



Digital Rights: A Critical analysis of Data Protection, Privacy and cyber law issues

Aradhana Tripathi

Assistant professor, Juris Law College, B. K. T., Lucknow

Corresponding Author Email: juriscollege@gmail.com

ABSTRACT:

People in the 21st century experience complete changes in their social interactions and business operations because of the digital revolution. The process generates enormous amounts of personal information which creates difficult problems that affect technology and legal matters and human rights issues. The research paper evaluates the present-day development of digital rights through its assessment of data protection systems and privacy matters and cyber law disputes. The study investigates different regulatory methods which include the European Union General Data Protection Regulation GDPR and various legal systems and new technological developments that include artificial intelligence and surveillance capitalism to find essential shortcomings in present-day security measures and recommend upcoming policy advancements. The results show that although the legal systems for digital rights have advanced significantly, the process of enforcing these rights faces multiple challenges related to jurisdictional issues and technological updates.

Keywords: Digital Rights, GDRP, Human Rights, Technology, Artificial Intelligence.

1. INTRODUCTION:

1.1 Background and Context

Scholars describe the current state of society as an "information society" which emerged because digital technologies became widely used and data became vital for all economic and social and political activities. Digital users create data through their online activities which researchers can use to study their personal habits and preferences and belief systems and social connections. Human life has become fully datafication which creates basic digital age issues that involve personal freedom and human dignity and control over personal information.

The right to privacy which exists in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights exists as a legal protection that predates the digital age. The digital space needs major changes because of existing legal frameworks which need new

definitions. Privacy rights which protect people from physical entry and direct observation become ineffective against modern techniques which include algorithmic profiling and behavioral tracking and personal data monetization.

1.2 Research Objectives

This paper pursues three primary objectives. The first objective of this research study investigates the theoretical basis of digital rights which it connects to existing human rights frameworks. The second objective of this study examines key data protection and privacy regulatory frameworks to assess their strengths and weaknesses. The third objective of this research study highlights new technological challenges which require solutions to enhance digital rights protection.

1.3 Methodology

The research conducts doctrinal legal analysis through examination of primary legal documents which include treaties and statutes and regulations and secondary sources which comprise academic literature and policy documents and empirical studies. The study uses a comparative method to analyze different legal systems which helps to reveal both shared legal principles and different legal approaches.

2. Theoretical Foundations of Digital Rights

2.1 Conceptualizing Digital Rights

Digital rights refer to the application of fundamental human rights standards in online spaces. The rights include digital technology access which enables online expression and guarantees digital communication privacy and personal data protection. Digital citizenship rights depend on multiple rights which exist in an interconnected relationship. Privacy theorists distinguish between several dimensions relevant to digital contexts. Informational privacy concerns control over personal data. Decisional privacy enables individuals to make personal decisions without being monitored or interrupted. The law protects proprietary privacy because it allows people to maintain ownership rights over their personal data. Every dimension encounters specific security challenges in digital environments which companies use to extract customer data.



Fig 1-Components of Modern Governance and Innovation Framework

2.2 The Surveillance Capitalism Paradigm

Shoshana Zuboff's concept of "surveillance capitalism" explains how economic systems function through the collection of personal data which companies use to develop systems that forecast consumer habits. Technology corporations acquire extensive user data through their software systems which they utilize to create models that forecast user behavior to increase their commercial revenue. The system functions as a power system that enables organizations to collect user data while users remain unaware of its existence and lack authority to manage its processing and usage.

The surveillance capitalism paradigm challenges liberal notions of informed consent and contractual freedom. The consent framework fails to function as a protective mechanism when digital services become necessary for social and economic participation and when terms of service become long complex and unchangeable.

2.3 Data as Power

People in modern societies use data as a tool for control which enables them to monitor others and categorize their social status and change their behavior. Governments seek to obtain data because they need it for their security operations and administrative work. Corporations need to collect data so they can increase their profits. The concentration of data power in modern society creates dangers that allow organizations to misuse data which leads to discrimination and enables them to control social behavior.

3. Global Regulatory Frameworks for Data Protection

3.1 The European Approach: GDPR as Gold Standard

The General Data Protection Regulation of the European Union which started in May 2018 serves as the most comprehensive data protection framework that exists worldwide. The GDPR establishes principles-based regulation together with its mandatory requirements which impose severe penalties for organizations that fail to comply. The main principles of the framework require data processing to follow lawful and fair and transparent methods and organizations need to restrict their data collection activities to achieve specific designated legal purposes. The principle of data minimization requires organizations to collect only necessary information while maintaining data accuracy.

