Journal of Applied Research and Technology

www.jart.icat.unam.mx

ICAT
Instituto de Ciencias Aplicadas y Tecnología

Journal of Applied Research and Technology 24 (2026) 66-74

Original

Assessing Privacy Benefits in the Digital Age: A Study of Tor and the Dark Web

Gabriel Alejandro Silva-Atencio[*1]

[1]*Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), San José, Costa Rica*

Received: 19 12 2024; Accepted: 12 02 2025
Available: 28 02 2026

Abstract: The onset of the fifth industrial revolution presents significant challenges in the interaction between organizations and people, positioning cybersecurity as a strategic pillar to safeguard infrastructure, data, and collaborators. This study aimed to identify the positive factors that the dark web can contribute to a corporate cybersecurity strategy, focusing on the supervision, monitoring, and evaluation processes. Using a qualitative-exploratory approach, a survey applied to cybersecurity experts was used to gather key perspectives and feedback. The findings revealed the absence of robust policies, processes, and procedures to ensure business continuity, highlighting critical risks associated with the lack of mitigation and contingency plans in the face of potential cyberattacks. In conclusion, the strategic use of tools and approaches derived from the dark web can contribute to strengthening business cybersecurity, provided that clear policies are implemented and aligned with business continuity objectives.

Keywords: **Cybersecurity, dark web, digital, privacy, Tor.**

*Corresponding author.
E-mail address: gsilvaa468@ulacit.ed.cr (G.A. Silva-Atencio).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

In today's technological society, digitization has redefined the boundaries of privacy, becoming a key tool for the surveillance and exploitation of personal data. According to the report of the Office of the United Nations High Commissioner for Human Rights (OHCHR, 2022), the right to privacy is under increasing pressure due to the use of modern digital technologies that act as powerful instruments of control and monitoring. An emblematic example of this issue is the case of Edward Snowden's leaks in 2013, which revealed mass surveillance programs such as PRISM, administered by the US National Security Agency (NSA), which compromised the privacy of millions of users (BBC, 2014).

In this context of digital surveillance, there is growing concern about the abuse of personal data. In response, many users have chosen to surf anonymously through tools such as the dark web (Raman et al., 2023). Although this hidden part of the Internet has been conceptualized as a negative and risky environment, recent research has highlighted its positive impact, particularly on privacy protection (Sirola et al., 2022). For example, technologies such as the Tor Browser, with over two million active daily users, have proven to be a key tool for online anonymity and security (Jardine et al., 2020).

The present study aimed to explore the use of the Tor tool in dark web browsing to avoid digital surveillance. Through its layered routing technology, known as "onion routing", Tor offers anonymous connections that encapsulate messages in multiple layers of encryption (Pastor-Galindo et al., 2023). The research seeks to answer the central question: What are the privacy benefits offered by Tor as a tool for browsing the dark web? To do so, this study analyzed the causes of digital surveillance, its influence on the use of the dark web, the user experience, and the benefits associated with privacy.

Knowing the benefits of surfing the dark web allows for validating its usefulness as a tool to safeguard a right that is frequently violated on the superficial web. This knowledge also contributes to fostering freedom of expression and strengthening data privacy rights in an environment where corporations and governments use personal information for commercial and control purposes (Cayford & Pieters, 2018; Schäfer et al., 2023).

The dark web, with its unique properties, represents a potential solution in the face of the global digital surveillance problem. This article seeks to highlight the positive impact of this technology, rescuing its initial purpose: anonymous communication, privacy protection, and the promotion of freedom. In this way, it aims to expose the legal and ethical utilities that the dark web can offer to safeguard data privacy.

2. Materials and Methods

The study was developed under a qualitative-exploratory approach, designed to evaluate the benefits of the Tor tool in browsing the dark web and its impact on digital privacy. The methodology included three main phases: data collection, evaluation, and analysis, aimed at identifying patterns and trends related to digital surveillance, dark web use, and user experience with the browser.

