ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(2):1-8

REVIEW ARTICLE

A Survey on Digital Privacy: Technologies, Regulations, and Public Awareness

Hemant N. Patel*

Department of Computer Engineering, Sankalchand Patel College of Engineering, Sankalchand Patel University, Visnagar, Gujarat, India

Received on: 15-03-2025; Revised on: 02-05-2025; Accepted on: 10-06-2025

ABSTRACT

The issue of digital privacy has become one of the fundamental issues in the contemporary technologically interconnected world, as it appears in technological, legal, and social aspects. The paper examines the theoretical propositions, technological improvements, and regulatory context, and how public education is useful in creating a safe digital environment. As the process of digitization increases exponentially, the issue of the use of personal data, its storage, and security has become acute. The survey has provided the main ideas of data anonymity, consent, data breaches, and the list of the main stakeholders, people, corporations, governments, and regulators. The paper explores the use of new technologies, such as encryption, differential privacy, privacy-enhancing technologies, and zero-knowledge proofs that aid in data security and ensure safe data exchange. Simultaneously, global laws, such as GDPR, CCPA, and PDP Bill of Indonesia are examined to evaluate legal regulations in the field of data privacy and challenges of their application. Digital literacy and understanding of privacy are highlighted as one of the key factors that will guarantee that each person is capable of making a well-informed decision about his or her privacy. The paper also provides a comparative literature review that outlines the various views, interdisciplinary research, and real-life models that can be used to enforce digital privacy. The importance of this integrated effort is to ensure synergy between technology, law and education to develop sustainable, and ethical as well as user-centered digital ecosystems.

Key words: Anonymization, Cybersecurity, Data protection, Digital literacy, Digital privacy, Encryption, GDPR, Privacy regulations, Privacy-enhancing technologies, Public awareness

INTRODUCTION

The issue of privacy is gaining some traction in the media and regulatory discussions. This increased awareness of privacy is because of the increased usefulness of information of data.[1] The price of gathering data, storage, transmission, and analysis is very cheap due to digitization. This has led to the growing popularity of the use of digital data in decision-making.[2] Information significantly enhances the well-being of customers by empowering them to receive customized services and products at a significantly lower price. Companies can raise their revenues using this fact and customers can obtain higher-quality products and services that will fit their needs. Nonetheless, the use of such data has several disadvantages. Some of these consequences are apparent. People are naturally resentful of the gathering and use of personal information. To be able to collect and protect customer data, it is direct to businesses. Furthermore, individuals and companies can find out that someone uses this information against them.

Striking the right balance between safeguarding the fundamental right to privacy of the people and the leverage of the benefits of the AI-driven innovations will be an important issue that will receive enhanced focus as the technologies evolve further in the future. Privacy is one of the important human rights that must be enjoyed to have a free and democratic society. It encompasses the right of an individual to protect his or her personal conversations, activities, and personal information on one hand and protects against unauthorized access.[3] However, the importance of the right to confidentiality can be explained in a number of ways. Privacy is closely

Address for correspondence:
Hemant N. Patel
E-mail: hp15284@gmail.com

associated with the concept of personal autonomy or the ability of a person to make independent choices in his or her life without any external influence or pressure.[4] The right to privacy involves exercising the freedom to select personal relationships, beliefs, and preferences among others. It is important because it allows individuals to decide regarding their lives.

Data privacy regulation, particularly in the U.S., lacks an overarching federal mechanism to standardize data privacy.[5] The GDPR and CCPA, among other regulators, are digital privacy laws that help individuals control their information through transparency, collective consent, and accountability. Nevertheless, individuals are quite ignorant and most of the users do not know their rights, and they are oblivious about the use of their data. Although digital literacy and infrastructure are basic concerns in developing countries, in developed countries, some of the concerns are digital privacy and sophistication of services.[6,7] These differences point to the necessity of the overall appreciation of the elements that affect the use of digital services, particularly the impact of mass awareness and education on closing the digital divide.[8] One important element in the effective implementation of digital public services is education. The gap in knowledge should be addressed using education and awareness campaigns and people must be enabled to make informed decisions about privacy in the digital era. This paper aims to explore digital privacy by reviewing protective technologies, analyzing global regulations, and assessing public awareness, highlighting key challenges and opportunities for improving data protection practices.

