AI and Telecommunication Privacy: Rethinking Legal Protections against Algorithmic Surveillance

Submitted: 2 February 2025
Reviewed: 20 April 2025
Revised: 5 July 2025
Accepted: 8 August 2025

Sheikh Inam Ul Mansoor*
https://orcid.org/0000-0001-8636-4769

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v17i2.57121

Abstract

[Purpose] This paper explores how artificial intelligence (AI) can aid in the integration of telecommunication networks, and how it will affect privacy. It talks about the threats that AI brings to consumer privacy, such as algorithmic monitors that are challenging and explain what does and doesn't seem to be working to protect consumer privacy in present legislation. The purpose is to study the integration of AI and telecommunication data privacy to find that there is a need to have new set of laws and weighty privacy protection in this age of digital transformation.

[Methodology/approach/design] The paper critically analyses historical interactions of AI with telecommunication privacy, discusses how existing policies work and what gaps exist in current legislation. Examining the validity of such risks in telecommunication networks when it comes to privacy violation, data exploitation, and the need for clear regulations of the system. Moreover, the methodology proposes an interdisciplinary approach comprised of legal, technological, and ethical stakeholders to handle the problems in question.

[Findings] And finally, the paper concludes that the existing legal frameworks cannot secure privacy of consumer in the framework of AI-based telecommunication systems. That is why it emphasizes the need for international privacy standards, independent audits and robust national regulatory bodies. It calls for new legal guidelines that would guarantee transparency, responsibility and consumer consent as well as foster collaboration among the different stakeholders to improve privacy protection and data control in AI systems.

[Practical implications] The paper parallels strong privacy protections and ethical practices of AI in telecommunication systems. It calls for new legal and international standards of privacy. The intention behind these recommendations is to maintain the privacy and control of the consumer's data within AI powered systems.

*Assistant Professor of Law, Symbiosis Law School, Hyderabad Campus, Symbiosis International (Deemed University), Pune, India. E-mail: sheikh.mansoor@slsh.edu.in.

[Originality/value] Finally, this research uniquely combines legal, technological, and ethical aspects of litigation involving AI and privacy in telecommunications all into one. It draws the gaps in the existing laws and provides innovative solutions for privacy protection. The modern concern addressed by the paper is privacy, and the value of the paper is in the interdisciplinary approach it uses to address that specific concern.

Keywords: Artificial Intelligence, Surveillance, Ethics, Privacy, Technology, Society, Data.

INTRODUCTION

A technological breakthrough emerged when artificial intelligence fused with telecommunications networks to reengineer both network operations and service delivery. Telecommunications face two divergent transformations from AI adoption which brings operational improvements while creating substantial privacy and surveillance challenges and data protection dilemmas **(Khan, 2023).** The exponential growth of AI-driven innovation across network automated service along with predictive maintenance coincides with profound concerns about user privacy rights because these systems collect massive user data for analytical purposes **(Secundo et al., 2024).** Telecommunication expands through technological evolution which challenges outdated legal systems because these frameworks lack sufficient skills to manage complex artificial intelligence development in telecommunications **(Balmer et al., 2020).** The initial telecommunications network design featured simple connections which have evolved into complex information sharing systems worldwide. The implementation of AI technology optimizes network control procedures while producing better services and superior customer interactions as it accelerates telecommunications growth **(Li et al., 2020).** Machine learning algorithms together with natural language processing provide telecommunication systems with predictive abilities and personalized service while carrying out routine human tasks with automated systems **(Priyadarshi et al., 2023).** Due to its capabilities AI lets networks develop autonomous systems called "self-optimizing networks" (SON) that detect problems independently and execute solutions instantly. Mobile telecommunications adopt artificial intelligence to monitor user datasets for application optimization and consumer behavior prediction **(Mao et al., 2022).**

The undeniable advantages of AI in telecommunications carry serious privacy risks for private information distribution among users. Telecommunications networks naturally deal with a large quantity of personal and sensitive information encompassing call history alongside the way people use the internet and their locations and their communications' contents **(Agubor et al.,**

2015). By integrating artificial intelligence into these networks the collection of data becomes both larger in scale and more comprehensive which permits increased monitoring practices that make invasions of privacy easier to execute **(El-Hajj, 2025).** Unparalleled speed in data processing by AI systems creates complex privacy protections because service optimization collections merge with unauthorized surveillance practices **(Mumuni & Mumuni, 2025).** The growing urgency for legal protection of privacy rights emerges because technological progress exceeds the speed of legislation which safeguards individual privacy. Technical communications require absolute protection of individual privacy. Service provider and consumer trust rests on the fundamental human right and foundational principle of privacy when data is shared in electronic contexts **(van Daalen, 2023).** Personal data enjoys protected status through multiple international human rights treaties starting with the Universal Declaration of Human Rights and continuing with the European Convention on Human Rights and other instruments **(Bygrave, 1998).** Telecommunications companies maintain vital personal information and must protect it from unauthorized access together with misuse and exploitation **(Sargiotis, 2024).** Privacy breaches in telecommunications networks result in identity theft alongside financial fraud while damaging reputations which seriously devalues trust in providers and the legal procedures meant to guard customers **(Gorrepati et al., 2021).**

