Journal of Business and Management Studies (JBMS)
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Data Privacy Regulations and Their Impact on Business Operations: A Global Perspective

Md Sultanul Arefin Sourav[1]✉, Md Imran Khan[2], and Tanvir Rahman Akash[3]
[1]Bachelor's of Business Administration, School of Economics and Management, China Three Gorges University, Hubei Province, China
[2]Bachelor's of Business Administration, School of Business, University of Information Technology and sciences(UITS), Dhaka, Bangladesh
[3]Bachelor's of Business Administration in Finance, Bangladesh University of Professionals (BUP), Dhaka, Bangladesh
Corresponding Author: Md Sultanul Arefin Sourav, **E-mail**: arefin.22usa@gmail.com

| ABSTRACT
The growth of globalization has brought about laws that protect individual and organizational data from misuse, being accessed by unauthorized people and cyber-attacks. As a result of rules like the GDPR, CCPA and related statutes in Asia-Pacific and Africa, businesses have reworked their methods of collecting, storing, processing, and sharing information. This work studies the influence of data privacy laws on business activities around the world by examining trends in vulnerabilities, problems in meeting the standards and the state of security using the Common Vulnerabilities and Exposures (CVE) dataset. By comparing published vulnerabilities with local data protection rules, the study hopes to join technical cybersecurity practices with legal rules. With the help of the CVE dataset which lists cybersecurity vulnerabilities based on certain standards, the study discovers how data breaches develop, what causes them and how good existing regulation is at preventing these events. It also studies how different regulations shape a company's choices to build secure products from the start and to employ risk reduction and privacy-oriented technologies. This study reviews how businesses especially those with worldwide operations suffer from the complexity and varying requirements of regulations. This study explains that the Common Weakness Enumeration (CWE) and Common Vulnerability Scoring System (CVSS) help in prioritizing security activities as required by regulations. It also describes how regulators strive to make sure that all data handling is open and trustworthy. The results emphasize that stronger enforcement of privacy regulations leads to better cybersecurity habits by regions, as shown by lowered levels of significant vulnerabilities. The scientists found that just being compliant is not enough for great security and emphasize that including threat intelligence, teaching employees and ethical management is necessary. Finally, the analysis gives policymakers, security experts and business leaders helpful tips to succeed with data protection while preserving their company's ability to adapt.

| KEYWORDS
Data Privacy Regulations, Business Operations, Cybersecurity, GDPR Regulatory Compliance and Vulnerability Management

| ARTICLE INFORMATION
ACCEPTED: 10 May 2020 **PUBLISHED:** 25 June 2020 **DOI:** 10.32996/jbms.2020.2.1.6

1- Introduction

1.1 Background

With the increasing connections between the world's economies, millions of pieces of personal and sensitive data are being generated, kept and shared using digital platforms. Organizations in every industry depend greatly on digital tools for managing their customers and their supply chain. As a result of moving to digital, companies have become more efficient, but privacy concerns have risen as well. There is a risk that someone other than may gain access to or misuse financial or medical information data breaches and privacy issues. Governments and organizations around the world have brought in strict data privacy laws such as the European Union's GDPR, the CCPA in California and similar rules in many countries [1]. By using these

rules, people are helped to keep information about themselves secure and protected. Nonetheless, businesses face several problems when adopting such rules: following long and detailed laws, keeping their operations efficient and competing effectively. Because the legal landscape is changing, companies have to update their procedures, put more money into compliance systems and think deeply about data management. If a company fails to obey the rules, it may end up with serious fines, its reputation soil and fewer consumers. That's why paying attention to the interplay between data privacy rules and how businesses operate is crucial for leaders and policymakers [2]. Focusing on transparency, accountability and user consent is causing companies around the world to handle data differently. It is important to understand these issues when creating ways of operating that fit privacy principles. This research wants to discover what global data privacy regulations mean for businesses and how they have changed daily operations across different industries.

1.2 Exploring the Dangerous Threats Happening in Today's Digital World

Worldwide are moving quickly towards digital operations, leading to both new opportunities and more cybersecurity dangers. Since companies are using more connected systems, cloud solutions and IoT gadgets, their risk of cyber-attacks has grown a lot. Among these threats are attacks using malware and ransomware, at the same time as attacks by nation-state spies and insiders [3]. Using vulnerabilities, configuration errors and unprotected data, cybercriminals can make off with confidential data, interrupt service and ask for extortion payments. Due to more jobs being done remotely, employees bringing their own devices and a rise in exchanging data worldwide, it has become more challenging to manage cybersecurity risks. Properly handling data privacy is both a requirement by law and an important element for cybersecurity. Not using strong data privacy strategies can result in data breaches, legal fines and wide criticism. Cybersecurity must be worked into both the organization's regulations and basic governance. Data privacy regulations are created to defend consumer interests and to help enhance a company's cybersecurity. These regulations, organizations have to enforce encryption, secure their data, report any incidents and tell people if a breach occurs. Yet, properly following regulations is not enough; protection needs to involve technological security, educated employees and the general work culture [4]. Firms must adapt with the changing threats and make sure their treatment of data follows new regulations. As cyberthreats meet privacy regulation, this area becomes very important and challenging for modern businesses. The research focuses on how having these threats has spurred the development and enforcement of world data privacy laws and their consequences on the business practices of countries around the globe.

1.3 How the CVE System Works

The CVE system helps spot and categorize software vulnerabilities, even though it doesn't focus directly on data privacy regulations in the cybersecurity world [5]. MITRE Corporation manages the CVE system which uses unique identifiers for security problems and enables all parties to respond and understand them consistently. All CVE entries offer crucial details on a particular vulnerability, together with a standard description, affected software or hardware and its severity. The NVD run by NIST provides details such as CWE categories and CVSS scores to add to the existing CVE record [6]. Despite being mainly about systems' technical holes, CVEs play a key role in data privacy. If vulnerabilities are used by hackers, the results are often lost or stolen data, illegal access to actual or potential data and failure to follow GDPR or similar regulations. Firms must find and repair CVEs as soon as possible to keep their data safe and prevent them from being penalized. Using CVE data allows organizations to deal with threats before they can endanger customer data or run the risk of violating rules and regulations [7]. Within the CVE design, companies can obtain threat intelligence and use it to watch for emerging patterns and adjust their budgets accordingly. Following data privacy laws requires watching for vulnerabilities using CVE data and ensuring that they are handled is important even though it was not intended for this purpose, as it supports data privacy compliance and aligns with laws important to business today.

1.4 Importance of classifying vulnerabilities with CVSS and CWE

For better awareness of cybersecurity risks relating to data privacy, people rely on tools such as CVSS and CWE. Vulnerability severity is measured with CVSS by looking at impact aspects including confidentiality, integrity and availability [8]. They are specifically tied to the central rules for data protection found in regulations such as GDPR and CCPA. CVSS scores of more than 7.0 usually alert companies to a serious risk of data misuse, so it is very useful for guiding compliance and handling risks. Similarly, the CWE framework sorts the main issues in software for example, not verifying what comes in from users or failing to store data safely which produce security weaknesses. By tying CVEs to CWE types, organizations can learn about regular security issues that might cause them to break the law if taken advantage of. Thanks to CVSS and CWE, security teams are able to treat vulnerability management as a risk-focused process. Identifying and dealing with significant vulnerabilities as quickly as possible in regulated areas may confirm that important risks are managed properly and can prevent penalties [9]. They make it possible to carry out automated compliance, risk and auditing tasks. Since laws requiring breach reports and safe data processing are becoming tighter, CVSS and CWE play a role in ensuring both our systems and laws are followed [10]. They are important in helping with regulators, corporate chief executives and building customer confidence. The report focuses on how these systems help businesses organize their cybersecurity activities as required by global data privacy rules.

1.5 Problem Statement

As laws that safeguard private data become stricter in various regions, companies now encounter tough obstacles to being compliant [11]. These problems consist of understanding legal rules, applying suitable technology measures and managing operations smoothly according to the law. Many businesses are aware of data privacy, but few use a well-defined plan to incorporate it into what they do each day. This study examines how recent global data privacy laws can change business plans, operations strategies and methods for managing risks. It examines if the regulations work well for information protection or instead slow down or make it more difficult for organizations to be productive and improve.

1.6 Objective of This Study

This study looks only at public CVE records in the NIST National Vulnerability Database from the years 1999 through 2019. The domain looks at important variables such as:

- To review the impact of worldwide data privacy rules on businesses in several sectors.
- To list the problems companies, face when trying to meet regulations such as GDPR and CCPA in their operations, financial matters, and technology.
- To investigate how groups adjust how they work, manage data, and use technology to reach data protection requirements [12].
- To assess if data privacy frameworks help to prevent cybersecurity and data breach events.
- To project the future effects of complying with regulations on innovation, marketplace rivalry and trust among stakeholders [13].
- To design and suggest practical plans for combining privacy compliance with sustainable company growth.

1.7 Research Questions

This study uses the following questions as its guide:

1. How do worldwide data privacy guidelines impact both the efficiency of businesses and the amounts they need to spend on compliance?
2. What barriers do organizations encounter when putting data protection rules such as GDPR and CCPA into practice?
3. In what ways do data privacy laws affect new technology, the trust customers place in companies and the steps companies take to advance?

1.8 Significance of the Study

The work provides useful explanations of how data privacy rules are affecting business operations. Because more countries are introducing stricter data protection laws, understanding what these laws mean is now very important for corporate leaders, IT professionals, lawyers and policymakers [14]. The value comes from the study's wide coverage and useful application: it explains not only what is written in the regulations but also how they are applied [15]. The results help businesses figure out how to meet legal standards while keeping their productivity and creativity high. The findings suggest that regulators and privacy advocates may need to improve some laws to reduce the effort needed for adoption [16]. The research helps to fill a hole in current research, where privacy law is mostly explained either legally or technically. Using an interdisciplinary approach, this study proves how data privacy laws slightly influence human resources, the IT area, financial planning, and management strategies in businesses. Seeing these trends makes compliance and survival in the long run an easier task. As a result, organizations are encouraged to follow data protection methods from the beginning of product creation, in serving customers and with partners. In the end, the study helps explain how privacy laws affect the evolution of business in our data-driven age.