The Paper's Structure

This document has the following structure: Section II outlines the fundamentals of digital privacy. Section III discusses global data protection laws and regulatory frameworks. Section IV explores public awareness strategies and educational tools. Section V presents a comparative analysis of reviewed studies. Section VI concludes with key findings and future work.

FOUNDATIONS OF DIGITAL PRIVACY

The control of personal information in the digital world, where data are constantly being gathered, processed, and shared, is known as digital privacy. The economics of privacy examines the compromises between the advantages of data sharing and the possible risks of data abuse, according to Acquisti, Taylor, and Wagman. Data can enhance efficiency and personalization but may also expose individuals to risks, such as discrimination or identity theft.[9] These dynamics create a privacy paradox, where individuals value privacy but often act against it. Understanding these economic incentives is crucial for designing effective privacy protections that balance innovation with individual autonomy.

Historical Evolution of Digital Privacy

With the rapid development digital environment, privacy legislation is increasingly needed to safeguard individuals' rights. The expansion of the Internet, social networks, and data analysis technology made possible an explosion of the generation, gathering, and global exchange of personal data. Consequently, traditional privacy law, in most instances developed for the pre-digital world, lagged behind the accelerated pace of technology innovation. This has brought a deep shift in the conception of, and legal protection of, privacy. The legal definition of privacy dates back to the early 1900s, but laws pertaining to privacy were not developed until the late 1900s in response to the digital revolution. The United States Privacy Act of 1974 was one of the first significant pieces of law pertaining to privacy protection, aiming to control how government agencies gather and handle personal data. However, by creating a framework for the protection of personal data within the EU, the 1995 Data Protection Directive of the European Union established a global standard for privacy regulations. The GDPR, which was adopted in 2018, marked the latest advancement in privacy laws.

Key Concepts in Digital Privacy

Data anonymity

Anonymization and de-identification are techniques used to eliminate identifying information from electronic record data.[10] De-identifying is the procedure that eliminates or substitutes personal Although a de-identified dataset may include an encrypted person identifier

that would enable authorized personnel to re-establish a connection between an individual and their data, it must not contain information that would allow an unauthorized person to infer an individual's identity from the existing data components.

Consent

Concerns about the use of personal data are common. According to people want to be certain that the information they provide is being used only and lawfully for the purposes for which they have given their consent. Users should also have the option to revoke their permission at any moment.[11] Consent is recorded legally and can be used as evidence in court cases or disagreements.

Data breach

Phishing schemes, a common cyberattack technique, take advantage of human mistakes by deceiving users into disclosing their login information by using phoney emails or websites that look authentic. Credential stuffing attacks exploit login credentials that have been stolen or disclosed from a single data breach to access other user accounts on several platforms without authorization.[12] Brute-force attacks, which are more computationally demanding, employ automated tools and powerful computers to exploit weak or widely used credentials by methodically guessing passwords through trial and error. In the case of a data breach, a compromised central server might expose a great deal of sensitive biometric data, making it unreliable or useless for further verification.

Major Stakeholders in Digital Privacy

Representing the most susceptible stakeholders in the realm of digital privacy, they are generally referred to as the "data subjects."[13] The major stakeholders include individuals, corporations, governments, and regulatory bodies. People are interested in keeping their personal information safe and ensuring control over their digital identities. Corporations are in control of large quantities of user information and are required to guarantee adherence to privacy regulations. Governments act as both regulators and data collectors, whereas regulatory groups bring law frameworks to guarantee the preservation of people' privacy and ethical data usage in the digital ecosystem.

TECHNOLOGIES FOR DIGITAL PRIVACY

Throughout the past 20 years, digital technologies have revolutionized all facets of marketing and elevated consumer privacy to the forefront of both study and discussion.[14] Digitalization has undoubtedly benefited businesses and consumers by making data more accessible and useful, but consumer privacy concerns pose significant challenges.[15] In a world where digital technologies affect every part of their lives as consumers, their understanding of privacy and its implications is always shifting. In fact, consumers' understanding of what privacy entails has greatly increased.