Information was gathered from diverse sources, including academic articles, scientific research, forums, news, and surveys, for the purpose of integrating multiple perspectives. Specific search criteria were defined with keyword combinations such as: "digital privacy," "dark web," "Tor" and "anonymity." Searches were conducted in databases such as EBSCO, Google Scholar, and ResearchGate, among others. To ensure the relevance of the data, results were limited to papers published between 2016 and 2023, in Spanish and English.

Theoretical sampling was used to progressively build the sample composition as data were collected. The selected documents were filtered by expert judgment analysis, discarding those that did not provide information relevant to the study topic. This process allowed the initial sample to be reduced to documents containing specific data related to the study objectives.

To understand the user experience, the Tor tool was downloaded and used. Observation was used as the main method, understood not only as a perceptual activity but as a formative process that involves the use of all senses, allowing researchers to explore, describe, and analyze key patterns (Hernández-Sampieri & Mendoza, 2020). From this stage, patterns, themes, and trends were established, which were compared and triangulated to ensure the validity of the findings.

The selected documents had to meet the following criteria:

1. Thematic relevance to digital privacy, surveillance, and the dark web.
2. Publication within a time range between 2016 and 2023.
3. Availability in English or Spanish.
4. Content with verifiable data applicable to the context of the study.

The final analysis was based on the selected documents and direct experience with the Tor tool, allowing the identification of privacy benefits and their applicability in the era of digital surveillance.

3. Theoretical Framework

Digital technology has transformed numerous aspects of everyday life, including political discourse, personal relationships, and business activities. This environment has turned data into a strategic asset that drives digital surveillance. Dormandy (2019) defines surveillance as the detailed observation of individuals for purposes of control or profit. With the advancement of technology, tools such as data mining make it possible to analyze every digital footprint generated, from interactions on social networks to online transactions (Dormandy, 2019). However, the Office of the High Commissioner for Human Rights (OHCHR, 2022) warns that this practice represents a systematic violation of the fundamental right to privacy.

Mass data collection includes information such as contacts, locations, purchasing behaviors, and publications, which are exploited by corporations and governments for a variety of purposes, from targeted marketing to crime analysis (Dormandy, 2019). According to Grinin et al. (2022), Internet freedom has significantly diminished due to the lack of technological regulation and the increasing use of surveillance tools by authoritarian governments, as evidenced in cases such as China and Iran.

In this context, a growing concern for digital privacy arises, which has led to the development of technologies such as The Onion Router (Tor), a tool that hides the user's Internet Protocol (IP) address and hinders online tracking (Bergman & Popov, 2023). Since the Edward Snowden leaks, Tor usage has doubled, reflecting a global interest in preserving privacy in the face of mass surveillance (Patsakis et al., 2018). Currently, more than two million daily users resort to this tool, highlighting its relevance in contexts of censorship and restrictions of freedoms (Huete Trujillo & Ruiz-Martínez, 2021).

The dark web, part of the deep web, is accessible through networks such as Tor, FreeNet, and I2P, and has been commonly associated with illegal activities. However, recent research shows that a considerable part of its content (47.7%) is legal, as indicated by Burnett and Lloyd (2020). Moreover, it provides a safe space for journalists, human rights activists, and whistleblowers, allowing anonymous communications and collaboration without fear of reprisal (Nazah et al., 2020).

Despite the stigmatization of the dark web as a criminal environment, studies such as Sirola et al. (2024) highlight its benefits for information transparency and privacy protection. These properties were originally conceived by the U.S. Naval Research Laboratory to protect users against surveillance on the surface web (Haasio et al., 2020).

Online privacy continues to be a growing need. According to Özdal et al. (2024), 86% of Internet users have tried to hide their behavior or avoid online tracking. This reflects the importance of tools such as Tor, which make it possible to limit the collection and misuse of personal data (Haddad, 2024). Cases such as the Cambridge Analytica scandal provide evidence of how data exploitation can pose a threat to privacy and digital freedom (Dommett et al., 2024).

The right to privacy is supported by international frameworks, such as the United Nations Human Rights Council (OHCHR, 2022). This normative framework underlines the connection between privacy, anonymity, and freedom of expression, highlighting that both are essential for the protection of human rights in the digital age (Saltarella et al., 2024). However, a gap persists in the academic literature regarding the positive impacts of the dark web, due in part to its secretive nature and the bias toward associating it solely with illicit activities (Gupta et al., 2021).

