Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 20 April 2026
Revised 22 May 2026
Accepted 18 June 2026

Natural Resources for Human Health 2026, Vol. 6 (5s): 381–396

KEYWORDS:
Digital Privacy, Human Rights, Artificial Intelligence, Digital Surveillance, Data Protection, Technology Governance.

Privacy and Human Rights in the Digital Age: Challenges of a Technology- Centric Society

Shivika Jain [1], Prof. (Dr.) Jageshwar Nath Singh[2]

[1] College of Legal Studies, College of Engineering Roorkee (COER) University, Roorkee, India. Email: advshivvikajain@gmail.com
[2] College of Legal Studies, College of Engineering Roorkee (COER) University, Roorkee, India. Email: dean.legal@coeruniversity.ac.in

ABSTRACT: Digital technologies impact communication across education, healthcare, employment and administration. In addition to increasing communication through technology, the technologies also increased the collection storage and processing of personal data. This paper provides a review of privacy and human rights as they relate to an entire society that is built around technology. This study examines informational privacy, physical privacy, decision privacy. It examines mass surveillance using commercial data, algorithmic discrimination, cybersecurity threats, Digital inequality and weak consent. Additionally, it examines corporate responsibility, artificial intelligence (AI) ethics and the relationship between privacy and security. A framework is developed connecting technologies to data practices and privacy risks; technologies to human rights outcomes and governance responses. These processes include collection, storage sharing profiling and automated decisions making. The process is moderated by standards, public awareness and Digital literacy. The review finds harm results from collecting too much data, lack of oversight over the data collected, unfairness in automated decisions made with respect to data and limited access to remedies.

1. INTRODUCTION

In today's world, it seems like every single thing we do is becoming "digital". We are using digital systems more frequently in our daily lives. From internet platforms and mobile apps to AI, Cloud Computing, Biometric Systems and all sorts of devices, the way we get and exchange information has completely changed [1].

Digital services have made accessing some things easier and convenient. Using the internet and digital tools helps us communicate with each other over long distances quickly (Hoxhaj et al., 2023). Health care is being provided by doctors remotely, so patients don't need to go into a doctor's office to see them; this creates electronic medical records. Learning at home is being done via digital learning platforms (e.g. MOOCs) allowing people who might not otherwise have been able to afford access to higher education to learn from anywhere they want. Digital governance has allowed government agencies to deliver services electronically [2].

This rapid increase in digital services comes with a cost: large-scale data collection of individuals' personal info [3]. When you perform searches, check your GPS location, pay bills, send messages and share preferences on a smart device; that data is being tracked by digital platforms. Some devices track users' habits and physical movements. Biometric systems collect facial recognition images, fingerprints and even voice patterns; this data remains within these digital systems for years and passes through multiple organizations [4].

Therefore, the role of data has dramatically changed in contemporary society. Data is no longer just used to identify individuals or provide them with a service. It is also used to predict behaviour, target advertisements, automate decision-making and monitor citizens [5].

As a result of the rapid growth of digital systems, most laws and institutions have not kept pace. Therefore, there continue to be significant gaps between the technological practices that govern the way personal data is collected, used and protected; and the protections afforded to individual rights.

1.2 Why are Privacy & Human Rights Important?

Protecting one's privacy is essential for protecting one's dignity and individual freedom. An individual's right to privacy protects their personal life, their family relationships, their communications and their personal information from unjustified intrusion. In a digital environment, privacy extends beyond this and includes the collection, utilization, retention and transmission of personal data. This is important since data can reveal an individual's identity, their health status, their financial situation, their political opinions, their location and their social connections [5].

Protecting an individual's right to privacy also serves to safeguard other fundamental human rights. For example, if an individual feels that their online communication is constantly monitored then their ability to express themselves freely may be diminished. Similarly, if an organization monitors its members' communication or participation in social groups then those group members may feel restricted in their ability to associate freely. Finally, if automated systems generate discriminatory results against certain racial or ethnic groups or women or men due to income or social status then those individuals may experience inequality. An individual's dignity may also be compromised when an unauthorized third party discloses their personal information.

While human rights exist regardless of whether they are exercised in either a physical space or a virtual/digital space; the existence of digital technologies does not eliminate the obligation of states/governments/organizations to respect individual freedoms (i.e., equality), dignity (i.e., non-discrimination) and liberty (i.e., free speech). Therefore, digital technologies must operate within established legal frameworks/limits. An organization collecting an individual's personal information must collect only the amount of data that is needed for a specific legitimate purpose. Organizations collecting an individual's data must inform that individual clearly of how their data will be utilized [6].

Additionally, protecting an individual's privacy enhances public trust in organizations that utilize digital technologies. If an individual believes that his/her/their personal information is safe or that the organization(s) utilizing their data are transparent about how their data is being used; then that individual will likely participate in public discourse. Conversely, fear of surveillance may prevent individuals from participating in public discussions and/or concern about how an organization utilizes an individual's data may cause that individual to lose confidence in services offered by healthcare providers/banks/educational institutions/public administrators [7].

1.3 Problem Statement

Technology has grown exponentially and simultaneously caused a conflict between the potential technological improvements available; and the protection of human rights. Governmental entities and corporations typically describe data collection as a means to improve national security, increase operational efficiencies; or enhance customer experiences. However, the very same actions can facilitate pervasive monitoring/profiling/control of individuals. The core issue revolves around the degree to which technological objectives can justify invasion upon an individual's right to privacy as well as other rights.

Most digital systems collect far more information than needed for a particular legitimate objective. Many consumers give consent after reading lengthy terms-of-use agreements which do not provide reasonable alternatives. Consumer personal data may subsequently be used for purposes such as advertising decisions etc. These uses may take place without sufficient prior knowledge/approval from the consumer [8].

Further concerns arise when applying artificial intelligence and automation systems for decision-making processes related to employment/credit/insurance/policing/public benefits. While these decisions may be generated by computer algorithms; errors or biases contained in those algorithms may lead to adverse treatment of individuals.

The principal challenge is not with the fact that there exists some kind of technology. The main challenge is when technological uses are made without appropriate limits by law; ethical responsibility; or accountability to the public. A technology-centred culture has the potential for prioritizing efficiency and monetary value over human dignity; freedom; and equality. Therefore, this research will explore how developments in digital technologies affect an individual's right to privacy as well as their other human rights. Furthermore, this research will also investigate the types of legal; ethical and institutional requirements which would be necessary to achieve a fair equilibrium between technological use and protecting rights.