Encryption and Cryptography

Cryptography is the process of converting data from a readable form to an unreadable form to achieve the security requirements. Cryptography or encryption is also provides authentication to users as well as protecting the data. Usually, the original data are called plaintext, and encrypted data are called ciphertext. Hence, the result of converting plaintext to ciphertext is called encryption, as well as the result of converting ciphertext to plaintext is called decryption.[16] Cryptography could be classified into two groups, which are symmetric and asymmetric encryption. Cryptography is so important in cloud computing because the user must transfer his particular data through the internet to be stored in the cloud. Hence, without encrypt, the data are easily discovered by the attackers in the cloud storage. The data must be applied to strong encryption to be protected against attackers.

End-to-end encryption

A user's messages cannot be read by the server hosting them or by any adversary who intercepts data while the message is being sent thanks to the encryption used in "end-to-end" encrypted messaging.[17] "End" in "end-to-end" encryption refers to the "endpoint," which is the user's client device rather than the server.

Public key infrastructure (PKI)

A comprehensive system that offers digital signatures and public-key encryption is known as PKI. Keys and certificates are managed by PKI. PKI might assist a company in establishing and maintaining a reliable and trustworthy networking environment. PKI is commonly used interchangeably with asymmetric encryption because, as illustrated in Figure 1, it is more secure than symmetric encryption.[18] Mathematically, a public key and a secret key are related; the former is used for encryption, and the latter for decryption. Everyone knows the public key, but only the owner knows the private key.

Privacy-Enhancing Technologies (PETs)

The protecting people's privacy through technology is aim of PETs.[19] Their objective is to safeguard user identities by making users and data subjects anonymous, pseudo-Nymity, unlikable, and unobservable. Many PETs based on various building elements, such as cryptographic primitives or information separation, have been suggested in the past ten years to address network traffic anonymization, identity management, or anonymous data storage. Since privacy is a multifaceted notion, PETs can target all elements of information privacy, making PET categorization a challenging endeavor. A number of taxonomies and classifications, including the outstanding taxonomy of safe and reliable computing.

Differential privacy

The curator's algorithm for releasing information is the randomized function *K*. Thus, the data set is the input, and the information that has been made public, or the transcript, is the output.[20] It is not necessary to distinguish between interactive and non-interactive situations. A database is a collection of rows. Databases D1 and D2 differ by no more than one element when one database is a valid subset of the other and the larger database include only one extra row. The differential privacy equation is illustrated in Equation (1):

$$Pr[K(D1)i\ S] \leq exp(\epsilon) \times Pr[K(D2)\ S] \quad (1)$$

If every S ⊆ Range (K) and every data set A randomized function K provides differential privacy if D1 and D2 differ by no more than one element. The probability is computed over a total of K coin flips.

Zero-knowledge proofs

By using a "zero-knowledge proof" cryptographic technique, one party (the prover) can demonstrate to another (the verifier) that they are aware of a certain fact without actually disclosing it. This might be very useful in circumstances when private information needs to be kept secret to preserve its security and privacy. To convince the verifier that they are aware of a secret input, the prover must present proof. This is accomplished by utilizing QAPs and R1CS to convert the function into an arithmetic circuit. A conversation between the verifier and the prover takes place through a setup process that generates proving and verifying keys to ensure mathematical soundness and secrecy of the proof.[21] This structured process enables secure, non-interactive validation without exposing the private input or revealing the computation's internal logic, as shown in Figure 2.

Anonymization and Pseudonymization Tools

The original data are altered by data anonymization, making it more difficult to identify a specific person. This process is facilitated by two popular open-source programs: Amnesia and ARX Data Anonymization. Data anonymization is mostly employed by businesses that gather and retain personal information for use in direct or

