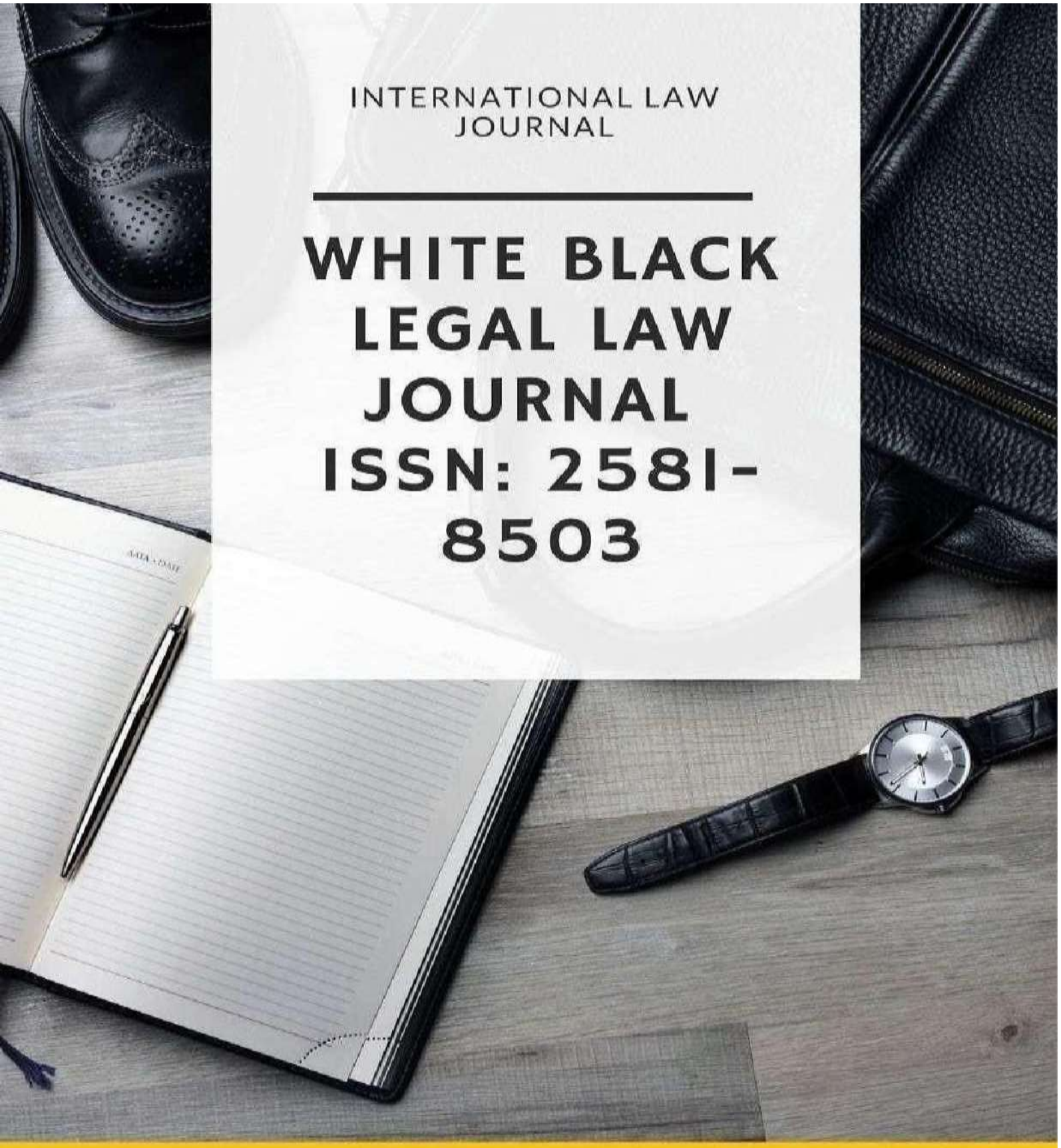

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

WHITE BLACK

LEGAL

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

HUMAN RIGHT VIOLATIONS IN THE DIGITAL AGE

AUTHORED BY - ADV REBECCA SARA GEORGE

The growth of digital rights in the twenty-first century has accelerated globally. Traditionally, the digital right has been associated with the information era. The law is currently adjusting to the needs of this new phase by establishing digital rights and digital citizenship, authorising and regulating encrypted and open access to internet information. As a result, digital technologies have revolutionised how fundamental freedoms like freedom of expression and access to information are exercised, safeguarded, and violated, while also paving the way for the recognition of new rights. Human rights incorporate ancient wisdom that can help us overcome today's challenges. Human rights, most importantly, offer a normative, legally enforced framework that not only directs but also unlocks all liberty for everyone, everywhere, resulting in the checks and balances they establish. They are ultimately concerned about human agency and dignity. In a nutshell, they propose a long-term, intergenerational governance approach that will secure our future. Human rights are based on the concept that people should be protected from certain abuses committed by their governments, as well as individuals, private entities, and businesses. However, despite recent advancements in new technology, the government and other agencies in India continue to infringe many of human beings' digital rights. However, as the use of digital technologies has risen, a number of individuals' human rights have been abused and infringed. Some of the rights include the right to privacy and data protection, the right to free speech and expression, the right against indecent representation of women on online platforms utilising AI tools.In this article, we will analyse the digital rights and human rights, the national and international framework for the protection of digital rights, human rights violations in the digital age, and the conclusion and recommendations.

Keyword: Digital rights, Human rights, digital citizenship, privacy, Data protection DIGITAL

RIGHTS AND HUMAN RIGHTS