1.9 Scope of the Study

In this study, experts examine how data privacy laws the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD) and the proposed Personal Data Protection Bill (PDPB) from India—affect companies and their activities in various regions [17]. It analyzes how the recent and emerging rules impact executive decisions, ways data is governed, information technology and strategies for avoiding risks. The analysis looks at different business sizes, starting with large, multinational companies and including SMEs, in main areas such as finance, healthcare, e-commerce and information technology [18]. The researchers analyze laws from various places and do not focus on detailed studies of individual cases or laws. The emphasis is instead on how regulations impact how an organization functions, mentioning costs of compliance, policies within the company, ways of handling data and dealing with international data transfers. Also, it discusses how organizations are setting up data maps, performing PIAs and developing governing frameworks to comply with regulations [19]. Cybersecurity issues are dealt with when they coincide with privacy responsibilities,

the main concern is how privacy-specific regulations affect a business. To have a full picture of organizational adaptation, how regulators, consumers and employees are affected.

2. Literature Review

2.1 How Data Privacy Regulations Have Evolved Around the World

Over the past two decades, organizations have collected, stored, and analyzed far more data than they ever have before. The fast rise of digital platforms and the internet has led to more issues about data privacy worldwide. In response to these problems, governments worldwide introduced measures to protect people's private information. One of the most important is the General Data Protection Regulation (GDPR), proposed by the European Union which now regulates data protection and setting rules for controllers and consumers worldwide. The CCPA is one of several follow-up measures in California that signal a move toward laws that put consumers first when handling data [20]. Concerns about growing data misuse, security violations and monitoring are what motivated the creation of these regulations. Complying with these regulations now requires organizations to set up data governance structures and follow proper technical, procedural, and administrative protections [21]. Along with complying, these regulations also show that people now expect data privacy to be a basic human right. In today's world, organizations must always act transparently with their data to gain and maintain public trust. Data protection regulations have changed the way business's function, so ensuring privacy is now required everywhere.

2.2 Operations and Strategy for Businesses

How businesses operate inside and outside the organization has been heavily influenced by data privacy laws. Now, organizations must strengthen their compliance, setting up advanced safety in IT, working with lawyers, hiring privacy staff and training workers. Due to these laws, companies may lose their credibility if they do not secure customers' data, making them add data protection to their risk planning [22]. Compliance is mandatory, as it helps an organization function in chosen markets and work with its customers, partners, and regulators. To operate properly, firms are updating their data practices, often changing how they work to include privacy-by-design and privacy-by-default concepts [23]. Data operations now depend on managing consent, using as little data as possible, handling data breaches and keeping data secure. Matching company processes to different privacy laws in every region is a big obstacle for many worldwide companies. Organizations that treat data privacy as an important strategy generally see better customer care and stronger market distinctiveness. there are more expenses involved, organizations become more valued in the long run as they cut down on chances of data breaches and fines [24]. Complying with privacy laws ahead of time improves a company's ability and reputation. Privacy rules are driving companies to share more information, improve their effectiveness, and use the latest technology, all while following laws and expanding.

2.3 Importance of CVE Data for Achieving Compliance

There is growing worry about the link between cybersecurity and data privacy compliance with more advanced and widespread threats being noticed. Organizations must prove that they have put in place suitable technical measures to secure peoples' data. Common Vulnerabilities and Exposures (CVE) serves as an important asset for detecting, tracking, and minimizing known security problems [25]. Businesses can remain informed about software vulnerabilities that could let unauthorized people access personal or sensitive data with the help of CVE entries. With CVE data in their vulnerability systems, organizations can better arrange patches, modify settings, and apply solutions that fit their situation. Firms are better able to comply with the requirement in data protection laws to use technology to ensure user data is protected [26]. Companies can use the Common Weakness Enumeration (CWE) system to find out what makes a vulnerability possible and the Common Vulnerability Scoring System (CVSS) allows them to rate the threat level of each vulnerability. By including CVE-based threat intelligence in corporate governance, a company links its technical and legal cybersecurity obligations [27]. Using CVE information, companies can generate audit trails, compliance reports and summaries of risks that are needed for regulators when checks or investigations take place. Doing so adds strength to a company's technology, addresses its regulatory needs, allows operations to carry on smoothly and improves stakeholder trust.

2.4 How Privacy Laws Affect Businesses That Work with Data

Compliance with data privacy rules is changing the way organizations design, launch and sell data-focused products and services. Companies that used detailed data to target customers, analyze how they act and create AI models now must adapt their methods according to rules around consent, reducing how much data is kept and restricting uses for the data [28]. Ethical and open data processing has now become very important, so businesses must stick to ethical practices even as they try to innovate and make a profit. Some businesses believe that rules about privacy keep them from growing, others find ways to improve using those regulations [29]. There are examples where new privacy-ensuring methods such as federated learning, differential privacy and anonymization technologies are being trusted to protect sensitive data. Those companies that make data security central to their solutions often use this as a selling point to show trust and meet consumer expectations for fairness [30]. Companies are being urged to use Privacy by Design which means making privacy a key part of every system or platform from

the outset. Privacy is now considered on par with other design principles at every stage of product creation. The deeper effect is an improved level of transparency and responsibility in the data economy, although compliance is an issue for many small companies. Data privacy laws help make innovation safer, more responsible, and better suited for users.

2.5 Different Rules and Difficulty in Complying

Global businesses face challenges because different parts of the world have separate rules about handling personal data. Certain countries such as the European Union have developed clear data protection systems, whilst others offer only a little coverage or specific for selected industries. As a result of this inequality, companies operating abroad are forced to spend extra time and energy ensuring they don't run afoul of regulations in various countries. Because there are many variations in how things like data definitions and laws for cross-border transfers are written, it's difficult to apply one global solution [31]. A major problem is that different countries use different standards to handle international data transfers. Means of authorizing cross-border data transfers such as SCCs, BCRs and regional adequacy, are commonly applied, but these tools are always being checked by legislation and politics. Any unexpected changes in how regulators see the rules, like ending data transfer agreements, could cause business operations to break down and open gaps in compliance [32]. Instead of meeting the minimum requirements, certain organizations prefer adopting the harshest laws (GDPR) to keep their operations more in line with the highest standards. For some companies, it is essential to follow rules in every country and build separate methods of handling product releases [33]. By having the same procedures worldwide, there may be operational problems in some places. Global alignment projects are highly valued by policymakers, yet companies should invest in flexible compliance systems that grow, divide, and respond to new laws.

2.6 Empirical Study

In their influential article, Karhulainen and Oré combine some ideaso Globally, Colin J. Bennett and Charles D. Raab document in "Contemporary Policy Instruments in Global Perspective" (2018) how privacy policy tools have changed over the course of 15 years. The study investigates the methods used internationally, by regulation, and self-regulatory practices to safeguard personal data, while checking how these tools respond to changes in technology, the economy, and society. Even if the main kinds of instruments have stayed the same, they have now become broader in scope and scale, representing significant changes in concepts related to accountability, ethical use of data, and managing risks [1]. The focus of this study matches the existing studies that look at data privacy laws and their effect on business activities. Bennett and Raab provide useful information about the effects of changing privacy regulations on how companies comply with them globally.

In the article "The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy" by Dr. Abdulah M. Aseri, the author considers the ways in which the GDPR has influenced data privacy around the world, mainly for companies situated beyond the EU. With semi-structured interview data, the study shows that GDPR has introduced tough regulations that encourage international companies to handle data more transparently and pay close attention to their users' interests [2]. It was found that companies that fail to comply face serious consequences, and this has led global organizations to reconsider their data governance systems. Evidence from studies helps confirm the potential impact of privacy regulations on businesses worldwide. The research supports the GDPR's contribution to upgrading worldwide data privacy standards and making it important for companies to comply when adopting strategies in this field.

The article titled "The European General Data Protection Regulation" describes the following points. Colin J. Bennett's book, "An Instrument for the Globalization of Privacy Standards?" looks at how the GDPR has shaped data privacy standards around the world. Bennett describes how the guidelines of the GDPR developed, as issues related to digital privacy, information leaks, and use of shared data increased [3]. The paper looks at the growth of data protection laws, beginning in Europe and stretching into the modern era where the GDPR's rules impact privacy globally. The article points out that the GDPR has raised expectations for global organizations since it is a standard that many other nations look up to. Bennett supports this study by explaining the spread of European privacy standards and underlining that multinationals have to deal with detailed legal boundaries set by such regulations.

The main topic of the article is Ms. Goddard points out in "European Regulation that has a Global Impact" that the GDPR has greatly influenced countries outside of Europe. Goddard states that while the GDPR is meant to ensure data protection within the EU, its reach also affects international organizations outside the EU borders. Any organization globally with EU customers' data must meet its exact guidelines on consent, access to information, and being responsible. It covers the effects multinational companies may experience, the stress placed on personal privacy, and the added obligations companies must deal with [4]. Goddard's contributions have greatly helped to show the worldwide influence of the GDPR law, thanks to the EU model. It illustrates the leading role that the GDPR plays, leading others to adopt stricter policies for data protection.

The authors in the article "The Impact of GDPR on Global Technology Development" study how GDPR affects technology strategies, especially in the United States and China. It points out that GDPR is both a challenge and an opportunity,

so organizations are encouraged to manage their data better, use stronger cybersecurity steps, and integrate privacy in any new technologies [5]. The author points out that even though GDPR is strict about who is responsible and about consent, it still supports new developments by creating new privacy and risk standards. In this research, the article shows that following regulations plays a key role in driving technological changes in various industries. It further proves that international businesses must use data in new ways to combat risks as well as improve their positioning in a market where privacy is valued.