Telecommunication systems continue to experience an increase in AI-driven surveillance tools which raises significant dangers for individual privacy because of these systems invasive capabilities **(Balmer et al., 2020).** Continuous user behaviour monitoring made possible by AI algorithms absorbs real-time data collection along with analysis capabilities permits illegal individual profiling but it raises concerns about discrimination and privacy breaches of confidential communications **(Ranjan & Kumar, 2022).** Law enforcement agencies with help from national security entities can use modern artificial intelligence systems to tackle cyber threats yet publicity rights might face encroachment from excessive operational reached of these systems **(Sachoulidou, 2024).** The growing dependence on data-driven methods poses serious risks because unclear AI model accountability undermines privacy protection that legal safeguards are meant to deliver **(Saura et al., 2021).** Proposed telecommunication privacy regulations create fundamental legal parameters which govern how AI systems function. Both domestic and international laws function to reconcile privacy safeguard needs against technological progress objectives **(Sumartono et al., 2024).** Since AI advancement advances at a speed that legislators find difficult to match their ability to establish well-functioning regulatory frameworks. Telecommunication privacy laws require essential development to keep pace with the advancements of algorithmic surveillance risk and challenges posed by artificial intelligence

technologies **(Lakhani, 2024).** The legal framework demands reinvention because appropriate adaptable concepts must be established to specify how data is used properly alongside processes needing transparency while ensuring responsible privacy-related violations receive proper consequences **(Sampson, 2021).** Privacy law establishes its essential role through the General Data Protection Regulation (GDPR) and parallel data privacy regulations from the European Union that mandate strong personal data protection requirements across territory **(Hoofnagle et al., 2019).** Telecommunications regulations provide essential guidelines which determine how Artificial Intelligence systems must function during data acquisition while complying with user authorization requirements and maintaining user rights protection **(Penttinen, 2013).** Despite their importance AI-based regulations face challenges because continued AI development makes them less effective over time. Lawmakers must take a dedicated approach to regulate AI technology in telecommunications because privacy protection stands against innovation framework development in ongoing legal discussion **(de Almeida et al., 2021).**

An intersection of privacy in telecommunication with artificial intelligence, with emphasis on the legal challenges of algorithmic surveillance is what is studied in this paper. It evaluates the validity of currently existing legal frameworks to locate gaps in the privacy protection and proposes to make legal changes that improve privacy safeguards yet do not hinder technological development.

Research Question: Within this context the central research question considered in this study is: 'What are the legal reforms required to deal with the problems presented by the use of algorithms in the telecommunication systems based on AI in such a way that is compatible with robust user privacy while enabling continued technological advancement.

Methodology: In this paper, the qualitative, interdisciplinary approach towards the analysis of the AI driven surveillance in the telecommunication systems is used. To identify regulatory gaps, it does the work of doctrinal legal analysis of the existing privacy laws. Based on a review of policies, case law and academic literature, privacy risks and data exploitation, the study is conducted. The methodology incorporates legal, technological and ethical perspectives, aiming to propose reforms, which are sufficiently robust in protecting one's privacy, yet still allowing for technological development.

THE RISE OF ALGORITHMIC SURVEILLANCE IN TELECOMMUNICATION

Artificial intelligence integration (AI) in telecommunications networks drove swift advancements within network administration while transforming

service provisioning and user participation procedures **(Qi, Wu, Li, & Shu, 2007).** Telecommunications networks obtained excessive complexity and interconnectivity, making AI transform from an operational task helper into a powerful influence guiding network system operations **(Sergiou et al., 2020).** Algorithmic surveillance represents the primary effect that emerges from this structural evolution. AI algorithms now analyse massive datasets quickly and detect user patterns, but this development brings essential privacy risks to user data security **(Murphy, 2017).** The steady expansion of Artificial Intelligence technologies in telecommunication settings produces improved surveillance methods that collect large datasets for efficiency optimizations alongside user prediction capabilities **(Balmer et al., 2020).** The adoption of algorithmic surveillance in the telecommunication sector brings both hindrances and possibilities which call for detailed research about data privacy preservation **(Park & Jones-Jang, 2023).** Machines employ AI algorithms for algorithmic surveillance which examines network or system members' actions and behaviours while tracking their movements. The telecommunications system uses algorithmic surveillance to gather phone call records and text messages and examine internet usage behaviours while tracking user locations **(Lyon, 2014).** Such surveillance tools use algorithms that search for patterns so they can predict upcoming actions while generating data-informed insights from previous records. Modern telecommunications generate large volumes of data which algorithms leverage to perform detailed examinations of both group and single user interactions **(Kastouni & Lahcen, 2022).** AI systems automate this procedure, so they monitor large populations of users continuously and independently of human supervision. Algorithmic surveillance tools implemented by telecommunications systems improve service delivery and network efficiency but create privacy concerns because they extract vast amounts of personal data which could be misused by untrusted entities **(Fontes et al., 2022).**

Telecommunication networks embrace algorithmic surveillance primarily because of Artificial Intelligence which functions as their main catalyst. Through usage of AI technologies including machine learning and natural language processing telecom companies seem able to analyze and understand enormous datasets automatically **(Edozie et al., 2025).** Telecommunication network management, as well as fraud detection services and optimized customer services with personalized service offerings became possible through these technologies **(R. H. J. & Mohana, 2022).** AI system sophistication enables telecom providers to analyse data in real-time which allows immediate network conditions and user need adjustments. The real-time data processing capacity that AI offers user behaviour surveillance while presenting concerns about striking the right balance between service development and user privacy protection **(Balmer et al., 2020).**

The basis of algorithmic surveillance systems depends on accumulated data. Networks containing telecommunication data collect abundant information about user interactions that create behavioural profiles. The use of each mobile communication type and internet session automatically produces digital tracking information that leads to complete user profiles **(Murphy, 2017).** The data patterns in user behavioural traces enable predictive updates through machine learning models which provide anticipatory user needs without request. AI systems perform telecom network optimization tasks by processing traffic statistics to anticipate emerging network congestion thus enabling proactive resource distribution to reduce performance interruptions **(Ranjan & Kumar, 2022).** Recommendation engines designed through AI technology construct individualized product and content suggestions by analysing both user activity sessions and demonstrated preferences. The service-associated powers these systems offer grant providers continuous observation of user activities that generates concerns about privacy threats and improper access of personal information **(Fanca et al., 2020).**