1.4 Research Gap

Digital privacy has typically been examined from a variety of different viewpoints (such as surveillance, data protection, AI, Cyber Security, Online Consent). Separate examinations of these viewpoints often overlook the fact that new forms of digital technology often simultaneously impact multiple aspects of human rights. Loss of privacy may also negatively impact the enjoyment of freedom of expression; equality; dignity; and personal autonomy.

This document recognizes an existing disparity between the way that technology functions and how it protects individual rights. This document also highlights that there exists another type of disparity in regards to the manner in which technology generates rights-related harms. While digital systems have evolved rapidly over recent years, many legal and institutional responses to this rapid evolution have moved at a slower pace.

Another disparity concerns the manner in which technology creates rights-related harm. Technology does not independently generate violations of human rights. Rather, rights-violations occur as a result of data collection; data storage; data sharing; data-profiling; and automated-decision-making. There is often limited consideration given to the combined effects of these various processes.

The purpose of this paper is to fill this gap by combining technology with data practices; privacy risks; human rights impacts; and governance responses. In addition to focusing on laws; ethical guidelines; public awareness and digital literacy, the paper examines how all of these elements can contribute to either reducing or increasing the level of harm generated by digital technologies.

1.5 Purpose of the Paper

The purpose of this paper will be to explore how digital technologies interact with both privacy and human rights in today's technology-based world. A second objective of the paper will be to illustrate how surveillance; data collection; commercial-profiling; automated-decisions; and poor cyber-security can violate an individual's right to privacy and freedoms associated with expression; equality; dignity and autonomy.

A third objective will be to relate the selected theoretical perspectives to the major privacy concerns that were addressed in the literature-review. The theoretical perspectives include: surveillance-theory; information-ethics; a Human Rights-Based approach; and the debate regarding whether technology-determinism or human-agency most appropriately describes how people behave when interacting with digital technologies.

In addition to connecting theoretical perspectives to major privacy concerns, we will also develop a conceptual-framework that illustrates how digital technologies interact with data-practices; privacy-risks; human-rights-outcomes and governance-responses. The Framework will also help us understand how laws; ethical-standards; public-awareness; and digital-literacy can support or undermine efforts to protect peoples' rights.

1.6 Research Questions

The paper will seek to answer the following research questions:

1. What types of privacy-risk generating actions can be attributed to digital technologies?

2. In what ways do data-collection; data-storage; data-sharing; profiling and automated-decision-making link digital technologies with human rights outcomes?

3. How do large-scale-surveillance; commercial-data-use; discriminatory-algorithmic-applications; insecure-cyber-systems; unequal-access-to-digital-technology hinder individual-human-rights?

4. How can laws; ethical-standards; public-awareness, and digital-literacy mitigate harm resulting from privacy-loss?

1.7 Contributions to the Paper

The paper makes a conceptual contribution by integrating issues relating to the technological, ethical, legal, and human rights implications into one model. Privacy is seen as going beyond being merely about confidentiality or data-protection. Instead, privacy is viewed as being linked with freedom-of-expression; equality; dignity; autonomy and redress-for-harm.

The proposed framework provides an explanation of how digital technologies may generate human rights violation or protection. Digital technologies represent the input variables. Data-practices-and-algorithms represent mediation variables. These processes produce privacy-risks, which produce human-rights-outcomes. In addition to providing a conceptual contribution, the paper also relates theory to practical problems. For example, Surveillance Theory explains why continuous-observation should be problematic. Information-Ethics discusses what constitutes "fair" use of personal data. The Human Rights-Based Approach emphasizes that dignity; equality; accountability and remedies should be central components of any digital-governance strategy. Lastly, Human Agency explains how law-policy-institutional decisions can shape the use of technology in relation to human rights (Nandy, 2023). Finally, the proposed framework can serve as a guide for assessing policies and subsequently conduct empirical-research. The Framework could potentially be applied in domains including healthcare; education; employment-banking-social-media-public-surveillance etc.

2. CONCEPTUAL FOUNDATIONS

The key to understanding how digital technology impacts individual freedom and dignity is the foundation of two major themes: privacy (the right to control personal data) and human rights (protection from unreasonable state or private sector intrusion). In order to develop an appropriate technological structure that supports both themes, we need to understand what they mean. Privacy is defined as having control over personal data, being able to protect your own body and make decisions about your life.

2.1 Privacy: Meaning and Dimensions

Privacy refers to the protection of personal life from unwanted access, observation or interference. It also concerns the ability of a person to control access to personal information, the body, private spaces and personal decisions. Privacy does not require complete isolation from society. Rather, it permits individuals to determine which parts of personal life may be shared and under what conditions [9].

The meaning of privacy has changed with the expansion of digital technology. Earlier discussions often connected privacy with the home, family life and private communication. Digital systems have extended privacy concerns to online activity, location records, biometric data, financial information, health records and patterns of behaviour. Personal information can now be collected without direct contact with the person concerned. Data can also be copied, combined and transferred across several systems [10]. Privacy may be examined through three main dimensions. These dimensions are informational privacy, physical privacy and decisional privacy. Each dimension concerns a separate area of personal freedom. However, the boundaries between these areas often overlap in digital settings as shown in figure 1.

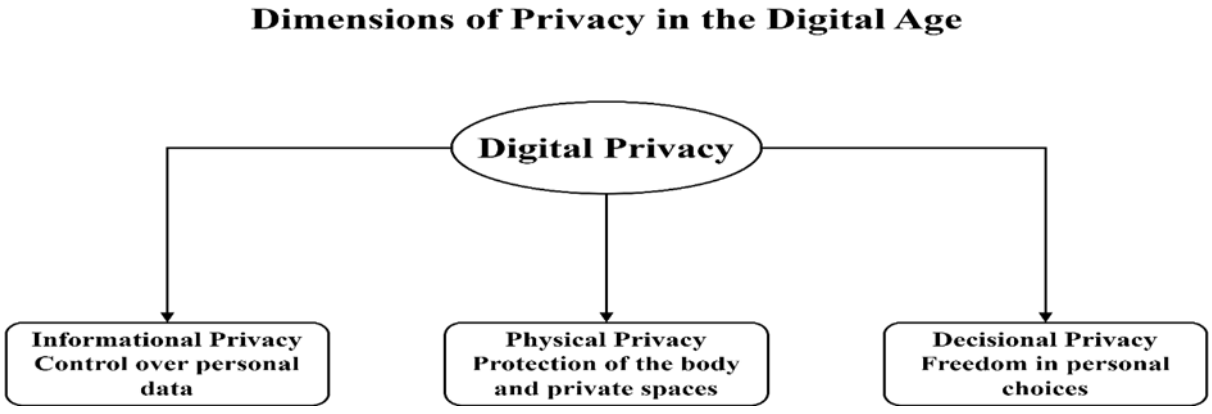

Figure 1. Dimensions of Privacy in the Digital Age

2.2 Human Rights in the Digital Era

Digital technology can support human rights by widening access to information, education and public services. Online platforms can provide opportunities for communication and participation. At the same time, the same systems can support surveillance, censorship, discrimination and manipulation. The protection of human rights therefore depends on the purpose, design and control of digital systems.

2.3 Technology Centred Society

A technology centred society is a social order in which digital systems shape major areas of daily life. Communication, employment, education, banking, health care, entertainment and public administration rely heavily on digital tools. Access to services increasingly depends on online identification, data processing and automated decision making.

The term does not refer only to widespread ownership of digital devices. It also refers to the authority given to technological systems in social and institutional decisions. Data based systems may determine which information becomes visible, which services remain available and how individuals are classified. Technology therefore becomes part of the structure through which social participation takes place [11].

3. THEORETICAL PERSPECTIVES

The relationship between digital technology, privacy and human rights can be examined through several theoretical perspectives. Each perspective explains a different aspect of technological power and personal freedom. Surveillance theory explains how observation can influence behaviour. Information ethics examines moral duties connected with data collection and use. The Human Rights Based Approach places dignity, equality and accountability at the centre of digital governance. The debate between technological determinism and human agency considers whether technology controls social change or remains subject to human choice. Together, these perspectives provide a suitable theoretical basis for examining privacy and human rights in a technology centred society [12].

3.1 Surveillance Theory

Surveillance theory examines the observation, recording and assessment of human behaviour. Surveillance may be conducted by governments, private companies, employers, educational institutions or digital platforms. The purpose may include public security, service management, advertising, employee monitoring or social control [13].

A major idea within surveillance theory is the panopticon. Jeremy Bentham first proposed the panopticon as a prison design. The structure allowed a central observer to watch prisoners without allowing prisoners to know when observation was taking place. Michel Foucault later used the panopticon as a model for understanding social control. The possibility of constant observation could lead persons to regulate personal behaviour even when no observer was present [14]. The concept of the digital panopticon applies this idea to digital society. Digital devices and platforms can create a condition in which observation becomes continuous and difficult to detect. Search activity, location records, online purchases, messages and social media use may be recorded. A person may not know which organisation has access to such information or how long the information will remain stored.

3.2 Information Ethics

Ethics of Information addresses concerns associated with creating, collecting, storing, using and distributing information. The field focuses upon the impact of information practices upon privacy, dignity, equity and individual liberty. Additionally, the field evaluates organizational obligations to protect users' personal data [15].

As a result of rapid growth of digital societies, individuals' personal data are now a valuable commodity. Personal data can be collected by online platforms (such as Facebook) to provide services, targeted advertising and predictions about behaviour. Similarly, government agencies, healthcare organizations, banking organizations, employers and educational institutions collect, store and analyse vast amounts of individuals' personal data [15].

Ethics of Information is concerned with the issue of whether these practices are justifiable. The availability of the capability to collect personal data does not create an obligation to do so. For example, an organization could potentially collect geolocation records, health information and/or communication data; however, ethical use of this capability depends upon clearly articulating a legitimate purpose and respecting the individual whose information is being collected [16]. One aspect of ethical use of data is obtaining consent from those whose information is being collected. Consent must be based upon informed choices regarding what types of personal data will be collected and how it will be used. Unfortunately, many digital services rely on lengthy "Privacy Policies" and vague terms and conditions to obtain consent. In some cases, acceptance of a Privacy Policy/ Terms & Conditions may be a condition of access to communications, employment or other governmental services. Therefore, it can be argued that consent is often not given freely [17].

Another area of ethical use of data is ensuring that the purpose for which the data was collected remains the same throughout the time the data is stored. This is referred to as limiting the purposes of processing. Organizations cannot collect personal data for one purpose and then use it for another without adequate authorization. For instance, medical information collected for diagnosis/treatment should not be used for marketing/advertising purposes unless the individual has been specifically notified. Students' educational records should not be transferred to companies that sell products/services unrelated to education [18].

Another area of ethical use of data is minimizing the amount of data that is collected. Organizations should only collect sufficient personal data to fulfil their stated purpose. Collecting excessive data increases the risk of misuse, unauthorized disclosure/theft and unfair assessments. Just because there is no longer significant cost associated with storing large volumes of data, it does not provide a justification for retaining personal data for indefinite periods without a valid business or regulatory requirement [19].

3.3 Human Rights-Based Approach

The Human Rights-Based Approach serves as both a legal and philosophical foundation for evaluating digital policies and technologies. The Human Rights-Based Approach positions recognized human rights at the centre of all policy/planning processes, including evaluation/review. Technologies are evaluated based upon their effects on dignity, equality, privacy, expression and individual liberty.

In the Human Rights-Based Approach, individuals are viewed as right-holders and institutions are considered duty-bearers. Right-holders possess entitlements to protections and recourse when their rights have been violated. Duty-bearers consist of governments/public authorities. In addition, private sector entities can assume duty-bearing responsibilities when they develop digital services that impact human rights.

A Human Rights-Based Approach incorporates four primary principles: dignity, equality, participation/accountability and access to redress/recourse. All four principles relate directly to protecting digital privacy [20].

Dignity demands recognition/respect for an individual's identity/personal life. Data should never serve to reduce a person into a numerical/risk profile or categorize them. When making critical decisions relating to job placement/education/access to public services/support systems/healthcare, consideration must be afforded to an individual's unique situation. Human oversight must always remain an option for those who are subject to automated decision-making mechanisms where the decision impacts substantial interests (Smuha, 2021).

3.4 Technological Determinism and Human Agency

Technological Determinism views technology as driving the evolution of social structures/institutions/human behaviour. From this viewpoint, technological developments occur independently and generate changes in society. Digital systems are consequently regarded as powerful agents shaping communication/employment/education/politics and interpersonal relations [20].

Examples of this perspective include claims that artificial intelligence will automatically supplant human judgment or that digital surveillance will inevitably emerge as an acceptable normative practice. Technology can seem to predetermine how institutions function and how people act. As such, technological determinism can distract us from the choices we exercise in law/social norms/political spheres.

While technological determinism explains why digital systems hold considerable sway over social structures (e.g., social media affects both access to information and public discourse; automated decision systems affect job prospects/financial opportunities; connected devices record our daily lives), technological determinism also suggests that technology exists independent of human choice/design/funding/governance. The design and deployment of digital systems are ultimately determined by human decision-making processes. We choose which data is collected; we decide which objectives are pursued; and we select which safety measures are implemented. Our choices are guided by institutional self-interest/economic imperatives/legal frameworks [21].

An alternative perspective is offered by human agency. By human agency we mean the ability of people and organizations to make decisions that produce certain results. Humans exert social control over technology. Governments can regulate the

collection/use of data; courts can limit unreasonable surveillance; organizations can implement privacy-protective procedures; citizens can fight against deleterious systems through litigation/political actions.

4. KEY CHALLENGES TO PRIVACY AND HUMAN RIGHTS

Digital technology has increased the amount of and ways to collect/use individual's personal information among both public & private institutions. Data is used for communications, public administration, healthcare, education, banking, employment, & commerce. This allows for better services & improved access. That being said, due to weak regulations & poorly managed data use, many citizens are exposed to surveillance, discrimination, fraud & loss of their personal freedoms. Privacy issues with digital technologies go beyond simply disclosing an individual's private information. The negative impacts will be intensified as digital services become increasingly required for social & economic participation. In addition, refusal to provide data (and therefore, allow collection) will cause an individual to be excluded from employment opportunities, educational resources, financial products/services, & government aid.

Table 1. Major Challenges to Privacy and Human Rights

Challenge	Main source of risk	Rights affected
Mass surveillance and data tracking	Continuous monitoring of location and communication. Collection of biometric and online activity data.	Privacy Freedom of expression Freedom of association Autonomy
Commercial use of personal data	Profiling for advertising and behavioural prediction. Exchange of data for financial gain.	Privacy Dignity Autonomy
AI bias and algorithmic discrimination	Biased data and unsuitable system design. Limited explanation and human review.	Equality Dignity Fair access to services
Cybersecurity threats and data breaches	Hacking and weak data protection. Exposure of financial health or biometric records.	Privacy Dignity Security
Digital divide and inequality	Unequal access to devices internet services and digital skills.	Equality Social participation Access to services

Table 1 presents the main privacy and human rights challenges discussed in the paper. These challenges include mass surveillance and commercial data use. AI bias and cybersecurity failures are also included. The table also covers digital inequality. It shows the source of each risk and the rights that may be affected.

4.1 Cybersecurity Threats and Data Breaches

Privacy violations occur as a direct result of cybersecurity failures that expose personal data to unauthorized access, theft, destruction or interruption. The risks of such exposures are high due to cyber threats from hackers, weak passwords, insecure software, errors made by employees, and improper data management practices. Data breaches — whether they include financial records, medical information, log-in credentials, identification documents, or biometric data — have the potential to impact one individual, thousands of individuals, or millions of account-holders. Additionally, the ramifications of a data breach may extend over many years. Financial information stolen during a data breach can be used to commit fraudulent activities. Identification information stolen during a data breach can be used to open new accounts (legitimately) or make unauthorized purchases (illegally). Biometric information stolen during a data breach creates an especially high level of concern. Passwords can be changed; fingerprints, facial patterns or iris records cannot. Therefore, once biometric data is compromised, there will always be some degree of ongoing privacy risk associated with it.

Cyberattacks against hospitals, banks or public agencies can also affect human rights. Disruption of a health system may delay treatment. An attack on public records may prevent access to benefits or legal documents. A breach involving journalists or activists may expose confidential communication [22].

4.2 Digital Divide and Inequality

The digital divide refers to unequal access to digital devices, internet services, digital skills and online opportunities. Differences may arise from income, location, age, education, disability or social position. Unequal access can limit participation in employment, education, health care and public administration.

Many services have moved online. Job applications, banking, educational materials and government forms may require internet access. Persons without reliable devices or connections may face delay or exclusion. Rural communities may have limited network coverage. Low-income households may share one device among several family members [23].

Digital inequality also concerns skill. Access to a device does not ensure safe or effective use. Some persons may lack knowledge about privacy settings, online fraud or data collection. Limited digital knowledge can increase exposure to scams, identity theft and unfair terms.

5. ETHICAL CONCERNS IN THE DIGITAL AGE

The way in which personal information is gathered, saved and utilized has evolved due to technological advancements. In today's world, both government organizations and businesses rely heavily on data to assist them in delivering services, communicating with customers, forecasting, and making decisions.

These methods can provide positive impacts upon society as well as business. However, there are numerous ethical issues that arise when data usage exceeds acceptable bounds or restricts a person's right to privacy, their dignity, their equality and their freedom [23].

An ethical evaluation assesses if a digital method is either justifiable and accountable. Even though a digital method may fulfil a technical need it can still have negative consequences. Although a method collects data using formal consent the actual choices given to consumers may not provide meaningful choices. An automated decision-making process may be accurate most of the time; however, in some instances this process could be discriminatory towards specific groups. While security measures may offer protection to the general population they may also allow for unreasonable surveillance [24].

There are several key areas where ethics are concerned including consent, transparency regarding data gathering, corporate accountability, fair use of artificial intelligence and balancing individual privacy and security.

5.1 - Consent & Transparency

Consent is typically the legal and moral basis for collecting and processing personal data. To create valid consent the consumer must be provided with sufficient information prior to the collection of data so that the consumer understands what data is being collected, why the data is being collected, how long the data will be retained, who will have access to the data (other than the original collector) and that no other parties will gain access to the same data. Additionally, the consumer must have multiple options and be free to make a conscious decision about whether to agree to allow the collection of their data [25].

In addition, the term "consent" should refer to a specific purpose that was agreed upon by the two parties prior to the data being collected. If one party pressures another into consenting then that does not constitute voluntary consent. Likewise, if a person is confused about the terms and/or has very few alternative choices in order to obtain something they want/need, then that too would not be considered voluntary consent.

Typically, digital services will utilize privacy notices and Terms of Use. Those documents are usually written in legal jargon and sometimes even lengthy legalese. Therefore, many people simply click through those screens without actually reading nor understanding what they are agreeing to. Just because someone formally accepts terms of use don't mean they have truly granted informed consent [25].

5.2 - Corporate Accountability of Technology Firms

Many organizations possess massive amounts of personal data pertaining to each user. Social Media Platforms, Search Engines, Online Retailers, Cloud Services Providers and Mobile App Developers collect personal identifiable information from millions of users [26].

6. PROPOSED CONCEPTUAL FRAMEWORK

The conceptual framework illustrates how technology affects rights such as privacy. These four stages are linked in sequence; they are the input of technology, creation of risk, outcome for human rights and governmental response to those outcomes. Some mediating variables have been found to exist as data collection and processing (algorithm) processes. Also, some moderating variables have been found to exist which include law, ethics, public awareness and their relationships may be expressed as follows;

Technology → Data/Algorithms → Privacy Risk → Human Rights Outcome → Governmental Response

A feedback loop exists. An organizations response to an issue will typically affect the design and/or use of a system. As a result of having strong laws and institutions controlling harmful data collection, the harm caused by data collection will be limited. On the other hand, if there are weak laws and institutions to prevent it, then surveillance, discriminatory profiling and improper use of personal identifiable information can occur.

Purpose of this conceptual model is to create a structured format to examine the relationship between technology and human rights. Technology itself does not violate human rights but damage occurs because of how data is collected, processed, distributed/shared and ultimately utilized to make decisions [26].

Facial Recognition technology has two uses; one is for identification verification purposes and the second is for continuous public monitoring. It all depends on what you want to do with the technology; i.e., the amount of data collected, its accuracy and whether or not there is applicable law.

The framework therefore avoids treating technology as either fully harmful or fully beneficial. Attention is placed on the practices that connect technology with social outcomes. This approach allows assessment of both rights violations and rights protection.

The model also connects the earlier sections of this paper. Surveillance theory explains the power created through observation. Information ethics addresses responsible data use. The Human Rights Based Approach provides standards for dignity, equality and accountability. Human agency explains the role of institutional and social choice. These theoretical perspectives support the relationships included in the proposed framework.

6.2 Main Structure of the Framework

The framework contains four main parts:

1. Inputs: Digital technologies that collect or process information
2. Mediators: Data practices and algorithmic processes that shape technological use
3. Outcomes: Effects on privacy and other human rights
4. Moderators: Legal, ethical and social factors that can reduce or increase harm

As an outcome of assessing rights outcomes (i.e. governance), responses to governance may take the shape of legal regulations, institutionally established standards, technological safeguards, education for users, and redress mechanisms.

The above-mentioned model can also be expressed as follows:

Inputs → Mediators → Risks → Results → Governance Response

Moderators influence the relationships at every stage.

6.3 Inputs: Digital Technologies

Inputs represent those digital technologies that start the processes of collecting data, communicating and/or automated assessments. Within the context of the above-mentioned model, examples of inputs include artificial intelligence (AI) systems; Internet of Things (IoT); big data systems; social media platforms; biometric technologies; cloud services; and digital surveillance tools.

Artificial Intelligence

Systems using artificial intelligence can analyse and interpret data to find trends, categorize information and assist in making decisions. Artificial intelligence systems have been utilized by employers; banks; healthcare organizations; educational institutions; police departments and public administrations. AI becomes a problem regarding privacy when it is collecting personal data without a sufficient basis for doing so. Additionally, AI represents a potential source of privacy risk if automated decision-making results in limiting someone's ability to gain access to goods/services/employment opportunities. The amount of damage caused by these factors will be determined by how well the data was obtained; the design of the AI system itself; and whether there were opportunities for human intervention.

Internet of Things

Devices that are "connected" to each other via internet technology are referred to as Internet of Things (IoT). Some examples of IoTs include smartwatches; home assistants; security cameras; medical devices; and connected automobiles. These devices can capture a variety of types of information including where you've gone; what activities you're performing physically; your household habits/routines; and your health-related issues. In many cases, continuous operation makes it difficult to recognize when data is being collected. If the settings for the device are unclear or if the organization collecting the data intends to share it with third parties, then privacy risk increases.

Big Data Systems

Big Data systems collect data from multiple sources. A large number of different types of data could be included within a single database or repository, e.g., public records; data related to online behaviours/activity; financial transactional history; location tracking records; etc. When individual records are combined together, they can provide very comprehensive and detailed pictures of individuals. For example, something that might appear innocuous when taken individually (e.g., web surfing behaviour) can reveal very sensitive information once linked with other data. Therefore, Big Data has the potential to significantly increase the scope of profiling and predicting human behaviour.

Social Media Platforms

Social media platforms collect data about people's communications; their interests; who they contact; and what they view. Social media collects personal data that enables content recommendations, advertising, and behavioural predictions. On the one hand, social media provides forums for self-expression and participation in public affairs. On the other hand, social media companies' practices may disclose private information and restrict access to information. People's rights outcomes depend upon the terms under which their personal data is collected by social media companies; the nature of social media's content guidelines/policies; and their ability to control their accounts.

Biometric Technologies

Biometric technologies utilize physical or behavioural characteristics for purposes of identification. Biometric identifiers include face recognition; fingerprint scans; voice patterns and iris scanning. Because biometric identifiers represent part of an individual's body (or its functions), there is need for them to receive robust protections against unauthorized use/misuse. Unauthorized misuse of biometrics may result in mass surveillance; identity theft/fraudulent use of identity; and discriminatory denial of services/goods based upon certain characteristics.

Digital Surveillance Tools

Digital surveillance tools include cameras; computer/network traffic monitors; GPS-enabled locational trackers; and software applications designed to monitor employees in work environments. Public agencies may employ surveillance technology for purposes of securing communities/law enforcement. Businesses/organizations may employ monitoring techniques for

purposes of preventing fraudulent activity/evaluating performance/employee conduct. There exists a risk to individuals' right to privacy/expression/association when digital surveillance does not have a clearly defined objective or limitations imposed upon its use. Prolonged/sustained surveillance may negatively impact an individual's right to privacy/expression/association.

6.4 Mediators: Data Practices & Algorithms

Mediators describe how digital technologies give rise to both privacy risks/human rights outcomes. Whether technology is used in ways that are helpful or harmful depends on how information is processed/used. The primary mediators include data collection/practices; consent/data subjects provided prior knowledge that their personal data would be collected/processed/use/shared/disclosed; data storage/retention (i.e., duration in which personal data is retained in a system/database/etc.) ; data sharing/transfers among various entities/service providers/advertisers/public agencies/data processors; profiling/analytics/bias contained within algorithms/data modelling methods/models/tools/data mining processes/data aggregation processes/data matching processes etc.; automated decision-making/recommendation/enforcement/evaluation systems/processes etc.

Data Collection

Data collection serves as the initial mediator involved in processing personal information. Digital technologies may collect identity details/location-based records/communications-related data information related to human behaviour/consumption patterns etc. Limited collection is likely required for legitimate provision of services. Overcollection increases risk of surveillance unauthorized disclosure uses. Purpose and scope of collection thus directly influence subsequent rights outcomes.

Data Storage and Retention

Personal data may reside in digital systems for extended periods. Risk escalates if the reasons for retaining the personal data cease to exist after the intended purpose(s) for storing the data expires.

More opportunities exist for unauthorized access or secondary use when longer retention periods are employed. Clearly establishing retention periods reduces this type of risk. Data subject deletion should occur when there is no longer a lawful basis for continued storage.

Data Sharing

Personal data may flow from one service provider to another; from advertisers to service providers; from public agencies to service providers/advertisers/data processors etc. Each transfer adds additional points of entry/access into an individual's personal data.

Concerns for individuals' rights arise when personal data is transferred without due notice or authority. Secondary uses may vary from the original purpose for which personal data was originally collected. Limitations on transferring personal data can protect individual rights to privacy.

Consent Practices

Consent legitimizes data processing. Clear information and freedom of choice are key for valid consent. Consent becomes weaker when privacy notices are hard to understand. Concern also arises when refusal blocks access to something necessary. Methods that encourage acceptance also reduce meaningful choice.

Profiling

Profiling uses personal data to classify behaviour, interests or risk. Digital profiles can affect advertising, employment, credit and insurance. Profiles may contain assumptions that are inaccurate. Group patterns can also replace consideration of individual circumstances. Such practices can affect equality and dignity. Algorithmic Decision Making

Risks Formed Interaction

The interaction between technological input and mediation processes can cause both privacy and human rights risks. Six major risks have been identified in this framework. The first is that of too much surveillance; i.e., constant monitoring of an individual's location, communications, etc. is done so that there are no justifications (other than a potential emergency). A second risk is the use of data for financial gain or to transfer an individual's data for reasons unknown at time of collection. A third risk is

bias from algorithms and discrimination; e.g. a system that produces a different response based upon either inherently biased data or indirect social indicators. A fourth risk is the loss of security for an individual's data; i.e. weak protections provide little safeguard against loss of confidential information due to theft, hacking, etc. A fifth risk is the ability to manipulate using an individual's data to send targeted advertising messages to affect purchasing, voting, and/or other types of social behaviours. The sixth risk is exclusion; i.e. digital systems exclude individuals from access to goods/services, whether it be as a result of incorrect data, an automated score, or lack of digital access.

6.5 Violation of Rights and Protection of Rights

Outcomes refer to impacts digital systems have on privacy and human rights. Outcomes can be good or bad. Results depend on data practices and design as well as strength of moderating factors. Privacy Outcomes

Negative outcomes happen when personal information is collected or used without legal justification. Unauthorized disclosure and constant monitoring also cause privacy harm. Positive outcomes happen when data use is limited and secure.

Equality and non-discrimination

Automated systems also result in unequal treatment in employment, credit or public services. Bias arises from past records or from lack of diversity in data sets. Rights protection involves testing for disparate results and remediation follows if unfair treatment is detected. Review by humans reduces reliance on results that are automated.

Dignity

Dignity can be compromised if personal information is exposed or if people are reduced to profiles of data. Automated classification can ignore personal circumstances. Respect for dignity requires fair treatment and access to explanations. Personal data should not be used to take advantage of someone's weakness or cause embarrassment. Autonomy

Autonomy can weaken when digital systems profile personal choices behind the scenes. Design methods can also pressure acceptance of collection of data.

6.6 Governance Response

A governing response to a risk means a combination of legal, institutional, ethical, and technical ways to respond once an issue has been defined. A governing response needs to have two key components, first it needs to be preventive; secondly, it needs to provide remedies.

In terms of legal response there could be new rules, enforcement activity, or limitations placed upon certain types of technology. In terms of institutional response there would need to be regular reviews (audits), some form of oversight (regulatory agencies) and the ability for complaints to be reviewed. An ethical response might involve developing internal standards and review mechanisms. In terms of a technical response this would mean implementing safe designs and reducing the amount of information being gathered.

A governing response will depend on the nature of the risk. Therefore, systems that relate to important aspects of life like health care, policing, employment and public benefits require stronger levels of review since errors can impact people's fundamental rights.

Also, governance needs to continue to be active even after the initial system is introduced. When large amounts of data are being collected, or when organizations start using their data in new ways, the risks associated with those data collections can change. Therefore, ongoing assessments are necessary during the entire time that a system is operating.

6.7 Feedback Loop

Feedback loops exist between technological inputs and governance responses. For example, regulations and oversight can influence later design. Limiting the application of facial recognition software limits the potential for public surveillance. Limiting the type of personal data that can be collected reduces the amount of data collected by applications. Similarly, post-harm feedback exists. For example, when a data breach occurs companies will often face stricter obligations regarding their security. If evidence demonstrates that an algorithm was discriminatory then testing or restrictions may be put in place on how many

automated decisions are allowed. These examples demonstrate that development on line is not static. Humans, institutions and regulatory bodies can guide technological advancements.

Relationships Identified

Proposition 1: The greater use of advanced forms of data-intensive technologies will increase the risks to individuals' privacy unless proper limits are established around the collection and processing of data.

Proposition 2: The intermediate process of data practices and algorithmic processes mediate the relationship between the use of digital technologies and resulting human rights impacts.

Proposition 3: Weak consent and excessive and hidden profile-based data collection/processing increases the likelihood of privacy violation and discrimination against individuals.

Proposition 4: Stronger laws and regulations along with high ethical standards and greater awareness among members of the general public concerning digital technologies can help mitigate harms caused by digital technologies to human rights.

Proposition 5: Effective governance can transform digital technologies from sources of risk to protectors of rights.

Proposition 6: Human involvement in decision-making processes and providing individuals with recourse to correct errors made by automated decisions can decrease the negative impacts caused by these decisions.

Academic Contribution

The framework ties together three distinct factors (technological, ethical, and legal) into a single model. It asserts that harm to privacy arises not solely due to the existence of digital technologies but rather through the actions taken involving data practices and automated processes and poor governance. Furthermore, this model places individual human rights at the centre of assessment [27]. As discussed previously, privacy is closely related to other significant human rights including expression, equality, dignity, and autonomy. The framework supports treating privacy as a broad human right rather than strictly as an issue of data protection. Finally, the framework provides researchers with direction toward empirically assessing specific proposed relationships using methods including surveys/interviews/case studies/policy comparisons etc., as well as toward conducting assessments on specific subject matters such as healthcare/education/employment/banking/surveillance.

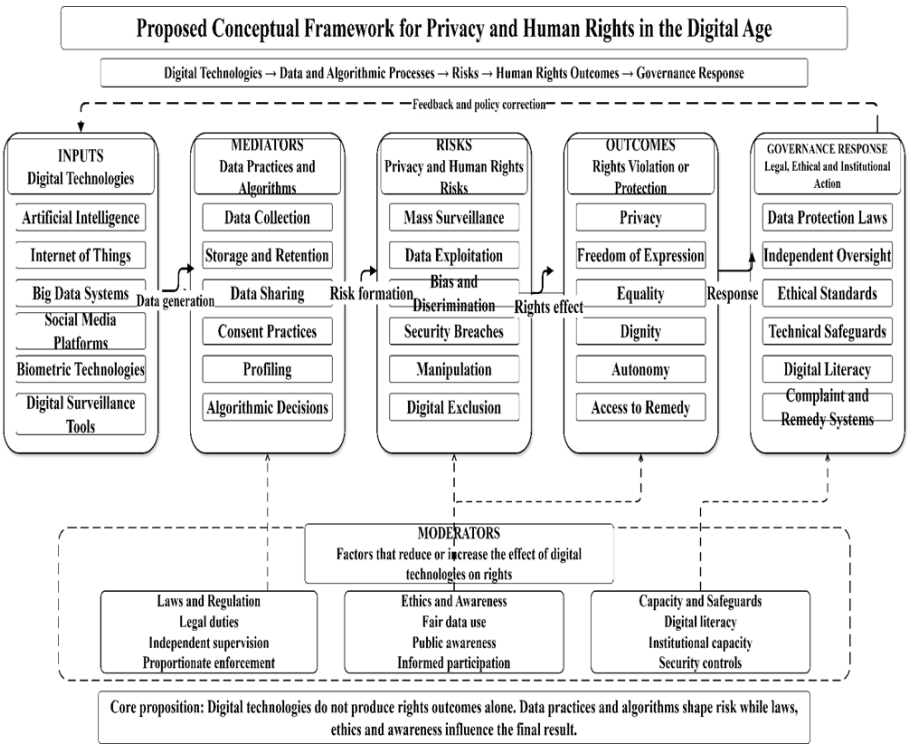

Figure 2: Proposed Conceptual Framework for Privacy and Human Rights in the Digital Age

Figure 2 illustrates how different forms of digital technology may have an impact on both privacy and human rights. The model begins with artificial intelligence. Artificial Intelligence in addition to the Internet of Things, Big Data, social media, biometric systems and digital surveillance tools are included in the model.

7. DISCUSSION

The key point here is the connection between digital technology, privacy and human rights. The literature analysis suggests that digital technology can be an important medium for both public service delivery (e.g. healthcare) and for personal freedoms (e.g. online communications). However, it can also lead to increased levels of surveillance by governments and corporations alike; the use of commercial data for targeted advertising purposes; the increasing potential for automation to discriminate against certain groups within society; and a decrease in individual's ability to exert their own free will [28].

It follows that whether or not the impact of technology is positive or negative largely depends upon how individuals' personal data is being collected, processed, distributed, and regulated.

Therefore, the research results demonstrate that privacy is much more than simply about an individual's right to keep their affairs to themselves. Privacy provides many benefits including respect for the individual's dignity, autonomy, freedom of speech and equality before the law. Therefore, a violation concerning an individual's data may have a number of different implications depending upon what type of violation it was. For example, if location tracking is being used, then there could be implications relating to either private activities or the discouragement of legitimate political protest. Automated profiling, on the other hand, may limit an individual's ability to gain credit or employment because they were identified by computerized systems. Additionally, the profiling process may be unfair to particular types of people based on their economic circumstances or social status.

This model illustrates this relationship as sequential. First, digital technologies provide the input. Secondly, data processing methods and/or algorithms serve as mediators. Thirdly, these two elements combine to generate privacy risk. Fourthly, as a consequence of those risks, violations of human rights occur. Finally, laws, codes of ethics and public awareness of data processing issues and its consequences determine the extent to which those relationships are strong or weak. Thus, once violations occur, governance solutions can emerge to mitigate them and possibly direct the design and implementation of subsequent technological innovations.

These findings suggest that a balanced view exists regarding the nature of digital technology. On one hand, digital systems can enhance public well-being by providing easy access to services. However, on the other hand, digital systems can undermine both privacy and human rights if limitations do not exist in regards to data use [29].

The major problem is not choosing between using technology versus protecting human rights. Rather, the question revolves around what rules must be established in order for technology to be developed and implemented in a way that protects human rights. The creation of rules that protect human rights does not need to prohibit all uses of lawful technology [30].

8. CONCLUSION

Digital technologies have shaped communication and several public services. There was an increase in the amount of personal information that is being gathered and processed. Due to this trend, there are growing concerns regarding both the privacy and human rights. The main issue is not with the technology itself but rather the lack of a defined and controlled purpose for the collection and/or use of personal data.

Mass surveillance and the commercialization of private data represent two significant threats to privacy. Discrimination through algorithmic decision making and cyber security issues also represent dangers to individual freedoms. Additionally, unequal access to digital platforms, inadequate informed consent mechanisms and a lack of personal control over one's own data may all negatively impact both privacy and free speech. Furthermore, equality and human dignity may be diminished. Personal autonomy will be diminished if individuals rely on algorithms and/or other forms of automation in their most critical life decisions.

The framework outlined here creates a linkage between digital technologies, data practices, risk to privacy and the potential negative impacts on human rights. A reduction in the potential harms resulting from digital technologies can occur through laws and ethical standards. Protecting privacy can also occur through increasing public awareness of potential risks and

enhancing digital literacy. Legal regulation and institutional oversight, secure data storage systems and human review of algorithmic decisions are all necessary components of governance responses to mitigate harm from digital technologies.

Protecting privacy needs to be incorporated into the development of digital policies and systems. Both government agencies and technology companies need to take responsibility for how they collect, store and utilize personal data. The framework provides a foundation for reviewing current policy and for conducting additional research to create a fair balance between the benefits of utilizing digital technologies and protecting human rights.

AUTHOR CONTRIBUTIONS

Shivika Jain: Conceptualization, Investigation, Formal Analysis.

Prof. (Dr.) Jageshwar Nath Singh: Methodology, Laboratory Analysis, Supervision, Writing—Review & Editing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

ETHICS STATEMENT

Ethical approval was not required for this study.

REFERENCES

[1] Dung, N.P., Hanh, V.T., 2025. Safeguarding Personal Data and Privacy in the Era of Artificial Intelligence Through the Human Rights Lens. *Safeguarding Personal Data and Privacy in the Era of Artificial Intelligence*, 10–20.

[2] Ahmed, M.W., Ahammed, M.M., 2024. Human Rights and Technology: Exploring How Technological Advancements Impact Human Rights, Particularly in Surveillance and Data Collection. *International Journal of Arts and Humanities Studies* 4(4), 19–27.

[3] Nováková, J., 2025. The Digital Transformation of Law and Justice: Proposing a New Normative Framework in the Context of Artificial Intelligence, Autonomous Systems, and Human Rights. *International Congress Proceedings*, 102–116.

[4] Lane, L., 2022. Clarifying Human Rights Standards Through Artificial Intelligence Initiatives. *International and Comparative Law Quarterly* 71(4), 915–944.

[5] Cheong, B.C., 2024. Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making. *Frontiers in Human Dynamics* 6.

[6] (Retd.), Prof. (Dr.) A.K., 2026. India's Constitutional Heritage in the Era of Artificial Intelligence. *Indian Journal of Law* 4(2), 23–36.

[7] Donahoe, E., Metzger, M.M., 2019. Artificial Intelligence and Human Rights. *Journal of Democracy* 30(2), 115–126.

[8] Prasad, N.R., 2025. Technological Progress vs. Human Rights: Privacy, Free Expression, and Reputation in the Era of AI and Deepfakes. *Journal of Legal Research and Polity* 2(2), 89–102.

[9] Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., Makhmari, M., 2024. The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards. *Jurnal Media Hukum* 31(2), 333–350.

[10] Aslam, H., 2022. Critical Analysis on the Intersection of Technology and Human Rights: Emerging Obstacles to Justice and Accountability. *Annals of Human and Social Sciences* 3.

[11] Kalagi, S., Gubbewad, R.S., Sahu, R., Dubey, S., 2025. Law Technology and Human Dignity: Shaping Rights Respecting Digital Future. *International Journal of Innovative Science and Research Technology*, 2519–2525.

[12] Brandusescu, A., Sieber, R., 2025. Missed Opportunities in AI Regulation: Lessons from Canada's AI and Data Act. *Data & Policy* 7.

[13] Hoxhaj, O., Halilaj, B., Harizi, A., 2023. Ethical Implications and Human Rights Violations in the Age of Artificial Intelligence. *Balkan Social Science Review* 22(22), 153–171.

[14] Khalaileh, Y., 2023. Accommodating Artificial Intelligence in International Law: An Overview and New Frontier. *Journal of Human Security* 19(1).

[15] Yam, J., Skorburg, J.A., 2021. From Human Resources to Human Rights: Impact Assessments for Hiring Algorithms. *Ethics and Information Technology* 23(4), 611–623.

[16] Tsimpourla, C., 2014. Rikki Don't Lose That Number: Enumerated Human Rights in a Society of Infinite Connections. *Future Internet* 6(3), 482–497.

[17] Dhok, S.P., 2026. The Evolving Relationship Between Technology, Law, and Human Rights. *Research Hub* 7(1), 212–219.

[18] Smuha, N.A., 2021. Beyond the Individual: Governing AI's Societal Harm. *Internet Policy Review* 10(3).

[19] Ghalijaei, L., Siri, S., 2024. Modern Technologies and Human Rights: Challenges and Solutions. *International Studies in Law and Legal Policy* 3(5), 167–179.

[20] Wang, X., 2025. A Review of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *Journal of Politics and Law* 18(4), 68.

[21] Albulayhi, O.S., 2026. Artificial Intelligence and Corporate Accountability in International Law: A Conceptual Exploration. *American Journal of Business Science Philosophy* 3(1), 46–56.

[22] Krishnan, A., 2025. The Integrated Impact of AI-Powered Military Technologies and Algorithmic Governance on Human Rights and the Rule of Law. *International Congress Proceedings*, 412–427.

[23] Muralinathan, S., 2025. Balancing Data Protection and Human Rights in the Digital Age: A Review. *International Journal of Science and Research Archive* 16(1), 505–515.

[24] Su, A., 2022. The Promise and Perils of International Human Rights Law for AI Governance. *Law, Technology and Humans* 4(1).

[25] Nandy, D., 2023. Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns. *Journal of Current Social and Political Issues* 1(1), 13–17.

[26] Edwards, L., Veale, M., 2018. Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? *IEEE Security & Privacy* 16(3), 46–54.

[27] McGregor, L., Murray, D., Ng, V., 2019. International Human Rights Law as a Framework for Algorithmic Accountability. *International and Comparative Law Quarterly* 68(2), 309–343.

[28] Srivastava, S., 2021. Algorithmic Governance and the International Politics of Big Tech. *Perspectives on Politics* 21(3), 989–1000.

[29] Bakıner, O., 2023. The Promises and Challenges of Addressing Artificial Intelligence with Human Rights. *Big Data & Society* 10(2).

[30] Reis, O., Eneh, N.E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., Abrahams, T.O., 2024. Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences* 6(1), 73–88.