sciendo

Understanding Public Perception of Internet Security in the European Union

Vanesa Madalina VARGAS
Bucharest University of Economic Studies, Bucharest, Romania
Institute for Economic Forecasting, Romanian Academy
[*]Corresponding author, vanesa.vargas@fabiz.ase.ro

Marian OANCEA
Bucharest University of Economic Studies, Bucharest, Romania

Cosmin Alexandru TEODORESCU
Bucharest University of Economic Studies, Bucharest, Romania

Bogdan Paul SAFTIUC
Bucharest University of Economic Studies, Bucharest, Romania

Abstract. *This paper presents an extensive analysis of Internet security experiences and perceptions among European Union (EU) citizens, as detailed by data within commented graphics highlighting awareness of online privacy practices, security-related aspects and data tracking methods. The paper also examines the implications of the General Data Protection Regulation (GDPR) regarding businesses operating within the EU and the European Economic Area (EEA). Via a thorough investigation of Internet users' awareness of cookies as tracking tools and the prevalence of security-related incidents, the paper provides insights into the evolving landscape of online privacy and security. It elucidates the challenges and opportunities presented by GDPR compliance for businesses, compliance requirements, spanning core principles and broader implications of data processing practices. The findings mark the imperative to align businesses' operations with GDPR provisions, addressing key aspects such as consent mechanisms, lawful bases and the importance of robust data security measures. The conclusion reveals the significance derived from the intersection of internet security perceptions, GDPR compliance, and business operations within the EU and EEA. Synthesizing empirical data with regulatory analysis, the paper provides a valuable understanding of the challenges and opportunities within the evolving regulatory landscape, thereby equipping businesses with actionable strategies în order to safeguard data privacy rights and uphold regulatory compliance in the digital age.*

Keywords: Internet Security Perceptions, GDPR Compliance, Data Privacy Rights, Business Operations European Union (EU).

Introduction

In the era where modern business operations are sustained by backbones of digitalization, the protection of personal data became a critical concern. The European Union's General Data Protection Regulation (GDPR), that was implemented in May 2018, represents an important starting point for a better protection of the online consumer. It impacts the way businesses handle and process personal information. This regulatory framework, along with its far-reaching implications, has sparked widespread discussions and raised numerous questions regarding its effects on business strategies, practices, and compliance measures.

DOI: 10.2478/picbe-2024-0121

The GDPR was designed to strengthen privacy rights and standardize data protection regulations across the EU. The regulation has influenced scientific research by implementing stricter rules to safeguard individuals' privacy rights within and outside the EU (Chassang, 2017). It introduces a strategic approach to overseeing personal data and establishes normative foundations for data protection (Hoofnagle et al., 2019).

The current research presents the implications of the consumer trust in online businesses and main issues identified by them in the cyberworld. By analyzing reports, Eurostat data and various scientific articles, we present the main results to inform policymakers, academics and industry professionals about the evolving landscape of data privacy regulation and its impact on the global business environment.

Literature review

In the following segment of this paper, we will discuss about the way in which internet security is perceived. Because internet security is a broad topic, and we want to generate a clear image of a complex problem, in the following segment we will refer strictly to the way in which internet security, or rather the lack of it is affecting the modern day, digitally dependent, society.

Bederna and Rajnai have identified two cybersecurity stakeholders, which represent different typologies of entities. In general, stakeholders represent a broad category of beneficiaries, and include, among others "persons; neighbourhoods; institutions; groups; organisations; society;" (Benn, Abratt and O'Leary, 2016). On one hand, there are the stakeholders from "National and supra-national levels", which are mostly organisations such as "agencies, councils, […] non-profit and for-profit organisations" (Bederna and Rajnai, 2022), whose main goal is "to ensure cybersecurity and resilience at the operational level." (ibidem). On the other hand, there are the stakeholders situated at "organisational level" which are consisting of "individuals with non-profit and for-profit organisations" (Bederna and Rajnai, 2022). Even though Bederna and Rajnai offer broad categories of entities which are affected by cybersecurity policies we believe, they omitted an important element of society, the average individual, which might not be part of any organisation or institution. Democracies are based on the multi stakeholder model, which functions on the principle that "all categories of stakeholders have ownership rights and control". (Costa and Pesci, 2016). The multi-stakeholder model leads to good governance, which "raises issues such as: stakeholder engagement;" (Bovaird and Löffler, 2016)," making it imperative that all of the stakeholders are taken into considerations, including individuals.