The regulation establishes limits on data retention which organizations must follow to ensure their information remains accurate. The regulation requires organizations to maintain data security through measures that protect both data integrity and confidential information. The regulation provides people with numerous rights which include their right to access information and correct details and erase data under the right to be forgotten and limit data processing and transfer their data and oppose data processing activities.

The GDPR applies to all organizations worldwide that handle personal data belonging to EU residents because of its extraterritorial reach. The territorial approach has resulted in worldwide adoption of European standards because multinational companies choose to implement GDPR-compliant

operations throughout their business activities instead of using different approaches for different territories. The GDPR encounters multiple challenges during its implementation process. The regulation becomes difficult to understand because organizations must handle its intricate rules. The member states show different levels of enforcement when it comes to executing the law. The international data transfer adequacy decision mechanism creates trade obstacles for the United States and other trading partners.

3.2 The American Sectoral Approach

The present system of data protection within the United States government functions through an industry-specific framework which creates unique data security standards for each business sector and data type. The current system creates protection shortcomings because it allows certain data to remain unprotected in areas that lack specific regulatory frameworks. The government requires Constitutional Fourth Amendment protections which restrict its power to perform deep search operations while it allows companies to gather consumer information without major federal regulation. The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) which states have adopted demonstrate that people desire total privacy protection despite different privacy laws each state implements. The American system supports economic development through its emphasis on innovation because people believe that tight regulations will hinder both technology progress and business competition. The critics present evidence that this practice leads to a regulatory race which diminishes individual rights while benefiting corporate entities.

3.3 Emerging Frameworks in Asia and Beyond

The Personal Information Protection Law (PIPL) of China became operational in November 2021 and this law establishes extensive data protection standards which incorporate various General Data Protection Regulation (GDPR) principles while adding unique elements that stem from Chinese governmental control requirements for data storage and extensive state access rights. The Digital Personal Data Protection Act of 2023 in India establishes a consent-based system which enables government agencies to process personal data without requiring user permission and this system does not include any data storage requirements that existed in previous document drafts. The law expresses the efforts to find a middle ground between individual freedoms and economic progress and government authority.

The different methods create conflicts between data protection rights which people consider essential human rights and data protection rights which people see as business assets and government authority tools. The different political systems and economic approaches and cultural attitudes toward privacy rights create obstacles for the process of bringing systems into agreement.

4. Critical Issues in Contemporary Data Protection

4.1 The Consent Paradox

The primary method which most data protection systems use to establish their validity through consent face challenges during actual implementation. Privacy policies are notoriously lengthy and

complex, written in legal terminology inaccessible to average users. Research shows that people do not read terms of service, and they do not comprehend data practices which they already know about.

The total mental effort required to give proper consent for the many services people use throughout their day becomes too difficult to handle. Users typically face dark patterns through consent systems which use design elements to push them toward sharing their information without their consent. The use of pre-checked boxes together with unclear wording, and the unbalanced display of options which invade privacy and protect privacy, limits people's ability to make free decisions.

The system of granular consent which lets people choose specific data handling procedures, creates new challenges while offering potential for deceitful practices. The need for social or economic participation through mandatory services creates doubts about whether true voluntary consent exists.

4.2 Cross-Border Data Flows and Jurisdictional Challenges

Digital networks which operate without borders create conflicts with legal systems that depend on geographic boundaries which makes it difficult to enforce data protection laws. The system of cloud computing enables simultaneous data distribution across multiple legal territories. Multinational corporations operate data processing facilities in different countries to achieve operational advantages while exploiting variations in international regulations.

International data transfer systems work to solve these problems which continue to create obstacles. The European Court of Justice invalidated the EU-US Privacy Shield which served as a framework for transatlantic data exchange because the court found US surveillance methods violated privacy rights according to its judgment in the Schrems II case. The European Union and the United States established the Data Privacy Framework to replace the previous agreement but this new framework faces doubts about its ability to endure.

The practice of data localization requires that countries store their citizens' personal information within their own territorial boundaries which leads to operational problems and higher expenses while creating risks that data security will fail because backup systems cannot function across different sites. The requirements show that countries want to protect their sovereignty while allowing local police to access data instead of determining privacy regulations.