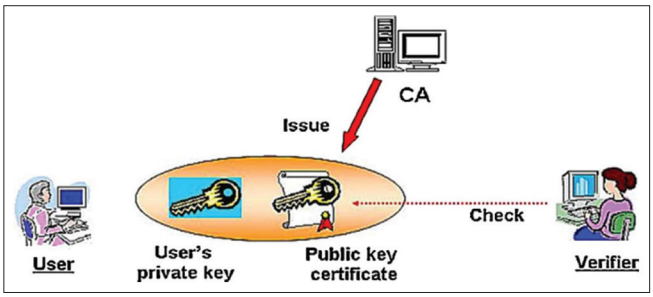

Figure 1: Public key infrastructure

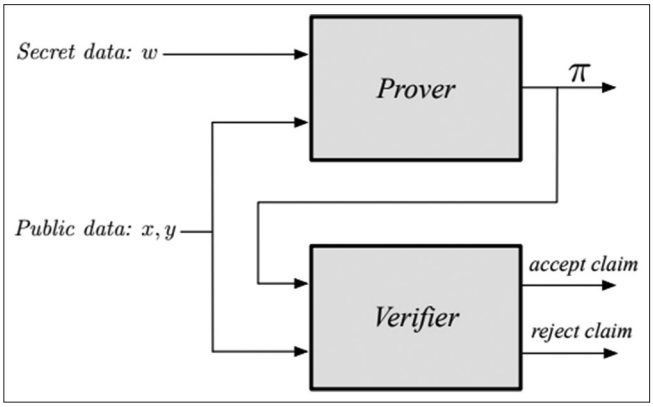

Figure 2: Generic prover and verifier interaction

indirect purposes (public health, marketing, and research).[22] In these situations, the data must be anonymized as it contains sensitive information that might threaten privacy.

In biomedical research, pseudonymization is a frequently used data-level approach. It is recommended or required as a fundamental data protection measure by several laws, rules, and recommendations.[23] The privacy-by-design measure of pseudonymization, as opposed to other PETs like differential privacy, is often implemented throughout the phases of data collection and integration. Certain areas use terms, such as "linked-anonymization" and "pseudo-anonymization" interchangeably. Some commonly used pseudonymization tools that help protect personal data by replacing identifying fields with pseudonyms are ARX (Data Anonymization Tool) and Amnesia.

DIGITAL PRIVACY REGULATIONS AND PUBLIC AWARENESS

The goal of digital privacy law is to address information asymmetry and other market failures. Some proponents have downplayed the expenses associated with digital privacy rules, despite lawmakers supposedly creating them to protect consumers.[24] A sizable portion of people think that government regulation is the required remedy for privacy issues, notwithstanding governments' own histories of digital privacy infringement.

Global Privacy Laws

The global privacy laws refer to the national and International laws and rules that control how personal data are gathered, used, stored, shared, and protected across national boundaries.[25] These regulations are intended to safeguard individuals' right to privacy in a world that is growing increasingly digitally connected and interconnected.

General data protection regulation

The GDPR requires EU Member States to exercise discretion in implementing certain GDPR requirements, such as administrative fines, to conform to local legal procedures, even while it creates standardized data protection laws that are applicable across the EU.

California consumer privacy act

The 2018 CCPA, which becomes operative in January 2020, has given Californians greater control over their personal information. It enables people to refuse to sell or share personal information with third parties, to request disclosure of the data that businesses gather about them, and to file a lawsuit against businesses that infringe upon these rights.[26] In a similar vein to the GDPR in the EU, the CCPA is an act that attempts to enhance transparency and accountability by extending consumer control, restricting organizational data behaviors, and empowering regulators to penalize non-compliant parties.

Personal data protection (PDP) bill

PDP Bill, which was produced by the Indonesian government and forwarded to the parliament for review and potential enactment into law, aims to secure the personal information of Indonesians.[27] If the PDP law is implemented with few changes, it mostly adopts the principles of international privacy procedures, such as the Organization for Economic Cooperation and the EU GDPR.

Role of Digital Literacy and Education

The capacity to learn, unlearn, and adjust to changing technology is part of literacy in today's digital culture, which goes beyond reading and writing. Digital literacy now encompasses not only technical skills, such as file management, but also cognitive and social abilities, such as interpreting user interfaces and engaging safely online.[28] As technology advances, the definition of digital literacy continues to evolve, requiring ongoing updates in educational content. To enable people to safely traverse the digital world, safeguard their privacy, and fully engage in digital settings, it is imperative that digital literacy be promoted.