In a world where data is a commoditized resource and privacy is under constant threat, the dark web and tools such as Tor represents a haven for ensuring anonymity and digital freedom (Gehl, 2016). This study seeks to fill the gap in the literature by highlighting the legal and ethical benefits that these technologies can offer in the face of mass surveillance.

4. Analysis of Results

In a highly digitized world, the privacy paradox emerges as a complex problem that reflects the tension between the desire for privacy and the conveniences offered by technologies. The amount of data generated is growing exponentially, as is digital surveillance, underscoring the importance of understanding its causes and effects.

Identifying the causes of digital surveillance

A preliminary search on the topic yielded 9,380 articles, of which 2,700 related to the causes of surveillance were filtered out. Subsequently, 50 authors were selected for in-depth discussion, identifying eight main causes.

1. Advancement of technology: According to Dinev et al. (2008), Ribeiro-Navarrete et al. (2021), the growing capacity of technological systems to collect and process data has significantly boosted digital surveillance. This has enabled government and corporate sectors to optimize the flow of information for control and monetization purposes.
2. Value of data: Chen et al. (2021), Yu et al. (2024) highlight that personal data is a valuable resource, facilitating data mining and big data. Examples such as the "dotcom crisis" show how companies used user data to generate revenue (Srinivas et al., 2019).
3. Corporate interests: Zuboff (2015) describes "surveillance capitalism" as an economic model that turns human experiences into raw material for targeted marketing.
4. Political control: autocracies such as China and Russia adopt technologies to monitor their citizens, exemplified by China's "Great Firewall" system (Hodgetts et al., 2017). In democracies, surveillance is justified in the name of national security but often lacks transparency (Burr et al., 2020).
5. Public perception: Loannou and Tussyadiah (2021) stress that acceptance of surveillance depends on factors such as trust in the government and the perceived benefits of social networks.
6. Social control: According to Reisach (2021), partisan actors manipulate online information to influence elections, as occurred in at least 24 countries.
7. Geopolitics: Yan et al. (2024) note that espionage and diplomatic negotiations are key motivators for surveillance. Recent examples include the conflict between China and the U.S.
8. Health sector: The COVID-19 pandemic accelerated the use of surveillance systems to track contagions, raising concerns about their reuse for other purposes (do Carmo Barriga et al., 2020).

Influence on the use of the dark web

Based on the causes identified, a specific search was conducted on their impact on the dark web, obtaining 442 results, of which 379 were related to the use of Tor. Users seek alternatives such as the dark web to protect their privacy from mass surveillance. Tools such as Tor offer anonymity and encryption, providing a secure alternative to circumvent censorship and protect digital privacy.

The Tor tool, accessible from torproject.org, allows anonymous connections through onion routing. Although the installation process is straightforward, a slower browsing speed was observed compared to traditional browsers such as Google Chrome. Its functionality includes:

1. Anonymity: it hides the user's IP address, making it difficult to trace.
2. Encryption: Protects communication through multiple layers of security.
3. Censorship circumvention: It allows overcoming government blockades, such as in Hong Kong and Burma during political censorship events (Reisach, 2021).

Impact of surveillance on the use of Tor

Digital surveillance drives users to seek tools such as Tor to protect themselves. Recent examples include:

1. Hong Kong (2019): Figure 1 shows that government restrictions following pro-democracy protests led to an increase in Tor users (Reisach, 2021).

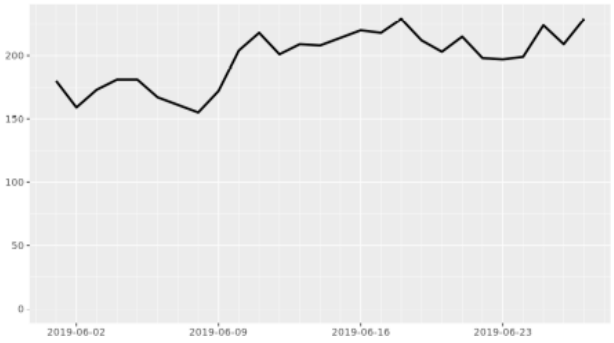

Figure 1. Bridge users in Hong Kong.

