1), the crime is defined as "the act provided for by the criminal law, committed with guilt, unjustified and imputable to the person who committed it" (Lege 5, 2023).

Thus, the definition of the offence, as provided for by the legislator, is of interest from the point of view of "delimiting the scope of criminal wrongdoing from that of non-criminal wrongdoing, i.e. delimiting acts which are offences from other wrongful acts (administrative, civil, disciplinary) or from lawful acts".

Cybercrime has become a problem for many states because the only need for an individual to commit criminal acts is to have access to an internet connection, for which only a small fee is charged to cause huge damage. Most criminal activity in the online space is also supported by the environment outside the group, through providing the IT resources needed to carry out their activities in optimal conditions in order to obtain a direct or indirect benefit, both financial and competitive, for them and its supporters. By way of example, it is the case that the criminal activity consists in the unavailability of the targeted user's data storage systems, an activity that requires both hardware space and state-of-the-art processors to produce the desired impact, all of which amounts to hundreds of devices as well as equipment in to carry out the procedures for copying the data held by the victim of the cyber attack, to publish or trade data and information obtained illicitly in exchange for a fee. General data protection laws, such as the GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), have implications for Software-as-a-Service providers in handling and protecting personal data. Here's a description of how these laws impact SaaS providers:

1. The GDPR applies to SaaS providers when they process personal data belonging to individuals in the European Union (EU). SaaS providers function as data processors by managing and storing personal data on behalf of their customers, who act as data controllers. SaaS providers need to consider several important factors regarding the GDPR guidelines:

- SaaS providers must establish suitable data processing agreements with their customers, delineating the respective responsibilities of both parties concerning the processing of personal data;

- to safeguard personal data, SaaS providers must implement adequate security measures, such as encryption, access controls, frequent security audits, and incident response plans;

- as a SaaS provider, it is your responsibility to help your customers with fulfilling data rights. This includes responding to data subject access requests, rectifying, erasure, and portability.

- when transferring personal data outside the EU, SaaS providers must comply with GDPR, implementing appropriate safeguards such as Standard Contractual Clauses and relying on the EU-US Privacy Shield (if applicable).

2. The CCPA applies to SaaS providers that collect personal information from California residents and fulfill specific revenue or data processing volume criteria. SaaS providers should consider several significant factors in compliance with the CCPA:

- SaaS providers should actively inform their customers (businesses utilising the SaaS platform) regarding the specific categories of personal information being collected and the explicit purposes for which such information is being processed;

- SaaS providers are encouraged to actively assist their customers in upholding the consumer rights bestowed by the CCPA, which include facilitating the implementation of mechanisms to honour opt-out and deletion requests;

- under CCPA regulations, SaaS providers may fall under “service providers.” To comply with these regulations, providers must establish written agreements with their customers (businesses) outlining limitations on using and retaining personal information;

- to comply with the CCPA, SaaS providers must ensure the implementation of adequate security measures to safeguard personal information and establish proper procedures to respond to and report any data breaches.

It’s important for SaaS providers to carefully review and understand the specific requirements of the GDPR, CCPA, and other relevant data protection laws to ensure compliance. This may involve conducting privacy impact assessments, updating privacy policies, enhancing security measures, and maintaining transparency in data processing practices. Compliance with these laws helps SaaS providers meet legal obligations, fosters customer trust and demonstrates a commitment to protecting personal data.

Sector-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS), provide guidelines and requirements for data protection and security within specific industries. Here’s an explanation of these regulations:

1. Health Insurance Portability and Accountability Act (HIPAA): a US federal law that sets standards for protecting sensitive healthcare information. It applies to healthcare providers, health plans, and healthcare clearinghouses, collectively known as covered entities and their business associates, who handle protected health information (PHI).

Key provisions of HIPAA include:

- The HIPAA Privacy Rule sets guidelines to safeguard people’s medical records and identifiable health information. It mandates that entities obtain patient consent before using or disclosing PHI and guarantee individuals’ access and control over their health data.

- The HIPAA Security Rule requires covered entities to implement administrative, physical, and technical safeguards to protect electronic PHI (ePHI) from unauthorized access, disclosure, alteration, or destruction. This involves access controls, encryption, and regular risk assessments.

- The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, the US Department of Health and Human Services (HHS), and sometimes the media in case of a breach of unsecured PHI.

- Compliance with HIPAA is crucial for healthcare organizations to safeguard patient privacy and maintain the security of health information.