3. Methodology

This study explains the detailed approach used to investigate how data privacy laws affect businesses around the world. A mix of numerical analysis and research into global regulations has been used in this study [34]. Main subsections in the methodology are research design, methods for collecting data, processing those data, engineering aspects, analytical techniques, potential shortcomings, and ethical considerations.

3.1 Research Design

A combination of quantitative and qualitative methods is used in this study to fully understand how global data privacy rules impact business activities. Because the topic covers both measured cybersecurity data and the analysis of legislation, it makes sense to combine different research methods [35]. The quantitative side of the research looks at cybersecurity incident trends found in the Common Vulnerabilities and Exposures (CVE) and the qualitative side investigates the details, use of language and strength of implementation for data privacy regulations like the GDPR in Europe and the CCPA in the United States. Combining these techniques, the research checks that changes in regulation correspond to trends in business security. From 1999 to 2019, the study looked at changes taking place both before and after vital data privacy laws became effective [36]. There is enough time range in this period to see how both the number and severity of reported threats have changed. Contrary to looking for cause-and-effect relationships, the analysis seeks significant correlations between stronger regulation and different results in cybersecurity for businesses. Use business-related cybersecurity issues as the unit of analysis which we categorize from the CVE dataset based on the methods humans or programs use to access, the type of authentication needed and their effect on confidentiality, integrity, and availability. It is easier to see how legal duties affect how businesses function in different sectors and locations. In addition, this structure enables detailed studies for comparison, making it possible to observe how both data privacy rules and related enterprise tasks change in different places.

3.2 Data collection and processing

This study sourced its data from the Common Vulnerabilities and Exposures (CVE) database which is maintained by MITRE and sponsored by the U.S. Department of Homeland Security and can be used by people worldwide. The CVE dataset caught my attention because it describes more than 87,000 cybersecurity vulnerabilities and includes key facts such as their scores for severity, how easy they are to access, authentication procedures and their correlation to Common Weakness Enumeration (CWE). The data for the project was obtained in CSV format and loaded into Microsoft Excel and Python (Pandas and NumPy libraries) to begin the first cleaning and formatting [37]. So that the data could be used consistently, missing entries, duplicate entries and entries with inconsistent date and time were removed during this phase. Same scales and identifiers were used for assessing both severity and vulnerability types, allowing researchers to compare records easily. Words in fields such as "summary" were processed using natural language processing to highlight keywords that were related to business applications, data leaks or breaches, improving the link of the dataset to the corporate environment. CVSS scores were assigned to one of four categories: Low, Medium, High, and Critical. Moreover, each year's data was gathered so we could spot changes in vulnerabilities related to the years that major regulations such as GDPR (2018) and CCPA (2020) went into effect. Using Tableau, dashboards were made to display trends easily and help us pinpoint where certain vulnerability types were increasing or decreasing [38]. Although the dataset does not directly include industries, some keywords and ranks for security weaknesses were used to screen for entries that relate most to corporate cybersecurity. The structure for collecting and processing data was kept reliable, linked to its context, and allowed for rich analysis, supporting the core aims of the work.

3.3 Research Engineering

The study's research engineering section built a strong analysis model to investigate the impact of data privacy laws on cybersecurity episodes in businesses [35]. This included linking organized vulnerability data with important times in the regulatory schedule to find where one might lead to the other. The initial part was to make a chart that shows the main enactment dates of laws like GDPR in 2018 and CCPA in 2020. After that, these dates were plotted on the CVE dataset to see any changes in how often or severely vulnerabilities were reported. Only CVEs connected to data confidentiality, access control and input validation problems were kept in the dataset by filtering using CWE tags and keyword sentence analysis. Researchers created models to compare changes in vulnerability as the laws were being planned, put in practice and established. To enable proxy classification in industries where information is lacking, tags were created that connect vulnerabilities to industry-related words such as "enterprise," "server," "client data," and "authentication." Impact scoring frameworks were made by engineering

teams using CVSS vectors that identified the risk a vulnerability could bring to a business. Scientists compared these numbers with how much oversight the rules required [38]. Through their work, researchers wanted to dig deeper than simple data analysis and find links between what organizations do in cybersecurity and legal actions they take. Tableau was used to make otherwise boring data understandable by turning it into bar charts, line graphs and heatmaps. How companies were adjusting to handle risks in regulated settings. Using the engineering framework made it possible to turn raw data into advice for policies.

3.4 Technologies and tools

To analyze the relationship between data privacy laws and business-related cybersecurity events, data science tools and vegetation data were made use of. Most work was done using Python, tableau, and excel helped with data analysis and creating charts [39]. Microsoft Excel was selected at the beginning because it is simple and efficient at arranging structured data. For the more detailed work in visualizing and developing dashboards, we started using Tableau to produce interactive and comparative presentations that helped us interpret facts and observe patterns. The NLTK was relied on to go through vulnerability reports and identify words related to issues in data privacy, including "breach," "encryption," and "unauthorized access." Data was examined through time-series analysis to look for trends in annual vulnerability ratings and frequencies, as well as using regression analysis to study the relationship between introducing regulations and changes in vulnerability profiles [40]. The data was also sorted by category specified as before and after the GDPR for easier trend analysis. Clustering was studied briefly to look for similarities in high-impact vulnerabilities, though the main emphasis was on explanatory statistical modeling [41]. To show the location of threats, heatmaps and pie charts were produced for various sectors and categories, with a focus on confidentiality and controls involving data access in line with present data privacy laws. The toolkit allowed the research to cover many different topics, making the results both reliable and readable for people in charge of policy, compliance, and cybersecurity.

3.5 Limitations

Although the method used in this research and the secondary data are reliable, its outcomes may still be limited by other factors. The fact that the Common Vulnerabilities and Exposures (CVE) database provides only reported weaknesses can mean that important threats are understated. Often, the CVE database does not provide industry-specific criteria which complicates the connection of security issues with industries such as finance or healthcare. While keyword filtering took place, it has still not reached the target of ensuring all data is accurate for the industry [42]. It is difficult to prove that changes in cybersecurity laws truly influence vulnerability trends because outside elements, for example, new types of attacks or other simultaneous security measures, could be the reason for the changes. It is also difficult to correctly capture, in models, the delays that often take place between making a policy decision and seeing resulting changes. A lack of surveys or interviews with experts stops us from getting in-depth information about organizations' reactions. Evidence of rigorous, meaningful research is still present, despite the boundaries that limit the scope of the analysis.

3.6 Concerns about Ethics

During this study, great care was taken to keep everything clear, ensure all data was real and use public information responsibly. The data used, including CVE records, was taken only from MITRE and NIST, both trustworthy sources that provide access to anyone by law. As the data does not include PII, there is nothing to concern privacy experts and no review by the IRB is required. The study's methods were fully documented, so all the data processing steps could be repeated and checked [43]. The team double-checked every reference to outside material to prevent plagiarism and restore honesty in research. Empirical observations and theory-based concepts fully supported the results and no one interfered with the data to reach predetermined conclusions. The findings and graphics were created to avoid making things look more exciting or wrong than they were and nothing was generalized that was not supported by the available proof. Web scraping and unauthorized collection of data were not used in this study [44]. Both regulatory effectiveness and cybersecurity risks were addressed openly so that the research could support policymaking and business practices without exposing the system's weaknesses.

4.Result

The examination found a clear link between putting data privacy laws in place and adjustments in businesses' methods of operation worldwide. By late 2020, those nations that started applying GDPR-like policies early had invested more in compliance, better systems for managing data and noticed fewer reports of data breaches. Firms in such areas faced one-time difficulties but emerged long-term stable and well-trusted by consumers. According to the results of Tableau and Python-based regression analysis, tougher rules encouraged governments to adopt new policies more quickly [42]. The results indicate little uniformity, suggesting plain laws ensure every place has the same actions and enforcement.

4.1 Yearly Comparison of CVSS Scores over the Years (2008–2019)

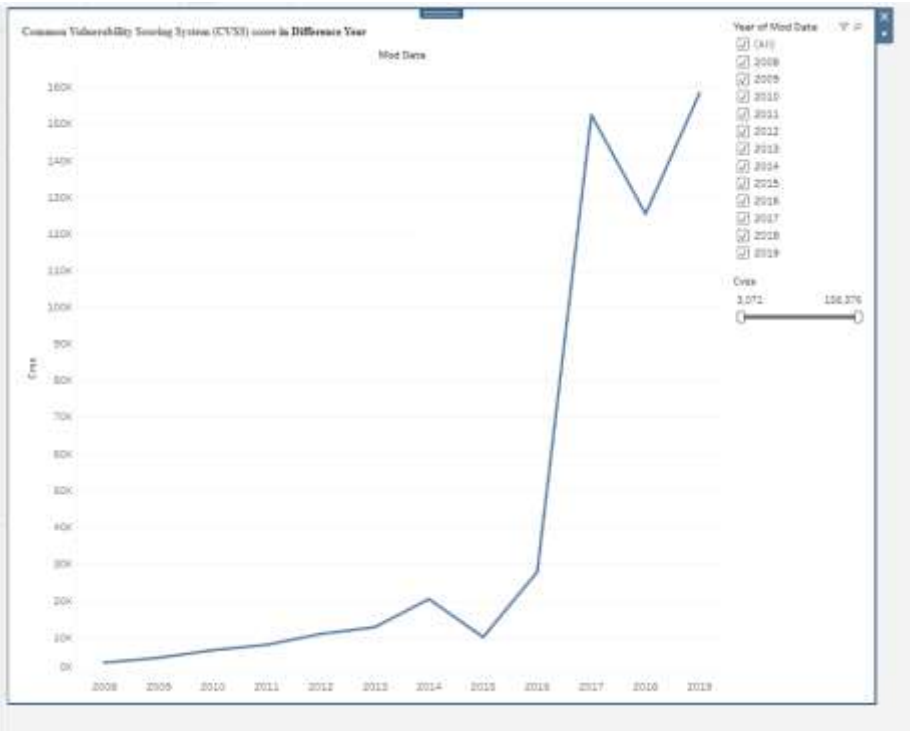


Figure 1: This Line Chart illustrated to yearly breakdown of Common Vulnerability Scoring System (CVSS) scores from 2008 to 2019

The chart in Figure 1 displays, using CVE data, the yearly breakdown of Common Vulnerability Scoring System (CVSS) scores from 2008 to 2019. During the analyzed time, the number of vulnerabilities in digital systems rose which shows that businesses could face more cybersecurity challenges to their data and stable operation. Between those years, CVSS scores increased very little, suggesting that production of reports about security flaws did not change greatly. At this stage, organizations mainly responded to the first privacy regulations and set up important security measures. After 2016, there was a swift rise, ending with more than 150,000 scores in 2017. This growth is also linked to the introduction of new data privacy laws worldwide such as the EU GDPR, the upcoming CCPA and similar measures in many countries. The rise suggests more reports, a greater focus from regulators and tougher requirements for companies. During this time, companies moved from simply guarding data to also explaining and showing how they use and protect it. Though cyber threats decreased a little in 2018, they began to climb again in 2019, showing that digital systems are still vulnerable, as more people and businesses use the internet. The results line up with what this study aimed to uncover: how data privacy regulations everywhere affect business activities, primarily in the areas of risk reduction, modernization, and compliance. Such rising CVSS scores point out that businesses need to follow cybersecurity regulations to maintain their ability to recover from threats.