2. Birmania (2021): Figure 2 shows that Internet blockades after the military coup increased Tor use (Prabha & Mittal, 2023).

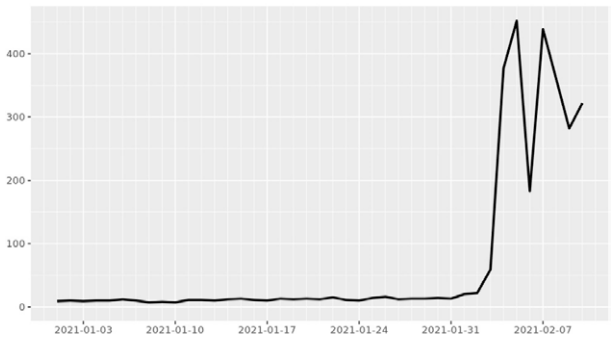

Figure 2. Bridge users in Birmania.

3. Russia and Ukraine (2022): Figure 3 shows how the war intensified the use of Tor to access blocked information (Yan et al., 2024).

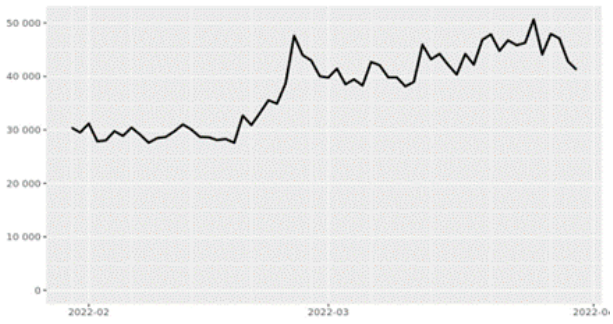

Figure 3. Bridge users in Russia during the war with Ukraine.

The use of tools such as Tor is confirmed as essential to protect digital privacy against mass surveillance. Its benefits include:

1. Anonymity: protection against tracking of online activities.
2. Advanced encryption: Ensures secure communications.
3. Access to blocked content: Overcomes censorship restrictions.
4. Profiling protection: Reduces exposure to targeted marketing strategies.

The analysis shows that the dark web, through Tor, offers a space to preserve fundamental rights such as privacy and freedom of expression, highlighting its relevance in the context of global digital surveillance.

5. Discussion

Digital privacy is a fundamental right that seeks to ensure the protection of users' data when accessing online services. According to Wang et al. (2024), this right includes control over how data are collected, processed, and shared. In this context, anonymity plays a crucial role in allowing individuals to protect their privacy and engage in digital activities without fear of being identified or exploited. This concept is particularly relevant for dissident and minority communities in authoritarian regimes, which use tools such as Tor to avoid persecution (Gulati et al., 2018).

Anonymity and encryption: fundamentals of digital privacy

Online anonymity allows users to safeguard their freedom of expression and protect their privacy rights (Moyakine, 2016). Tor excels in this area thanks to its layered routing system, known as "onion routing," which encrypts and redirects web traffic across multiple nodes, ensuring privacy and making it difficult to track data (Hall, 2008). This process not only protects the user but also ensures that online activities are invisible to potential surveillance agents.

From a security perspective, Tor is not only a tool to protect privacy, but also a means to securely access services that support free speech and independent journalism, such as BBC and ProPublica (Prabha & Mittal, 2023).

Overcoming censorship and preserving net neutrality

Access to blocked content is another key benefit of Tor, especially in contexts where governments restrict access to critical information or censor dissenting views. A University of Michigan study found that Internet censorship has increased in 103 countries, including democratic ones such as Norway and Japan, highlighting the importance of tools to circumvent these restrictions (Huete Trujillo & Ruiz-Martínez, 2021). By using hidden services such as ".onion" sites, Tor protects the user's identity and ensures secure access to censored content.