Digital technology is the representation of information or physical elements (e.g., images and sounds) using discrete values, typically in binary form with 0s and 1s. Its transformative potential stems from its ability to convey diverse realities (sounds, visuals, texts, human behaviors, industrial processes, etc.) in a universal language, allowing for systematic and interconnected treatment. In India, digital technology has brought about significant changes in the telecommunications, transportation, banking, and other sectors, resulting in numerous technological, economic, and societal improvements. The Digital technology in India has paved way for digital rights which is often associated with the information age. So now question arises what are digital rights ?whether digital rights are human rights in this digital age ? To answer the first question we will give a broad definition of digital rights. Digital rights are the rights that allow people to access, use, produce, and publish digital media, as well as access and utilize computers, other electronic devices, and communication networks.[1]. The right to personal data protection (a) and the right to internet access (b) have emerged as responses to the challenges brought by the advent of digital technology. [2]Although they are frequently presented as being associated with the rights to privacy and freedom of expression. Digital technologies are altering the way basic liberties like freedom of expression and access to information are exercised, protected, and infringed, while also contributing to the recognition of new rights. The law is thus adjusting to this new century by developing digital rights and digital citizenship, authorising and regulating access to internet information in a secure and transparent manner. Now to answer the second question. Digital rights are simply an extension of the human rights in the internet age .It has been outlined in the United Nations' Universal Declaration of Human Rights that apply to the online environment. Its primary goal is to ensure Internet access, thereby preventing the so-called digital divide, as well as proper use of the network as a shared asset of humanity. However, the absence of international consensus on human rights on the internet has prompted each government to create its own Digital Rights Charter. Each country creates its own Digital Rights Charter, there are some common criteria that all countries observe. 1)Universal and equal access2) Right to Freedom of expression, information and communication 3) Right to privacy and Data Protection -4) Right to anonymity 5) Right to be forgotten 6) Protection of Minors 7) Intellectual property

[1] "What are Digital Rights and their Importance?" Iberdrola, https://www.iberdrola.com/innovation/what-are-digital-rights. Accessed 22 May 2024.