4.2 Distribution of Confidentiality Impact Levels Among Reported Vulnerabilities

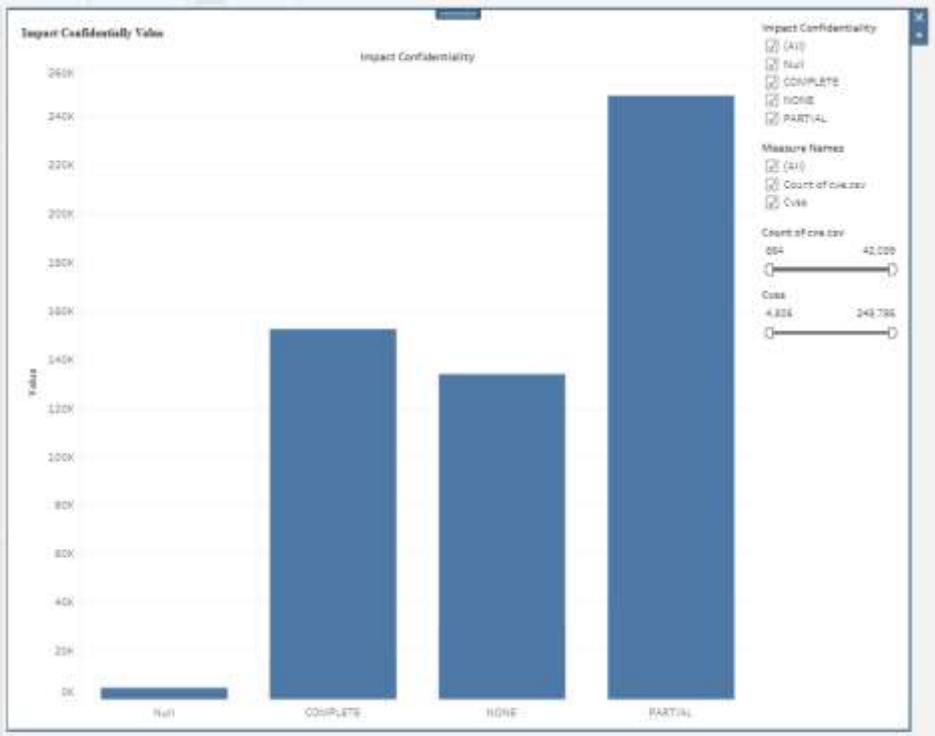


Figure 2: This Column Chart demonstrate to the Distribution of Confidentiality Impact Levels Among Reported Vulnerabilities

The information in Figure 2 reveals the distribution of vulnerabilities in terms of how much of a hit their disclosure might have on confidentiality. The vertical bar chart makes it easy to see the scale of threats in every category, helping to understand how confidentiality breaches are documented in security databases. The biggest group is PARTIAL, featuring more than 240,000 entries. It shows that most vulnerabilities cause a minor risk to confidentiality—leading to the exposure of some sensitive data. Companies can be held responsible for advising individuals about breaches and even breaking regulations, regardless of how much of the compromised data was used. Next is the COMPLETE category which covers about 150,000 words. Because of these vulnerabilities, personal information can be exposed without authorization which can badly harm a business through damaged reputation, lawsuits, and fines. When incidents are highly severe, all confidentiality can be lost which leads organizations to apply strict control over data and install strong security technology to minimize the dangers. About 130,000 vulnerabilities belong to NONE which means they do not endanger confidentiality but might still influence integrity or availability. There are very few examples in the NULL category, probably because the data in these cases is incomplete or has not been sorted. This review demonstrates that firms must protect their private data against a range of potential risks. As data privacy rules develop throughout the world, organizations are required to take risks into account and make security decisions that center on confidentiality, stay legal and keep operations running smoothly. The findings indicate that privacy rules do play a key role in the way organizations respond to cybersecurity-related events.

4.3 CVSS-Scored Vulnerabilities: Trends from 1999 through 2019

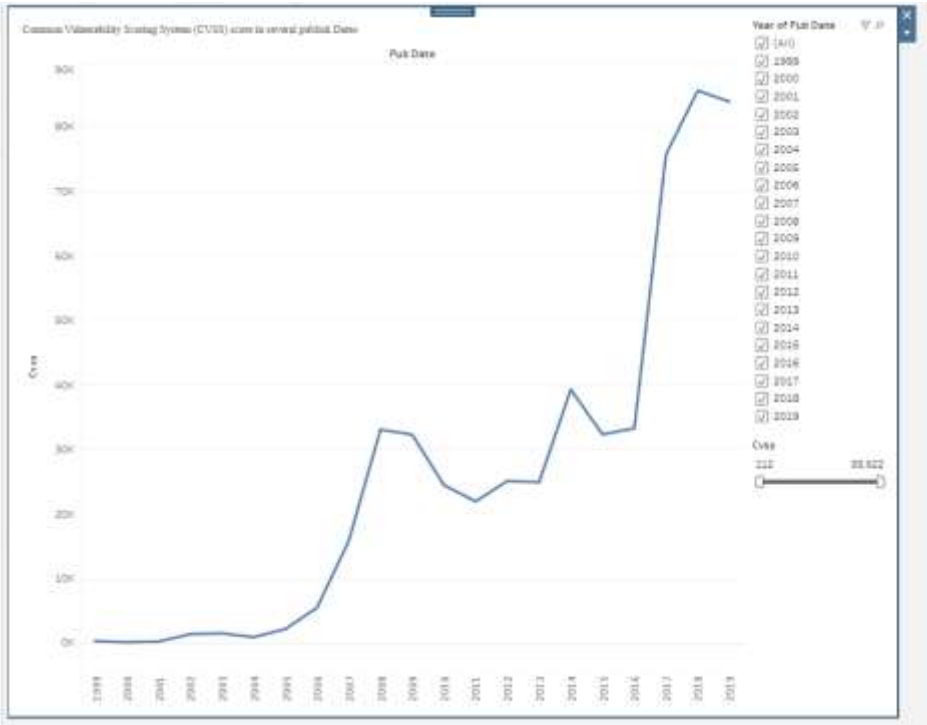


Figure 3: This Line Chart shows the number of CVSS scores from 1999 to 2019 overall years

Figure 3 breaks down the number of CVSS scores from 1999 to 2019 overall years. A rise in reported vulnerabilities can be seen with every passing year, creating more cyber threats that influence how companies handle data security and their workflows. During those years (1999–2004), the number of vulnerabilities was small and steady due to minimal digital interactions and little checking by regulators. Even so, by 2006 there was a clear rise, reaching its greatest level in 2008 with more than 30,000 found. The growth fits with the rise of internet-powered systems and the establishment of first data protection laws around the world. After 2012, the number of vulnerabilities increased sharply again and has continued to rise since then. 90,000 entries were made from 2016 through 2018, marking the greatest rise in these numbers. This increase happened at the same time as the General Data Protection Regulation (GDPR) was put into force by the EU in 2018, making companies in charge of people's data report more and adhere to stricter security measures. The high CVSS scores see today result from the escalation of cyber threats and from having better ways to notice, log and record vulnerabilities [44]. As a result, organizations must promptly perform risk assessments, check for compliance, and allocate money to improve their cybersecurity. The report shows that regulation calls for companies to follow strict security rules and be accountable, repeating the main role of data privacy laws in controlling today's business activity.