In addition, Tor contributes to the preservation of net neutrality by ensuring that users can access any type of legal content without restrictions, maintaining equality in the treatment of data (Almeida Teixeira et al., 2019). This is essential to avoid censorship practices that limit the flow of information and opinions online.

Protection against profiling and data manipulation

Digital profiling, an invasive practice used by corporations to collect user data, represents a significant threat to privacy. Analytics and targeted marketing technologies often cross ethical boundaries by manipulating users based on their online behaviors (Taherdoost, 2022). Tor offers a practical solution by anonymizing online activities and preventing individual profiling.

Impact of hidden services

Hidden ".onion" services allow users to browse and engage in digital activities without leaving electronic traces. This is especially relevant in countries with strict

surveillance and censorship, where expressing opinions contrary to the regime can have serious consequences (Huete Trujillo & Ruiz-Martínez, 2021). In addition, these services have been used by journalists, human rights activists, and whistleblowers to share information securely and protect their identities.

The discussion confirms that tools such as Tor are critical to safeguarding digital privacy, especially in a world where mass surveillance and data profiling are ubiquitous. The benefits of this technology include:

1. Anonymity: Protection against tracking and identification.
2. Encryption: Ensures the privacy of online communications.
3. Uncensored access: Allows free access to blocked information.
4. Net neutrality: Preserves the right to equal access to data.

Tor and the dark web offer a viable solution to protect fundamental rights such as freedom of expression and privacy, becoming an essential tool for facing the challenges of global digital surveillance.

6. Conclusions

Digital surveillance is an evident problem to which everyone is exposed. During the research, the use of the Tor tool was shown to counteract manifestations of surveillance through anonymity, data privacy protection, prevention of profiling, access to blocked content, and the use of hidden services. In addition, Tor helps maintain net neutrality by promoting equal and non-discriminatory access to information.

The causes of digital surveillance can be categorized into two broad groups: governmental and corporate. Governments often justify these practices as measures to ensure national security, while corporations use surveillance as a means to maximize economic benefits by collecting data for targeted marketing. However, both practices share a common problem: a lack of transparency and oversight.

Lack of transparency makes it difficult for citizens to understand the scope of surveillance activities and how their data is collected, stored, and used. On the other hand, the absence of adequate oversight allows for misinterpretations and possible misuse of data, creating an environment conducive to abuses and violations of privacy rights.

It is necessary to actively work against the misuse of personal data in the context of digital surveillance, as this poses significant risks to privacy, security, and democratic processes. Concrete actions should be undertaken, such as:

1. Legal reforms: establishing stricter regulations that protect privacy rights and limit indiscriminate data collection.
2. Promoting transparency: Requiring governments and corporations to report clearly on the scope and methods of their surveillance activities.
3. Developing privacy-enhancing technologies (PETs): Encouraging the creation and adoption of tools such as Tor that strengthen data protection and anonymity online.

Finally, it is critical to conduct additional research to identify and accurately delimit the scope of digital surveillance. This will make it possible to balance its existence with privacy rights, ensuring that security measures do not compromise the fundamental principles of democratic societies.

7. Future research lines

The practical implications of the results lead to a change in the perspective of the *Tor* tool and the dark web. Therefore, seeking alternatives to address the threat to digital privacy is a valid reaction to concerns about privacy, censorship, or repression. While the tool offers anonymity, among other benefits, it is important to recognize that like any technology it has its vulnerabilities, so the following recommendations are made: use the web carefully, enter only trusted .onion sites, do not use or publish personal information, always have basic device security (antivirus), avoid downloading unknown files, use the *Tor* network in conjunction with a VPN to increase security, stay within the ethical and legal margin and the most relevant is always to be informed about the news of the tool, as new threats or benefits may arise.

The implications for academia indicate that the current digital surveillance framework will continue to develop in the future. Therefore, it is important to foster education on the topic, to promote the autonomy of individuals in defending their privacy rights. Tor is a relevant tool for digital privacy due to its capabilities, however, more research is proposed to thoroughly understand its scope in anonymity and effectiveness in achieving this goal. In addition to conducting studies about the impact of emerging technologies, such as artificial intelligence, on de-anonymization techniques could reveal new threats to digital privacy.