What makes user behaviour monitoring through AI technologies vital for privacy protection. Telecommunications companies maintain complete control over users' highly sensitive personal information because they gather data as part of their operations **(Shin et al., 2022).** Phone companies detect user activity through monitoring communication logs and how users browse along with location monitoring and occasionally they collect biometric information. Algorithms powered by AI generate composite profiles of users by linking their data activity which becomes valuable for personalized marketing and platform customization and police monitoring operations. Data collection approaches remain poorly transparent to users while existing consent procedures fail to adequately alert users about their surveillance scope **(Whang et al., 2023).** The reduced level of transparency breaks down the essential requirement of informed consent as specified in privacy laws throughout Europe under GDPR and California through CCPA regulations **(Singhal et al., 2024).** Beliefs about privacy erosion in telecommunications sector have grown stronger since AI started delivering predictive analytics along with real-time surveillance capabilities. Moreover, AI algorithms both analyse existing user conduct in real-time using recorded historical patterns to generate projections of future user behavior **(Fast & Jago, 2020).** Predictive analysis by AI systems determines potential network congestion times through examination of user service patterns and helps discover customers directed toward customer defection. Time-to-time prediction methods allow for early issue prevention while generating new prospects for focus that tracks beyond active movements. Predictive analysis allows telecom entities to detect customer requirements prior to their actual declaration thus enabling useful

interventions yet raising privacy concerns **(Fu et al., 2023).** User privacy has become more valuable in today's society yet increasing company capability to forecast user activities using algorithmic models triggers essential doubts about the acceptable extent of societal surveillance.

Artificial Intelligence (AI) plays an active role in developing both network design principles and operational systems for telecommunications frameworks. Traditional telecommunications networks required human operators for all steps of network management including troubleshooting and resource allocation as well as network optimization **(Alhammadi et al., 2024).** Today's AI-derived networks run as self-optimizing networks (SONs) which automatically fix issues through autonomous detection mechanisms apart from human supervision. AI networks fulfill several roles by automatically adapting according to demands and routing protocols and by finding security risks during real-time monitoring. These technological advancements improve telecommunication system performance yet create expanded opportunities for system surveillance capabilities. Autonomous networks have independently acquired the ability to monitor all user activity because they operate under reduced supervision and input control from users or monitoring bodies. The lack of awareness among users about ongoing surveillance operations together with minimal authority to control collected data maintains serious privacy concerns **(Dev et al., 2023).** Telecommunications networks based on artificial intelligence technology prompt new difficulties for regulatory enforcement. Traditional telecommunications systems original legal standards struggle to handle the intricate aspects of algorithm-based surveillance information processing **(Balmer et al., 2020).** Regulatory frameworks of the GDPR were established when personal data involved human-controlled explicit collection and processing measures. The fast AI technological deployment in telecommunications has generated continuous real-time data collection which proves difficult to monitor. Hardwiring AI systems to function autonomously turns the enforcement of privacy regulations into a daunting problem for operators. Telecom organizations need to build a system between AI-driven network optimization advantages and legal privacy regulations and user data protection requirements **(Hoofnagle et al., 2019).**

The transformative power of AI over telecommunications networks necessitates updated laws and regulations now because the demand is becoming critical. To protect users' rights while promoting telecommunication system innovation our privacy laws need modernized approaches that handle algorithmic surveillance challenges **(Balmer et al., 2020).** The existing consent models need re-evaluation while transparency requirements must be strengthened, and individuals need additional protection against personal data misuse. Medium to effective regulatory controls become unattainable because regulatory reforms fail

to address the surge of algorithmic surveillance within telecommunications which threatens privacy protection and leads to an excessive surveillance environment.

Current Legal Frameworks for Telecommunication Privacy

Telecommunication technology advancement speeds up rapidly because of artificial intelligence (AI) and machine learning integration while creating major privacy concerns. Telecommunication providers now collect large volumes of user information using sophisticated algorithms to process and track data accumulated through their platform. The contemporary legal safeguards of telecommunication privacy face increasing tensions because governments and international bodies must work together to defend privacy rights and support technological development **(Kastouni & Ait Lahcen, 2022).** The existing legal protections intended to guarantee telecommunication privacy remain inadequate for handling the complex challenges posed by algorithmic surveillance techniques. The current lack of sufficient legal protection puts significant strain on privacy enforcement authorities who oversee privacy rights in data-driven interconnected societies **(Wang et al., 2017).** The interpretation of telecommunication privacy standards differs significantly worldwide because national laws blend their individual legal histories with existing political structures and protection priorities. The development of telecommunications privacy laws originally prioritized tracking voice communications while maintaining basic transmission confidentiality for traditional networks in numerous legal territories **(van Daalen, 2023).** Under these laws companies must establish technical measures because they require limitations on unauthorized access to communication content. Telecommunication privacy protection at the national level depends largely on three fundamental legal frameworks consisting of constitutional safeguards and telecommunication-focused legislation together with data safety guidelines **(Bélanger & Crossler, 2011).** The United States protects telecommunication privacy through regulations created by the Federal Communications Commission (FCC) combined with rules from the Communications Assistance for Law Enforcement Act (CALEA) that require service providers to assist police investigations **(Guhl & Pendse, 2008).** Under the Electronic Communications Privacy Act of 1986, the government faces restrictions when trying to access communications without obtaining a warrant. The protective frameworks once designed to regulate telecommunications technology now face challenges from newer monitoring tools such as cloud storage in addition to artificial intelligence and algorithmic data collection that deliver persistent real-time user tracking **(Kabay, 2003).** Telecommunication privacy within the European Union receives protection through both the General Data Protection Regulation (GDPR) and the e-Privacy Directive that deliver

strong privacy safeguards for users' personal information and communications. Under GDPR requirements data processing operations must adhere to detailed standards that specify requirements for consent along with transparency standards and personal data access and erasure rights **(de Carvalho et al., 2020).** The Lei Geral de Proteção de Dados also known as General Data Protection Law (LGPD) that regulates personal data in Brazil is based on the GDPR (Carvalho *et al.*, 2022). However, there are no such specific AI or surveillance regulations (Filho et al., 2024). Despite rising digital surveillance, ethics for the affected, privacy risks and control, are abysmally weak (Rocha et al., 2024). Gaps in the regulation and inequality are further deepening the public distrust; and hence there is a demand for stronger, more inclusive, and ethical ways of governing the AI technologies. Telecom providers must follow the e-Privacy Directive requirements by protecting both the confidential nature of electronic communications while preventing unauthorized interceptions or access to users' data. The implementation of GDPR requirements confronts major obstacles within algorithmic surveillance despite reaching high data protection levels. AI systems analyze massive datasets through processes that lack both user consent and understanding, thereby damaging the transparency requirements of the General Data Protection Regulation **(Brunner, 2018).**