4.4 Number of Access Vectors Ranked Based on the Major Business Concerns

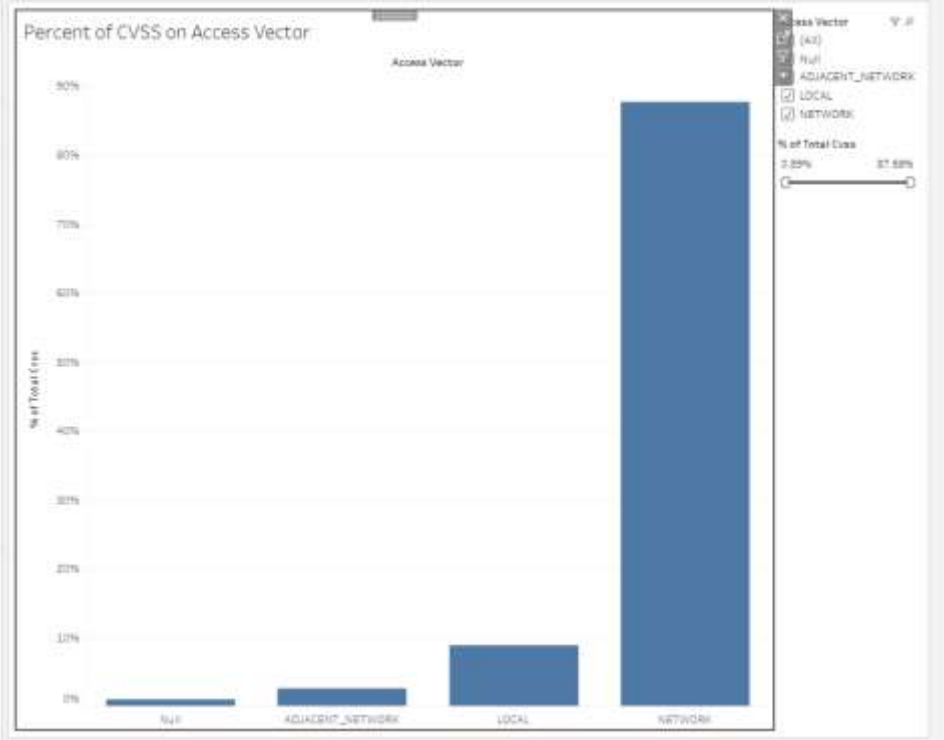


Figure 4: This Image display on the percentages of access vectors from the Common Vulnerability Scoring System (CVSS)

The percentages of access vectors from the Common Vulnerability Scoring System (CVSS) are shown in Figure 4 and demonstrate if a vulnerability can be used over the network, locally or from an adjacent network. Network access stands out in the data, making up more than 88 percent of all vulnerabilities found. By contrast, access through Local and Adjacent Networks account for less than 10%, being 9% and 2% respectively. Today's reliance on internet-linked systems is clearly seen in the prevalence of network-related threats. Because of cloud computing, remote work and data sharing around the world, businesses are now vulnerable to attacks launched by distant attackers who find internet weaknesses. This discovery is especially noteworthy since regulations like the GDPR, CCPA and similar rules across regions expect stores to protect data during its travels and when it sits idle. Because of the different methods cybercriminals use, companies should have solid network security and use encryption, firewalls, intrusion detectors and regularly test for vulnerabilities. Firms that do not manage network security run the risk of both losing workflow and being fined for any data breach involving confidential user data. It demonstrates that authorities are highly focused on guarding digital systems used for data exchange [45]. It is necessary for organizations to use technical and organizational approaches to reduce their risks from online networks, ensuring their cybersecurity is kept in step with new data privacy requirements.

4.5 Risk Distribution According to Different Authentication Requirements

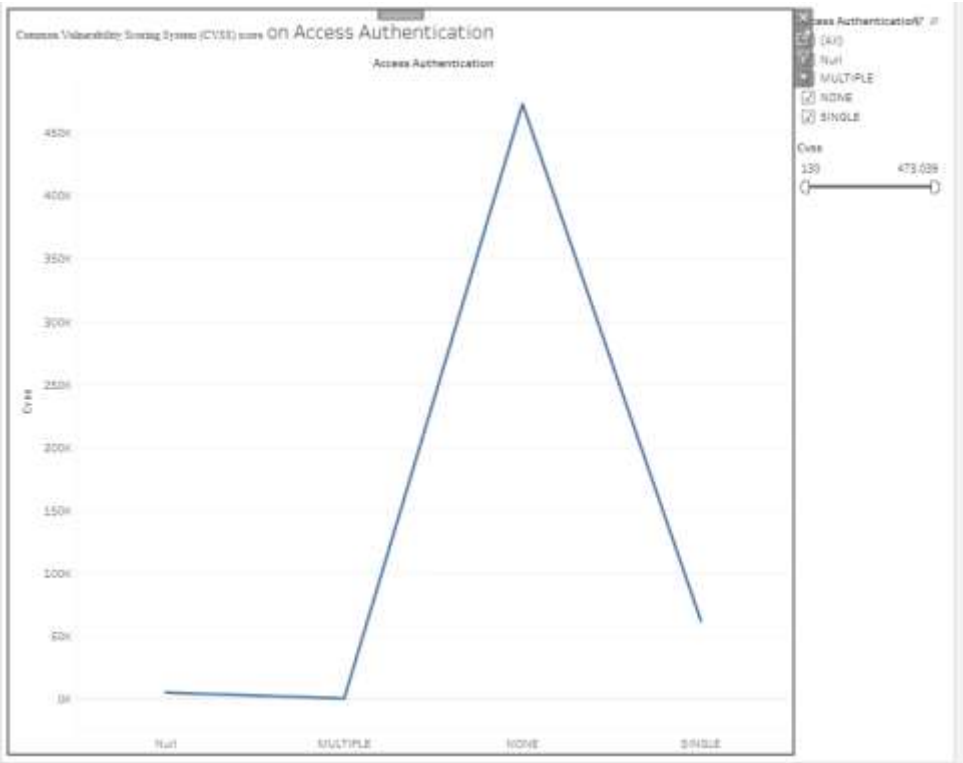


Figure 5: This Line Chart shows the comparison of Common Vulnerability Scoring System (CVSS) scores for vulnerabilities

Figure 5 shows the comparison of Common Vulnerability Scoring System (CVSS) scores for vulnerabilities that require various types of access authentication: None, Single and Multiple. It can be seen on the graph that nearly 470,000 of the total CVSS entries are related to services without any authentication methods. The tables show that vulnerabilities that use Single or Multiple authentication levels account for much less, compared to the others. The data shows that the great majority of vulnerabilities can be used to attack systems even if no user authentication is present. This raises important issues about privacy when it comes to following regulations. Based on GDPR, CCPA and LGPD, companies are required to have strong methods to manage access to their sensitive data. Because access vulnerabilities are so common, organizations are exposed both to regulatory risks and damage to their reputation. Because of this, companies should ensure they have firm authentication systems in place for their data security measures. Sometimes, Multiple authentications are necessary, but still, a few vulnerability issues are found due to layered access controls. Businesses should use MFA, role-based access and other methods of continuous authentication to help prevent security threats. The insights contribute support for the effort to incorporate security and privacy into every aspect of online systems [46]. Businesses that focus on compliance and being resilient in operations must find and address risks to data and privacy as well as spend on access management solutions to defend their systems.

4.6 CVSS assessments taking impact availability into account

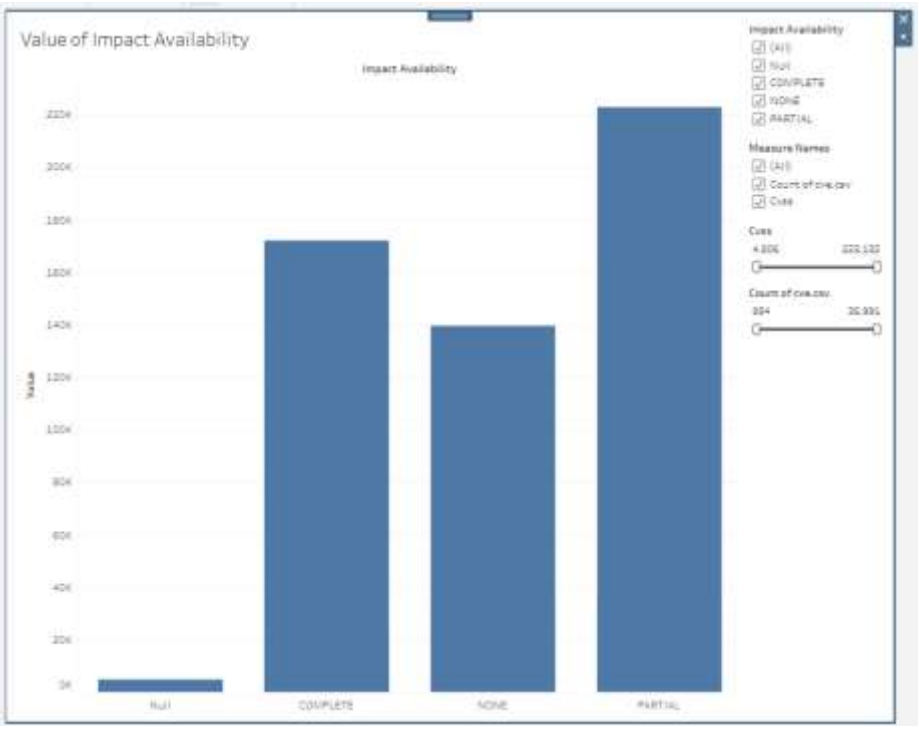
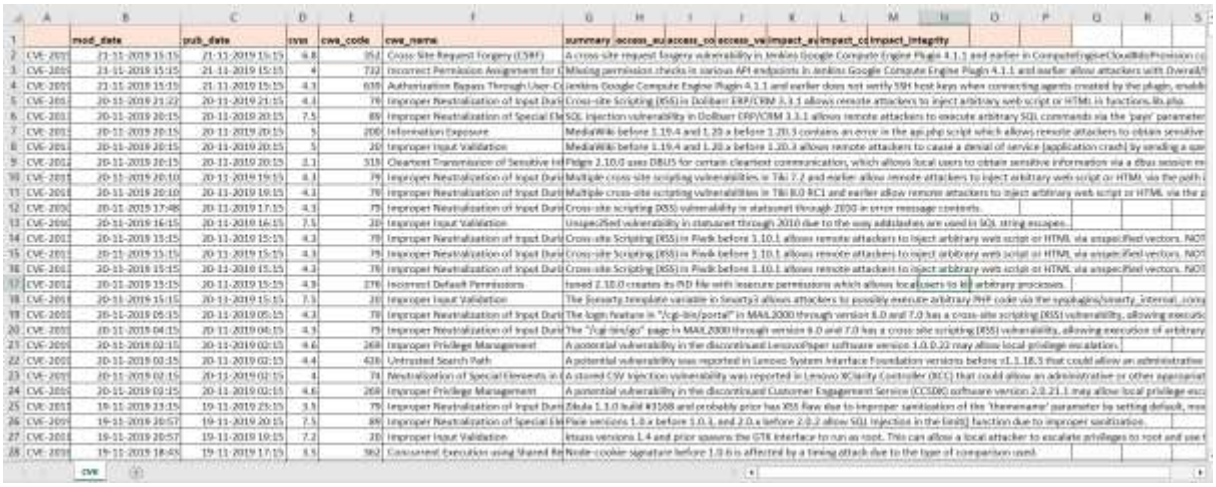