2. Payment Card Industry Data Security Standard (PCI-DSS) is a security standard established by the Payment Card Industry Security Standards Council (PCI SSC) to protect cardholder data and secure credit card transactions. It applies to any organization that stores, processes or transmits payment card information.

Key requirements of PCI-DSS include:

- Building and Maintaining a Secure Network involves implementing firewalls, using unique passwords for system access, and securing cardholder data transmission over public networks.

- To ensure the safety of cardholder data, PCI-DSS requires the encryption of the information, restricting access to those who need to know it, and securely storing the data.

- PCI-DSS requires implementing and maintaining security measures, including vulnerability scanning, penetration testing, network and system activity monitoring.

- Maintaining a Vulnerability Management Program involves regularly updating and patching systems and addressing vulnerabilities promptly.

- Implementing Strong Access Control Measures includes assigning unique IDs to individuals with system access, restricting physical access to cardholder data, and implementing two-factor authentication.

PCI-DSS compliance is essential for organizations involved in payment card transactions to protect cardholder data and mitigate the risk of data breaches and financial losses.

These sector-specific regulations play a crucial role in protecting sensitive information and ensuring the privacy and security of individuals' data within specific industries. Adhering to these regulations helps organizations comply with legal requirements, and fosters trust among customers and stakeholders.

Cross-border data transfers involve transferring personal data from one country to another. The laws and regulations governing such transfers vary across jurisdictions. Under the GDPR, transfers of personal data from the European Economic Area (*EEA*) to countries outside the EEA are subject to specific requirements. Transfers to countries with an adequacy decision from the European Commission are considered lawful. In the absence of an adequacy decision, SaaS providers must rely on appropriate safeguards, such as Standard Contractual Clauses (*SCCs*) approved by the European Commission, Binding Corporate Rules (*BCRs*), or other approved mechanisms to ensure adequate data protection.

SaaS providers operating within the EEA should carefully assess their data transfer practices and implement the necessary safeguards to comply with GDPR requirements. The CCPA does not explicitly restrict cross-border data transfers. However, businesses subject to the CCPA must inform consumers if they sell their personal information to third parties. If a SaaS provider sells personal information, including through cross-border transfers, they must disclose this to consumers and provide an opt-out mechanism.

While the CCPA does not impose specific requirements for cross-border data transfers, SaaS providers should still consider applicable laws and regulations if they transfer personal information across borders, particularly when dealing with California residents' data.

Several countries and regions have enacted data protection laws that impose specific requirements for cross-border data transfers. For example, Canada has the Personal Information Protection and Electronic Documents Act (*PIPEDA*), which restricts transfers to countries without adequate protection unless the organization obtains appropriate consent or relies on other permitted grounds.

Similarly, countries in the Asia-Pacific region, such as Singapore and Australia, have data protection laws that include provisions for cross-border data transfers and require organizations to ensure adequate protection for transferred data.

SaaS providers operating globally or providing services to customers in different jurisdictions must know and comply with the applicable data protection laws and regulations concerning cross-border data transfers. This includes implementing appropriate safeguards, conducting data transfer impact assessments, and ensuring compliance with specific obligations, such as obtaining consent or utilizing approved mechanisms like *SCCs* or *BCRs*.

Failure to comply with cross-border data transfer regulations can result in legal consequences, including regulatory penalties and reputational damage. Therefore, SaaS providers must stay informed about the requirements in relevant jurisdictions and establish robust data transfer mechanisms to protect the privacy and security of personal data during cross-border transfers.

5. How do Legal Frameworks Actively Engage with Cybersecurity

It should be noted that no state is currently able to manage its security in the face of cross-border cybercrime, nor can it effectively deal with such a threat, which is growing every day on its own.

The transition of legal/policy instruments to establish a stable cybersecurity at EU level is presented in Figure 1.