Regarding the implementation process of the proper measures in order to avoid security threats on the internet, "companies should check whether proper controls exist" (Cristea, 2020). The risk-assessment process should occur frequently. Moreover, in order to assure data safety, proper legislation should be put in place, based on which both public and private companies are obliged to undertake online security checks, with a frequency which will be determined by the lawmakers. In this case, all the stakeholders of digital security policies will take part in the security process and will be reassured that their personal information is kept safe.

A 2023 report issued by the European Council, showed that institutions, businesses, and individuals faced multiple threats when using the internet. These digital hostilities did not affect only the safety of personal data stored online, but also many aspects which concern all of the cybersecurity stakeholders.

DDoS (distributed denial-of-service) which represents a "malicious attempt to disrupt the normal traffic of a targeted server" (Cloudflare, n.d.) and malware which can "disrupt access to a device" (www.consilium.europa.eu, n.d.) are methods which undermine core principles of

democracy. First and foremost, freedom of speech is affected by these practices, which are perceived as "an increasingly serious threat to media freedom" (International Press Institute, 2024) Personal liberties are also affected by these practices, because due to 'hindering the free flow of information and obstructing the public's access to independent journalism." (ibidem) people are not able to access the desired information. Ransomware attacks represent another procedure through which access to online resources is restrained. In this case, "cybercriminals take control of a target's asset" (www.consilium.europa.eu, n.d.). However, even though it is similar to *DDoS* and *Malware*, in the sense that it disables access to a certain website or application, the main goal of these procedures differs. While *DDoS* and *Malware* are generated with the intent to disable online structures, people who use ransomware are rather interested in the money they will receive, after they restore the ability of the site/application. (ibidem). Thus, we believe that ransomware has a lower negative effect on democratic principles but is still able to affect all the cybersecurity stakeholders.

Disinformation or misinformation is a practice which is widely associated with fake news. We perceive this type of threat as a double-edged sword, because it affects more than the individuals which are targeted by the fake news. There are two different ways in which misinformation can impact people. Second, people's health might be impacted as well, causing "psychological disorders and panic, fear, depression, and fatigue" (Rocha et al., 2021). People's actions, which are motivated by the influence exerted by disinformation campaigns, ultimately affect the national and supranational stakeholders. For example, fake news focused on the subject of the Covid-19 Pandemic generated "inaccurate knowledge seemed to increase their vaccine hesitancy and decrease behavioural intention to get vaccinated" (Lee et al., 2022) which in turn facilitated the spread of Covid and aggravated the general health situation.

At organisational level, the stakeholders which are more likely to be affected by online threats are SMEs. Almost half of them are "more worried about cyber threats than a year ago" (Sharp, 2023) and "two thirds (68%) lack confidence in ability to deal with the risk" (ibidem). Moreover, almost a third "of European organisations face significant challenges in fully utilising data due to concerns surrounding data security" (Dan Willis, 2023). We believe that corporations may deal better against cyber threats than SME's due to their expertise and available resources. The companies' inability to perform at full capacity, due to online security threats, is affecting the other digital security stakeholders. First and foremost, individuals are affected for two separate reasons: their personal data might be at risk and because companies might not be able to provide quality services due to digital threats. Identity theft, based on the data which was stolen from companies might affect national and supranational institutions, and other private organisations.

According to a special Eurobarometer report, half of the respondents (47%) "say they are not well informed" (European Commission and Directorate-General for Migration and Home Affairs, 2020) in regard to the risks of cybercrime. According to the same study, younger men, with higher education believe they are well informed regarding online threats.

Besides peoples' responses, there are two other important indicators which reflect their attitude towards internet security. First, how often they change their account's password for social media platforms, email addresses and other applications. A third of the respondents "have changed an email account password," or "an online banking password" (European Commission and Directorate-General for Migration and Home Affairs, 2020, p.6). Moreover, young people are prone to take "more specific security-related actions" (ibidem).

