

International Journal Research Publication Analysis

Page: 01-15

CYBERSECURITY AND DATA PROTECTION: EMERGING THREATS AND PROTECTION STANDARDS

***Shweta Bisht**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies, Amity
University, Noida, Uttar Pradesh, India.

Article Received: 13 September 2026

Article Revised: 03 October 2026

Published on: 23 October 2026

***Corresponding Author: Shweta Bisht**

Student LL.M. (Master of Laws), Amity Institute of Advanced Legal Studies,
Amity University, Noida, Uttar Pradesh, India.

DOI: <https://doi-doi.org/101555/ijrpa.5800>

ABSTRACT

With the rapid growth of technological advancement everything got connected digitally. And with this expansion of technology cyber-attacks also increased which now forces states to come up with a robust infrastructure to protect its citizens from digital threats. Keeping in mind this view different nations tried to come up with have data protection and cybersecurity regulations, still due to fast paced developments in technology specifically Artificial Intelligence the cybersecurity risks and threats have been doubled. Therefore, in this digital age, the concepts of data protection and cyber security become absolutely necessary.

This paper examines the emerging threats in the digital world and how these threats can be tackled with the regulations enacted by different nations. It also explores whether the created rules and regulations are sufficient to deal with the increasing cyber-attacks and how these regulations can be made more effective to protect the data of people and systems from external attacks. An attempt has been made through this paper to understand the different safeguards that are available to protect data from cyber-attacks and how the legal framework can be improved to protect the cyber systems.

KEYWORDS: Data Protection, Cybersecurity, Digital Threats, Artificial Intelligence, Legal Framework.

INTRODUCTION

Technology is a useful servant but a dangerous master.

-Christian Lous Lange

Technology has mushroomed in the past few years which has definitely worked in the favour

of many but has also resulted in cybercrimes and data breach. To control the evolving digital threats, cybersecurity systems and data protection policies must be formulated in such a manner that it could limit and detect diverse and multifaceted digital attacks.

Evolving artificial intelligence systems has also enhanced the threats; recently in June, 2026 during a research task an OpenAI agent got unauthorised access to an Australian government health data portal and accessed public and non- public files. This data breach incident was disclosed by the Australian Prime Minister and it was seen as the first case that hacked government portal. This is an example of how technology, if remained uncontrolled, can soon become a major threat which would become impossible to manage.

Now, in a world where everything is connected digitally, opportunities for hackers increase and this give rise to phishing, data breach and misuse of personal data, ransomware and many other digital threats. Thus, it becomes necessary to have a robust cybersecurity system and data protection framework. Having a strong and effective digital infrastructure is absolutely important and to make the system more effective it is requires that those who are responsible must be held accountable. Therefore, for the purpose of free flow of data and secured networking system, different nations have built various legal frameworks for instance, General Data Protection Regulation (GDPR), Digital Personal Data Protection Act, etc. but to make these regulations effective, enforcement mechanisms must be made proper and effective, otherwise these regulations would be of no use.

Therefore, it has now become a need to balance between technological advancement and privacy of individuals or organisations; thus enacting a framework is not sufficient, it must be made effective by making cyber attackers held liable for their actions including data breach or cyberattacks.

RESEARCH QUESTIONS

1. To what extent does existing legal framework of India provide an effective protection standard for the emerging threats in the digital world?
2. What lessons can be taken from the European Union's legal framework of data protection and cybersecurity, United Kingdom's data protection laws and United States' approach to have a better digital infrastructure in India?

RESEARCH METHODOLOGY

This research article adopts a doctrinal legal research methodology where multiple legal sources have been analysed. The Constitution of India, Information Technology Act, 2000,

Digital Personal Data Protection Act, 2023, data protection laws and cybersecurity framework of European Union, United Kingdom and USA have been analysed to have a multidimensional perspective.

In this paper comparative legal analysis is used to compare different legal protection standards that govern different nations to analyse and assess the frameworks.

CYBERSECURITY AND DATA PROTECTION

Emergence of technological advancement has not just broken walls and made the world as a single territory but it has also increased the risks of cyberattacks globally. Fast paced growth of internet, social media, and now artificial intelligence has definitely helped and evolved us but it has also made our personal data available at a global level which ultimately is attracting digital threats. Thus, there is an immediate need to balance technological development and cybersecurity to protect the digital space and data of individuals.