The speed at which AI technologies and algorithm surveillance grow exposes deficiencies for telecommunication privacy protection within current legal frameworks. The current legal guidelines rely on concepts concerning privacy protection that focus primarily on blocking unapproved communication access while barring unwanted information spread. The real-time data gathering nature of intelligent systems which require minimal human supervision reveals new privacy concerns that exceed legal frameworks first designed for traditional privacy protection **(Fontes et al., 2022).** Discrimination-based profiling by AI algorithms extracts privacy-sensitive information from benign user data including browsing records alongside location details and social network communications. The resulting inferences often escape legal interrogations comparable to those imposed upon actual communication content leaving numerous privacy protections without coverage **(Moussawi et al., 2024).** Many governments have passed data protection laws, yet these regulations fail to address effectively the special problems caused by algorithmic surveillance operations. The place where I must focus is the absence of acceptable legal consent. Classic telecommunication privacy regimes gather user consent beforehand when collecting their communication information through traditional protocols **(Seetharamu et al., 2024).** As AI becomes prevalent the practice of obtaining general consent from users shows insufficient clarity regarding data extent of analysis and desired usage purposes. Due to their opaque nature and algorithm

complexities, users find it challenging to grant informed consent which violates multiple privacy principles protected by laws that value both transparency and autonomy **(Jones et al., 2018).** AI systems that multiply their data collection sources create complicated barriers protecting personal privacy information. Telecommunications data typically pairs up with information fetched from multiple platforms including social media to build detailed personal profile databases **(Zhang et al., 2021).** Data triangulation between multiple platforms raises major privacy concerns because users lack full knowledge about the extent to which their data will be shared. While current national regulations for telecommunication privacy do not provide specialized rules regarding cross-platform data aggregation and sharing they create major gaps in legal protection **(Quach et al., 2022).**

The creation of international harmonized frameworks for telecommunication privacy faces substantial difficulties because national priorities for privacy conflict with their diverse approaches to privacy frameworks. Through international treaties including the International Telecommunication Union's (ITU) Telecommunication Standardization Sector member nations receive guidelines for protecting telecommunications security as well as preserving confidentiality **(Hill, 2014).** Despite their existence, these frameworks provide weak enforcement abilities and do not clarify whether they should extend to new tech including AI. Gaps in worldwide standards regarding data protection increase difficulties when managing telecommunication privacy across different regulatory environments which telecom providers operate due to multiple nations' laws **(Rodrigues, 2020).** International groups try to protect people's privacy through the OECD's Privacy Guidelines by promoting member countries to develop legislation supporting digital economy privacy rights. User consent together with transparency and accountability form core elements of the OECD guidelines which regulate personal data collection and processing **(Mattoo & Meltzer, 2018).** Despite their significant influence, these guidelines fall short of treaty status and fail to manage the sophisticated challenges created by AI surveillance systems. Regional agreements including both the Asia-Pacific Economic Cooperation (APEC), Privacy Framework and the African Union's Convention on Cyber Security and Personal Data Protection offer minimal direction regarding algorithmic surveillance issues **(Greenleaf, 2009).** The oversight of algorithmic surveillance poses considerable difficulties to existing monitoring institutions. The excessive complexity of AI systems prevents regulators from evaluating whether telecommunications firms obey privacy laws through their algorithmic practices **(Power et al., 2021).** Because of algorithm complexity regulators need specialized technical understanding both of algorithmic operations and related data processing procedures. The requirement

for specialized expertise in algorithmic system operation leads to problems that hinder effective oversight and accountability mechanisms. The gap in privacy protections becomes worse each time new AI technologies emerge because regulators struggle to maintain pace with these advancements **(Timan & Mann, 2021).**

Challenges to Telecommunication Privacy in the Age of AI

The transformation of technology into contemporary systems creates dramatic obstacles for privacy defence mechanisms. Next-generation telecom data management becomes possible through AI operations which allow companies to handle enormous individual data sets to generate privacy threats beyond traditional predictions **(Verhoef et al., 2021).** The combination of surveillance risks poses dual threats to communication privacy along with extended ethical and legal frameworks affecting consumer rights as well as personal data protection. The growing presence of AI systems in telecommunication operations creates expanding privacy risks and escalating ethical questions about surveillance which needs pressing intervention by legal experts and policymakers and regulatory organizations **(Power et al., 2021).** The extensive quantity of collected data represents a fundamental obstacle to privacy in telecommunication systems under current artificial intelligence production methods. The existing telecommunication privacy laws protect both message content and metadata, but their primary function is to stop unauthorized interception and secure message confidentiality. The emergence of AI technologies enables telecommunication companies to obtain massive user information which extends past basic communication metadata **(Cuzzocrea & Soufargi, 2025).** Modern system tracking demonstrates abilities to monitor online actions of users simultaneously alongside their physical locations and platform interactions spanning social media to search engines and shopping services. The collected data enables organizations to develop comprehensive consumer profiles which help them predict user behaviour alongside psychological attributes and preferences. The depth of collected personal information leads to great privacy concerns beyond standard communication content because the systems capture deeply personal aspects of people's lives **(Akram et al., 2021).** AI surveillance of telecommunication networks produces many ethical considerations. Machine learning algorithm-based AI systems function without providing transparency about what data gets collected or how the data gets used as well as what purposes these activities support. Complex algorithms in combination with their unclear operate as obstacles that interfere with obtaining users' knowledge-based consent **(Edozie et al., 2025).** Traditionally speaking users need to explicitly allow data collection under privacy laws yet AI systems create complicated situations.