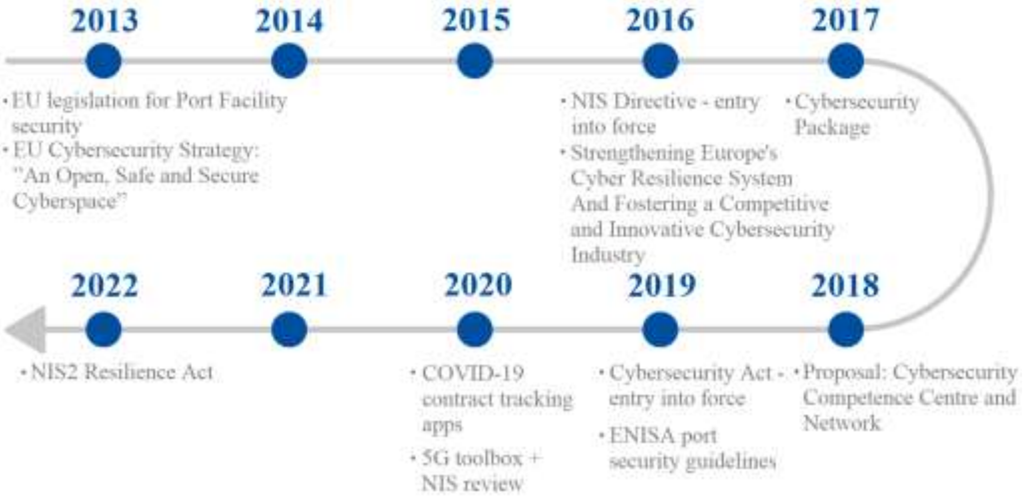
2013
2014
2015
2016
2017
• EU legislation for Port Facility security
• EU Cybersecurity Strategy: "An Open, Safe and Secure Cyberspace"
• NIS Directive - entry into force
• Strengthening Europe's Cyber Resilience System And Fostering a Competitive and Innovative Cybersecurity Industry
• Cybersecurity Package
2022
2021
2020
2019
2018
• NIS2 Resilience Act
• COVID-19 contract tracking apps
• 5G toolbox + NIS review
• Cybersecurity Act - entry into force
• ENISA port security guidelines
• Proposal: Cybersecurity Competence Centre and Network

Figure 1. Transition of Legal/Policy Instruments to Establish a Stable Cybersecurity at EU Level (Polemi & Praça, 2023)

The current situation is such because the sector to combat cyber-attacks has been poorly developed. The inability of state authorities to train officials to intervene in incidents, the failure of the public to report cyber incidents, and the lack of timely response have led to the relatively uncertain situation of states in combating cybercrime. Therefore, states need to turn to cooperation and mutual assistance. With the support of organizations and authorities responsible for dispute resolution and procedural disputes, as well as to limit the dangers and damage, they can also intervene and provide a firm and timely response to cross-border crime.

Legal frameworks are critical in addressing cybersecurity threats by establishing norms, rules, and penalties for using and protecting digital and information technologies. Legal frameworks can set standards for how organisations should protect their data and systems. For example, they may require companies to implement certain security measures, such as firewalls, encryption, and two-factor authentication.

As a result, the world's countries have become aware of the extent of this phenomenon, which is why they have cross-border cooperation between them. At the EU level, the following aspects are considered in the negotiation procedures:

The structure of the negotiations is based on free cooperation between the states concerned, including civil society interested in close cross-border cooperation in the fight against cybercrime and academic entities. The private sector, and NGOs are also willing to contribute to the work. The members involved in drafting the conventions benefit from assistance from the European Union, sufficient time for analysis and reaction on the collaboration and normative acts so that there is a homogenization of laws between states, with the main objective of combating cybercrime on a global scale.

In 2017, the Joint Communication of the European Parliament and the Resilience Council, some ideas and issues on "*building a strong cyber security for the EU*" (UE, 2017) were outlined with regard to the situation of states in the face of cyber attacks. In the fight against an invisible enemy, where national barriers are no obstacle, it is imperative that states have the necessary resources to defend themselves in first and foremost, against these attacks, but also to develop the skills to prevent and deter them. This must be facilitated by instruments and bodies developed and implemented within the European Union, including:

1. Eurojust's activities start when a referral of a criminal offence taking place in the territory of two Member States of the European Union, or in the territory of a Member State of the Union and a Member State with which Eurojust has concluded a cooperation agreement. Eurojust's modus operandi is to provide Member States with information and procedures for resolving divergences of jurisdiction, conflicts of competence and procedures relating to the taking and handling of evidence and the issuing of extradition warrants. Eurojust may also make a request for the opening of a criminal file following its own referral of an offence. Eurojust's assistance is prompt, as each case is different and the speed of reaction is important given the scale of the criminal act and the extent to which it is organised. At the same time, there are also cases where the scale of the investigation requires months of preparation and information gathering by Eurojust's intervention bodies, such as the setting up of joint investigations by the Member States, the provision of the necessary tools to solve the case by the European Union in terms of judicial cooperation, setting up joint meetings between the investigation teams in order to establish coordination directions. New living conditions brought on by the pandemic have amplified the problems of the system security of citizens, both physically and in the digital space, which is why there has been an explosion of international, cross-border cooperation requests and situations.