Cybersecurity is one of the significant strategies or defences to protect technological systems and resources from digital attacks. The National Institute and Technology(NIST) defines ‘cybersecurity as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.’¹ This definition makes it clear that cybersecurity ensures ethical access of computer systems and data by authentic users only. It also specifies that the provided data would be reliable and is not tampered. It mainly ensures that the authentic services and data is available to those who genuinely require to use it. Anti-virus, firewalls, anti-malware software etc. are the examples of cybersecurity.

Data protection is another safeguard that helps the users to protect their information from any kind of threat which could lead to data loss or breach. Its main concern is to protect any data available on digital platforms from getting corrupted or stolen through any external as well as internal attack. One of the examples of data protection is the right to be forgotten which was incorporated into Article 17 of the European Union’s General Data Protection Regulation (hereinafter referred as GDPR) after the case of Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) and it is also protected under S. 12 of Digital Personal Data Protection Act, 2023 (hereinafter referred as DPDP Act) which means the right to have information erased or de- indexed from the digital platform. Digital signatures, end to end encryptions of chats, automated backups are other examples of

data protection.

Thus, a combination of effective legal measures and robust technological infrastructure is required to protect information systems and networks.

EMERGING DIGITAL THREATS

Digital revolution has led to variety of cybersecurity threats and data breach. Following are the major emerging threats:

- Using malicious software to harm computer systems
- Phishing scam to deceive people and get access to their sensitive data
- Supply chain attacks that infiltrates computer network and system
- Injecting malicious codes and software in computer systems to tamper or steal data from organisations
- Stealing passwords for financial fraud and transactions
- Intercepting messages of any two parties with the purpose of stealing sensitive information
- Blocking real users to access data or computer systems by disrupting network
- Using artificial intelligence to create fake information, videos, photos and disseminating them

¹ <https://csrc.nist.gov/glossary/term/cybersecurity>

EXISTING LEGAL FRAMEWORK RELATED TO DATA PROTECTION INDIA

In the landmark judgement of Justice K.S. Puttaswamy and Ors. Vs. Union of India (UOI) and Ors the Hon'ble Supreme Court held that right to privacy is a fundamental right and is protected under Article 21 of the Indian Constitution. From this right to privacy flowed our right of data protection but this is not the origin of our right to protect data as it has already been provided by the Information Technology Act, 2000 which was later amended and certain rules were also added that provided security measures to protect personal data. Further, Digital Personal Data Protection, 2023 was enacted by Indian Parliament to protect the data of its persons.

Information Technology Act, 2000 was enacted with the main aim of preventing cybercrime and securing digital space for the users by ensuring cybersecurity and data protection. It was amended in the year 2008, and several significant changes were made. Following are the key provisions of the IT Act before and after the amendment-

'S.43 of the IT Act specifies penalty and compensation for causing damage or deletion of any computer resource; stealing, concealing, destroying any computer resource; destroying,

deleting, altering any computer resource; causing any kind of contamination in the computer system; etc.

S.43 A provides for the compensation in case of any failure to protect data that is when any intermediary fails to protect the sensitive personal information of any person which causes loss to that person then such corporate is liable to compensate the person whose data the corporate failed to protect.

Chapter XI of IT Act is an important area which explains certain offences and punishment for those offences-

S. 65. Tampering with computer source documents.—Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Explanation.—For the purposes of this section, —computer source code¹ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

S.66. Computer related offences.—If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

S. 66A. Punishment for sending offensive messages through communication service, etc.—Any person who sends, by means of a computer resource or a communication device,— (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

66B. Punishment for dishonestly receiving stolen computer resource or communication device.—Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh

or with both.

S. 66C. Punishment for identity theft.—Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

S. 66D. Punishment for cheating by personation by using computer resource.—Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

S. 66E. Punishment for violation of privacy.—Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

66F. Punishment for cyber terrorism.—(1) Whoever,— (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by— (i) denying or cause the denial of access to any person authorised to access computer resource; or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism. (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

S. 67. Punishment for publishing or transmitting obscene material in electronic form.—

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

S. 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

S. 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.—Whoever,— (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or 26 (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or (d) facilitates abusing children online, or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form— (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or (ii) which is kept or used for

bona fide heritage or religious purposes.

