DIGITAL PRIVACY - A NEW FRONTIER FOR FUNDAMENTAL RIGHTS

T Saroja Devi, VISTAS

ABSTRACT:

Demanding re- evaluation of privacy as a fundamental right in the digital world is the concept of privacy will become a pressing concern that has rapidly evolved significantly for individuals, Governments, and Organizations alike. The technological development of the 21st century has made how personal data is collected, processed, stored and shared. Digital privacy as a fundamental right, a New Frontier to Constitution and other Statutes to establish as a cornerstone, in regards to safeguarding the personal information in the online domain. The protection of personal data leads towards freedom of expression, thought and decision-making. The need for the digital privacy for fundamental rights is In order to avoid unauthorized profiling identity theft and misuse of their information. And the term 'privacy' is tied up with preserving Human Dignity. Today's challenges in the digital age is the technological growth in the rise of big data, AI and IOT devices. Lack of robust systems to prevent data breaches, hacking, unauthorized access exacerbates privacy vulnerabilities etc which falls towards cyber crime. Challenges faced in surveillance - boundaries of privacy and individual freedoms. In Technological Accountability the developers and companies should focus more on designing systems with the core principle of privacy. So in order to control all the issues in digital privacy a pathway ahead is to include it as Fundamental Right so that the Government must prioritize individual rights interest. As a fundamental right Digital privacy not only protects individuals but also Democratic Principles, human dignity and social trust. Along with that Educating individuals about their rights and digital safety is essential.

Introduction:

Demanding re- evaluation of privacy as a fundamental right in the digital world is the concept of privacy will become a pressing concern that has rapidly evolved significantly for individuals, Governments, and Organizations alike. The technological development of the 21st century has made how personal data is collected, processed, stored and shared. Digital privacy as a fundamental right, a New Frontier to Constitution and other Statutes to establish as a cornerstone, in regards to safeguarding the personal information in the online domain. The protection of personal data leads towards freedom of expression, thought and decision-making. The need for the digital privacy for fundamental rights is In order to avoid unauthorized profiling identity theft and misuse of their information. And the term 'privacy' is tied up with preserving Human Dignity. Today's challenges in the digital age is the technological growth in the rise of big data, AI and IOT devices. Lack of robust systems to prevent data breaches, hacking, unauthorized access exacerbates privacy vulnerabilities etc which falls towards cyber crime. Challenges faced in surveillance - boundaries of privacy and individual freedoms. In Technological Accountability the developers and companies should focus more on designing systems with the core principle of privacy. So in order to control all the issues in digital privacy a pathway ahead is to include it as Fundamental Right so that the Government must prioritize individual rights interest. As a fundamental right Digital privacy not only protects individuals but also Democratic Principles, human dignity and social trust. Along with that Educating individuals about their rights and digital safety is essential.

Digital Rights as a Fundamental rights :

The digital age has significantly expanded privacy rights, encompassing control over personal information shared across digital platforms. However, this evolution poses challenges as technologies like artificial intelligence, big data analytics, and IoT often erode user autonomy and expose individuals to risks of surveillance, profiling, and misuse of personal data. Legal frameworks like the European Union's GDPR and California's Consumer Privacy Act (CCPA) aim to balance innovation with ethical practices, enforcing measures like the right to be forgotten, data localization, and restrictions on automated decision-making.

Unresolved issues persist, such as social media platforms gathering vast data through opaque practices, biometric technologies and smart devices offering convenience but at the expense of

user privacy, and ethical questions about ensuring equitable privacy protections for marginalized groups and bridging the digital divide. The future of privacy rights lies in developing technologies like blockchain, which promises secure, decentralized data storage, and advancing legal standards that accommodate emerging challenges. Efforts to create universal privacy principles may further protect individuals in an increasingly digital and borderless world, ensuring innovation respects human dignity and autonomy.

The Right to control one's personal information, to protect against unauthorized surveillance and to ensure data security are the inclusion of digital privacy as a Fundamental Right is important in today's digital age due to the technological advancements that have deeply spread into every aspect of Human life. Ever expanding scope of digital technologies has raised concerns about data issues, cyber threats and the exploitation of personal information by both private entities and governments. Individuals will have great autonomy over their digital footprint and safeguard their personal data from unauthorized access by Recognizing Digital Privacy as a Fundamental Right. Challenges like mass surveillance, data breaches, misuse of AI, would strengthen the legal framework in order to make Digital Privacy within the ambit Fundamental Rights. The collection and use of personal data are transparent and lawful; the only safeguard would serve as a right to digital privacy, a fundamental right.