Continuous algorithm operations gather user information while lacking transparency and understanding from users to make autonomous choices regarding their personal data. Due to how AI surveillance systems operate they frequently use methods that allocate higher tracking to specific social groups such as victimized populations and politically exposed people causing worry about biased data processing discrimination **(Power et al., 2021).**

The main topic of debate within ethical discussions concerns the accountability systems must demonstrate. Algorithms which analyse consumer data face an inherent risk of containing biased preferences while making choices that shape advertising direction or control insurance costs and service eligibility. System training requires historical data which occasionally exhibits invisible biases that ultimately produce discriminatory results **(Machado et al., 2023).** When AI algorithms receive training data from past discriminatory systems, they frequently continue performing the same biased actions which produce undeserved mistreatment against specific population segments. System decision processes remain unclear which obstructs people from challenging or contesting these actions. Consumer rights lose vital protection because non-existent oversight systems fail to address ethical concerns which worsen because there is no established accountability system in place **(Belenguer, 2022).** The way AI surveillance influences consumer rights conflicts sharply with telecommunication privacy regulations. Personal data has become a valuable resource in our digital times because companies can convert it into revenue. By utilizing AI telecommunication companies can transform consumer data points into critical business intelligence for marketing analysis while developing new products while optimizing their services. The conversion of personal information into business commodities threatens to violate consumer rights for both privacy preservation and personal information control **(Singh, 2024).** The surveillance processes which leverage artificial intelligence abuse personal behavioural patterns to reduce consumer autonomy while failing to offer meaningful control over the data collection. The methods organizations use to commodify personal data lead to a few dominant telecom and tech companies obtaining significant power which they leverage to sway market behaviour and reshape public discourse **(Fontes et al., 2022).** When AI surveillance techniques grow more advanced the risk of data exploitation including security breaches become more substantial. The large volume of data which AI processes naturally makes these systems prime targets for cyber criminals. Unsecured personal information becomes vulnerable because data breaches and hacking incidents and unauthorized access expose sensitive data to major privacy risks **(Ali et al., 2025).** AI systems which process financial transactions along with medical records and sensitive data create exposure challenges that produce severe consequences for individual people. When

personal data falls victim to breaches, it can lead to attacks that compromise identity or result in financial loss together with emotional trauma. The central collection of personal data inside AI systems creates a greater threat of big breaches because hackers can access detailed datasets which contain millions of people's sensitive information **(Dilmaghani et al., 2019).**

AI surveillance technologies present the problem of data manipulation where crooks can change or transform information automatically gathered by the systems to serve their bad goals. AI surveillance systems gather data that permits attackers to create faux or deceptive content which then targets specific individuals who can subsequently develop adjusted behavior or modified political ideas **(Power et al., 2021).** The manipulation of data becomes dangerous for elections precisely when AI systems distribute false information to control who voters select during elections. Because AI systems rapidly analyze data they create an environment where misinformation spreads without control which permanently harms individual freedoms and public trust **(Zachary, 2020).** When artificial intelligence systems monitor telecommunication infrastructure it leads to concerns about democratic rights becoming diminished. Democratic states consider privacy rights as essential human freedoms protected either through constitutional law or major international agreements **(Jungherr, 2023).** Unrestrained use of AI surveillance systems reduces human right guarantees by allowing complete probing into what people do and how they act. Boundless monitoring goes beyond privacy invasions to create an atmosphere which harms both speech and social connections between citizens **(Saheb, 2023).** People in such an environment reject sharing oppositional opinions or taking political action because they suspect monitoring will lead to negative consequences or discriminatory treatment. government agencies as well as large corporations operating algorithmic surveillance systems present a threat which suppresses open idea exchange and impairs civil liberties for affected individuals.

CONCLUSION

Telecommunication networks have experienced a fundamental transformation due to artificial intelligence (AI) which delivers unprecedented capabilities for efficient communication and individualized experiences and optimal operational performance. Technological development brings major privacy-related obstacles for telecommunications sector protection. The adoption of AI-driven surveillance through innovation creates major risks which endanger both consumer protection and societal framework along with individual privacy safeguards. Existing legal protections require reform to safeguard privacy rights because the growing threats demand a reassessment of legal measures from technological progress. This analysis unveils an urgent reality about how

profoundly AI network components operate to gather analyze and exploit personal telecommunications data. Data-collecting systems maintain opaque operational procedures because consumers remain unclear about the scope of gathered data along with its utilization practices and resulting consequences. The absence of transparency from data collection operations along with their large volume contributes to severe privacy risks. AI can efficiently analyze and make accurate behaviors predictions about consumers, yet this capability generates important ethical issues regarding consumer self-determination and authorization consent. Current privacy laws did not account for the advanced surveillance capabilities of AI which present unidentified risks to user privacy and require reconfiguring existing legislation. Modern legal frameworks require urgent revision to protect human beings against exploitation and unauthorized data utilization and discrimination. The analysis shows how existing legislation fails to capture the dynamic aspects of AI algorithms that manipulate data. The General Data Protection Regulation (GDPR) from Europe along with the United States' Communications Privacy Act represent traditional privacy laws which were meant to work with older systems but focus strictly on data management. The existing laws prove successful in some applications yet fail to address adequately the data profiling capacity and predictive algorithm analytics conducted by AI systems. The continued prospective presence of algorithmic bias becomes a persistent concern because AI systems utilize incomplete databases to create discriminatory patterns against selected demographic groups. Lawmaking controls fail to grasp the fundamental risks of AI surveillance methods thus weakening their protections for privacy alongside consumer rights.