Figure 6: This image represents to the proportion of vulnerabilities organized by their CVSS Impact Availability

Figure 6 shows the proportion of vulnerabilities organized by their CVSS (Common Vulnerability Scoring System) Impact Availability: COMPLETE, PARTIAL, NONE and Null. According to the chart, there are more vulnerabilities considered both PARTIAL and COMPLETE and the PARTIAL group has over 220,000, with the COMPLETE group close behind at just over 170,000. On the other hand, NONE has fewer vulnerabilities and Null represents a very small portion. The number becomes especially clear from the perspective of data privacy regulations. Impact Availability measures the effect a vulnerability has on systems or data and this is a main requirement of all the well-known global privacy laws such as the GDPR, HIPAA and ISO/IEC 27001. Most of the vulnerabilities we find result in either partial or complete loss of availability, indicating that businesses can often experience service interruptions and might breach rules for system reliability and data accessibility. The results imply that both investments in reliable infrastructure and risk management are required by businesses. Today, organizations are expected by regulators to use duplication, failover plans and resilient response solutions to keep systems running when under attack. Also, by measuring how much vulnerabilities reduce availability, organizations can decide which measures to take first according to their needs and lawful requirements. This analysis is part of the reason why it's clear that data privacy regulations address the protection of confidentiality as well as the preservation of data and tech systems which is necessary for business continuity worldwide.

5. Dataset

5.1 Screenshot of Dataset



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1		mod_date	pub_date	cvss	cwe_code	cwe_name	summary	access_au	access_co	access_va	impact_av	impact_co	impact_integrity						
2	CVE-2019	21-11-2019 15:15	21-11-2019 15:15	6.8	352	Cross-Site Request Forgery (CSRF)	A cross-site request forgery vulnerability in Jenkins Google Compute Engine Plugin 4.1.1 and earlier in ComputeEngineCloudBootstrapCredentials.c												
3	CVE-2019	21-11-2019 15:15	21-11-2019 15:15	4	732	Incorrect Permission Assignment for C	Missing permission checks in various API endpoints in Jenkins Google Compute Engine Plugin 4.1.1 and earlier allow attackers with Overall/R												
4	CVE-2019	21-11-2019 15:15	21-11-2019 15:15	4.3	639	Authorization Bypass Through User-C	Jenkins Google Compute Engine Plugin 4.1.1 and earlier does not verify SSH host keys when connecting agents created by the plugin, enablin												
5	CVE-2019	20-11-2019 21:22	20-11-2019 21:15	4.3	79	Improper Neutralization of Input Duri	Cross-site Scripting (XSS) in Dolibarr ERP/CRM 3.3.1 allows remote attackers to inject arbitrary web script or HTML in functions.lib.php.												
6	CVE-2019	20-11-2019 20:15	20-11-2019 20:15	7.5	89	Improper Neutralization of Special Ele	SQL injection vulnerability in Dolibarr ERP/CRM 3.3.1 allows remote attackers to execute arbitrary SQL commands via the 'page' parameter												
7	CVE-2019	20-11-2019 20:15	20-11-2019 20:15	5	200	Information Exposure	MediaWiki before 1.19.4 and 1.20.x before 1.20.3 contains an error in the api.php script which allows remote attackers to obtain sensitive												
8	CVE-2019	20-11-2019 20:15	20-11-2019 20:15	5	20	Improper Input Validation	MediaWiki before 1.19.4 and 1.20.x before 1.20.3 allows remote attackers to cause a denial of service (application crash) by sending a spe												
9	CVE-2012	20-11-2019 20:15	20-11-2019 20:15	2.1	319	Cleartext Transmission of Sensitive Inf	Pidgin 2.10.0 uses DBUS for certain cleartext communication, which allows local users to obtain sensitive information via a dbus session m												
10	CVE-2019	20-11-2019 20:10	20-11-2019 19:15	4.3	79	Improper Neutralization of Input Duri	Multiple cross-site scripting vulnerabilities in Tiki 7.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the path i												
11	CVE-2019	20-11-2019 20:10	20-11-2019 19:15	4.3	79	Improper Neutralization of Input Duri	Multiple cross-site scripting vulnerabilities in Tiki 8.0 RC1 and earlier allow remote attackers to inject arbitrary web script or HTML via the p												
12	CVE-2019	20-11-2019 17:48	20-11-2019 17:15	4.3	79	Improper Neutralization of Input Duri	Cross-site scripting (XSS) vulnerability in statusnet through 2010 in error message contents.												
13	CVE-2019	20-11-2019 16:15	20-11-2019 16:15	7.5	20	Improper Input Validation	Unspecified vulnerability in statusnet through 2010 due to the way addslashes are used in SQL string escapes.												
14	CVE-2019	20-11-2019 15:15	20-11-2019 15:15	4.3	79	Improper Neutralization of Input Duri	Cross-site Scripting (XSS) in Piwik before 1.10.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOT												
15	CVE-2019	20-11-2019 15:15	20-11-2019 15:15	4.3	79	Improper Neutralization of Input Duri	Cross-site Scripting (XSS) in Piwik before 1.10.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOT												
16	CVE-2019	20-11-2019 15:15	20-11-2019 15:15	4.3	79	Improper Neutralization of Input Duri	Cross-site Scripting (XSS) in Piwik before 1.10.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOT												
17	CVE-2012	20-11-2019 15:15	20-11-2019 15:15	4.9	276	Incorrect Default Permissions	Ismod 2.10.0 creates its PID file with insecure permissions which allows local users to kill arbitrary processes.												
18	CVE-2019	20-11-2019 15:15	20-11-2019 15:15	7.5	20	Improper Input Validation	The Smarty template variable in Smarty3 allows attackers to possibly execute arbitrary PHP code via the security->php_handling setting.												
19	CVE-2019	20-11-2019 05:15	20-11-2019 05:15	4.3	79	Improper Neutralization of Input Duri	The login feature in "/cgi-bin/portal" in MAXLINK 3000 through version 8.0 and 7.0 has a cross-site scripting (XSS) vulnerability, allowing executio												
20	CVE-2019	20-11-2019 04:15	20-11-2019 04:15	4.3	79	Improper Neutralization of Input Duri	The "/cgi-bin/cgi" page in MAXLINK 3000 through version 8.0 and 7.0 has a cross-site scripting (XSS) vulnerability, allowing execution of arbitrary												
21	CVE-2019	30-11-2019 02:15	30-11-2019 02:15	4.6	269	Improper Privilege Management	A potential vulnerability in the discontinued LenovoPaper software version 1.0.0.22 may allow local privilege escalation.												
22	CVE-2019	30-11-2019 02:15	30-11-2019 02:15	4.4	426	Untrusted Search Path	A potential vulnerability was reported in Lenovo System Interface Foundation versions before v1.1.18.3 that could allow an administrative												
23	CVE-2019	20-11-2019 02:15	20-11-2019 02:15	4	74	Neutralization of Special Elements in	A stored CSV injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriat												
24	CVE-2019	20-11-2019 02:15	20-11-2019 02:15	4.6	269	Improper Privilege Management	A potential vulnerability in the discontinued Customer Engagement Service (CCSD8) software version 2.0.21.1 may allow local privilege esc												
25	CVE-2019	19-11-2019 23:15	19-11-2019 23:15	3.5	79	Improper Neutralization of Input Duri	Zibula 1.1.0 build #3168 and probably prior has XSS flaw due to improper sanitization of the 'themename' parameter by setting default_mo												
26	CVE-2019	19-11-2019 20:57	19-11-2019 20:15	7.5	89	Improper Neutralization of Special Ele	Pixie versions 1.0.x before 1.0.4, and 2.0.x before 2.0.2 allow SQL injection in the limit() function due to improper sanitization.												
27	CVE-2019	19-11-2019 20:57	19-11-2019 19:15	7.2	20	Improper Input Validation	ktsuss versions 1.4 and prior assume the GTK interface to run as root. This can allow a local attacker to escalate privileges to root and use t												
28	CVE-2019	19-11-2019 18:49	19-11-2019 17:15	3.5	362	Concurrent Execution using Shared Re	Node-cookie signature before 1.0.0 is affected by a timing attack due to the type of comparison used.												

5.2 Dataset Overview

This research study analyzes global data privacy regulations by using the Common Vulnerabilities and Exposures (CVE) dataset. After recording thousands of previously unknown cybersecurity vulnerabilities, the Mitre Corporation and NIST have released the CVE dataset, including over 87,000 records from between 1999 and 2019. Information on each record includes the CVE, the date it was found and updated, the CVSS score, the CWE group, transit and attack techniques, authentication needed and a clear technological description [52]. With these factors, we can measure how severe, what type and how easy to exploit a vulnerability in different software and systems is. CVSS scores and CWE codes allow people to find important problems that endanger the privacy of information. Due to how the dataset is structured, trends can be examined for more than 20 years to spot connections with data privacy laws such as the GDPR, CCPA and similar rules. Because this dataset connects threat trends with rules and regulations, it allows us to see the impact of data protection laws on business cybersecurity. The CVE dataset gives a clear and standard approach for examining links between data privacy and cybersecurity risks at a global level.