Regulatory Bodies and Enforcement Mechanisms

Since they are required to make sure that businesses adhere to data protection policies and standards, regulatory agencies and enforcement frameworks are essential to maintaining digital privacy. The Federal Trade Commission in the US, promoting compliance, investigating user complaints, and punishing infractions, is the responsibility of the

EDPB in Europe and the Data Protection Board in India. These authorities embrace the norms of transparency, consent, and accountability of data handling practices.[29] There also ought to be efficient enforcement measures, such as audits, fines, and legal prosecution, which would make sure that personal information is not misused and individuals have confidence in digital platforms and technologies.

LITERATURE OF REVIEW

This section explores diverse perspectives on digital privacy, highlighting individual expectations, global legal frameworks, educational interventions, and technical models. It emphasizes interdisciplinary approaches and emerging privacy-preserving technologies to address the complex challenges in safeguarding data across digital environments.

Ahmadon *et al*. emphasize the necessity of representing the expectations of individuals regarding their privacy, which must be taken into consideration in the digital realm. Present a digital privacy idea map after that to illustrate the intricacy of putting in place efficient privacy safeguards that encompass a wide range of areas and elements. Last but not least, make use of a digital privacy model that reframes the privacy debate to propel solutions that begin with the people and their needs. The combined conversation can assist IT workers in comprehending and addressing the opportunities and difficulties related to digital privacy.[30]

Birrell *et al*. give a taxonomy of the rights and responsibilities imposed by 24 privacy laws and data protection rules selected from across the world, accounting for both those that have and have not been the focus of regular research by computer scientists. Then, arrange 270 technical research papers that look at the consequences of these laws and how technology developments might strengthen legal protections using this classification. These articles were published in computer science journals. Finally, use an interdisciplinary approach to evaluate the findings in this area and offer suggestions for further study conducted at the intersection of computer science and law.[31]

Alghamdi *et al*. (2023) an online survey comprising 26 questions about mobile privacy was completed by sixty-six computer science students from Saudi Arabian universities. The survey was broken down into five sections: Information protection, public networks, applications and permissions, browsers, and accounts and passwords. According to the poll, even while computer science students are aware of the potential hazards of their mobile devices disclosing personal information, over half of them are nevertheless eager to do so when using apps that demand sensitive or private data.[32]

Ihsan *et al*. offer a game design architecture that safeguards cybersecurity information and privacy. A platform game called Datanion was developed to assess the design and inform the public about online data privacy protection. Computer equipment, private information, and mental health are all negatively impacted by this ignorance. Players may enjoyably learn the fundamentals of cybersecurity with these games, including how firewalls operate, how to identify and steer clear of phishing websites, and how to create strong passwords. Playing these games has the advantage of increasing player motivation, engagement, and comprehension of cybersecurity ideas while also helping end users who are not experts in the field increase their awareness and understanding of cybersecurity.[33]

Ogunseyi and Adedayo offer a framework for understanding the industry's data privacy issues and analyzing the many privacy strategies that may be employed to resolve them for researchers and investigators working in digital forensics. Examine the cryptographic methods used in digital forensics to safeguard privacy in particular, and group them according to whether they facilitate multi-keyword searches, numerous investigators, or trustworthy third parties. It lists a few disadvantages of using cryptography-based techniques in digital forensics that protect privacy and offers possible fixes for the issues found.[34]

Kasera *et al*. examine earlier studies and focus on concerns related to large data security and privacy. The importance of technology in relation to big data is highlighted in the study. The issues with data privacy that big data-related technologies must deal with are discussed in this paper. The article outlines some privacy-friendly measures designed to protect privacy. To ensure large data security, the study proposes a few privacy-friendly technologies and methods.[35]

Table 1 presents a summary of the literature review, highlighting each study's focus, approach,

Table 1: Comparative analysis of literature on digital privacy technologies, regulations, and public awareness