2. Europol was set up in response to serious crime on the territory of the European Union and beyond. Europol currently supports 27 countries and contributes to the development of criminal law enforcement rules and procedures in line with the different legal systems of the countries involved. Europol is made up of specialists and analysts in the field of organized crime of all kinds, selected among the best trained in Europe and beyond. The aim is to guarantee the security of European countries and those with whom cooperation agreements have been concluded, to provide law enforcement assistance to the Member States, to share information as quickly as possible on the issues concerned and to ensure the necessary training and expertise for the States concerned to resolve legislative differences.

3. The European Judicial Cybercrime Network was established in 2016 and is another cooperative networking tool provided by the Council of Europe, which is available to member states and law enforcement authorities. They are encouraged to make use of these services and sources information services and resources for judges, prosecutors and law enforcement authorities' criminal investigations and prosecutions with a view to carrying out justice. The European Judicial Network, as a basic structure, has been active since 1998 and facilitating international judicial cooperation. The way in which institution carries out its tasks is through the use and encouragement of links between the States concerned, by facilitating the access to information and to other European Union institutions, by providing the judicial bodies of the States concerned with the assistance, cooperation, logistics and necessary procedural support in resolving the case in question, and by facilitating the exchange of best practice and information in the field.

4. INTERPOL's began its work in 1923 as an international organisation with the task of ensuring management and cooperation between police authorities. Interpol has members from 100 countries, with whom it has established a relationship of collaboration and partnership in preventing and combating international crime of all kinds. The institution's tasks in the fight against crime include, first and foremost, assisting the States concerned in establishing the legal basis, and also provides training and assistance in the investigative work of the prosecuting authorities and provides them with secure communication channels. The main aim is to streamline judicial proceedings, to facilitate the handling of evidence, especially where several countries are involved, and assistance is available 24 hours a day, 7 days a week, and in 4 official languages: English, Arabic, Spanish and French. Interpol is also responsible for intervening in international situations where diplomatic relations have not been successful, intervening with neutral policies to de-escalate the situation, to create a framework for judicial cooperation under the given conditions, legislation, social values and public interests. This civil recourse can serve as a deterrent for negligent behaviour and poor security practices. Legislation often establishes dedicated bodies for cybersecurity, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the United States. These bodies play a crucial role in developing and enforcing cybersecurity standards. Certain sectors have specific rules requiring businesses to report cybersecurity incidents to the relevant authorities, which can provide a better understanding of the current threat landscape and aid in developing effective countermeasures.

Cybercrime is a topical issue of interest to all European states, an interest that has taken shape with the 2004 Hague Programme which addressed the issue of "*Information sharing between law enforcement and judicial authorities, ensuring an appropriate balance between privacy and security*" (European Parliament, 2008), the 2009 Stockholm Programme which addressed the issues of "A Europe that protects" and the need to implement stable cooperation between states and the Digital Agenda for Europe, both the one that ended in 2020 and the Digital Agenda for Europe 2020-2030, which aims to develop digital technology platforms and encourage the implementation of artificial intelligence in the lives of citizens.

All these innovations need to be developed within an appropriate legislative framework that ensures a secure development for citizens but also a set of procedures and rules that act quickly to sanction cybercrime behaviour and forms of cybercrime.

In essence, these legal frameworks act as both a deterrent against cybercrimes and a mandate for businesses and organisations to maintain robust cybersecurity practices to protect themselves and their customers or users.

Software as a Service (SaaS) and cybersecurity legislation interact in ways that can create certain legal gray areas and conflicts. Since SaaS often involves data storage and transfer across national borders, there can be jurisdictional complexities regarding data protection laws. For instance, a European user's data might be stored in the US, leading to conflicts between the European Union's GDPR and US privacy laws. There can be gray areas around who owns and controls data in a SaaS environment. It often needs to be clearly defined whether the responsibility for data protection lies entirely with the service provider or the user. This uncertainty can complicate compliance with cybersecurity legislation. Many SaaS companies use third-party services for various tasks, which can lead to security issues. If these third parties do not adhere to the same security standards or are not compliant with certain regulations, it can create legal ambiguities and challenges. In certain jurisdictions, laws might allow government or law enforcement agencies to access data stored by SaaS providers. This can potentially conflict with privacy and data protection laws, leading to dilemmas for SaaS providers.