Pros and Cons of Digital Privacy in the 21st century:

Digital privacy in the 21st century the individual control over their personal data, that reduces identity theft, misuse of sensitive information and unauthorized surveillance. Individuals can themselves freely express their view without fear of being monitored that ensures the freedom of speech and association. Prevention of Surveillance abuse extends the limit to governments and corporations that can help to engage in mass surveillance that will prevent the authoritarian control and protection of the democratic values. Individuals have trust in digital platforms enabling users to engage in online activities such as e-commerce, social networking, and remove work with confidence. Reduces the vulnerabilities to cyberattacks and breaches due to the regulations that come with requirements for strong data protection mechanisms. When there is more priority in Digital world in the 21st century, tech companies are compelled to focus on the development of more privacy security and a separate online platform is created for privacy-Compliant technologies with more innovation in fields like encryption, AI ethics and secure communication tools. GDPR (General Data Protection

Regulation) helps Digital Privacy to align national laws with Global frameworks promoting International Collaboration and Consistency in addressing cross- border data issues.

Small and Medium Sized enterprises which can be costly and resource-intensive often struggle to comply with stringent privacy regulations. Reduced personalization towards the data collection in the areas like customer service, target advertising, leads to reducing the user experience may limit the ability of companies in privacy protection. Potential for misuse by criminals on privacy can inadvertently empower malicious actors, such as hackers and terrorists. Sometimes barriers to innovation in the name of privacy over regulation can stifle innovation, emerging technologies and particularly for startups that rely on data analysis for development and growth. Global disparities in privacy laws due to the absence of universal digital privacy standards creates inconsistencies, making it difficult for multinational corporations and individuals to navigate varying legal requirements across jurisdictions. Privacy protection leads towards the advanced technological infrastructure, potentially leaving behind regions and populations with limited access to such resources. Privacy-centric technologies, which in turn slows the adoption of these innovations because many users remain unaware of the importance of digital privacy.

Freedom of Expression:

The digital age enabling individuals to share opinions, connect with global audiences, empower marginalized voices has revolutionized freedom of expression. In public discourse, to participate with anyone in internet access the social media platforms, logs and instant messaging services have enabled democratized information. These Digital tools also introduced new challenges, complicating the balance between freedom of expression and the regulation of harmful content. The challenges without infringing on the Right to free speech are often faced by governments and platforms. The internet's vast reach and anonymity have the ability to disseminate diverse opinions creating spaces for hate speech, misinformation and online harassment. In democratic societies, freedom of expression is protected under the Constitutional law with exceptions for speech that incites violence or harm. Legal and ethical frameworks vary globally, reflecting diverse cultural, political and social priorities. However, digital technologies are exploited by some authoritarian regimes to stifle dissent and curb civil liberties. Digital Governance is essential to ensure freedom of expression towards encouraging transparency, accountability and respect for human rights.

E Governance and Digital Democracy:

Introducing E-Governance and Digital Democracy has revolutionized governance and democracy as transformative forces in the relationship between citizens and the state. These innovations leverage technology to enhance public administration, improve transparency and foster greater civics engagement. Challenges such as data security, ethical considerations remain the same.

The use of Digital tools and technologies to improve the Government service delivery, promote accountability, to improve Government operations. Examples: Digital Platforms like India's Aadhaar system, digital payments, mobile apps and online portals etc allows citizens to establish and manage businesses entirely online.

Human Dignity tied up with Digital Privacy:

Privacy is threatened by data collection, surveillance and cyberattacks, robusting data protection laws. The Right to fair trial is threatened by digital technologies like AI and facial recognition in law enforcement. Access to information causes a lack towards necessary tools that is hindered by the digital divide. In digital systems, non discrimination and equality are at risk due to algorithm biases, necessitating fairness and transparency in digital systems. Cyber crime, harassment, and digital violence etc that the individuals to be protected by Digital Security. Thus, legal frameworks and ethical development are crucial to ensure digital advancements that uphold fundamental freedoms.

Strengthening the legal Framework:

Digital Privacy by addressing the unique challenges posed by technological advancements needed for strengthening legal frameworks. In order to make strong a legal framework is needed to safeguard Fundamental Rights and foster trust in digital systems. The rapid pace of innovation has created gaps in areas like data protection, cybersecurity, intellectual property and digital rights.

Individual privacy and ensure transparent handling of data must protect the data protection as a key area requiring attention as per existing laws. Responsibilities lie between both private and public sectors in cyber security is another critical area with stronger laws

governing online security. Legal frameworks establish clear accountability for breaches, ensure cross-border cooperation in tackling cybercrime should mandate cybersecurity measures. Legal reforms needed in areas like e-commerce, digital contracts and taxation to ensure fairness and consumer protection. Intellectual Property laws must adapt to address digital content creation, distribution and copyright enforcement, new approaches to copyright protection are necessary to balance creator rights with public access to knowledge.