Internet security in a highly digitalised world is a complex issue, which can be properly addressed only through a strategic partnership between the private sector and public institutions,

whether national or supranational, because "governments and the private sector have a shared interest and responsibility to face that threat together." (Mee and Chandrasekhar, 2021). However, the current study will present that a third stakeholder, the citizen, can be introduced in this process to better understand the cyber threats and how to react in dangerous virtual situations. Thus, all the three major cyber security stakeholders will stan together in the fight against digital threats.

Results and discussions

The internet serves today as a vital conduit for communication, commerce, and social interaction. However, alongside its benefits, the digital environment also presents significant challenges, particularly concerning security and privacy. Within the European Union (EU), a diverse and dynamic collective of nations, citizens' perceptions of internet security are shaped by various factors including technological advancements, regulatory frameworks, cultural norms, and evolving cyber threats.

The perception of internet security among EU citizens is a multifaceted phenomenon, influenced by their experiences, beliefs, and the prevailing socio-political environment. The expansion of online platforms and services brought awareness for individuals regarding vulnerabilities inherent in digital interactions. Cyberattacks, high-profile data breaches and online fraud stressed the importance of securing personal information and maintaining digital privacy.

At the same time, in order to enhance Internet security and to protect the rights of its citizen, the EU has implemented robust regulatory measures. Initiatives such as the General Data Protection Regulation (GDPR) have set global standards in data protection, giving individuals greater control over their personal data and enabling strict obligations on businesses and organizations that collect and process such information.

However, despite these regulatory efforts, the realm of internet security is still challenging. The rapid evolution of technological innovation often outruns the capacity of regulators to adapt, leaving gaps that may turn into exploits for cybercriminals to profit from. Furthermore, the borderless framework of the Internet complicates enforcement actions, as threats can originate from anywhere in the world, therefore transcending national jurisdictions.

In this line of sight, EU citizens encounter a complex landscape of digital risks and opportunities, striving to balance security with convenience in their online activities. Their perceptions of internet security are shaped not only by external factors such as cyber incidents and regulatory developments but also by individual attitudes towards risk, trust in technology, and the trade-offs inherent in digital participation.

Being aware of the nuances of public perception for the Internet security is crucial for policymakers, industry stakeholders, and cybersecurity professionals. By acknowledging the priorities, concerns and expectations of EU citizens, stakeholders become able to develop more effective strategies in order to promote cyber resilience, build trust in digital technologies and protect the fundamental rights of individuals in the current digital age.