4.3 Artificial Intelligence and Algorithmic Decision-Making

The artificial intelligence systems which use personal information for their training and operational needs create new problems for existing data protection systems which were developed to handle regular data processing tasks. The machine learning algorithms which identify patterns through their predictive capabilities create essential results which directly affect people who work in the fields of employment assessment credit evaluation healthcare delivery educational systems and criminal justice procedures. The process of using algorithms for decision-making creates issues because it lacks transparency and explainability and it fails to achieve fairness and accountability standards. The deep learning systems

function as "black boxes" because their internal mechanisms which transform inputs into outputs remain hidden from all users including their developers. The lack of clarity in deep learning systems which operate as black boxes creates a conflict with data protection laws which establish transparency requirements and double back the right to receive explanations. The design of algorithms and training data results in bias which leads to either bigger or smaller social discrimination issues. Facial recognition systems demonstrate different facial recognition accuracy rates for different demographic groups because they experience higher error rates when identifying people of color and women. The historical crime data used to train predictive policing algorithms creates a system which replicates existing patterns of discriminatory law enforcement practices. The existing data protection frameworks fail to provide adequate solutions for these challenges which are specific to artificial intelligence. The European Union's proposed AI Act creates complete regulations for artificial intelligence because it divides systems into different risk categories which require different compliance standards. The European Union's AI Act creates regulations which extend too far while it lacks essential specific details about AI systems.

4.4 Data Breaches and Security Vulnerabilities

The problem of personal information breaches continues to occur with serious frequency despite the fact that authorities have started to pay more attention to data protection methods. Healthcare organizations together with financial institutions and government agencies, report continuous incidents of unauthorized data access to their protected information.

The current data protection laws require organizations to notify individuals about security breaches which serve two essential purposes. The process of notifying people about breaches becomes less effective because people develop a psychological barrier that prevents them from understanding security alerts. The actual harm from security breaches takes multiple years to develop through identity theft and fraud which creates a gap between security alerts and their actual effects.

Criminal hacking creates security vulnerabilities, while insider threats and system misconfigurations and third-party vendors with data access create additional security risks. Modern information systems create multiple ways to fail, while attackers continue to target personal data combining with their ongoing efforts against the system.

5. Privacy in the Age of Ubiquitous Surveillance

5.1 Commercial Surveillance Technologies

The current digital world contains complete tracking systems that operate continuously. The combination of web cookies and device fingerprinting and cross-device tracking methods enables researchers to create detailed profiles of user online activities. Mobile applications ask for permission to access users' location and contacts and camera and microphone functions while they gather excessive data that exceeds their necessary operational needs.

The Internet of Things enables data acquisition through its implementation in physical environments and its integration into common objects. Smart home devices and wearable fitness trackers and connected vehicles and voice assistants maintain continuous observation of their users' surroundings and physical activities. The sensing systems that operate everywhere in society create new personal data about individuals' daily activities which organizations transmit to their data centers using weak security protections that people do not know about.

The digital advertising industry uses real-time bidding systems which generate complicated data streams that transmit personal data to multiple advertisers within milliseconds thus enabling unauthorized access and secondary data usage. The advertising technology ecosystems operate as black boxes which prevent users from exercising meaningful control while they remain oblivious to the data transmission process.

5.2 Government Surveillance and National Security

The government surveillance programs which Edward Snowden leaked through his whistleblower activities show how governments possess extensive monitoring capabilities. Mass surveillance programs collect metadata from communications networks which they use to create social graphs that show population movement patterns across entire communities.

People continue to argue about whether privacy rights or security measures should take precedence. Governments require surveillance systems because these systems enable them to combat both terrorism and major criminal threats while protecting national security. Privacy advocates state that mass surveillance practices exceed acceptable boundaries because they fail to achieve their intended purposes and they violate essential democratic governance standards. Each region establishes its own legal requirements which determine how government agencies conduct surveillance activities. The Foreign Intelligence Surveillance Act in the United States establishes a distinct legal framework which allows minimal supervision of foreign intelligence operations. European countries typically require judicial authorization before surveillance operations begin yet they allow emergency situations and bulk data collection activities to occur without such authorization.

The enhanced development of surveillance systems which use facial recognition technology in public areas and employ predictive analytics to detect potential dangers creates new challenges for safeguarding fundamental rights to free speech and group membership. People who believe that others are observing them tend to limit their political expression and choose not to interact with specific people and they will stop participating in legal activities which might lead to public scrutiny.