Factors like unequal access to technology, cybersecurity threats and data privacy breaches, algorithm-based decision making can undermine the fairness of legal proceedings. In the digital Privacy, legal systems must ensure digital innovation respects fundamental rights, such as the right to be heard, equal access to justice and protection from discrimination. This should make strong regulations, investments in digital infrastructure, ethical oversight of technologies.

Cyber security:

Cybersecurity involves protecting digital systems, data from unauthorized access, theft and damage etc has brought digital privacy unprecedented connectivity and convenience. As usage of digital technologies among society increasingly relies on communication, commerce, healthcare and governance so there should be a need to safeguard these systems from cyber threats. Sophistication of Cyber Criminals in order to prevent the advancements of cyber security in Artificial Intelligence and machine learning have made traditional defence mechanisms insufficient. Blockchain, advanced encryption, offers solutions for improving cybersecurity in emerging technologies. The Right of Individuals to control their personal data and information shared online, ensure freedom from unauthorised surveillance, data misuse or breaches. Digital privacy protects individuals dignity as a protection in the digital space recognized as one of the Fundamental right.

Mass surveillance:

Digital Privacy, in many democracies, ensures individual's ability to protect their personal information and maintain control over their online presence enshrined as a Fundamental right. Mass surveillance involves the large-scale viewing and collection of data by governments, corporations, crime prevention or public safety. Proponents of mass surveillance argue that it improves the detection and prevents threats, including the erosion of

civil liberties and discriminatory targeting. Surveillance systems can erode privacy, while misinformation and hate speech threaten societal harmony. Ensuring digital platforms uphold democratic ways without infringing on rights is an ongoing struggle for policymakers and judicial systems worldwide. In response, stronger data protection laws, constitutional frameworks must evolve to address challenges posed by AI are essential for safeguarding constitutional rights in a globally connected digital ecosystem.

Individual Rights:

Individual Rights in the digital age of privacy are increasing to protect personal freedom. Recognized by the Fundamental Human Rights grant individuals control over their personal data, ensuring that information such as financial records, health data, communications and online activities cannot be shared or misused without explicit consent. The government through regulations like the GDPR (General Data Protection Regulation) in the EU and the data protection law worldwide, helps to reinforce these rights by holding organisations accountable for data handling. Along with that the individual is also entitled to transparency regarding how their data is collected, stored and used. Individual Digital Privacy is not only essential for personal freedom but also for maintaining trust in the digital ecosystem.

The Digital Personal Data Protection Act,2023 (DPDP Act) establishes a comprehensive framework for processing digital personal data, passed on Aug 11, 2023. The aim of the Act is to balance the individual right to protect their personal data with the necessity of processing such data for lawful purposes. The main principles of this act - granted rights to access, correct, update and erase their personal data; the act introduces the right to nominate to exercise these rights in case of incapacity or death; in addition data protected related to minors in the digital environment are also safeguarded etc.

Case laws linked with privacy:

The landmark case K.S.Puttaswamy vs UOI, established the Right to Privacy as a Fundamental Right under the Indian Constitution, decided by the Supreme Court of India in 2017. Linking with the Privacy to the right to life and liberty - the government move to make AAdhaar mandatory for access govt services, the data protection, surveillance and Individual privacy should be protected under the Constitution.

Conclusion:

Digital privacy has brought about unprecedented access to information and connectivity, but it has also introduced complex constitutional challenges that demand careful consideration. One key issue is the right to privacy in the face of pervasive surveillance technologies, such as government monitoring and data collection by corporations. The Fourth Amendment, which guards against unreasonable searches and seizures, must be reinterpreted to address the realities of digital data. Another significant challenge is ensuring freedom of speech while regulating harmful content online. The rise of social media platforms has blurred the lines between private company policies and public rights, leading to debates over censorship and the spread of misinformation. Cybersecurity is another critical area, where the need to protect national security pand public safety must be balanced against individual rights. Cyber attacks and data breaches raise questions about the extent to which the government can intervene in private networks and data storage. Intellectual property laws are also being tested by digital advancements, as the ease of copying and distributing digital content challenges traditional copyright and patent protections. Overall, the constitutional challenges of digital privacy necessitate a nuanced approach that considers both the preservation of fundamental rights and the need to adapt to new technological realities. Legislators, judges, and policymakers must work together to navigate these complex issues and ensure constitutional protections evolve in tandem with technological progress.