Telecommunications privacy laws should undergo vital reforms because of outlined gaps in current regulations. Addressing both possibilities and challenges of AI requires legal mechanisms which focus on disclosure standards combined with user rights protection. The reform proposal calls for implementing strong regulatory standards which force companies to disclose their data gathering activities in transparent ways. Telecom businesses should disclose precise information about collected data together with usage purposes and sharing relationships to their customers. Modern data-processing algorithms must undergo thorough inspections which determine their bias levels as well as unveil their processing methods in a transparent fashion. Such audits require independent regulatory bodies who enforce penalties against organizations that fail to comply. The essential requirement now is international cooperation to standardize privacy protections between countries because telecommunication services function across global borders. Multiple nations maintain distinct privacy rules which create extensive regulatory differences and multiple regulatory spaces between countries. GDPR has achieved major success for the EU community, but

numerous nations remain without advanced privacy protection frameworks. The creation of multilateral privacy legislation for telecommunication services will assist in reconciling international privacy regulations so people irrespective of their residency maintain personal privacy protection. An international accord on AI and telecommunication privacy would function as a base for developing uniform global privacy standards while enabling mutual national support against privacy abuses that cross borders.

The creation of a universal right to be forgotten must be established to enable people to request data elimination from AI-run telecommunication platforms after key purposes terminate. GDPR's existing right to erasure should gain worldwide adoption because it enables individual control of personal information against the backdrop of Commodified data treated by algorithms repeatedly. By establishing this right, consumers would obtain stronger digital identification protection to counter potential AI system surveillance abuses. Telecommunication law needs future development which will match advancements in AI technology. As a promising solution we can develop AI ethics boards together with regulatory bodies that would monitor the application of AI systems inside telecommunication networks. Data scientists should join lawyers and ethics scholars along with consumer protection experts as members of boards which will oversee the development of AI systems that respect privacy boundaries. The public needs direct education about their rights so they understand what protection they have during surveillance conducted by artificial intelligence systems.

REFERENCES

1. Agubor, C. K., Chukwudebe, G. A., & Nosiri, O. C. (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. *Proceedings of the 2015 International Conference on Cyberspace (CYBER-Abuja)*, Abuja, Nigeria, 124–129. https://doi.org/10.1109/CYBER-Abuja.2015.7360500
2. Akram, N., Dagdeviren, Z. A., Akram, V., Dagdeviren, O., & Challenger, M. (2021). Design and implementation of asset tracking system based on Internet of Things. *2021 7th International Conference on Electrical, Electronics and Information Engineering (ICEEIE)*, 366–371. https://doi.org/10.1109/ICEEIE52663.2021.9616667
3. Alhammadi, A., Shayea, I., El-Saleh, A. A., Azmi, M. H., Ismail, Z. H., Kouhalvandi, L., & Saad, S. A. (2024). Artificial intelligence in 6G wireless networks: Opportunities, applications, and challenges.

International Journal of Intelligent Systems, 2024, 8845070. https://doi.org/10.1155/2024/8845070

4. Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms– A comprehensive review. *Information Fusion, 118*, 102922. https://doi.org/10.1016/j.inffus.2024.102922
5. Balmer, R. E., Levin, S. L., & Schmidt, S. (2020). Artificial intelligence applications in telecommunications and other network industries. *Telecommunications Policy, 44*(6), 101977. https://doi.org/10.1016/j.telpol.2020.101977
6. Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1041. https://doi.org/10.2307/41409971
7. Brunner, L. (2018). Digital communications and the evolving right to privacy. In M. K. Land & J. D. Aronson (Eds.), *New technologies for human rights law and practice* (pp. 217–242). Cambridge University Press.
8. Bygrave, L. A. (1998). Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology, 6*(3), 247–284. https://doi.org/10.1093/ijlit/6.3.247
9. Carvalho, H. E. R. H. de, Freitag, A. E. B., & Santos, D. R. dos. (2022). Impactos da implantação da Lei Geral de Proteção de Dados Pessoais no Brasil: Uma análise bibliométrica [Impacts of the implementation of the General Law for the Protection of Personal Data in Brazil: A bibliometric analysis]. *Revista de Gestão e Secretariado, 13*(3), 1398–1411. https://doi.org/10.7769/gesec.v13i3.1412
10. Cuzzocrea, A., & Soufargi, S. (2025). Privacy-preserving multidimensional big data analytics models, methods and techniques: A comprehensive survey. *Expert Systems with Applications, 270*, 126387. https://doi.org/10.1016/j.eswa.2025.126387
11. de Almeida, P. G. R., dos Santos, C. D., & Farias, J. S. (2021). Artificial intelligence regulation: A framework for governance. *Ethics and Information Technology, 23*, 505–525. https://doi.org/10.1007/s10676-021-09593-z
12. de Carvalho, R. M., Del Prete, C., Martin, Y. S., et al. (2020). Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. *SN Computer Science, 1*, 217. https://doi.org/10.1007/s42979-020-00218-8
13. Dev, K., Xiao, Y., Challita, U., de Alwis, C., & Magarini, M. (2023). Guest editorial: Autonomous networks: Opportunities, challenges, and

applications. *IEEE Communications Standards Magazine*, 7(2), 6-7. https://doi.org/10.1109/MCOMSTD.2023.10148968