Conflict of interest

The author has no conflict of interest to declare.

Funding

The author received no specific funding for this work.

Acknowledgments

The author would like to thank all those involved in the work who made it possible to achieve the research study's objectives.

References

Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402-418. https://doi.org/10.1108/DPRG-01-2019-0007

BBC. (2014). *Edward Snowden: Leaks that exposed US spy program*. BBC. https://www.bbc.com/news/world-us-canada-23123964

Bergman, J., & Popov, O. B. (2023). Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation. *IEEE Access*, *11*, 35914-35933. https://doi.org/10.1109/ACCESS.2023.3255165

Burnett, S., & Lloyd, A. (2020). Hidden and forbidden: conceptualizing Dark Knowledge. *Journal of Documentation*, *76*(6), 1341-1358. https://doi.org/10.1108/JD-12-2019-0234

Burr, C., Taddeo, M., & Floridi, L. (2020). The Ethics of Digital Well-Being: A Thematic Review. *Science and Engineering Ethics*, *26*(4), 2313-2343. https://doi.org/10.1007/s11948-020-00175-8

Cayford, M., & Pieters, W. (2018). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, *34*(2), 88-103. https://doi.org/10.1080/01972243.2017.1414721

Chen, Y., Hua, X., & Maskus, K. E. (2021). International protection of consumer data. *Journal of International Economics*, *132*, 103517. https://doi.org/10.1016/j.jinteco.2021.103517

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233. https://doi.org/10.1016/j.jsis.2007.09.002

do Carmo Barriga, A., Martins, A. F., Simões, M. J., & Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?. *Social Sciences & Humanities Open*, *2*(1), 100096. https://doi.org/10.1016/j.ssaho.2020.100096

Dommett, K., Barclay, A., & Gibson, R. (2024). Just what is data-driven campaigning? A systematic review. *Information, Communication & Society*, *27*(1), 1-22. https://doi.org/10.1080/1369118X.2023.2166794

Dormandy, K. (2019). Digital whiplash: The case of digital surveillance. *Human Affairs*, *30*(4), 559-569. https://doi.org/10.1515/humaff-2020-0049

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, *18*(7), 1219-1235. https://doi.org/10.1177/1461444814554900

Grinin, L., Grinin, A., & Korotayev, A. (2022). The COVID-19 pandemic was a trigger for the acceleration of the cybernetic revolution, the transition from e-government to e-state, and change in social relations. *Technological Forecasting and Social Change*, *175*, 121348. https://doi.org/10.1016/j.techfore.2021.121348

Gulati, S., Sharma, S., & Agarwal, G. (2018, January). The hidden truth anonymity in cyberspace: Deep web. In *Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC 2017* (pp. 719-730). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-10-7245-1_70

Gupta, A., Maynard, S. B., & Ahmad, A. (2021). The dark web phenomenon: A review and research agenda. *arXiv preprint arXiv:2104.07138*. https://doi.org/10.48550/arXiv.2104.07138

Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark web marketplace. *Information Processing & Management*, *57*(2), 102080. https://doi.org/10.1016/j.ipm.2019.102080

Haddad, Z. (2024). Enhancing privacy and security in 5G networks with an anonymous handover protocol based on Blockchain and Zero Knowledge Proof. *Computer Networks*, *250*, 110544. https://doi.org/10.1016/j.comnet.2024.110544

Hall, M. N. (2008). mTOR—What Does It Do? *Transplantation Proceedings*, *40*(10, Supplement), S5-S8. https://doi.org/10.1016/j.transproceed.2008.10.009

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Hodgetts, H. M., Vachon, F., Chamberland, C., & Tremblay, S. (2017). See No Evil: Cognitive Challenges of Security Surveillance and Monitoring. *Journal of Applied Research in Memory and Cognition*, *6*(3), 230-243. https://doi.org/10.1016/j.jarmac.2017.05.001

Huete Trujillo, D. L., & Ruiz-Martínez, A. (2021). Tor Hidden Services: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, *1*(3), 496-518. https://doi.org/10.3390/jcp1030025