5.3 Emerging Biometric Technologies

The specialized privacy issues from biometric identification systems use facial recognition and iris scanning and fingerprinting and gait analysis and voice recognition because biometric traits remain both unique and unchangeable. Biometric data establishes a permanent link to an individual which differs from

passwords and identification numbers because they need to be changed after a security breach. The increasing use of facial recognition technology by both government agencies and commercial businesses allows them to continuously monitor and identify people in outdoor areas. The technology establishes permanent records of human movement, which used to be too pricey to track, because it changes how people used to walk through public areas without being seen. Multiple regions have begun to enforce rules that restrict facial recognition technology. The AI Act which the European Union proposed establishes strict rules which restrict biometric identification methods used in public areas. San Francisco and other US cities have enacted a prohibition on facial recognition technology that government agencies can use. The speed of deployment continues to increase while comprehensive regulation of the technology remains unavailable.

6. Enforcement Challenges and Gaps in Protection

6.1 Regulatory Capacity and Resource Constraints

The complete data protection legal framework fails to operate effectively because authorities lack sufficient resources to enforce their duties. The organization has received more complaints and breach notifications and additional entities that need supervision than its current resources can handle for investigation and enforcement work. Modern data processing requires advanced technical skills which regulatory agencies find difficult to obtain because private companies offer better salary packages. The lack of specialized knowledge prevents organizations from effectively monitoring algorithmic systems and cloud technologies and new scientific advancements.

Enforcement actions tend to focus on large, visible violations by major corporations that attract media attention, while smaller violations and systematic non-compliance by less prominent entities receive limited scrutiny. The process of enforcing regulations creates different levels of punishment that vary between organizations.

6.2 The Compliance Industry and Performative Compliance

The data protection compliance industry has experienced significant growth because organizations choose to invest in multiple resources which include privacy officers and consent management platforms as well as data mapping tools and consulting services. The compliance system focuses on enforcing rules instead of delivering actual protection for individuals rights.

Websites display cookie consent banners which create user friction and annoyance because they offer only minimal choices while users must accept cookies to access website functions. Organizations use privacy policies to protect themselves legally through disclosure but these documents become longer because no one reads them. Organizations use data protection impact assessments to fulfill requirements instead of conducting real assessments of their potential risks.

The organization fulfills its regulatory obligations through visible compliance efforts which ultimately weaken the system's protective functions. Organizations show their commitment to compliance

through financial investments yet their actual data handling practices do not lead to reduced privacy risks or better user privacy controls.

6.3 Accountability Gaps in Data Supply Chains

The current methods used to process data require multiple interconnected systems which include data controllers and processors and sub-processors and third-party entities. One organization collects personal data and shares it with multiple partners who use the information for different purposes such as analytics and advertising and fraud prevention and service delivery. The existing accountability frameworks face challenges because they distribute responsibility across multiple parties. Users who interact with primary service providers actually grant permission to access their data without understanding which data will be shared with other entities. Data controllers and processors establish contractual relationships which expand their responsibilities; however, organizations find it challenging to monitor their adherence to these obligations.

It becomes difficult to identify which parties are responsible when an incident causes harm to others. The security breach happened because the data controller selected incompetent vendors or the processor failed to secure their systems or the sub-processor acted negligently. The process of establishing liability depends on tracking data movements and contractual arrangements which may involve multiple legal jurisdictions and corporate organizations.

7. Recommendations for Strengthening Digital Rights Protection

7.1 Moving Beyond Consent-Based Frameworks

The flaws found in existing consent methods require data protection systems to establish stricter rules that prevent organizations from collecting and using data without proper consent. Organizations must follow purpose specification rules because these rules require them to use data only for the purposes specified at the time of data collection. Organizations must implement data minimization practices because they must only collect essential data needed to achieve specific operational objectives. Organizations must establish data retention rules which require immediate data deletion after it no longer serves its intended purpose, thus preventing data from persisting indefinitely. The law requires special protection for sensitive data categories that include biometric information and exact location details and all health-related and sexual orientation and political and religious belief inferences, which can only be processed in exceptional cases, even with user consent.