[2] Digital Freedom Fund, 8 December 2020, https://digitalfreedomfund.org/wp-content/uploads/2020/12/Human-Rights_V3.pdf. Accessed 29 June 2024

PROTECTION OF DIGITAL RIGHTS IN THE NATIONAL AND INTERNATIONAL FRAMEWORK

DIGITAL RIGHTS PROVIDED UNDER THE INDIAN LEGISLATION -Digital rights in India are less precisely defined and structured than in other areas of the world. Yet the Indian government has made steps to recognise digital rights, implement regulations and codify these rights.

INDIAN CONSTITUTION-. The Indian Constitution is the supreme law of the land, guaranteeing citizens' basic fundamental rights. The Constitution's preamble states that all citizens are entitled to justice, social, economic, and political equality of status and opportunity. In various Judgement such as Anuradha Bhasin case[3], Faheema Shirin v State of kerala[4] The Supreme court and different high courts in India have recognised the basic existence of certain digital rights under the current fundamental rights in the constitution of India provided under Art 19[5], art 21[6] and art 21 A[7].

The Information Technology Act ,2000[8]

The IT Act of 2000 regulates electronic transactions and digital governance. Although it does not directly reference AI, key aspects of the Act apply to AI-related activity. Section 43A[9] The IT Act provides compensation in the event of a breach of data privacy caused by careless

[3] **Anuradha Bhasin vs. Union of India**, AIR 2020 SC 1308

[4] WP(C).No.19716 OF 2019(L)

[5] Article 19 : Right to freedom of Speech, Expression, Peaceful Assembly, Form Associations/Unions, Move Freely, Reside, Profession etc

[6] Article 21 : Right to Life and Personal Liberty

[7] Article 21A : Right to Education

[8] The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000

[9] Sec 43 A of IT act **Compensation for failure to protect data.**--Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.--For the purposes of this section,--

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.]

treatment of sensitive personal information. This provision is especially important in the context of AI systems that handle user data. Another provision is Section 73A[10] of the legislation. In Justice K.S. Puttaswamy (Retd.) v. Union of India [11]The Supreme Court of India recognized privacy as a basic right guaranteed by the Indian Constitution. This verdict underscores the importance of protecting personal data from AI-based systems.

India's Personal Data Protection Bill (PDPB)[12]

This measure is still in draft form, but it is worth examining because it is modeled after the GDPR, which is the current gold standard for data protection regulations. If implemented, the PDPB will apply to enterprises that process personal data acquired, released, or processed in India, making it transnational in scope, similar to the GDPR. The PDPB's scope is similar to that of GDPR. Consumers now have the right to access, correct, and delete their data, as well as the right to be forgotten and data portability between companies. However, just because an organization is GDPR-ready does not imply that it is also PDPB-ready. The two regulations have slightly different scopes, and the PDPB has yet to be finalized. The intricacies of the legislation are likely to change, so any organizations with relations to India should keep a watch on it.

The Digital Personal Data Protection (DPDP) Act, 2023.[13]

The Indian government has recently passed a new privacy law, the Digital Personal Data Protection Act of 2023, which it can use to address some of the privacy concerns raised by AI platforms. The new law marks India's first cross-sectoral personal data protection law. The 2023 legislation permits personal data to be handled for any authorized reason.[14] It requires consent before personal data is handled and includes a small number of exceptions that are explicitly

[10] Sec 73 of IT act Penalty for publishing 1 [electronic signature] Certificate false in certain particulars.–(1) No person shall publish a 1 [electronic signature] Certificate or otherwise make it available to any other person with the knowledge that– (a) the Certifying Authority listed in the certificate has not issued it; or (b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a 1 [electronic signature] created prior to such suspension or revocation. (2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

[11] (2017) 10 SCC 1

[12] ("The Digital Personal Data Protection Bill, 2023") "The Digital Personal Data Protection Bill, 2023." *PRS India*, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. Accessed 29 June 2024.