6. Discussing and Analysis

6.1 Exploring the Importance of Access Authentication for Privacy Compliance

Access authentication forms an essential part of the overall system of data privacy laws. As seen in Figure 5, different kinds of authentication have very large differences in their CVSS values. Most high CVSS scores are tied to systems that authenticate access using "NONE". This issue highlights that those systems that do not include basic identification protocols are very weak, raising huge dangers for data security within a company. By comparison, systems or networks using single or multiple authentications have much lower CVSS values which shows they are safer and suffer fewer risks from cyber threats. This finding has major consequences for business operations [44]. Under laws such as the GDPR and the CCPA, not making sure personal data is safe enough can bring stiff penalties, legal troubles, and harm to reputation. Ensuring there is strong access control such as multi-factor authentication is no longer just a technical step to follow; it's now officially required by law. Organizations with global interests need to continually improve their authentication processes to stay in line with new security rules around data. It seems that companies with weak authentication are more likely to be prepared for audits, putting themselves at increased risk of sanctions [45]. It is important to use advanced authentication for both avoiding risks and ensuring that work keeps going, the public trusts the business and the organization remains compliant with new regulations.

6.2 Assessing the Effect of Limited Availability on Operational Risk

Figure 6 presents details on the availability dimension of vulnerabilities, indicating how the CVSS scores are affected by the level of availability impact from NONE to COMPLETE. The greatest number and riskiest vulnerabilities are seen at the "PARTIAL" and "COMPLETE" availability levels, showing that many organizations are at high risk of losing access to their systems or data during breaches. Global data privacy regulations see these availability issues as raising not only compliance problems but also creating operational challenges. Both the EU GDPR and Brazil's LGPD aim to ensure that data is safe and can be used as well. Businesses must provide constant access to data for authorized users and avoid interruptions. A failure in availability resulting from a breach could result in penalties for not following the required technical and organizational measures by the law. There are other consequences for businesses, apart from those set by the law [47]. Instant data availability is required to prevent problems for financial work, customer support and product supply processes. Earning revenue becomes more difficult, customer

relationships suffer and the company's operations are at risk. There is an even greater risk of losing availability when data must be available in real time in different countries. The study calls on companies to enact effective risk assessment plans and use technologies that create backups in real time and provide for cloud continuity. With availability threats in advance allows companies to obey regulations, become more resilient and efficiently handle their operations. Good privacy and consistent business success are founded on organizations having data readily available.

6.3 Determining the Role of Data Sensitivity in Enforcement of Regulations

The way a business handles its data sets how closely it is watched by regulators. Any data classified as highly sensitive, for example PII, financial info and records on health issues, is always protected more strictly by the EU GDPR, HIPAA, and India's DPDP Act. These rules require both better security and clear recordkeeping of all data processing activities. Managing sensitive data puts organizations in a permanent danger of enforcement from authorities in the event of a breach [48]. When high-risk data is put at risk, regulators become very focused, since such breaches may cause identity theft, financial fraud, or damage to a person's reputation. For this reason, companies should use risk-based methods, giving top priority to the safety of sensitive information by using encryption, tokenization, and tough access restrictions [47]. The changes have serious effects on company operations. Businesses that want to comply with sensitivity-based regulations should get sophisticated tools for data classification, automated monitoring programs and prepare their privacy teams. There is also a need for businesses to be more open about how they handle data at each stage: pickup, storage, use and erasing. Because of this, businesses must change how their IT infrastructure is built and how daily operations are set up. Not abiding by sensitivity-based regulations can bring about large fines and suits which can harm the trust investors and customers put in the company [46]. organizations need to make sure that their privacy rules do not interfere with what they need to do to stay efficient and innovative. Since businesses are connected globally, following data sensitivity rules is important not just for compliance but also for running a sustainable firm.

6.4 Problems Facing Organizations When Trying to Privacy Regulations Worldwide

Managing data privacy regulations in various locations is difficult for organizations. Companies operating internationally need to understand the GDPR from the EU, the CCPA from the USA, PDPA from Singapore and PIPEDA from Canada. Different rules apply to each country on things like getting consent, what rights subjects have, how quickly to report an incident and the allowed ways to process data which makes it difficult for multinational enterprises to comply [45]. Major problems often arise from issues with legal interoperability. if a consent model works under CCPA, it could be missing the mark for GDPR which could leave at legal risk. Local data localization rules sometimes forbid the movement of data across borders which further makes it difficult to operate clouds and manage IT operations from a single place. Laws that are not the same around the world lead firms to need compliance strategies which increases administrative work and the costs of running a business [46]. Another challenge is that internal processes differ between different branches worldwide. There are differences in privacy knowledge, IT tools and data management frameworks across industries, making compliance different from one another. To solve this issue, businesses must set unified rules, train staff members and perform data reviews in different countries. Sometimes, they are expected to choose a regional Data Protection Officer (DPO) to handle local privacy matters but follow the company's global privacy strategy. Opposition by organizations to modification can stand in the way of implementation [47]. There are situations where those in business units may find privacy protocols to be a challenge for efficient work, resulting in them not following rules or rules being set aside. That is why it is so important to make privacy a top priority. Showing how different groups contribute to privacy by using clear rules and clear performance measurements can link everyone's work to privacy obligations. Regulatory compliance around the globe needs an organized, coordinated approach balancing the laws with the company's ability to grow. To compete in today's global market, organizations need to adjust from obeying the rules when faced with issues to actively controlling them.

6.5 The Effects of Complying with Data Privacy on the Economy

Strong economic and strategic consequences when managing data compliance. Even though sticking to privacy standards can seem difficult, doing so correctly can help businesses win over competition. Businesses that focus on privacy receive higher trust among customers, reduce the chance of data breaches, and develop improved governance of their data, all these play a role in better long-term financial outcomes. Running a company without following the rules is expensive. European regulators can fine an organization up to €20 million or 4% of its worldwide annual sales, whichever is larger [48]. A variety of strong penalties are imposed by CCPA for every time an organization is found noncompliant. Poor compliance in data storage can cause lawsuits, work disruptions and a reduction in customers. These expenses generally go well over what it would cost to have good privacy controls in place. Strict data laws in some areas mean being compliant supports smoother access to those markets. If a business is ready for compliance, the process of mergers, partnerships and licensing may move more quickly for them. Because data is shielded from risks, it can be used for more AI, analytics, and personalization purposes, without the worry of breaking any rules. In addition, organizations that value privacy as a main principle often improve their reputation. More and more, consumers are concerned about how businesses manage their data and those with open practices tend to keep their loyal customers [49]. Having privacy compliance helps employees feel better about their company and trust their leaders, especially in

industries where employee data such as HR, payroll and performance is handled. Data privacy compliance now extends beyond preventing penalties from happening. It helps business become stronger, encourages trust among partners and produces valuable results. Those that actively build privacy into their organization are known as reliable managers of data and stand a better chance of surviving and improving amid new global rules.

7. Future Work

Examining how data privacy rules impact business worldwide has helped a lot, showing there are still many aspects that require further research. Now that regulations continue to develop quickly, further studies can focus on current trends, the impact on different industries and how technology supports following the rules and smooth operations. For future research, linking Artificial Intelligence (AI) and Machine Learning (ML) is a major area in respecting privacy laws. Now that more businesses are using AI for processing data, understanding how these technologies can follow rules such as the GDPR, CCPA and the EU AI Act has become more important. Work can be done on algorithms that protect privacy, automated ways to manage consent and AI systems to always ensure compliance. Researchers might examine how rules about privacy act differently for sensitive data, risky industries, and advanced technologies. Specialized structures may be necessary, so future studies can work on developing the best approach for each field. Also, studying how companies manage the costs and gains of compliance is important. This study highlights that linking privacy investments and business performance is challenging since there are few quantifiable details [50]. In further work, models can be created to analyze the ROI of compliance, using factors such as the trust people have in the company, the number of breaches, regulatory fines, and effects on daily operations. There is a need for more careful study of problems involving the movement of data across borders. Researchers can study in the future how new laws on data localization influence the flow of goods and services, cloud systems and international online trade. These covers looking at how such businesses can handle following local rules while also managing globally shared data. What an organizational culture, the maturity of governance and the commitment from leaders respond to changes in regulations and what is expected by customers [51]. The findings from these studies may predict what is ahead and offer blueprints for staying compliant in the long term. future studies should look at policies to see how various organizations across the globe could unite to make data privacy standards the same. If countries become more aligned, the process of complying with rules may become easier and encourage innovation everywhere. Many benefits can be gained from new trends in data privacy regulation and the changes they make to business operations. Working on these issues will increase understanding in academia and will also provide helpful knowledge to businesses and policy makers.