S. 67C. Preservation and retention of information by intermediaries.—(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. (2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

S. 72A. Punishment for disclosure of information in breach of lawful contract.—Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

S. 84B. Punishment for abetment of offences.—Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. Explanation.—An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

S. 84C. Punishment for attempt to commit offences.—Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.’²

Under S. 43A of the IT Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were enacted with the aim of protecting sensitive data of individuals and ensuring that the body corporate take effective security measures to protect such information.

Another important legislation is DPDP Act which was introduced in the year 2023 with main objective of data privacy in India. This Act protects personal data of an individual and such data must be processed in a legal manner otherwise it would attract liability. DPDP Act

clearly mentions that data must be processed after taking consent of that individual whose information is being processed only for legal purposes and once the organisation uses the information and the purpose is served, it must delete that data. There is one exemption in this rule, that is storage limitation and right to erasure will not apply if government entities process the data for the purpose of security, public order, research, etc.

² Information Technology Act, 2000.

(https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf)

DATA PROTECTION AND CYBERSECURITY STANDARDS IN EUROPEAN UNION, UK AND USA EUROPEAN UNION

Data Protection Law

The right to protection of personal data flows from Article 8 of Charter of Fundamental Rights of European Union which clearly specifies that everyone has the right to the protection of personal data and with the aim of protecting this right, GDPR was enacted by European Union. GDPR specifically provides protection of personal data and it also ensures free movement of data within Europe. Chapter V of GDPR also allows transfer of personal data to third countries or international organisations if the security standards and measures are properly taken by the 3rd party for instance, if the 3rd country follows a certain security standard which may be similar to what European Union follows, then free flow of data may be allowed. These security measures mentioned in Chapter V ensures that the personal data of natural persons is not misused in any manner. In case of any breach of security, it also imposes penalties.

Cybersecurity Framework

For safeguarding the digital infrastructure, EU cybersecurity framework provides a comprehensive level of resilience. Following are the key legislations regarding cybersecurity applicable in EU:

1. NIS2 Directives- It was introduced in 2023 replacing the original NIS Directive with the aim of making a robust cybersecurity infrastructure to deal with the emerging cyberattacks or risks and ensuring a secured society. As cyber-attacks effect the organisations and industries, NIS2 Directions ensures that entities adopt certain risk management policies and continuously assess cyber-attacks by adopting technical measures. These directives primarily focuses on securing digital infrastructure of different significant sectors involving energy, healthcare, banking, public administration, etc.

2. EU Cybersecurity Act- It gives a permanent mandate to European Union Agency for Cybersecurity which establishes a certification framework for cybersecurity. It basically provides certification to information and communications technology products and service which ensures trust among consumers and transparency in business.

3. Cybersecurity Resilience Act- It ensures that cybersecurity standards are being followed by the 'products with digital elements' that are sold in the EU markets. It places an obligation on the manufacturers so that the products are safe from any cyber-attack.

4. Digital Operational Resilience Act- It was enacted to protect the financial sector from digital threats and cyber-attacks. Its main aim is to make sure, through risk management strategies that financial entities of EU respond and recover from any cyber-attack.

UNITED KINGDOM

Data Protection Laws

1. United Kingdom General Data Protection Regulation(UK GDPR)- It is the primary law that provides for data protection regulations. It governs how data can be processed by organisations in United Kingdom. The law is based on the European Union's GDPR model.

UK GDPR ensures that the data of individuals is secured from unauthorised entities and that it is processed in legal manner for lawful purpose only. It also provides certain rights to individuals including right to erasure, right to stop or restrict the processing of data, etc. thus, these regulations make sure that personal data of individuals is protected and in case of any breach those who responsible will be hold accountable for their actions.

2. Data Protection Act, 2018- It works along with the UK GDPR in protecting the personal data of individuals by maintaining privacy.

3. Data (Use and Access) Act, 2025 – It introduces certain changes in the existing data protection rules with the aim of enhancing public security and protecting data of individuals. It was introduced to make regulations easier for economic growth and technological innovations.³⁴

4. Privacy and Electronic Communications Regulations, 2003- It protects digital communications by maintaining confidentiality of electronic communication.