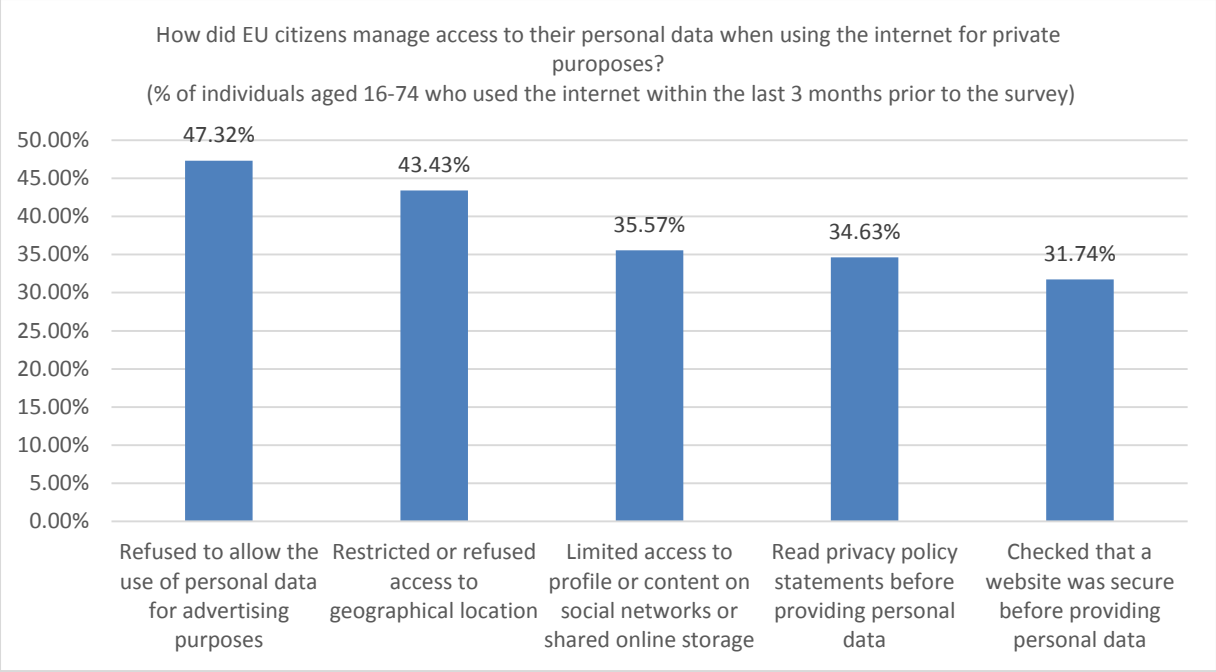

Figure 1. Management of personal data in the EU
Source: Eurostat, 2023. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220127-1.

The above-mentioned graphic (figure 1) highlights the various strategies employed by EU citizens to manage access to their personal data when engaging in online activities for private purposes. It's notable that a significant portion of individuals, almost 50%, refuse to allow the use of their personal data for advertising purposes, indicating a growing awareness and concern about privacy and targeted advertising. Additionally, a substantial percentage, 43%, restrict or refuse access to their geographical location, underscoring the importance of location privacy. Furthermore, a significant proportion, 35%, limit access to their profile or content on social networks or shared online sites, demonstrating a desire for control over their digital footprint. It is interesting to observe the fact that more than 34% declared that they read the privacy policy statements before uploading any personal data or providing it to a website. This might show how important the transparency and informed consent in data practices is. On the EU average, only 31% check is a website is secured by having the https link included. Even if this this is the least time-consuming method to apply before giving personal data online, it was the last strategy applied by individuals. A reason for not using this last method is most probably the fact that is wide unknown that they have this possibility, because it is more than simple to check the link of the website they navigate.

The current survey shows also which issues individuals have when using the Internet and which security-related problems they experienced in the past 12 months. It's striking to note that while some issues, such as online identity theft and misuse of personal information, are relatively less common, they still pose significant concerns, with reported rates of 1.1% and 1.49% respectively. Financial loss resulting from various cyber threats, including identity theft and fraudulent messages, emerges as a more pronounced issue, with a reported rate of 1.76%.

Personal account hacking and subsequent content posting online, as well as fraudulent credit or debit card use, represent substantial security breaches, with reported rates of 2.47% and

2.67% respectively, underscoring the potential financial and reputational risks associated with cyberattacks. It is also described the possibility that children will access inappropriate websites. More than 3,2% of the surveyed individuals reported that they experienced this problem before.