The language used in end-user agreements (*EUAs*) and privacy policies can sometimes conflict with legislative requirements. Often, users must be fully aware of what they agree to, leading to potential issues around informed consent.

SaaS providers and users must work closely with legal and cybersecurity professionals to navigate these complexities and comply with all relevant laws and regulations. This is a continually evolving field, and the legislation can vary widely by country and region, so staying updated on the latest developments is crucial.

6. Recommendations and Future Directions

Cybercrime is becoming increasingly difficult to detect given the fact that that cyber attackers are investing huge amounts of money in their own networks and infrastructure to which is why the authorities responsible for combating this phenomenon have a delayed response. In the last two years, computer system denial of service offenses have included sectors such as banking, freight forwarding, healthcare systems and public administrations.

Improving cybersecurity and compliance is an ongoing and multifaceted process. SaaS providers can take various steps to improve their cybersecurity posture and achieve regulatory compliance. Establishing a robust *Information Security Management System* (*ISMS*), such as one based on the ISO 27001 standard (MYRA, 2023), can provide a comprehensive approach to managing information security risks. An ISMS includes policies, procedures, and controls for managing an organization's information risk management processes. Ensure that all software, systems, and applications are regularly updated and patched. This can help protect against vulnerabilities that cybercriminals could exploit. Implement strong access control measures such as two-factor authentication, role-based access control, and least privilege principles to minimize the risk of unauthorized access to sensitive data and systems. Adopt secure development practices to reduce the chance of introducing security vulnerabilities into your software. This could involve using security frameworks, conducting code reviews, and regularly testing your software for vulnerabilities. Conduct regular audits to ensure compliance with relevant laws and regulations. This can help identify potential gaps in your compliance program and correct them before they become issues.

The formulation of legal policies for better protection depends on the context you're referring to. However, given the context of cybersecurity and data protection, here are a few general policy recommendations:

- Broaden the Scope of Data Protection Laws: Many jurisdictions worldwide have specific data protection laws like the General Data Protection Regulation (*GDPR*) in Europe. However, in some regions, these laws must be improved. More countries should consider developing comprehensive data protection laws to protect individuals' personal data better. At the level of law enforcement and the administration of justice, it is more than necessary to hold meetings at international level to discuss new investigation techniques, new tools for managing this phenomenon, legislative changes applied in the field and the exchange of information on how to attack and combat the phenomenon. The cyber field is constantly changing and the measures that were implemented a year or a month ago will not have the same response to a crime that is taking place today.

- Right to be Forgotten: Legal policies should allow individuals to have their data erased from a company's records. This helps people maintain control over their data and can be particularly important in the digital age, where data can be easily replicated and distributed.

- Right to Data Portability: Individuals should have the right to receive the personal data they have provided to a controller in a structured, commonly used, and machine-readable format. They should also have the right to transmit those data to another controller without hindrance.

- Strengthen the Consent Mechanism: Policies should mandate organizations to seek clear and informed consent from individuals before their data is collected, used, or shared. Consent should be free, specific, informed, and unambiguous. The withdrawal of consent should be as easy as giving it.

- Security Breach Notification Laws: Laws should require organizations to notify affected individuals and relevant regulatory authorities in the event of a data breach. This can help individuals protect themselves from potential harm and allows regulators to hold companies accountable.

- Mandatory Privacy Impact Assessments (*PIA*): Organizations must conduct a PIA for personal data projects. This can help identify potential privacy risks and take steps to mitigate them before the project is implemented.

- Increased Penalties for Non-compliance: Increase fines and penalties for non-compliance with data protection laws to deter organizations from lax data handling practices.

- Regulation of Data Brokers: Enact stricter regulations on data brokers who collect, aggregate, and sell personal data. This includes requiring them to be transparent about their practices and giving individuals the right to opt out of their databases.

- Children's Data Protection: Given the sensitivity of children's data, strict laws should provide additional protections for children's data, such as requiring parental consent for data collection.

- Cross-border Data Transfers: Enforce more stringent policies for cross-border data transfers to ensure that personal data is adequately protected even when it is transferred to other countries.

- Artificial Intelligence and Machine Learning Regulations: As *AI* and *ML* technologies advance, laws should be enacted to address these technologies' unique privacy and ethical challenges.