Cybersecurity Framework

1. Computer Misuse Act, 1990- It was enacted with the objective of protecting computer systems and network from digital threats including hacking, damaging data, etc.

2. Network and Information Systems Regulations, 2018- It is an important legislation which was introduced to provide effective cybersecurity measures in certain sectors important economic growth and welfare of the society.

USA

Data Protection and Cybersecurity Framework

1. Health Insurance Portability and Accountability Act (HIPAA)- It protects medical records and personal information of a patient from unauthorised users. It also standardises healthcare bills and protects healthcare insurance of those in need.
2. Children's Online Privacy Protection Act- It was introduced to protect the data of children which is available on digital platforms. It gives approval and denial authority to parents in regard of collecting any personal information of their child.
3. Gramm Leach Bliley Act- It ensures that financial institutions protect the sensitive information of their consumers.
4. Computer Fraud and Abuse Act- It protects computer system from hacking and prevents unauthorised users to access computer systems.
5. Clarifying Lawful Overseas Use of Data (CLOUD Act)- It was enacted with the aim to investigate offences related to cybercrime, sexual exploitation of children, etc. and for this investigation purpose it allows access to cross border data.

³ <https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes>

⁴ https://www.dpo-india.com/Resources/privacy_laws_in_UK/The-Data-Use-Access-Act-2025.pdf

ANALYSIS OF THE CYBERSECURITY AND DATA PROTECTION FRAMEWORK

Different states adopted cybersecurity and data protection regulations as per their needs depending upon the emerging cyber threats. India adopted DPDP Act and other guidelines to protect the data of its individuals and to prevent cybercrimes. Guidelines provided under Information and Technology Act, 2000 supplements the DPDP Act and fill those gaps which may not be covered by the newly formed legislation.

European Union's legal framework provide comprehensive guidelines to deal with the cyber-attacks that may arise in future. It protects data of its nationals from internal as well as external attacks and hold the organisations accountable in case of any breach. European Union's framework has made efforts to cover all the segments of data protection and

cybersecurity.

Even after Brexit United Kingdom's regulations regarding data protection and cybersecurity have an effective approach. Their guidelines provides a robust data protection system and risk management needs.

United States of America has a different approach from India, but their rules and regulations have made an attempt to cover different categories or areas including health related information, child security, financial sector, etc. There may be no uniform rights in terms of data protection and cybersecurity but their diverse approach tries to fulfil the data security requirements.

There is no uniformity and certainty in the laws made by these nations but they have tried to build a system as per their diverse requirements keeping in mind the evolving cyber-attacks. What is necessary is an effective digital infrastructure which could deal with the emerging digital threats and an equilibrium between the privacy rights of an individual and technological development.

FINDINGS AND SUGGESTIONS

The data protection and cybersecurity laws of different nations are comprehensive and may effective but the rapid rise in cyber-crimes especially with the developments in artificial intelligence require more than these regulations. A more robust monitoring system is required to observe the loopholes in the system and manage them accordingly otherwise there will be a tremendous rise in data breach. For instance, DPDP Act allows third party to provide information of any individual to the government under certain circumstances without informing that individual, now suppose if any unauthorised user gets access to that data, it could be misused and that individual who data has been stolen or misused may not be aware of it. This provision must be modified otherwise who would be held accountable in case of data breach here?

Technology is developing at a faster rate and legislations are required to move with the pace of these rising innovations. A common data protection and cybersecurity framework must be created by the international organisations to create certainty and uniformity in the system as it will also be convenient for the nations in terms deciding liability, accountability and jurisdiction.

For instance, the CLOUD Act of United States of America is in conflict with GDPR requirements of transfer of personal data as cross border access to data and information

creates privacy risks.

Therefore, uniformity in laws regarding data protection and cybersecurity is required. Such universal norms created must be clear and there is a balance between technological advancement and individual rights. These regulations must be transparent and effective so that organisations could infer and deter the digital attacks.

CONCLUSION

Cybersecurity and data protection are the most significant mechanisms in this technology driven world. Rising dependence of this generation on artificial intelligence, digital platforms, etc. makes us vulnerable and more prone to cyberattacks, thus security system is required to handle these threats. Different rules and regulations formulated by the nations are effective to some extent but the rising complexities in technology is resulting in cybercrimes, that is why it is expected from different states to join their hands and come forward with an uniform structure.