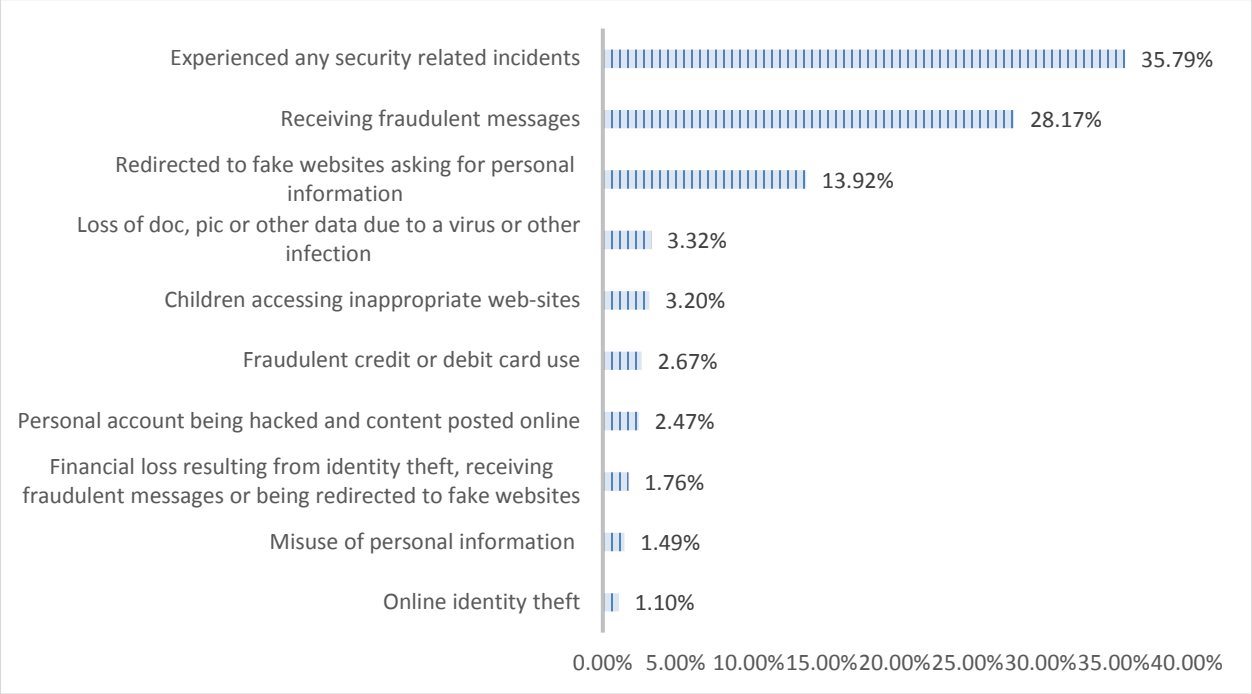

Figure 2. Security related problems experienced when using the internet
Source: Own research based on Eurostat Database [isoc_cisci_pb__custom_9493789] .

The data presented in the graphic above (figure 2) also reveals the widespread impact of malware infections, with 3.32% reporting loss of documents, pictures, or other data due to viruses or other infections, highlighting the need for robust cybersecurity measures and awareness campaigns.

Notably, incidents involving redirection to fake websites and receipt of fraudulent messages emerge as the most prevalent security concerns, with reported rates of 13.92% and 28.17% respectively. The immediate danger of phishing attacks is real and is shown through the data depicted above. The online users must be vigilent and careful when navigating online.

All in all, data described in figure 2 shows different security threats that the user face when navigating online. It is important to take proactive measures, create an environment of cybersecurity education and make stakeholders work together in order to mitigate risks and enhance online safety.