As technology continues to evolve, so will the threats and legal challenges we face. As *AI* and *ML* continue to grow in sophistication, they can be used in cyber attacks to identify vulnerabilities, automate attacks, or even mimic human behavior to fool security systems. In addition, using *AI* and *ML* raises significant legal and ethical questions, such as who is responsible when an *AI* system causes harm or how to prevent discrimination and bias in *AI* algorithms. The advent of quantum computing could render many current encryption methods obsolete, potentially opening up a new frontier for cyber attacks. On the legal side, there are questions about how to regulate the use of quantum computing and protect intellectual property in quantum algorithms and designs.

On the other hand, the proliferation of *IoT* devices is creating a vast new attack surface for cybercriminals. Many of these devices need better security measures, making them easy targets. The legal challenges here include questions of liability (who is responsible when an insecure *IoT* device is exploited in a cyber attack?) and how to ensure data privacy when these devices collect and transmit personal data. It's certainly concerning how vulnerable autonomous vehicles can be to cyber-attacks. In the unfortunate event that an autonomous vehicle is hacked and causes an accident, determining legal responsibility can be complex. Depending on the circumstances, it could be the manufacturer, the software provider, or the vehicle owner. It's important for all parties involved to take necessary precautions to prevent cyber attacks and ensure the safety of everyone on the road.

In all these areas, proactive legislation and regulation will be key to mitigating risks and addressing legal challenges. Policymakers must stay abreast of technological advancements and understand their implications to create relevant and effective policies.

7. Conclusion

Cybersecurity is crucial for Software as a Service (SaaS) providers. Not only to protect their own infrastructure but also to secure their clients' data. SaaS companies must proactively identify potential threats, mitigate risks, and respond effectively to security incidents. Policies and regulations play a vital role in protecting data and ensuring compliance with security standards. Legal protections can be enhanced by encouraging transparency, strengthening reporting requirements, implementing privacy by design, promoting encryption, and providing legal recourse for breaches. Technological advancements will lead to new types of cyber threats and raise new legal challenges. These include threats to artificial intelligence, machine learning, Internet of Things devices, quantum computing, and autonomous vehicles. These threats' legal and ethical implications need to be considered proactively, and laws and regulations should be updated accordingly. Cybersecurity is not a static field – as technology evolves, so do the threats we face. SaaS providers, and indeed all businesses, need to be aware of these emerging threats and prepare for them. Policymakers are also crucial in creating a regulatory environment that promotes security, protects individuals' rights, and fosters innovation. Ultimately, the goal should be to create a cyber ecosystem that is resilient, secure, and trusted by all stakeholders.

Cybersecurity and proper legislation are paramount in today's digital age, particularly for Software as a Service (SaaS) providers. As custodians of vast amounts of valuable customer data, SaaS providers have a crucial role in preserving digital assets' security, integrity, and confidentiality. Cybersecurity isn't merely a technological issue but is deeply intertwined with the trust and credibility that businesses establish with their clients and partners.

Proper legislation provides the structure and guidelines to ensure that SaaS providers implement robust cybersecurity measures. Laws and regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (*CCPA*), the Health Insurance Portability and Accountability Act

(*HIPAA*), and the Payment Card Industry Data Security Standard (*PCI-DSS*) provide the legal backdrop for SaaS providers' actions. These laws not only set minimum cybersecurity standards but also provide rights to individuals concerning their data.

The growing landscape of cyber threats and the increasing reliance on digital platforms and services make cybersecurity and robust legislation indispensable. A proactive approach to cybersecurity, focusing on prevention, detection, and quick response to threats, can make a significant difference.

However, it's important to remember that legislation alone cannot solve all cybersecurity challenges. An effective approach to cybersecurity should also involve the following: regular training; cultivating a security-focused culture; employing cutting-edge technology to combat evolving threats.

It requires a balanced and comprehensive strategy that blends technology, people, processes, and legislation. In closing, cybersecurity and proper legislation in the SaaS industry aren't just about risk mitigation - fundamentally tied to how businesses operate, innovate, and grow in the digital era. Staying ahead of cyber threats and regulatory changes isn't just a good business practice but is necessary in our increasingly interconnected world.