Nations must come up with effective remedies to deal with the evolving threats including by enacting a risk based legislation and continuous monitoring must be welcomed; complying with rules is not sufficient and organisations must be held responsible for their negligence; regulations must be clear and effective; there must be uniform and common international standards.

Data protection and cybersecurity ultimately becomes extremely necessary but it is of no use without effective implementation and accountability. But balance must be maintained between rights and developments.

BIBLIOGRAPHY

CONSTITUTION AND ACTS

1. The Constitution of India
2. Information Technology Act, 2000
3. Digital Personal Data protection Act, 2023
4. EU Cybersecurity Act, 2019
5. Cybersecurity Resilience Act, 2024
6. Digital Operational Resilience Act, 2022
7. NIS2 Directives, 2023
8. United Kingdom General Data Protection Regulation
9. Data Protection Act, 2018

10. Privacy and Electronic Communications Regulations, 2023
11. Computer Misuse Act, 1990
12. Network and Information Systems Regulations, 2018
13. Health Insurance Portability and Accountability Act, 1996
14. Children's Online Privacy Protection Act, 1998
15. Gramm Leach Bliley Act, 1999
16. Computer Fraud and Abuse Act, 1986
17. CLOUD Act, 2018

NEWSPAPER

18. Soumyarendra Barik and Anagha Jayakumar, 'In the first known AI hack of government website, a warning for public-facing systems', The Indian Express, 24th of September, 2026
19. Reuters, 'Australia says, OpenAI agent hacked govt website, checks for more breaches', The Indian Express, 24th of September, 2026

ARTICLES

20. Rohit Raikwar, 'Privacy As A Fundamental Right: Impact And Implementation After Puttaswamy' Volume VII Issue IV | ISSN: 2582-8878, IJLLR Journal, Aug 24, 2025
21. Tansi Mehrotra, 'the legal framework of data protection in india: the need for a comprehensive data protection law', Volume V Issue V | ISSN: 2583-0538, Indian Journal of Integrated Research in Law , 2025/10
22. Dr. Antima and Shweta Agarwal, 'legal dimensions of data privacy and cybersecurity in india's digital economy', Volume 13 issn: 2320-2882, International Journal of Creative Research Thoughts, 9 september 2025
23. Archana Sehrawat, Apoorva Singh, Katiyar, Vaishali and Mr. Bishnanand Dubey, 'cybersecurity laws in the digital age: gaps and recommendations', volume 5(2): 3839-3859, Journal of Informatics Education and Research, June, 2025
24. Jafar Ababneh, Abdulmajeed Alzara, Hani Attar, Ala'a Al-Shaikh, Amer Abu- Jassar and Mohamed Hafez, 'cybersecurity laws, digital crimes, and ethical considerations: a multidimensional perspective on cyber risk regulation', DOI: 10.1186/s13677-025-00824-y, Journal of Cloud Computing, June, 2026

25. CASE LAWS

26. Justice K.S. Puttaswamy (Retd.) v. Union of India *is* (2017) 10 SCC 1
27. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, Case C-131/12, 2014

WEBSITES

28. <https://www.ibm.com/think/topics/data-protection>
29. <https://www.microsoft.com/en-in/security/business/security-101/what-is-data-protection>
30. <https://www.snia.org/education/what-is-data-protection>
31. <https://www.imperva.com/learn/data-security/data-protection/>
32. <https://www.ibm.com/think/topics/cybersecurity>
33. <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html>
34. <https://www.microsoft.com/en-in/security/business/security-101/what-is-cybersecurity>
35. <https://www.microsoft.com/en-in/security/business/security-101/what-is-cybersecurity>
36. <https://www.dlapiperdataprotection.com/?t=law&c=US>
37. <https://www.upguard.com/blog/cybersecurity-laws-regulations-uk>
38. <https://www.gov.uk/data-protection>
39. <https://www.infosecurityeurope.com/en-gb/blog/guides-checklists/cybersecurity-laws-and-regulations-in-the-uk.html>
40. <https://gdpr.eu/what-is-gdpr/>
41. https://commission.europa.eu/law/law-topic/data-protection_en
42. <https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats>
43. <https://www.ibm.com/think/topics/cyberthreats-types>