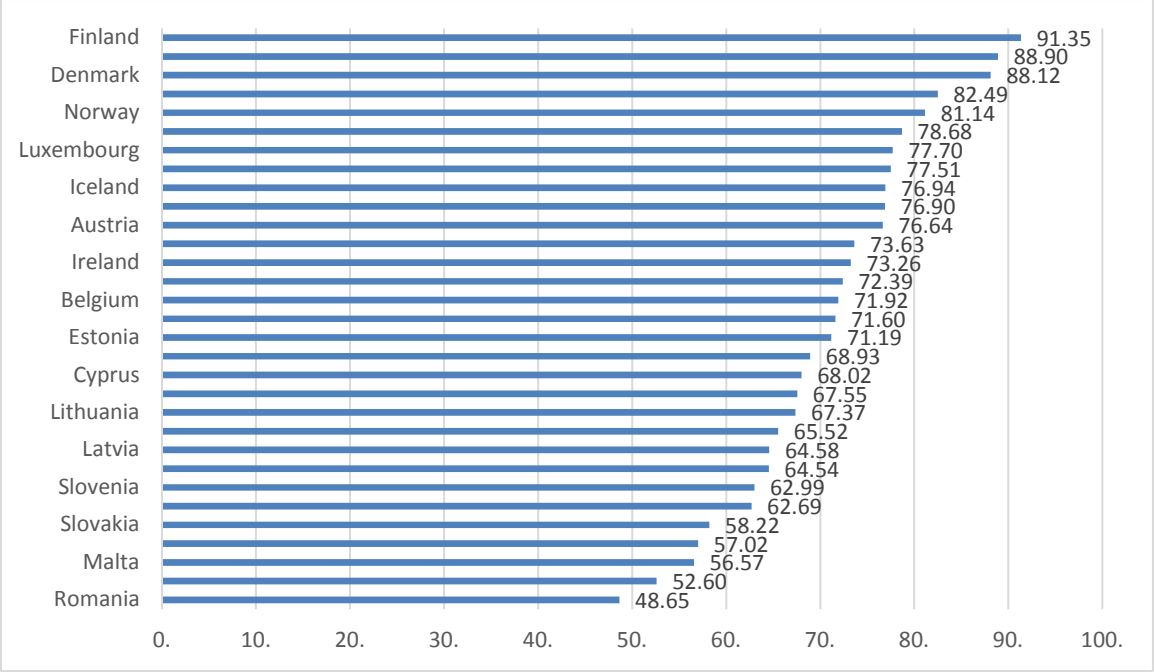

Figure 3. Percentage of individuals who know that cookies can be used to trace movement of people on the internet

Source: Own research based on Eurostat Database [isoc_cisci_pb__custom_9493789].

Figure 3 illustrates the percentage of individuals across various European countries who are aware that cookies can be utilized to track their movements on the internet. The highest level of awareness has been demonstrated by Denmark and the Netherlands with 88.12% and 88.90% respectively. These countries have a strong understanding of online privacy. Finland follows closely with 91.35%, indicating the highest level of awareness.

On the other hand, education in this sector and awareness initiatives regarding online tracking methods is needed by countries like Romania and Bulgaria, which have very low levels of awareness, with with 48.65% and 52.60% respectively.

All in all, there are great differences between the level of awareness of the citizens in different countries across the European Union. Some countries do really well, like Denmark and the Netherlands, while others will need to invest more in the education of their ordinary citizens. Even if in these countries there are good specialists in IT&C sector with many graduates in this sector, the ordinary citizen still does not have enough access to data and how to protect themselves on the Internet. European Union funds, European campaigns created by the European Parliament and the European Commission and distributed on social media might be a good idea on how the European institutions can close this gap between nations.

Conclusion

In conclusion, our research presents a full analysis of how citizens perceive the threats available online, how aware are the consumers of these threats, but also how they protect themselves through different measures. There is a big gap between European Union nations on each level of this perception. For instance, Denmark, the Netherlands, and Finland exhibit remarkably high levels of awareness regarding online privacy practices, with a significant majority of individuals

acknowledging the potential tracking capabilities of cookies. Meaning that these countries have a strong digital literacy and proactively ensures online privacy rights.

On the other hand, nations like Romania and Bulgaria show a possible need for focused education campaigns and awareness raising activities to close the knowledge gap. These results highlight the significance of adjusting cybersecurity education to the unique requirements and difficulties encountered by various European areas. Policymakers and educators can try to cultivate a more universally informed and resilient citizen that is capable of securely navigating the digital environment by addressing these disparities.

Security-related challenges faced by EU consumers when using the internet are diverse and have attracted significant attention in the academic environment. The growing dependence on the internet for various services has elevated the importance of secure computing and cybersecurity according to Djatsa (2020). The results of our study are also in accordance with Tsoukalas & Siozos (2011). They showed that the expansion of online platforms and digital data has amplified security and privacy risks for internet users. Li et al. (2018) also argue that users are now more cognizant of these risks and are actively seeking secure applications that prioritize their privacy. Moreover, Hudson & Liu (2022) sustains our idea that privacy regulations like the GDPR play a pivotal role in safeguarding users' online information privacy

In summary, the security-related issues experienced by EU consumers when using the internet encompass a wide range of concerns, including privacy issues, cybersecurity awareness, regulatory adherence, and data protection. Addressing these challenges demands a comprehensive approach that includes regulatory frameworks, user education, and technological advancements to ensure a secure and privacy-enhancing online environment for all users.

References

Bederna, Z. and Rajnai, Z. (2022). Analysis of the cybersecurity ecosystem in the European Union. *International Cybersecurity Law Review*, 3. doi:https://doi.org/10.1365/s43439-022-00048-9.

Benn, S., Abratt, R. and O'Leary, B. (2016). Defining and Identifying stakeholders: Views from Management and Stakeholders. *South African Journal of Business Management*, [online] 47(2), pp.1–11. doi:https://doi.org/10.4102/sajbm.v47i2.55.