14. Dilmaghani, S., Brust, M. R., Danoy, G., Cassagnes, N., Pecero, J., & Bouvry, P. (2019). Privacy and security of big data in AI systems: A research and standards perspective. In *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data)* (pp. 5737–5743). IEEE. https://doi.org/10.1109/BigData47090.2019.9006283
15. Edozie, E., Shuaibu, A. N., Sadiq, B. O., et al. (2025). Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review, 58*, 100. https://doi.org/10.1007/s10462-025-11108-x
16. El-Hajj, M. (2025). Enhancing communication networks in the new era with artificial intelligence: Techniques, applications, and future directions. *Network, 5*(1), 1. https://doi.org/10.3390/network5010001
17. Fanca, A., Puscasiu, A., Gota, D.-I., & Valean, H. (2020). Recommendation systems with machine learning. *2020 21st International Carpathian Control Conference (ICCC)*, High Tatras, Slovakia, 1–6. https://doi.org/10.1109/ICCC49264.2020.9257290
18. Fast, N. J., & Jago, A. S. (2020). Privacy matters… or does it? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology, 31*, 44–48. https://doi.org/10.1016/j.copsyc.2019.07.011
19. Filho, A., Santos, A., Rodrigues, I., Vale, L., Vieira, M., Santos, S., & Simas, D. (2024). A proteção de dados pessoais e a Lei Geral de Proteção de Dados (LGPD): limites e desafios na sociedade digital brasileira. *Contribuciones a las Ciencias Sociales, 17*, e11915. https://doi.org/10.55905/revconv.17n.10-343
20. Fontes, C., Hohma, E., Corrigan, C. C., & Lütge, C. (2022). AI-powered public surveillance systems: Why we (might) need them and how we want them. *Technology in Society, 71*, 102137. https://doi.org/10.1016/j.techsoc.2022.102137
21. Fu, M., Wang, P., Wang, Z., & Li, Z. (2023). Deep learning for network traffic prediction: An overview. In *2023 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 665–671). IEEE. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361459
22. Gorrepati, U., Zavarsky, P., & Ruhl, R. (2021). Privacy protection in LTE and 5G networks. *Proceedings of the 2021 2nd International*

Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 382–387. https://doi.org/10.1109/ICSCCC51823.2021.9478109

23. Greenleaf, G. (2009). Five years of the APEC privacy framework: Failure or promise? *Computer Law & Security Review, 25*(1), 28–43. https://doi.org/10.1016/j.clsr.2008.12.002
24. Guhl, S. D., & Pendse, R. (2008). The Communications Assistance for Law Enforcement Act (CALEA). *Journal of Information Technology & Politics, 17*(3), 1. https://doi.org/10.1080/19393550802297399
25. Hill, R. (2014). The 1988 International Telecommunication Regulations. In *The new international telecommunication regulations and the Internet*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-45416-5_2
26. Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law, 28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501
27. Jones, M. L., Kaufman, E., & Edenberg, E. (2018). AI and the ethics of automating consent. *IEEE Security & Privacy, 16*(3), 64–72. https://doi.org/10.1109/MSP.2018.2701155
28. Jungherr, A. (2023). Artificial intelligence and democracy: A conceptual framework. *Social Media + Society, 9*(3). https://doi.org/10.1177/20563051231186353
29. Kabay, M. E. (2003). Crime, use of computers in. In H. Bidgoli (Ed.), *Encyclopedia of Information Systems* (pp. 345–363). Elsevier. https://doi.org/10.1016/B0-12-227240-4/00023-X
30. Kastouni, M. Z., & Ait Lahcen, A. (2022). Big data analytics in telecommunications: Governance, architecture and use cases. *Journal of King Saud University - Computer and Information Sciences, 34*(6, Part A), 2758-2770. https://doi.org/10.1016/j.jksuci.2020.11.024
31. Khan, M. (2023). AI-enabled transformations in the telecommunications industry. *Telecommunication Systems, 82*(1–2), 1–2. https://doi.org/10.1007/s11235-022-00989-w
32. Lakhani, S. (2024). Bridging law and technology: Navigating policy challenges. *International Review of Law, Computers & Technology, 1*(3). https://doi.org/10.1080/13600869.2024.2364987
33. Li, M., Huo, M., Cheng, X., & Xu, L. (2020). Research and application of AI in 5G network operation and maintenance. *Proceedings of the 2020 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Exeter, United Kingdom,

1420–1425. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00212

34. Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714541861
35. Machado, H., Silva, S., & Neiva, L. (2023). Publics' views on ethical challenges of artificial intelligence: A scoping review. *AI Ethics*. https://doi.org/10.1007/s43681-023-00387-1
36. Mao, Y., Pranolo, A., Hernandez, L., Wibawa, A. P., & Nuryana, Z. (2022). Artificial intelligence in mobile communication: A survey. *IOP Conference Series: Materials Science and Engineering, 1212*(1), 012046. https://doi.org/10.1088/1757-899X/1212/1/012046
37. Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law, 21*(4), 769–789. https://doi.org/10.1093/jiel/jgy044
38. Moussawi, S., Deng, X. (N.), & Joshi, K. D. (2024). AI and discrimination: Sources of algorithmic biases. *Communications of the ACM, 55*(4). https://doi.org/10.1145/3701613.3701615
39. Mumuni, A., & Mumuni, F. (2025). Automated data processing and feature engineering for deep learning and big data applications: A survey. *Journal of Information and Intelligence, 3*(2), 113–153. https://doi.org/10.1016/j.jiixd.2024.01.002
40. Murphy, M. H. (2017). Algorithmic surveillance: The collection conundrum. *International Review of Law, Computers & Technology, 31*(2), 225–242. https://doi.org/10.1080/13600869.2017.1298497
41. Park, Y. J., & Jones-Jang, S. M. (2023). Surveillance, security, and AI as technological acceptance. *AI & Society, 38*, 2667–2678. https://doi.org/10.1007/s00146-021-01331-9
42. Penttinen, J. T. J. (2013). Standardization and regulation. In *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems* (pp. 23–48). Wiley. https://doi.org/10.1002/9781118678916.ch2
43. Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: A decision process guide. *Journal of Business Analytics, 4*(2), 155–170. https://doi.org/10.1080/2573234X.2021.1920856
44. Priyadarshi, H., Singh, K., & Shrivastava, A. (2023). Wireless communications using machine learning and deep learning. In *Machine Learning Algorithms for Signal and Image Processing* (pp. 361–370). IEEE. https://doi.org/10.1002/9781119861850.ch20
45. Qi, J., Wu, F., Li, L., & Shu, H. (2007). Artificial intelligence applications in the telecommunications industry. *Expert Systems, 24*.