Jardine, E., Lindner, A. M., & Owenson, G. (2020). The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences*, *117*(50), 31716-31721. https://doi.org/10.1073/pnas.2011893117

Loannou, A., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society*, *67*, 101774. https://doi.org/10.1016/j.techsoc.2021.101774

Moyakine, E. (2016). Online Anonymity in the Modern digital Age: Quest for a Legal Right. *Journal of Information Rights, Policy, and Practice*, *1*(1). https://doi.org/10.21039/irpandp.v1i1.21

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE Access*, *8*, 171796-171819. https://doi.org/10.1109/ACCESS.2020.3024198

OHCHR. (2022). *Spyware and surveillance: Threats to privacy and human rights growing, UN report warns.* OHCHR. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

Özdal Oktay, S., Heitmann, S., & Kray, C. (2024). Linking location privacy, digital sovereignty and location-based services: a meta review. *Journal of Location Based Services*, *18*(1), 1-52. https://doi.org/10.1080/17489725.2023.2239180

Pastor-Galindo, J., Mármol, F. G., & Pérez, G. M. (2023). On the gathering of Tor onion addresses. *Future Generation Computer Systems*, *145*, 12-26. https://doi.org/10.1016/j.future.2023.02.024

Patsakis, C., Charemis, A., Papageorgiou, A., Mermigas, D., & Pirounias, S. (2018). The market's response toward privacy and mass surveillance: The Snowden aftermath. *computers & security*, *73*, 194-206. https://doi.org/10.1016/j.cose.2017.11.002

Prabha, C., & Mittal, A. (2023). Dark Web: A Review on the deeper side of the Web. *2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON)*, 1-6. https://doi.org/10.1109/OTCON56053.2023.10113989

Raman, R., Kumar Nair, V., Nedungadi, P., Ray, I., & Achuthan, K. (2023). Darkweb research: Past, present, and future trends and mapping to sustainable development goals. *Heliyon*, *9*(11). https://doi.org/10.1016/j.heliyon.2023.e22269

Reisach, U. (2021). The responsibility of social media in times of societal and political manipulation. *European Journal of Operational Research*, *291*(3), 906-917. https://doi.org/10.1016/j.ejor.2020.09.020

Ribeiro-Navarrete, S., Saura, J. R., & Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technological Forecasting and Social Change*, *167*, 120681. https://doi.org/10.1016/j.techfore.2021.120681

Saltarella, M., Desolda, G., Lanzilotti, R., & Barletta, V. S. (2024). Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review. *International Journal of Human–Computer Interaction*, *40*(17), 4465-4483. https://doi.org/10.1080/10447318.2023.2219964

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. *Business horizons*, *66*(4), 493-504. https://doi.org/10.1016/j.bushor.2022.10.002

Sirola, A., Nuckols, J., Nyrhinen, J., & Wilska, T.-A. (2022). The use of the Dark Web as a COVID-19 information source: A three-country study. *Technology in Society*, *70*, 102012. https://doi.org/10.1016/j.techsoc.2022.102012

Sirola, A., Savolainen, I., & Oksanen, A. (2024). Who uses the dark web? Cross-national and longitudinal evidence on psychosocial, behavioral, and individual predictors. *Personality and Individual Differences*, *227*, 112709. https://doi.org/10.1016/j.paid.2024.112709

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178-188.
https://doi.org/10.1016/j.future.2018.09.063

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, *11*(14), 2181.
https://doi.org/10.3390/electronics11142181

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *computers & security*, *147*, 104051.
https://doi.org/10.1016/j.cose.2024.104051

Yan, J., Leidner, D. E., & Peters, U. (2024). Global techno-politics: A review of the current status and opportunities for future research. *International journal of information management*, *75*, 102729.
https://doi.org/10.1016/j.ijinfomgt.2023.102729

Yu, S., Carroll, F., & Bentley, B. L. (2024). Insights Into Privacy Protection Research in AI. *IEEE Access*, *12*, 41704-41726.
https://doi.org/10.1109/ACCESS.2024.3378126

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75-89.
https://doi.org/10.1057/jit.2015.5