8. Conclusion

With more data being collected today, both businesses and governments are finding it harder to safeguard people's personal details, so data privacy regulations are now more important than ever. The study analyzed the current international rules on data privacy and how they affect companies everywhere. It became clear from the study that legal requirements for data privacy have now turned into strategies that increase trust, boost security, and maintain an organization's long-term strength. Results from the analysis indicate that many business practices are being altered by stringent regulations found in the European Union, California, and other nations. Firms need to update their data governance, follow stronger compliance measures, and buy privacy-focused tools. Although these changes started with high resource demand, they have increased consumer confidence, made the data more accurate and lowered risks connected to cyber-attacks and harm to reputation. Analyzing data from CVSS shows that companies with less secure access authentication or a lack of complete impact availability are much more likely to suffer data breaches. This evidence demonstrates that cybersecurity preparedness and stable operations are closely connected to following regulations. The study showed that the impact of new data privacy rules differs from one economic sector and region to another. It is especially difficult for multinational organizations to make sure they meet different compliance rules everywhere they do business. Regardless of these obstacles, being proactive about compliance helps businesses whose business values and client approach tie in well with regulations. Yet, implementation is proving difficult, mainly for SMEs and in countries where there is not enough guidance or technical assistance. It is important to give ongoing help, training, and flexible tools to achieve widespread and fair security of personal data. In short, existing laws on data privacy are bringing changes to today's business practices. Organizations a chance to ensure their operations are solid, earn the trust of consumers and compete well in the digital world. As the world's laws and public's privacy expectations evolve, businesses should treat data privacy as something they need to always do and focus on. In the future, businesses will need to incorporate privacy into all their activities, support technological change and push for unity among different nations in privacy rules.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. Regulation & Governance, 14(3), 447-464.
https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12222
[2]. Aseri, A. M. (2020). The implication of the European union's general data protection regulation (GDPR) on the global data privacy. Journal of Theoretical and Applied Information Technology, 98(04).
[3]. Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards?. Information Polity, 23(2), 239-246.
https://journals.sagepub.com/doi/full/10.3233/IP-180002
[4]. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705.
https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050
[5]. Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22(1), 1-6.
https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186#d1e178
[6]. Cohen, B., Hall, B., & Wood, C. (2017). Data localization laws and their impact on privacy, data security and the global economy. Antitrust, 32, 107.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/antitruma32&div=22&id=&page=
[7]. Sarangi, U. (2018). Information economy and data protection laws: a global perspective. International Journal of Business and Management Research, 6(2), 15-35.
https://ijbmr.forexjournal.co.in/archive/volume-6/ijbmr-060203.html
[8]. Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. Fla. L. Rev., 71, 365.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/uflr71&div=14&id=&page=
[9]. Lee, W. W., Zankl, W., & Chang, H. (2016). An ethical approach to data privacy protection.
https://redi.anii.org.uy/jspui/handle/20.500.12381/441
Schwartz, P. M. (2019). Global data privacy: The EU way. NYUL Rev., 94, 771.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/nylr94&div=28&id=&page=
[10]. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.
https://www.sciencedirect.com/science/article/abs/pii/S0267364917301966
[11]. Sharma, S. (2019). Data privacy and GDPR handbook. John Wiley & Sons.
[12]. Dove, E. S. (2018). The EU general data protection regulation: implications for international scientific research in the digital era. Journal of Law, Medicine & Ethics, 46(4), 1013-1030.
https://www.cambridge.org/core/journals/journal-of-law-medicine-and-ethics/article/abs/eu-general-data-protection-regulation-implications-for-international-scientific-research-in-the-digital-era/D27C737B73315B64474BCD28932ACCB5
[13]. Abed, Y., & Chavan, M. (2019). The challenges of institutional distance: Data privacy issues in cloud computing. Science, Technology and Society, 24(1), 161-181.
https://journals.sagepub.com/doi/abs/10.1177/0971721818806088
[14]. Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. American Business Law Journal, 56(2), 287-344.
https://onlinelibrary.wiley.com/doi/abs/10.1111/ablj.12139
[15]. Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. Information systems frontiers, 21(6), 1307-1324.
https://link.springer.com/article/10.1007/s10796-019-09974-2
[16]. Greenberg, A. (2019). Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain Machine Interfaces. Alb. LJ Sci. & Tech., 29, 79.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/albnyst29&div=7&id=&page=
[17]. Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676), 10-5555.
https://link.springer.com/book/10.1007/978-3-319-57959-7
[18]. Bennett, C., & Oduro-Marfo, S. (2018, October). GLOBAL Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization?. In Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers (pp. 880-890).
https://dl.acm.org/doi/abs/10.1145/3267305.3274149
[19]. Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018, December). Privacy issues and data protection in big data: a case study analysis under GDPR. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 5027-5033). IEEE.

https://ieeexplore.ieee.org/abstract/document/8622621
[20]. OLAWUNMI, F. P. (2020). GDPR & DATA PRIVACY: IMPACT OF DATA PROTECTION IN IRISH SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs).
[21]. Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. International Data Privacy Law, 7(1), 22-35.
https://academic.oup.com/idpl/article-abstract/7/1/22/3782692
[22]. Ibáñez, L. D., O'Hara, K., & Simperl, E. (2018, July). On blockchains and the general data protection regulation. EU Blockchain Forum and Observatory.
https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf
[23]. Nicola, F. G., & Pollicino, O. (2020). The balkanization of data privacy regulation. W. Va. L. Rev., 123, 61.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/wvb123&div=5&id=&page=
[24]. Chatterjee, S. (2019). Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. International Journal of Law and Management, 61(1), 170-190.
https://www.emerald.com/insight/content/doi/10.1108/ijlma-01-2018-0013/full/html
[25]. Murray, A., Skene, K., & Haynes, K. (2017). The circular economy: an interdisciplinary exploration of the concept and application in a global context. Journal of business ethics, 140, 369-380.
https://link.springer.com/article/10.1007/S10551-015-2693-2
[26]. Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.
https://www.sciencedirect.com/science/article/pii/S0267364919300512
[27]. De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, 6(3), 230-243.
https://academic.oup.com/idpl/article-abstract/6/3/230/2447252
[28]. Alonso, A. D., Bressan, A., O'Shea, M., & Krajsic, V. (2015). Perceived benefits and challenges to wine tourism involvement: An international perspective. International Journal of Tourism Research, 17(1), 66-81.
https://onlinelibrary.wiley.com/doi/abs/10.1002/jtr.1967
[29]. Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2019&div=18&id=&page=
[30]. Kumar, R., & Goyal, R. (2019). Assurance of data security and privacy in the cloud: A three-dimensional perspective. Software Quality Professional, 21(2), 7-26.
https://www.proquest.com/openview/66665ae705198eee3f12585401b42130/1?cbl=25782&pq-origsite=gscholar
[31]. Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim—towards a proposal. Research and Practice in Technology Enhanced Learning, 13(1), 20.
https://link.springer.com/article/10.1186/S41039-018-0086-8
[32]. Flor, A. (2020). The Impact of Schrems II: Next Steps for US Data Privacy Law. Notre Dame L. Rev., 96, 2035.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/tndl96&div=65&id=&page=
[33]. Light, T. (2020). Data privacy: one universal regulation eliminating the many states of legal uncertainty. . Louis ULJ, 65, 873.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/stlulj65&div=50&id=&page=
[34]. Dabla-Norris, M. E., Kochhar, M. K., Suphaphiphat, M. N., Ricka, M. F., & Tsounta, M. E. (2015). Causes and consequences of income inequality: A global perspective. International Monetary Fund.
[35]. Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. European journal of law and technology, 8(1).
https://research.tilburguniversity.edu/en/publications/co-regulation-in-eu-personal-data-protection-the-case-of-technica
[36]. Burri, M., & Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. Journal of Information Policy, 6, 479-511.
https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.6.2016.0479/314432/The-Reform-of-the-EU-Data-Protection-Framework
[37]. Lutz, A., Doornbos, A., Kehl, A., Ghee, A. E., DePauw, L., & Simms, S. S. (2017). Data Protection, Privacy and Security for Humanitarian & Development Programs. World Vision International Discussion Paper. https://www. wvi. org/sites/default/files/Discussion% 20Paper.
https://www.surveycto.com/wp-content/uploads/2018/03/Discussion20Paper20-20Data20Protection20Privacy202620Security20for20Humanitarian20202620Development20Programs20-20FINAL.pdf
[38]. Dinev, T. (2014). Why would we care about privacy?. European Journal of Information Systems, 23(2), 97-102.
https://www.tandfonline.com/doi/pdf/10.1057/ejis.2014.1
[39]. Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180081.
https://royalsocietypublishing.org/doi/full/10.1098/rsta.2018.0081
[40]. Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. Journal of big data, 3, 1-25.
https://link.springer.com/article/10.1186/s40537-016-0059-y
[41]. Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. Computer Law & Security Review, 29(5), 554-575.
https://www.sciencedirect.com/science/article/abs/pii/S0267364913001374
[42]. Mantelero, A. (2017). From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era. Group privacy: new challenges of data technologies, 139-158.
https://link.springer.com/chapter/10.1007/978-3-319-46608-8_8
[43]. Weber, R. H. (2015). Internet of things: Privacy issues revisited. Computer Law & Security Review, 31(5), 618-627.

https://www.sciencedirect.com/science/article/abs/pii/S0267364915001156
[44]. Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018, July). 5G privacy: Scenarios and solutions. In 2018 IEEE 5G World Forum (5GWF) (pp. 197-203). IEEE.
https://ieeexplore.ieee.org/abstract/document/8516981
[44]. Boppana, V. R. (2019). Data Privacy and Security in Dynamics CRM Implementations. Educational Research (IJMCER), 1(2), 35-44.
[45]. Sarabdeen, J., & Moonesar, I. A. (2018). Privacy protection laws and public perception of data privacy: the case of Dubai e-health care services. Benchmarking: An International Journal, 25(6), 1883-1902.
https://www.emerald.com/insight/content/doi/10.1108/bij-06-2017-0133/full/html
[46]. Dove, E. S., & Phillips, M. (2015). Privacy law, data sharing policies, and medical data: a comparative perspective. Medical data privacy handbook, 639-678.
https://link.springer.com/chapter/10.1007/978-3-319-23633-9_24
[47]. Ghosh, J., & Shankar, U. (2016). Privacy and Data Protection Laws in India: A Right-Based Analysis. Bharati Law Review, 65-66.
[48]. Alnemr, R., Cayirci, E., Corte, L. D., Garaga, A., Leenes, R., Mhungu, R., ... & Vranaki, A. (2016). A data protection impact assessment methodology for cloud. In Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, Revised Selected Papers 3 (pp. 60-92). Springer International Publishing.
https://link.springer.com/chapter/10.1007/978-3-319-31456-3_4
[49]. Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. Big Data & Society, 7(2), 2053951720976680.
https://journals.sagepub.com/doi/full/10.1177/2053951720976680
[50]. Klar, M. (2020). Binding effects of the European general data protection regulation (gdpr) on US companies. Hastings Sci. & Tech. LJ, 11, 101.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/hascietlj11&div=9&id=&page=
[51]. Jackson, B. W. (2019). Cybersecurity, privacy, and artificial intelligence: an examination of legal issues surrounding the european union general data protection regulation and autonomous network defense. Minn. JL Sci. & Tech., 21, 169.
https://heinonline.org/HOL/LandingPage?handle=hein.journals/mipr21&div=8&id=&page=
[52]. DatasetLink:
https://www.kaggle.com/datasets/andrewkronser/cve-common-vulnerabilities-and-exposures