8. Acknowledgement

This work is supported by the project AiMedia - Open innovation platform for managing collaborative creativity in Digital Marketing (Platformă de inovare deschisă pentru gestionarea creativităţii colaborative în Marketingul Digital - AiMedia) in the framework of Competitiveness Operational Programme, financed from the European Regional Development Fund under the contract number 77/221_ap2/01.09.2020, SMIS Code: 129318.

References

Alhanahnah, M. J.; Arshad, J. & Sahel A. (2016). A multidimension taxonomy of insider threats in cloud computing. *The Computer Journal*, Vol. 59(11), pp. 1612-1622.

Banka, A.; Anshul S.; Mangal S. & Hoon, J. L. (2013). Exploration of security parameters to evaluate SaaS. *International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1-6. July 4-6. Tiruchengode, India.

Barona, R. & Anita, E. (2017). A survey on data breach challenges in cloud computing security: Issues and threats. *International conference on circuit, power and computing technologies (ICCPCT),* April 20-21, 2017, Kollam, India.

Basit, A.; Zafar, M.; Xuan, L.; Abdul, R. J.; Zunera, J. & Kashif, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, Vol. 76, pp. 139-154.

Carraro, G. (2006). *Understanding SaaS architecture: a simple SaaS maturity model*. *Web page*. Retrieved from http://msdn.microsoft.com/enca/architecture/aa699384.aspx, date: 12.07.2023.

Chinedu, P. & Nwankwo W. (2018). Security of cloud virtualized resource on a SaaS encryption solution. *Science Journal of Energy Engineering*, Vol. 6(1), pp. 8-17.

Court of Appeal Cluj (2012). *Dosare / Info Hotărâri (Files / Info Decisions Curtea de Apel Cluj)*. *Web page.* Retrieved from https://www.curteadeapelcluj.ro/index.php/dosare/info-hotarari.html, date: 13.07.2023.

Darwish, M.; Abdelkader, O. & Capretz, L. F. (2013). Cloud-based DDoS attacks and defenses. *International Conference on Information Society (i-Society 2013)*, June 24 – 26. Canada.

Dexonline (2023). *Infracțiune (Offence)*. *Web page*. Retrieved from https://dexonline.ro/definitie/infrac%C8%9Biune, date: 12.07.2023.

Dhiyanesh, B. & Sakthivadivu S. (2016). F2C: a novel distributed denial of service attack mitigation model for SAAS cloud environment. *Asian Journal of Research in Social Sciences and Humanities*, Vol. 6(6), pp. 192-203.

European Court of Auditors (2019). *Provocări pentru o politică eficace a UE în domeniul securității cibernetice/ Challenges for an effective EU cybersecurity policy*. *Web page.* Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf, date: 13.07.2023.

Gao, J.; Manjula, K.; Roopa, P.; Sumalatha, E.; Xiaoying B.; Tsai, W. T. & Tadahiro U. (2012). A cloud-based TaaS infrastructure with tools for SaaS validation, performance and scalability evaluation. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, December 3-6, 2012, Taipei, Taiwan, pp. 464-471.

George, A. S. & Sagayarajan S. (2023). Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS and SaaS Environments. *Partners Universal International Research Journal*, Vol. 2(1), pp. 24-34.

Guillén, D. L.; Ángel, M.; Morales-Rocha, V. & Fernández, Martínez, L. F. (2020). A systematic review of security threats and countermeasures in SaaS. *Journal of computer security*, Vol. 28(6), pp. 635-653.

Hussein, N. H. & Ahmed K. (2016). A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security*, Vol. 14(1), pp. 52-56.

Kandias, M.; Nikos, V. & Dimitris, G. (2011). The insider threat in cloud computing. *Critical Information Infrastructure Security: 6th International Workshop (CRITIS)*, September 8-9, 2011, Lucerne, Switzerland.

Kang, S.; Kang S. & Hur, S. (2011). A design of the conceptual architecture for a multitenant SaaS application platform. *First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, Jeju, Korea (South), pp. 462-467.

Legislation (2023). *Lege nr. 161 din 19 aprilie 2003 (Law no. 161 of April 19, 2003). Web page*. Retrieved from https://legislatie.just.ro/Public/DetaliiDocument/43323, date: 13.07.2023.

Lopez, M. & Buscetta M. (2021). *Vital pandemic industries foster unprecedented DDoS attack*. *Web page.* Retrieved from https://www.netscout.com/press-releases/vital-pandemic-industries-foster-unprecedented-ddos-attack, date: 13.07.2023.