7.2 Enhanced Accountability and Enforcement Mechanisms

The present data ecosystem needs more resources than existing regulatory bodies possess to handle its current size and intricate system requirements. The funding must support two essential needs which include offering competitive salaries to technical experts and providing essential monitoring and investigation tools and maintaining enough staff for complete operational oversight. The private rights of action which allow individuals to sue for data protection violations without demonstrating actual damage,

will establish extra accountability requirements. Collective redress mechanisms permit individual claims to be combined, which enables economical litigation and produces stronger deterrent effects through the possibility of class action liability. Publicly accessible algorithmic impact assessments for high-risk AI applications, which should be carried out by independent auditors, will allow external parties to evaluate algorithmic fairness and accuracy and proper usage.

7.3 International Cooperation and Harmonization

The jurisdictional challenges that exist between countries make it necessary for nations to establish international cooperation systems. Data transfers between countries will be possible through mutual recognition agreements because they allow jurisdictions with similar protections to exchange data while upholding their security standards despite the fact that full legal system harmony remains unachievable. International frameworks for government access to data should balance legitimate law enforcement and security needs with privacy protection through requirements for specificity and proportionality and independent judicial oversight and transparency reporting. Global technology companies must implement the highest applicable standard throughout their operations because this approach prevents them from creating different privacy protections according to different jurisdictions while allowing them to meet specific legal requirements that exist in different locations.

7.4 Addressing Emerging Technologies Proactively

Your training data extends until the month of October in the year 2023. The anticipated privacy effects of developing technologies should be addressed through preventive methods instead of waiting for technology deployment and resulting harm to occur. Privacy by design principles should be embedded in technology development through regulatory requirements and standardization processes and professional norms. The sandbox environments of this system enable testing of new technologies through controlled settings which include advanced monitoring to detect potential dangers before technology becomes widely used. The sunset provisions of this system require scheduled reauthorization which depends on verifying system advantages and proving that risks have been reduced to acceptable levels thus preventing the permanent use of systems that violate privacy rights. Public funding should support research into privacy-enhancing technologies which include differential privacy and homomorphic encryption and federated learning and secure multi-party computation because these technologies offer alternatives to centralized data aggregation that would enable secure achievement of computational objectives with reduced privacy threats.

8. Conclusion

Digital rights serve as an essential human rights area in which societies today work to protect their citizens from rights violations while addressing core issues which involve personal freedom and human dignity and social control over digital information. Despite the progress in developing data protection and

privacy laws, organizations still face major difficulties when they need to protect their data against unauthorized access from their business partners and government entities.

Existing frameworks fail to handle current data ecosystems because their dominant consent-based model does not match the power imbalance between individuals and data collectors who possess superior control over their personal information. The development of protective measures requires organizations to move from their current consent-based system toward creating strict rules which will govern how their data can be used.

The combination of cross-border data flows with algorithmic decision-making and continuous surveillance systems and new biometric identification methods creates new security problems which require both updates and expansions of existing privacy protection methods. The complete evolution of regulatory frameworks needs to occur so that organizations can address emerging issues while upholding their commitments to fundamental rights standards.

Regulatory bodies need to invest actively in building their enforcement strength through two main methods which include developing their operational capabilities together with new methods to hold organizations accountable through algorithm assessments and collective legal actions while working internationally to resolve digital network jurisdiction challenges. Legal changes together with new technology for privacy protection should work together to create better protection for people who hold formal rights.

Digital rights will determine how societies evolve because their development will decide whether datafication results in increased surveillance and control with growing social inequality or lets people maintain their digital self-determination rights. The decision-making process needs ongoing evaluation through critical analysis and effective policy solutions while citizens should stay involved with technological systems that now control their daily lives.

REFERENCES

- [1] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.
- [2] Solove, D. J. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 126(7), 1880-1903.
- [3] Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.
- [4] Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.
- [5] Raab, C. D., & Koops, B. J. (2009). Privacy Actors, Performances and the Future of Privacy Protection. *International Review of Law, Computers & Technology*, 23(3), 179-193.

- [6] Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
- [7] Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.
- [8] Citron, D. K., & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, 89(1), 1-33.
- [9] European Union Agency for Fundamental Rights. (2018). *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union.
- [10] Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford: Oxford University Press.

Cite this Article:

Aradhana Tripathi, "**Digital Rights: A Critical analysis of Data Protection, Privacy and cyber law issues**", *Aviradha International Journal of Law and Legal Studies (AIJLLS)*, ISSN: Applied (Online), Volume 1, Issue 1, pp. 01-13, October-December 2025.

Journal URL: <https://ajjls.com/>

DOI: : <https://doi.org/10.65785/ajjls.v1i1.01>