References	Study On	Approach	Key Findings	Challenges	Future Direction
Ahmadon *et al*. (2025)	Individual expectations in digital privacy	Conceptual framework, privacy model, and concept map	Emphasizes starting privacy solutions from user expectations; highlights the complexity of privacy systems	Aligning technical protections with subjective privacy expectations	Build privacy models centered on individual control and awareness
Birrell *et al*. (2024)	Global privacy laws and regulatory-taxonomy	Legal-technical mapping of 24 laws and 270 research papers	Developed a taxonomy of rights/obligations and mapped technical research to laws	Legal-tech gaps; some laws under-studied by the CS community	Encourage interdisciplinary collaboration and tech-legal integration
Alghamdi *et al*. (2023)	Mobile privacy awareness among CS students	Quantitative survey (66 students, 26 questions)	Found awareness of risks, but high willingness to share private info	Behavioral gaps despite knowledge; risk perception versus action	Enhance privacy education and practical awareness in curricular
Ihsan *et al*. (2023)	Public education through gamified cybersecurity	Game design (Datanion) for privacy literacy	Games improve understanding of cybersecurity basics in a fun way	Low awareness among general users; accessibility of educational tools	Expand gamified tools to broader audiences for scalable impact
Ogunseyi and Adedayo (2023)	Privacy in digital forensics	Review of cryptographic techniques and proposed PPDF model	Cryptography helps in investigator collaboration without a privacy breach	Limitations in cryptographic methods, key management issues	Develop optimized cryptographic schemes and real-world PPDF implementations
Kasera *et al*. (2023)	Big data privacy and security	An examination of massive data privacy-preserving technology	identifies the instruments and systems that protect privacy in large data settings. Identifies the instruments and systems that protect privacy in large data settings.	Scalability, data complexity, and evolving attack vectors	Create adaptive, lightweight, and transparent privacy technologies

key findings, challenges, and proposed future directions.

CONCLUSION AND FUTURE WORK

In a time when data-driven technologies are shaping society more and more, Digital privacy has grown to be a major concern for governments, businesses, and individuals. The survey on digital privacy examined the intersection of PETs, regulatory approaches, and public awareness. It emphasized the importance of encryption, consent management, and anonymization techniques in mitigating data-related risks. Regulatory frameworks, such as GDPR, CCPA, and Indonesia's PDP Bill were discussed to highlight the progress made and the gaps that still exist in enforcement and public understanding. Education emerged as a crucial factor in strengthening digital resilience, with initiatives like gamified cybersecurity training showing promise in raising user awareness. Despite these advancements, challenges remain, particularly in reconciling legal frameworks with technological realities and addressing user behavior patterns that undermine privacy efforts. Bridging these gaps requires collaboration across disciplines.

Future research should focus on designing adaptive, user-centered privacy tools, expanding digital literacy programs, and refining regulatory models to accommodate emerging technologies, such as AI, IoT, and blockchain, maintaining the right to privacy in the quickly evolving digital landscape.

REFERENCES

1. Thokala VS. Improving data security and privacy in web applications ata study of serverless architecture. Tech Int J Eng Res 2024;11:74-82.
2. Goldfarb A, Que VF. The economics of digital privacy. Ann Rev Econ 2023;15:267-86.
3. Gilani SR, Al-Matrooshi AM, Khan MH. Right of privacy and the growing scope of artificial intelligence. Curr Trends Law Soc 2023;3:1-11.
4. Prajapati V. Blockchain-based decentralized identity systems: A survey of security, privacy, and interoperability. Int J Innov Sci Res Technol 2025;10:1011-20.
5. Nicola FG, Pollicino O. The balkanization of data privacy regulation. W VA Law Rev 2020;123:61.
6. Prajapati NK. Federated learning for privacy-preserving cybersecurity: A review on secure threat detection. Int J Adv Res Sci Commun Technol 2025;5:520-8.
7. Prajapati V. Exploring the role of digital twin technologies in transforming modern supply chain