Bovaird, A.G. and Löffler, E. (2016). *Public management and governance*. London ; New York: Routledge.

Chassang, G. (2017). The impact of the eu general data protection regulation on scientific research. Ecancermedicalscience, 11. https://doi.org/10.3332/ecancer.2017.709

Cloudflare (n.d.). *What is a DDoS attack?* [online] Cloudflare. Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

Costa, E. and Pesci, C. (2016). Social impact measurement: why do stakeholders matter? *Sustainability Accounting, Management and Policy Journal*, 7(1), pp.1–47. doi:https://doi.org/10.1108/sampj-12-2014-0092.

Cristea, L.M. (2020). Current security threats in the national and international context. *JOURNAL OF ACCOUNTING AND MANAGEMENT INFORMATION SYSTEMS*, 19(2), pp.351–378. doi:https://doi.org/10.24818/jamis.2020.02007.

Dan Willis (2023). *European Companies Face Data Security Challenges Amidst Rising Cyberattacks*. [online] FinTech Global. Available at: https://fintech.global/2023/09/15/european-companies-face-data-security-challenges-amidst-rising-cyberattacks/.

Djatsa, F. (2020). Threat perceptions, avoidance motivation and security behaviors correlations. Journal of Information Security, 11(01), 19-45. https://doi.org/10.4236/jis.2020.111002

European Commission and Directorate-General for Migration and Home Affairs (2020). *Europeans' Attitudes Towards Cyber Security*. [online] *European Commission*, European Comission, pp.1–268. Available at: https://op.europa.eu/en/publication-detail/-/publication/468848fa-49bb-11ea-8aa5-01aa75ed71a1 [Accessed 22 Feb. 2024].

Hoofnagle, C., Sloot, B., & Borgesius, F. (2019). The european union general data protection regulation: what it is and what it means. Information & Communications Technology Law, 28(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Hudson, S. and Liu, Y. (2022). Mobile app users' privacy concerns: different heuristics for privacy assurance statements in the eu and china. Information Technology and People, 36(1), 245-262. https://doi.org/10.1108/itp-06-2021-0478

International Press Institute (2024). *New surge of DDoS attacks threatens media freedom in Europe*. [online] International Press Institute. Available at: https://ipi.media/new-surge-of-ddos-attacks-threatens-media-freedom-in-europe/ [Accessed 22 Feb. 2024].

Lee, S.K., Sun, J., Jang, S. and Connelly, S. (2022). Misinformation of COVID-19 vaccines and vaccine hesitancy. *Scientific Reports*, [online] 12(1), pp.1–11. doi:https://doi.org/10.1038/s41598-022-17430-6.

Li, R., Xiao, Y., Zhang, C., Song, T., & Hu, C. (2018). Cryptographic algorithms for privacy-preserving online applications. Mathematical Foundations of Computing, 1(4), 311-330. https://doi.org/10.3934/mfc.2018015

Mee, P. and Chandrasekhar, C. (2021). *Cybersecurity is too big for governments or firms to handle alone*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/?utm_content=04%2F05%2F2021+11%3A30&utm_medium=social_scheduler&utm_source=twitter&utm_term=Cybersecurity [Accessed 23 Feb. 2024].

Rocha, Y.M., de Moura, G.A., Desidério, G.A., de Oliveira, C.H., Lourenço, F.D. and de Figueiredo Nicolete, L.D. (2021). The impact of fake news on social media and its influence on health during the COVID-19 pandemic: a systematic review. *Journal of Public Health*, [online] 1(10). doi: https://doi.org/10.1007/s10389-021-01658-z.

Sharp (2023). *Cyber threat concerns amongst European SMEs on the rise in last 12 months as over a third admit to breaches*. [online] www.sharp.eu. Available at: https://www.sharp.eu/news-and-events/news/cyber-threat-concerns-amongst-european-smes-on-the-rise-in-last-12-months-as [Accessed 22 Feb. 2024].

Tsoukalas, I. and Siozos, P. (2011). Privacy and anonymity in the information society – challenges for the european union. The Scientific World Journal, 11, 458-462. https://doi.org/10.1100/tsw.2011.46

www.consilium.europa.eu. (n.d.). *Top cyber threats in the EU*. [online] Available at: https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/ :