Lupascu, D. (2023). *Codul penal și Codul de procedură penală / The Criminal Code and the Criminal Procedure Code*. Ed. Universul Juridic.

Mäkilä, T.; Järvi, A.; Rönkkö, M. & Nissilä, J. (2010). How to define software-as-a-service - An empirical study of finnish SaaS providers. *Proceedings 1. Springer Berlin Heidelberg*, *Software Business: First International Conference*, ICSOB 2010, June 21-23, 2010, Jyväskylä, Finland.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, Vol. 2(2), pp. 109-134.

Mietzner, R.; Metzger, A.; Leymann, F. & Pohl K. (2009). Variability modeling to support customization and deployment of multi-tenant-aware software as a service applications. *Proceedings of the ICSE Workshop on Principles of Engineering Service Oriented Systems (PESOS)*, pp. 18-25, May 18-19. Vancouver, Canada.

Minister of Interior Affairs of Romania (2021). *Operațiunea Gold Dust (Gold Dust Operation)*. *Web page*. Retrieved from https://www.politiaromana.ro/ro/stiri-si-media/comunicate/operatiunea-golddust, date: 13.07.2023.

Mozumder, D. P.; Mahi, J. N. & Whaiduzzaman, M. (2017). Cloud computing security breaches and threats analysis. *International Journal of Scientific & Engineering Research*, Vol. 8(1), pp. 1287-1297.

MYRA (2023). *What Is an Information Security Management System (ISMS)? Web page*. Retrieved from https://www.myrasecurity.com/en/knowledge-hub/information-security-management-system-isms/#:~:text=on%20IT%2DGrundschutz-A%20Definition%20of%20ISMS,in%20companies%20and%20government%20agencies., date: 13.07.2023.

Neto, N. N.; Stuart, E. M.; Anchises, M. G. & Borges, N. M. (2020). A case study of the capital one data breach. *SSRN Electronic Journal*, Vol. 1, pp. 1-24.

Parra, O. & Granda, M. F. (2021). Evaluating the meeting solutions used for virtual classes in higher education during the COVID-19 Pandemic. *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP)*, Vol. 2, pp. 190-197, ISBN: 978-989-758-488-6.

Polemi, N. & Praça, Isabel (2023). *Multilayer framework for good cybersecurity practices for AI*. *Web page*. Retrieved from https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6211/1/1687116981595.pdf, date: 13.07.2023.

Roumani, Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. *Journal of Cybersecurity*, Vol. 7(1), pp. 1-13.

Sharaf, A.; Fursan, T.; Fua'ad, H. A.; Anandakumar, H. & Sudhir J. (2021). The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications. *International Journal of Intelligent Networks*, Vol. 2, 2021, pp. 166-174, ISSN 2666-6030.

Shifu, H.; Aaron, S.; Yanfang, Y. & Lifei, C. (2016). Droiddelver: An android malware detection system using deep belief network based on api call blocks. *International Conference on Web-Age Information Management*, *Springer*, pp. 54-66, ISBN 978-3-319-47121-1.

Su, W.; Lin, C.; Meng, K. & Liu, Q. (2014). Modeling and analysis of availability for SaaS multi-tenant architecture. *IEEE International Workshop on Service-Oriented System Engineering (SOSE)*, April 7-11, 2014, Oxford, United Kingdom.

Suryateja, P. S. (2018). Threats and vulnerabilities of cloud computing: a review. *International Journal of Computer Sciences and Engineering*, Vol. 6(3), pp. 297-302.

Tam, T.; Asha, R. & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security*, Vol. 109, pp. 1-20.

The European Commission (2017). *Common communication to the European Parliament and the Council. Resilience, prevention and defence: building strong cyber security for the EU (Comunicare comună către Parlamentul European şi Consiliu. Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE)*. *Web page*. Retrieved from: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017JC0450&from=RO%20-%20EU,%202017, date: 12.07.2023.

Tripathy, D.; Rudrarajsinh, G. & Talal H. (2020). Detecting SQL injection attacks in cloud SaaS using machine learning. *The 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, May 6-8, Jinan, China.

Tsai, W. T.; Yu H. & Qihong S. (2011). Testing the scalability of SaaS applications. *IEEE International Conference on Service-Oriented Computing and Applications (SOCA)*, December 12-14. Irvine, California.

Tudor, C. (2022). The impact of the COVID-19 pandemic on the global web and video conferencing SaaS market. *Electronics*, Vol. 11(16), pp. 1-17.