management. Int J Sci Res Arch 2025;14:1387-95.
8. Amirullah I. The influence of education and public awareness on the use of digital-based public services. Int J Soc Sci Humanit 2024;1:93-106.
9. Acquisti A, Taylor C, Wagman L. The economics of privacy. J Econ Lit 2016;54:442-92.
10. Kushida CA, Nichols DA, Jadrnicek R, Miller R, Walsh JK, Griffin K. Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies. Med Care 2012;50:S82-101.
11. Khalid MI, Ahmed M, Kim J. Enhancing data protection in dynamic consent management systems: Formalizing privacy and security definitions with differential privacy, decentralization, and zero-knowledge proofs. Sensors (Basel) 2023;23:7604.
12. Gudala L, Reddy AK, Sadhu AK, Venkataramanan S. Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. J Artif Intell Res 2022;2:21-50.
13. Falebita OA, Famakinde OP. Guardians of the digital realm: Mapping key stakeholders in data privacy and digital credit universe. Int J Secur Priv Trust Manage 2024;13:13-23.
14. Modalavalasa G. Advanced blockchain mechanisms for strengthening data security and ensuring privacy in decentralized systems. Int J Recent Technol Sci Manage 2023;8:89-98.
15. Scarpi D, Pizzi G, Matta S. Digital technologies and privacy: State of the art and research directions. Psychol Mark 2022;39:1687-97.
16. Ubaidullah M, Makki Q. A review on symmetric key encryption techniques in cryptography. Int J Comput Appl 2016;147:43-8.
17. Ermoshina K, Musiani F, Halpin H. End-to-end encrypted messaging protocols: An overview. In: LNCS. Vol. 9934. Germany: Springer Science; 2016. p. 244-54.
18. Lozupone V. Analyze encryption and public key infrastructure (PKI). Int J Inf Manage 2018;38:42-4.
19. Heurix J, Zimmermann P, Neubauer T, Fenz S. A taxonomy for privacy enhancing technologies. Comput Secur 2015;53:1-17.
20. Xie M, Wang J, Chen J. A practical parameterised algorithm for the individual haplotyping problem MLF. Math Struct Comput Sci 2010;20:851-63.
21. Mallozzi P. Deploying ZKP Frameworks with Real-World Data: Challenges and Proposed Solutions. Berkeley: USA; 2023.
22. Tomás J, Rasteiro D, Bernardino J. Data anonymization: An experimental evaluation using open-source tools. Futur Internet 2022;14:167.
23. Abu Attieh H, Müller A, Wirth FN, Prasser F. Pseudonymization tools for medical research: A systematic review. BMC Med Inform Decis Mak 2025;25:128.
24. Fuller CS. The perils of privacy regulation. Rev Austrian Econ 2017;30:193-214.
25. Greenleaf G. Global data privacy laws 2019: 132 national laws and many bills. SSRN Electron J 2019:14-8.
26. Koenig TH. Florida law review towards a global data privacy standard. UF Law Scholarsh Repos 2019;71:90.
27. Rosadi SD, Noviandika A, Walters R, Aisy FR. Indonesia's personal data protection bill, 2020: Does it meet the needs of the new digital economy? Int Rev Law Comput Technol 2023;37:78.
28. Nawaz A, Kundi GM. Digital literacy: An analysis of the contemporary paradigms. Int J Sci Technol Educ Res 2010;1:19-29.
29. Kabanov I. Effective frameworks for delivering compliance with personal data privacy regulatory requirements. In: 2016 14th Annual Conference Privacy Security and Trust PST. United Status: IEEE; 2016. p. 551-4.
30. Ahmadon MA, Napp N, Rao S, Silva C, Lizar M, Gorog C, *et al*. Digital privacy: Trends, challenges, and the future. IT Prof 2025;27:69-77.
31. Birrell E, Rodolitz J, Ding A, Lee J, McReynolds E, Hutson J, *et al*. SoK: Technical implementation and human impact of internet privacy regulations. In: 2024 IEEE Symposium on Security and Privacy (SP). United States: IEEE; 2024. p. 673-96.
32. Alghamdi FA, AlAnazi WS, Snoussi S. Awareness of mobile operating system privacy among computer science students. In: 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC). United States: IEEE; 2023. p. 1-5.
33. Ihsan SN, Abd Kadir TA, Ismail NI, Yuan KZ, Jie YS. Implementation of serious games for data privacy and protection awareness in cybersecurity. In: 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS). United States: IEEE; 2023, p. 330-5.
34. Ogunseyi TB, Adedayo OM. Cryptographic techniques for data privacy in digital forensics. IEEE Access, 2023;11:142392-410.
35. Kasera S, Gehlot A, Uniyal V, Pandey S, Chhabra G, Joshi K. Right to digital privacy: A technological intervention of blockchain and big data analytics. In: 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA). United States: IEEE; 2023. p. 1122-7.