46. Quach, S., Thaichon, P., Martin, K. D., & et al. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*, 1299–1323. https://doi.org/10.1007/s11747-022-00845-y
47. R. H. J. & Mohana. (2022). Fraud detection and management for telecommunication systems using artificial intelligence (AI). *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, pp. 1016-1022. https://doi.org/10.1109/ICOSEC54921.2022.9951889
48. Ranjan, R., & Kumar, S. S. (2022). User behaviour analysis using data analytics and machine learning to predict malicious user versus legitimate user. *High-Confidence Computing, 2*(1), 100034. https://doi.org/10.1016/j.hcc.2021.100034
49. Rocha, N. A. de S., de Almeida, A. N., Nunes, A., & Angelo, H. (2024). Critical points for the processing of personal data by the government: An empirical study in Brazil. *Computer Law & Security Review, 54*, 106023. https://doi.org/10.1016/j.clsr.2024.106023
50. Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges, and vulnerabilities. *Journal of Responsible Technology, 4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005
51. Sachoulidou, A. (2024). Harnessing AI for law enforcement: Solutions and boundaries from the forthcoming AI Act. *New Journal of European Criminal Law, 15*(2), 117-125. https://doi.org/10.1177/20322844241260114
52. Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: A social science perspective. *AI Ethics, 3*, 369–379. https://doi.org/10.1007/s43681-022-00196-y
53. Sampson, F. (2021). Data privacy and security: Some legal and ethical challenges. In: Jahankhani, H., Kendzierskyj, S., & Akhgar, B. (Eds.), *Information security technologies for controlling pandemics. Advanced Sciences and Technologies for Security Applications.* Springer, Cham, pp. 109–134. https://doi.org/10.1007/978-3-030-72120-6_4
54. Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data Governance* (pp. 217–245). Springer. https://doi.org/10.1007/978-3-031-67268-2_6
55. Saura, J. R., Ribeiro-Soriano, D., & Palacios-Marqués, D. (2021). From user-generated data to data-driven innovation: A research agenda to understand user privacy in digital markets. *International Journal of Information Management, 60*, 102331. https://doi.org/10.1016/j.ijinfomgt.2021.102331
56. Secundo, G., Spilotro, C., Gast, J., & others. (2024). The transformative power of artificial intelligence within innovation ecosystems: A review

and a conceptual framework. *Review of Managerial Science*. https://doi.org/10.1007/s11846-024-00828-z

57. Seetharamu, S., Manasa, L. C. N., Bhattacharya, A., & Chitra, B. T. (2024). Digital data protection laws: A review. *International Journal of Scientific Research in Science, Engineering and Technology, 11*(5), 64–75. https://doi.org/10.32628/IJSRSET2411416
58. Sergiou, C., Lestas, M., Antoniou, P., Liaskos, C., & Pitsillides, A. (2020). Complex systems: A communication networks perspective towards 6G. *IEEE Access, 8*, 89007-89030. https://doi.org/10.1109/ACCESS.2020.2993527
59. Shin, D., Kee, K. F., & Shin, E. Y. (2022). Algorithm awareness: Why user awareness is critical for personal privacy in the adoption of algorithmic platforms? *International Journal of Information Management, 65*, 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494
60. Singh, T. (2024). AI-driven surveillance technologies and human rights: Balancing security and privacy. In A. K. Somani, A. Mundra, R. K. Gupta, S. Bhattacharya, & A. P. Mazumdar (Eds.), *Smart systems: Innovations in computing. SSIC 2023* (Vol. 392, pp. 611-620). Springer. https://doi.org/10.1007/978-981-97-3690-4_53
61. Singhal, A., Neveditsin, N., Tanveer, H., & Mago, V. (2024). Toward fairness, accountability, transparency, and ethics in AI for social media and health care: Scoping review. *JMIR Medical Informatics, 12*, e50048. https://doi.org/10.2196/50048
62. Sumartono, E., Harliyanto, R., Situmeang, S. M. T., Siagian, D. S., & Septaria, E. (2024). The legal implications of data privacy laws, cybersecurity regulations, and AI ethics in a digital society. *The Journal of Academic Science, 1*(2). https://doi.org/10.59613/29qypw51
63. Timan, T., & Mann, Z. (2021). Data protection in the era of artificial intelligence: Trends, existing solutions, and recommendations for privacy-preserving technologies. In E. Curry, A. Metzger, S. Zillner, J. C. Pazzaglia, & A. García Robles (Eds.), *The elements of big data value*. Springer, Cham. https://doi.org/10.1007/978-3-030-68176-0_7
64. van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review, 49*, 105804. https://doi.org/10.1016/j.clsr.2023.105804
65. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research, 122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022
66. Wang, Z., Wei, G. F., Zhan, Y. L., et al. (2017). Big data in telecommunication operators: Data, platform, and practices. *Journal of*

Communications and Information Networks, 2(3), 78–91. https://doi.org/10.1007/s41650-017-0010-1

67. Whang, S. E., Roh, Y., Song, H., & others. (2023). Data collection and quality challenges in deep learning: A data-centric AI perspective. *The VLDB Journal, 32*, 791–813. https://doi.org/10.1007/s00778-022-00775-9
68. Zachary, G. P. (2020). Digital manipulation and the future of electoral democracy in the U.S. *IEEE Transactions on Technology and Society, 1*(2), 104–112. https://doi.org/10.1109/TTS.2020.2992666
69. Zhang, Y., Wu, M., Tian, G. Y., Zhang, G., & Lu, J. (2021). Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems, 222*, 106994. https://doi.org/10.1016/j.knosys.2021.106994

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET