




Right of Privacy and the Growing Scope of Artificial Intelligence

Syed Raza Shah Gilani¹, Ali Mohammed Al-Matrooshi², Muhammad Haroon Khan³

¹ Assistant Professor, Abdul Wali Khan University Mardan. Pakistan. Email: sgilani@awkum.edu.pk

² Police Officer, Dubai Police, General Department of Human Rights Dubai, United Arab Emirates.

Email: a.matrooshi@gmail.com

³ Deputy Registrar & Assistant Professor Department of Shariah & Law, Islamia College Peshawar, Pakistan.

Email: haroon@icp.edu.pk

ARTICLE INFO

ABSTRACT

Article History:

Received: July 16, 2023
Revised: September 17, 2023
Accepted: September 19, 2023
Available Online: September 19, 2023

Keywords:

Artificial Intelligence
Rights of Privacy
International Law

Funding:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

The exponential progress of artificial intelligence (AI) technologies has presented unparalleled challenges to the fundamental right to privacy. This abstract examines the complex interplay between privacy and artificial intelligence (AI), with a particular focus on the widening reach of AI's influence on personal data, autonomy, and individual rights. The growing integration of AI systems into our everyday lives necessitates a heightened focus on comprehending and protecting the fundamental right to privacy within the context of the digital era. This abstract commences by outlining the fundamental principles of the right to privacy and artificial intelligence (AI), thereby establishing a fundamental comprehension of the essential components involved. The subsequent analysis explores the manner in which artificial intelligence (AI) technologies are altering established conceptions of privacy. The utilization of AI-driven techniques for data collection and analysis, encompassing facial recognition, biometric identification, and predictive analytics, has generated apprehensions regarding the potential infringement upon individual privacy. The increasing proliferation of artificial intelligence poses a range of prospects and obstacles for the preservation of the right to privacy. As the development of AI technologies progresses, it becomes crucial to establish a harmonious equilibrium between leveraging the advantages of AI-driven advancements and protecting the fundamental rights to privacy of individuals.



© 2023 The Authors, Published by iRASD. This is an Open Access article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: sgilani@awkum.edu.pk

Citation: Gilani, S. R. S., Al-Matrooshi, A. M., & Khan, M. H. (2023). Right of Privacy and the Growing Scope of Artificial Intelligence. *Current Trends in Law and Society*, 3(1), 1–11. <https://doi.org/10.52131/ctls.2023.0301.0011>

1. Introduction

There is no universally accepted definition of privacy. Particularly in the United Kingdom and the United States, it is considered a safeguard against governmental, corporate, and individual intrusions into personal privacy. In certain nations, citizens are guaranteed these protections by law. For example, tax legislation in many nations demands that citizens report their income and other private financial details to the government. Especially when laws demand public revelation of issues that other nations and cultures deem private, freedom of expression may be at odds with individual privacy rules in some countries.

A right to privacy has developed in tandem with the growth of the humanist tradition. Cherednychenko (2006) The idea that each person has value beyond what society

places on them underpins the concept of privacy as a fundamental human right. When this conviction is upheld, it becomes the bedrock on which all other human rights are built.

The right to privacy is a fundamental human right that is essential for the functioning of a free and democratic society. It encompasses the individual's right to keep personal information, communications, and activities private and protected from unauthorized intrusion. The importance of the right to privacy can be understood through various dimensions: Privacy is closely linked to personal autonomy, which is the ability to make decisions about one's own life without interference or coercion. The freedom to make decisions about one's own connections, ideas, and tastes, among other things, is a fundamental component of the right to privacy. It's important because it allows people to make decisions about their own lives.

The right to privacy is essential to protecting people's honor and safety. It allows people to cultivate their unique identities and safeguard their good names. Privacy protects people from being subjected to undue scrutiny, judgment, and stigma, enabling them to speak openly and freely without continual fear of unlawful intrusion or exposure. Physical and mental safety depend on one's ability to maintain privacy. It's a way for people to safeguard themselves from harassment, violence, and other dangers. An example of the positive effects of protecting individuals' privacy is that it makes it harder for criminals to steal people's identities by keeping their financial and medical information, as well as their physical addresses, under wraps. Trust between people, organizations, and governments thrives when personal information is kept confidential. When people know they can trust one another with their personal information, they are more likely to be open with one another, reach out for assistance when they need it, and provide sensitive information when it is called for. Brems (2005) For many social interactions and institutional processes to go well, this level of trust is crucial.

The rights to privacy are inextricably linked to those to free expression, assembly, and association. People need to be able to talk openly, try out new ideas, and hang out with their friends without worrying about being watched or punished. By shielding expressions of disapproval, originality, and invention, privacy promotes a rich and varied social fabric. It makes it so people may speak their minds in public without fear of having their conversations stifled or being watched. When it comes to the authority of institutions like governments and companies, privacy serves as a necessary check. It prohibits discriminatory or manipulative use of personal data, intrusive monitoring, and abuse of power. The right to privacy protects people from having all of their personal information gathered, used, and sold to other parties without their knowledge or consent. An individual's right to privacy is essential to maintaining their independence, worth, and safety. Building confidence, upholding democratic ideals, and protecting a stable social order all depend on it. In this age of widespread data collection and dissemination, protecting individuals' rights to privacy is more important than ever (Gilani, 2019).

The right to privacy is often regarded as a basic human right. Although not specifically stated, it can be inferred from several articles of the UDHR, including Article 12, which states that "no one shall be subjected to arbitrary interference with his privacy." Other international human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR), also protect the right to privacy. The right to privacy is one of the many human rights that the United Nations (UN) works to promote and preserve. Nowlin (2002) To highlight the significance of privacy rights in the digital age, the United Nations General Assembly has enacted many resolutions on connected concerns. An independent expert, the UN Special Rapporteur on the Right to Privacy, is appointed by the Human Rights Council to report on the enjoyment and preservation of the right to privacy across the globe and offer suggestions to the Council.

The United Nations has also acknowledged the right to privacy as a crucial component of the freedoms of speech, association, and peaceful assembly. This recognition highlights the indivisibility and interdependence of human rights, with privacy playing a critical role in allowing people to freely enjoy other rights (Sobel, 2013).

Furthermore, in 2016, the UN Human Rights Council adopted a resolution on the right to privacy in the digital age. The resolution called upon states to respect and protect

individuals' right to privacy online and offline and to ensure that their surveillance activities comply with international human rights obligations. We can say that while the right to privacy may not be explicitly mentioned in the UDHR, it is widely recognized and protected by the UN and other international human rights instruments. The UN plays a vital role in promoting and safeguarding the right to privacy, particularly in the context of the digital age (Gilani, Khan, & Zahoor, 2021).

2. When it Comes to Human Rights, How Significant is the Right to Privacy?

Maintaining human dignity necessitates the protection of individual privacy, which is a fundamental human right. No one shall be subjected to arbitrary interference with his privacy, family, home, or communications, or attacks upon his honor and reputation, as stated in Article 12 of the Universal Declaration of Human Rights. Everyone has the right to be secure from such violations or assaults under the law. An individual's right to regulate and direct the dissemination of information about themselves is synonymous with the right to privacy (Lohse, 2007).

In addition, privacy has been defined as the following: the right to be left alone; freedom from interruption, intrusion, embarrassment, or accountability; the right to control the disclosure of personal information; the right to protect one's independence, dignity, and integrity; the right to maintain one's anonymity and solitude; the right to be left alone. To protect one's physical autonomy (including the right to control personal matters), to limit access to oneself (for example, by controlling communication and intrusion into one's domestic and work space), and to control one's identity are all aspects of the right to privacy. There are several areas where privacy concerns collide with other rights and liberties, including free expression, national security, police surveillance powers, personal morality, information freedom, and electronic business.

The right to privacy is considered one of the most significant human rights, as it is closely linked to individual autonomy, dignity, and the exercise of other fundamental rights. Here are a few reasons why the right to privacy is highly significant. Privacy empowers individuals to make choices about their personal lives, relationships, and activities without unwarranted interference or surveillance. It promotes the freedom to form one's own identity and to act in accordance with one's own principles. Maintaining one's sense of worth requires a degree of privacy. It safeguards people from public shame by letting them conceal certain details about themselves. Personal development, introspection, and the risk-free exploration of new ideas are all aided by the protection that privacy provides. Polakiewicz (1994) It's a great way for people to avoid becoming victims of identity theft, harassment, or prejudice. Surviving domestic abuse, political dissidents, and members of disadvantaged groups are just some of the vulnerable people who greatly benefit from privacy protections. The rights to free speech and assembly are inextricably linked to the right to privacy. It establishes a protected environment in which people may speak freely without worrying about being monitored, censored, or punished. In addition to promoting variety, innovation, and societal advancement, privacy safeguards the right to freely interact and build communities among individuals.

The right to privacy serves as a safeguard against arbitrary state surveillance and control. It prevents governments from conducting unwanted monitoring, collecting data, or invading people's privacy. To avoid excessive government control and to advance democratic norms, privacy aids in maintaining a balance between security concerns and the preservation of civil freedoms. The protection of personal privacy is more important than ever in the Internet era. Personal information is being gathered, processed, and disseminated at an unprecedented rate because of technological developments. Individuals need privacy protections to prevent data breaches, identity theft, and unlawful monitoring in the digital sphere. The right to privacy is vital because it protects people's independence, self-respect, safety, and the ability to pursue other basic liberties. It protects citizens against tyrannical governments, advances the rights to free speech and association, and finds solutions to problems brought on by the information age (Coblentz & Warshaw, 1956).

3. The Security of Preexisting Privacy Laws

Existing privacy laws offer a variety of protections for the right to privacy. While local privacy frameworks will vary depending on the specific laws and regulations in place, many will share the following features. First, the collection, storage, processing, and sharing of personal data are regulated by data protection regulations in many countries. Consent is often required for data gathering, data security is guaranteed, individuals are given access to their data, and channels are set up so that people may exercise their privacy rights. Providing people with clear and open information on the collection, use, and sharing of their personal data is a common requirement for businesses. People have the right to know why their data is being collected, what data is being collected, and what they can do with that data. Obtaining people's informed permission prior to collecting and using their personal data is a common theme in privacy regulations. People should be able to make decisions about their data, such as whether or not to share it, revoke their permission, or have their data deleted. Gilani, Rehman, and Khan (2021) As most privacy regulations require, only gather and manage the bare minimum of personal data necessary for the stated purpose. In addition, they demand that businesses specify the goals of data collection and utilize it only for those goals. Businesses are legally obligated to take reasonable precautions to prevent the loss, misuse, unauthorized disclosure of, or damage to personal information in their care. Encryption, permissions, and regular audits are all part of these precautions.

Individuals are typically given rights under privacy regulations to have some say in how their information is used. A data subject may have the right to view their information, rectify any mistakes, have the information erased or rectified, have further processing limited, or raise objections to certain forms of processing, such as marketing (Josipović, 2016).

To prevent sensitive information from getting into the wrong hands if sent to nations without equivalent protections, privacy regulations govern data transfers across international borders. Lawful foreign data transfers are typically facilitated via the employment of mechanisms like data transfer agreements, binding business norms, or adequacy judgments. In the event of a breach, privacy rules provide for sanctions and remedies. Individuals may have the right to seek legal redress and compensation in the event of a violation of their privacy, which may take the form of fines, penalties, audits, or all of the above.

It's worth noting that privacy laws provide varying levels of protection depending on location and jurisdiction. In order to know their rights and responsibilities with regards to privacy protection, businesses and individuals should study the relevant privacy legislation in their country or region.

4. Laws Protecting Individual Privacy and Data

Since the purpose of data protection laws is to protect people's privacy, they go hand in hand with the right to privacy. With the intention of safeguarding people's privacy and avoiding the misuse of their personal information, data protection laws often create rules and standards for the collection, use, processing, and sharing of such data.

Some of the most important ways in which data protection regulations safeguard individuals' privacy are as follows: In order to collect, use, or share an individual's personal information, many data privacy regulations mandate that organizations first seek the individual's permission. This guarantees that people are informed of how their data will be used and offers them more control over their personal information. Organizations are generally required by data protection legislation to disclose their data practices, including the collection, use, and sharing of personal information. People are then better able to decide whether or not to provide information and, if so, for what purposes. DeMerieux (2001) Organizations are generally required by data protection rules to gather and use personal data only for specified, lawful reasons. This helps preserve people's privacy by preventing the misuse of their personal information. Organizations are generally required by data protection rules to gather just the minimum amount of personal data necessary to

fulfill their stated objectives. This lessens the likelihood of privacy infractions by limiting the gathering and use of personal data.

Organizations are obligated to take reasonable precautions to prevent the loss, misuse, and alteration of personal information in accordance with data protection legislation. This lessens the likelihood of data breaches and other privacy infractions and helps maintain the secrecy and integrity of sensitive information. Rights to access data, rectify data that is inaccurate, have data erased or removed, or limit data processing are all common provisions of data privacy legislation. Individuals are better able to safeguard their privacy and maintain control over their personal data thanks to these protections. The usual response to infractions of data protection rules is the establishment of enforcement procedures and remedies. Possible consequences for privacy violations include monetary fines, jail time, and the ability to sue for damages. Organizational compliance with privacy rules and the protection of people's personal information are aided by enforcement efforts (Jafari, 2003).

By setting norms and standards for the collection, use, processing, and sharing of personal data, data protection laws play an essential role in protecting the right to privacy. Data protection laws assist in promoting human autonomy, dignity, and personal security by requiring companies to secure personal information and comply with people's requests for its deletion or correction.

4.1. Transparency and Privacy Notices

Important parts of privacy protection under dataprotection legislation are privacy notifications and openness. Organizations are required by law to inform their customers and prospective customers about the data collection, usage, processing, and sharing practices that they have in place. The objective of privacy notifications is to educate customers about how the company handles their personal information. They need to make it very obvious to users why and how their personal information will be utilized. When people know why their data is being gathered, they may make educated judgments about whether or not to disclose it. Names, email addresses, and financial data are all examples of the kinds of personally identifiable information that should be included but not too complicated in privacy notifications. Data collection methods, including whether they are collected directly from individuals or from other sources, should also be specified.

Privacy notices should outline how the organization processes personal data, including details about storage, security measures, retention periods, and any data transfers to third parties or other countries. This ensures individuals are aware of how their data is handled and if it may be shared with other entities. Privacy notices should indicate the legal basis for processing personal data. Common legal bases include consent, legitimate interests, contractual necessity, or compliance with legal obligations. Misthal (1998) This helps individuals understand the lawful grounds on which their data is being processed. Privacy notices should inform individuals of their rights regarding their personal data. This may include the right to access, rectify, delete, restrict processing, and object to data processing activities. Individuals should be provided with instructions on how to exercise these rights.

If personal data is shared with third parties, privacy notices should clearly state the categories of recipients and the purpose of such sharing. It is important to disclose whether data will be shared with service providers, business partners, or other organizations. Privacy notices should address the use of cookies and other tracking technologies on websites or applications. They should inform individuals about the types of cookies used, their purpose, and any options to manage or disable them. Organizations should mention if and how the privacy notice can be updated or revised. If significant changes occur, individuals should be informed and, in some cases, provided with an opportunity to consent to the revised privacy practices.

Transparency in privacy notices ensures that individuals have access to clear and understandable information about how their personal data is handled. It promotes trust,

empowers individuals to make informed choices about their privacy, and allows them to exercise their privacy rights effectively.

4.2. Consent and Control

Privacy laws often emphasize the importance of obtaining individuals' consent and granting them control over their personal data. Here are key points regarding consent and control under privacy laws: Privacy laws typically require organizations to obtain individuals' informed consent before collecting, processing, or sharing their personal data. Informed consent means that individuals should be provided with clear and specific information about the purposes and scope of data processing, any third parties involved, and their rights regarding their data. Privacy laws require that consent be freely given without any form of coercion or undue influence. Individuals should have a genuine choice and not be compelled to provide their personal data or consent to its processing. Privacy laws often require organizations to use opt-in mechanisms for obtaining consent, meaning that individuals actively indicate their agreement. In some cases, opt-out mechanisms may be used for specific types of data processing, but they must be clearly explained and easily accessible for individuals to withdraw their consent (Rempel, 1991).

Individuals have the right to revoke their permission at any moment under most privacy regulations. Companies need to let customers know that they have this privilege and give them an easy way to revoke it. Unless there are other permissible reasons for processing, organizations should stop using the data after a withdrawal and, if necessary, destroy or anonymize it. It is the goal of privacy legislation to give people agency over their own information. Individuals should be able to view their data, correct any mistakes, seek deletion or limitation of processing, and object to some forms of data processing, such as direct marketing, from the organizations that collect and use their information. Organizations are generally obligated by privacy rules to provide users with control over the way in which their personal information is collected, used, and shared. For individuals to be able to efficiently manage their privacy choices, businesses should provide simple and straightforward interfaces.

When dealing with the personal information of minors, it is customary to first obtain their permission. Minors may need their parents' or guardians' permission to do certain things in some places. In order to comply with privacy regulations, businesses must typically provide evidence of informed consent. Consent records may need to be kept, the consent process may need to be documented, and compliance with consent laws must be verifiable. It is the goal of privacy legislation to give people more control over their personal information by including consent and control mechanisms. To protect individuals' right to privacy and promote trust in organizations' data-processing operations, privacy laws mandate that organizations acquire consent from individuals once they have been made aware of their options.

5. Rights of Individuals: Privacy laws

Privacy laws typically grant individuals certain rights regarding their personal data. These rights empower individuals to exercise control over their information and ensure that their privacy is respected. While specific rights may vary depending on the jurisdiction, here are some common rights of individuals under privacy laws: Individuals have the right to obtain confirmation from organizations as to whether their personal data is being processed and, if so, to access that data. They can request information about the purpose of processing, the categories of data being processed, and recipients or categories of recipients who have access to their data. Individuals have the right to request the correction of inaccurate or incomplete personal data held by organizations. If they believe that their data is outdated, incorrect, or no longer relevant, they can request its update or amendment. In accordance with Article 1 of the General Data Protection Regulation (GDPR), individuals have the right to request that their personal data be erased. However, there are circumstances in which this right does not apply, including when the data is no longer needed for those purposes, when the individual withdraws their consent, or when the processing of the data is illegal.

Individuals have the right to request that further processing of their personal data be restricted. This option is available if the data's veracity is disputed, the processing is illegal, or the information is no longer necessary for the purposes it was collected. Strossen (1992) individuals have the right to receive a copy of their personal data in a structured, commonly used, and machine-readable format. They can also request that the data be transmitted directly to another organization, if technically feasible and if the processing is based on consent or contract. Individuals have the right to object to the processing of their personal data in certain circumstances. They can object to direct marketing activities, processing based on legitimate interests, or processing for research or statistical purposes. If personal data processing is based on consent, individuals have the right to withdraw their consent at any time. Organizations must make it easy for individuals to withdraw consent and stop processing the data accordingly. Right to Lodge a Complaint: Individuals have the right to lodge complaints with the relevant data protection authority if they believe their privacy rights have been violated. They can seek investigation, remedies, and enforcement of their rights through the regulatory body.

Privacy laws aim to empower individuals and give them control over their personal data. By providing these rights, individuals can be actively involved in the management and protection of their information, fostering transparency, accountability, and trust between individuals and organizations that process their data.

6. Cross-Border Data Transfers: Privacy laws

Cross-border data transfers refer to the transfer of personal data from one country to another. Privacy laws often include provisions that regulate such transfers to ensure the protection of personal data when it is transferred outside the jurisdiction where it was originally collected. Here are key points regarding cross-border data transfers under privacy laws: Some privacy laws recognize specific countries or regions as having an "adequate" level of data protection. Adequate countries are considered to provide a level of protection that is essentially equivalent to the privacy standards of the originating jurisdiction.

Transfers to adequate countries are generally allowed without additional safeguards.

1. Standard Contractual Clauses (SCCs): Privacy laws may permit cross-border transfers of personal data using SCCs, which are contractual clauses approved by relevant authorities. SCCs include safeguards that protect personal data during the transfer and provide rights and remedies for individuals whose data is transferred.
2. Binding Corporate Rules (BCRs): BCRs are internal policies and rules adopted by multinational organizations that govern cross-border transfers of personal data within their group of companies. BCRs must be approved by relevant data protection authorities and provide adequate safeguards for the protection of personal data (Gutwirth, 2002).

Privacy laws may allow for cross-border transfers based on certification mechanisms or codes of conduct that provide sufficient safeguards for the protection of personal data. These mechanisms often require organizations to adhere to specific privacy standards and practices. Individuals' explicit consent may serve as a legal basis for cross-border data transfers in some cases. Privacy laws may require organizations to obtain informed and explicit consent from individuals before transferring their personal data to another country. Privacy laws may include derogations or exceptions that allow cross-border data transfers even in the absence of specific safeguards. These derogations could include situations where the transfer is necessary for the performance of a contract, the protection of vital interests, or the establishment, exercise, or defense of legal claims.

In certain cases, privacy laws require organizations to obtain regulatory approvals or seek authorization from relevant data protection authorities before transferring personal data across borders. This ensures that authorities can assess the adequacy of data protection safeguards in place. Privacy laws may require organizations to implement additional safeguards or measures to protect personal data during cross-border transfers. This could include encryption, pseudonymization, data anonymization, or contractual provisions that enhance data protection. Privacy laws aim to strike a balance between

facilitating international data flows and protecting individuals' privacy rights. By regulating cross-border data transfers, these laws seek to ensure that personal data is adequately protected even when it moves between different jurisdictions with potentially varying levels of data protection standards.

7. Right to Privacy Laws Can Change and Evolve

As privacy laws can change and evolve, it's important to consult up-to-date sources and seek legal advice to understand the specific provisions and implications of privacy legislation in Australia.

The High Court considered the potential for creating a tort if an adequate case involving a person was brought forward in *Lenah v. ABC*, which involved charges of invasion of corporate privacy. In 2003, *Gross v. Purvis* was decided by a District Court Judge in the state of Queensland; the plaintiff was awarded AUD\$180,000 for invasion of privacy.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and the Guidelines of the Organization for Economic Co-operation and Development (OECD) are largely implemented in the Privacy Act 1988 (Cwth), the fundamental Australian Federal legislation. The OECD Guidelines that govern the actions of most agencies of the Australian Commonwealth Government are reflected in the document's Information Privacy Principles (Pesapane, Volonté, Codari, & Sardanelli). A new set of regulations concerning the handling of consumers' credit information was enacted in 1989 and is binding on both the commercial and governmental sectors. Guidelines released by the Privacy Commissioner that are implemented as subordinate law also include the use of the Australian government's Tax File Number (TFN), which is granted to every citizen of Australia. The privacy act resulted from opposition to "The Australia Card Scheme," a national identity card that the government proposed in the 1980s. However, the tax file number was improved so that it could be used to match income from multiple sources after the proposal was scrapped due to the uproar it caused. The Privacy Act was able to offer some safety. Since then, the TFN has come to be used not only for tax purposes but also for managing benefits. The Privacy Act established certain regulations on such matching in 1990.

In April 2000, following significant debate, the Australian government passed the Privacy Amendment (Private Sector) Act to extend privacy protections to the private sector. The national privacy guidelines created by this law are based on the Federal Privacy Commissioner's earlier guidelines for the appropriate management of personally identifiable information. Private firms must now adhere to these regulations, although they can seek approval from the Privacy Commissioner for an internal code of practice that mirrors the National Privacy Principles. International privacy advocates have voiced concern that the Act falls short of their expectations.

All of the states and territories now have Freedom of Information Acts on the books, making it possible for citizens to request and make changes to their own records. Yes, you are correct. Privacy laws can change and evolve over time to address emerging challenges and developments in technology, societal norms, and legal considerations. Here are a few reasons why privacy laws may change. Rapid advancements in technology, such as the internet, social media, biometrics, and artificial intelligence, have led to new privacy concerns. Privacy laws may need to be updated or expanded to address these emerging technologies and their impact on individuals' privacy. High-profile data breaches and security incidents can highlight weaknesses in existing privacy laws. In response, lawmakers may introduce new regulations or strengthen existing ones to enhance data security and breach notification requirements. DeMerieux (2001) with the increasing globalization of data flows, countries often seek to align their privacy laws with international standards and frameworks. This harmonization can lead to changes in domestic privacy laws to ensure compatibility and facilitate cross-border data transfers. Privacy-related issues that gain public attention and concern can drive legislative action. Advocacy efforts by privacy groups, consumer organizations, and individuals can influence lawmakers to strengthen privacy protections or introduce new legislation. Judicial rulings and court decisions can shape the interpretation and application of privacy laws. Landmark cases and legal precedents can prompt lawmakers to revise privacy laws to align with evolving judicial interpretations.

Privacy regulators and authorities may issue updated guidance, frameworks, or codes of practice that reflect evolving privacy considerations. These updates can lead to legislative changes to ensure alignment between regulations and regulatory guidance. As societal norms and expectations regarding privacy evolve, lawmakers may respond by revising privacy laws to reflect these changing dynamics. This can include recognizing new privacy rights or expanding the scope of existing protections (Barański, 2021).

It is important for privacy laws to adapt and stay relevant to effectively protect individuals' privacy rights in a rapidly changing digital landscape. Governments, regulators, and policymakers regularly review and update privacy laws to address emerging challenges and maintain an appropriate balance between privacy and other societal interests.

7.1. Enforcement and Remedies

Enforcement and remedies are crucial aspects of privacy laws as they ensure that organizations comply with the requirements and provisions of the laws and individuals' privacy rights are effectively protected. The following are some of the most important aspects of privacy legislation, enforcement, and remedies:

1. To ensure that privacy rules are followed, they usually create independent regulatory agencies called Data Protection Authorities (DPAs), whose job it is to monitor and enforce such laws. DPAs are authorized to look into privacy-related complaints, perform audits, levy penalties, and offer advice.
2. To guarantee they are meeting their privacy commitments, businesses may need to set up internal procedures for monitoring and auditing compliance with privacy legislation. This entails doing privacy impact analyses, audits, and evaluations of data protection procedures on a regular basis.
3. Thirdly, if an individual feels their privacy rights have been abused, they may file a complaint with a data protection authority (DPA) or another recognized body. When citizens file complaints, authorities investigate and may take legal action against businesses (Gilani, Ali, & Zahoor, 2023).
4. Fourth, firms that don't comply with privacy regulations might face fines and other consequences if they're caught breaking the rules. Fines and punishments might be more or less severe, depending on the jurisdiction involved and the seriousness of the offense.
5. Corrective Measures and Orders: DPAs can force businesses to fix any privacy law violations by issuing corrective measures and orders. Data protection measures, data processing activities, and the deletion of illegally processed data may all fall under this category.
6. To prevent additional damage or improper data processing, DPAs may have the jurisdiction to issue injunctions or cease-and-desist orders to organizations that breach privacy regulations, depending on the specifics of the legislation.
7. Compensation and Damages: People who have their privacy violated may be entitled to monetary compensation or other forms of damages under the law. Damages might be monetary, in the form of lost income, or reputational, in the form of emotional pain, or both (Gilani, Zahoor, & Iqbal, 2022).
8. Criminal Sanctions: Privacy laws may contain criminal penalties for major privacy infractions in some jurisdictions. Intentional or flagrant infringements of privacy laws may result in criminal accusations, punishment, and maybe imprisonment.
9. To resolve privacy breaches and avoid future violations, businesses are generally required by privacy regulations to take remedial actions and adopt corrective measures. Notifying those who are directly affected, bolstering data security, providing privacy education, and reevaluating current procedures are all possible next steps (McBeth & Nolan, 2012).

Enforcement and remedies under privacy laws are essential for ensuring accountability, deterring non-compliance, and protecting individuals' privacy rights. By imposing penalties, conducting investigations, and providing avenues for individuals to seek redress, privacy laws aim to maintain the integrity of privacy protections and promote responsible data handling practices.

8. Conclusion

The right to privacy is a fundamental human right that protects individuals' autonomy, dignity, and personal space. While the right to privacy is not explicitly stated in all constitutions, it is recognized and protected through various legal mechanisms, including constitutional provisions, legislation, and court decisions. The purpose of privacy legislation is to find a happy medium between safeguarding individuals' rights to privacy and allowing for other legitimate interests, such as those of the government, law enforcement, the public good, and private enterprise. Individuals are given more control over their data, and more openness and accountability are encouraged by these regulations that regulate the gathering, use, and dissemination of this information. However, new technologies and the ever-changing digital landscape present fresh threats to individual confidentiality. Concerns concerning the erosion of privacy rights have been brought to light by issues including mass spying, data breaches, internet monitoring, and the acquisition of personal data by digital corporations. Since the world is becoming more and more interconnected, privacy laws and regulations are constantly being updated to meet these new threats. Protecting personal privacy should be a top priority for everyone, from citizens to businesses to governments at all levels. This entails being familiar with privacy regulations, pushing for more safeguards, and making sure regulations evolve alongside technology and social changes.

Ultimately, the right to privacy is crucial for fostering trust, preserving personal autonomy, and safeguarding individual freedoms in an increasingly digitized and interconnected world. Protecting and upholding privacy rights is an ongoing process that requires a collective effort from governments, organizations, and individuals to ensure that privacy remains a fundamental pillar of a democratic and rights-respecting society. Each person should be allowed to make his or her own choices without interference from the government in the most private and sensitive areas of life. If their activities only have an effect on themselves, then they should be allowed to do anything they choose. Although some people dispute the existence of an "implicit" legal right to privacy, which they claim exists in the shadows of certain Amendments, the debate can be settled by making this right explicit. Attempting to shift the law from its current state to where it should be is an eternal moral endeavor. The law should be an institution that protects people's right to make decisions about their own lives without interference from the state.

A privacy amendment would help bring the law in line with these ethical realities. The gap between the current state of the law and where it should be might be reduced with an amendment pertaining to privacy.

Author contribution

Syed Raza Shah Gilani: introduction section, and original draft

Ali Mohammed Al-Matroosh: Complete the Initial draft preparation and incorporate the comments.

Muhammad Haroon Khan: Justification of objectives, incorporate the comments and finalize the paper.

Conflict of Interests/Disclosures

The authors declared no potential conflicts of interest w.r.t the research, authorship and/or publication of this article.

References

- Barański, M. (2021). *Artificial intelligence in the workplace through the prism of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms*. Paper presented at the Artificial intelligence in the workplace through the prism of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.
- Brems, E. (2005). Conflicting human rights: an exploration in the context of the right to a fair trial in the European Convention for the protection of human rights and fundamental freedoms. *Human Rights Quarterly*, 294-326.

- Cherednychenko, O. O. (2006). EU fundamental rights, EC fundamental freedoms and private law. *European Review of Private Law*, 14(1). doi:<https://doi.org/10.54648/erpl2006002>
- Coblentz, W. K., & Warshaw, R. S. (1956). European convention for the Protection of human rights and fundamental freedoms. *Calif. L. Rev.*, 44, 94.
- DeMerieux, M. (2001). Deriving environmental rights from the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Oxford Journal of legal studies*, 21(3), 521-561. doi:<https://doi.org/10.1093/ojls/21.3.521>
- Gilani, S. R. S. (2019). *The significance of the doctrine of proportionality in the context of militant democracy to protect the freedom of expression*. Brunel University London, Retrieved from <http://bura.brunel.ac.uk/handle/2438/19725>
- Gilani, S. R. S., Ali, M. A., & Zahoor, M. S. (2023). Limitations on Parliamentary Sovereignty in the UK: A Critical Analysis. *Journal of European Studies (JES)*, 39(1), 47-47. doi:<https://doi.org/10.56384/jes.v39i1.288>
- Gilani, S. R. S., Khan, I., & Zahoor, S. (2021). The Historical Origins of the Proportionality Doctrine as a tool of Judicial Review: A Critical Analysis. *Research Journal of Social Sciences and Economics Review*, 2(1), 251-258. doi:[https://doi.org/10.36902/rjsser-vol2-iss1-2021\(251-258\)](https://doi.org/10.36902/rjsser-vol2-iss1-2021(251-258))
- Gilani, S. R. S., Rehman, H. U., & Khan, I. (2021). The Conceptual Analysis of the Doctrine of Proportionality and, its Role in Democratic Constitutionalism; A Case Study of UK. *sjesr*, 4(1), 204-210. doi:[https://doi.org/10.36902/sjesr-vol4-iss1-2021\(204-210\)](https://doi.org/10.36902/sjesr-vol4-iss1-2021(204-210))
- Gilani, S. R. S., Zahoor, S., & Iqbal, M. A. (2022). Child Labor in Pakistan: Causes, Consequences and Prevention. *Pakistan Social Sciences Review*, 6(2), 197-208.
- Gutwirth, S. (2002). *Privacy and the information age*: Rowman & Littlefield.
- Jafari, J. (2003). Attacks from within: Zimbabwe's assault on basic freedoms through legislation. *Human Rights Brief*, 10(3), 2.
- Josipović, T. (2016). The Role of Human Rights and Fundamental Freedoms for the Development of Croatian Private Law. *The Influence of Human Rights and Basic Rights in Private Law*, 199-246. doi:<https://doi.org/10.1007/978-3-319-25337-4>
- Lohse, E. J. (2007). Fundamental Freedoms and Private Actors-towards an Indirect Horizontal Effect. *Eur. Pub. L.*, 13, 159.
- McBeth, A., & Nolan, J. (2012). The International Protection of Human Rights and Fundamental Freedoms. *International Corporate Legal Responsibility*, 175-254.
- Misthal, M. P. (1998). Reigning in the Paparazzi: The Human Rights Act, The European Convention on Human Rights and Fundamental Freedoms, and the Rights of Privacy and Publicity in England. *Int'l Legal Persp.*, 10, 287.
- Nowlin, C. (2002). The protection of morals under the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Human Rights Quarterly*, 24(1), 264-286.
- Pesapane, F., Volonté, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. *Insights into imaging*, 9, 745-753. doi:<https://doi.org/10.1007/s13244-018-0645-y>
- Polakiewicz, J. (1994). The Implementation of the European Convention for the Protection of Human Rights and Fundamental Freedoms in the Field of Private Law. *Tel Aviv U. Stud. L.*, 12, 181.
- Rempel, R. (1991). Fundamental Freedoms, Private Actors and the Saskatchewan Bill of Rights. *Sask. L. Rev.*, 55, 263.
- Sobel, R. (2013). The right to travel and privacy: Intersecting fundamental freedoms. *J. Marshall J. Info. Tech. & Privacy L.*, 30, 639.
- Strossen, N. (1992). What Constitutes Full Protection of Fundamental Freedoms. *Harv. JL & Pub. Pol'y*, 15, 43.