[13] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023)

[14] Burman, Anirudh. "Understanding India's New Data Protection Law." *Carnegie Endowment for International Peace*, 3 October 2023, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en. Accessed 29 June 2024.

outlined in the legislation. It grants consumers the right to access, rectify, update, and delete personal data, as well as the right to nominate. It adds extra protections to the handling of children's data. For enterprises, it establishes purpose constraints, responsibilities to provide notice of data collection and processing, and security protections. Section 17(1)(c) of the legislation exempts notice and consent obligations, among others, for processing for "prevention, detection, investigation, or prosecution of any offence or contravention of any law." While this is acceptable, Section 17(2)(a) then gives a sweeping exception from the whole legislation to any government agency that the government may notify, in the interests of sovereignty, security, integrity, public order, and preventing incitement.

INTERNATIONAL LEGISLATION

More than 120 countries around the world have legislation in place to protect personal data and internet access. In 2022, the European Commission issued a Declaration on the preservation of its citizens' digital rights, which applies to all European citizens. Despite this, supranational groups such as the European Union (EU) are promoting a single framework, at least in terms of the right to personal data protection. For example, the General Data Protection Regulation (GDPR), which went into effect in 2018, requires member countries to simultaneously protect citizens' personal data and allow for the free flow of data. The Digital Services Act (DSA) in the European Union and the Online Safety Act in the United Kingdom are just two examples of such legislation.

DIGITAL SERVICES ACT -The Digital Services Act seek to create a safer digital landscape in which users' basic rights are safeguarded while also establishing a level playing field for enterprises. Digital services cover a wide range of online services, from basic websites to internet infrastructure services and online platforms.[15] The DSA rules primarily apply to online intermediaries and platforms. Consider online marketplaces, social networks, content-sharing platforms, app stores, and online travel and lodging platforms. The DSA specifies guidelines for extremely big internet platforms and search engines.

ONLINE SAFETY ACT -The Online Safety Act of 2023 is a new set of rules designed to safeguard both children and adults online. It imposes a number of additional responsibilities on

[15] "The Digital Services Act package | Shaping Europe's digital future." *Shaping Europe's digital future*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package. Accessed 29 June 2024.

social media businesses and search engines, making them more accountable for their users' safety on their platforms.[16] The Act would impose additional requirements on providers to create systems and processes to decrease the chance that their services may be exploited for criminal behavior, as well as to remove illegal content when it appears.

The General Data Protection Regulation (GDPR)-The GDPR is the most stringent security law in the world. It went into effect on May 25, 2018, and puts requirements on all companies worldwide that collect or process data about EU residents.[17] The primary principles, obligations, and rights under the GDPR are as follows: Data minimization entails collecting no more personal information from consumers than is really necessary. Integrity and confidentiality (security), Accountability, Access to data, Right to edit information, Right to deletion, Limitations on automated processing, Data portability are some of features

United States: California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

Unlike the EU, the United States lacks a comprehensive privacy law such as the GDPR. However, other states, notably California, have enacted data privacy legislation and rules to protect individuals' personal information. This includes the CCPA and its predecessor, the CPRA. The California Consumer Privacy Act (CCPA) was passed in 2018 and allows Californians more control over the personal information that firms collect about them. Since January 1, 2023, it has been revised by the CPRA. The CPRA applies to companies that meet the following criteria: Have a gross annual income of exceeding $25 million. Share, purchase, or sell the personal information of at least 100,000 California residents., Know who collects their personal information, how it's used, and who has access to it. Limit the usage of their data, Delete or modify their personal information., Likewise, it requires businesses to: Inform consumers on how their personal information is gathered and processed, Allow consumers to delete, obtain, correct, and share their personal information. Collect personal data only for legitimate and relevant purposes. Companies who fail to comply with the CPRA's provisions

[16] Home Online Safety Act: explainer." *GOV.UK*, 8 May 2024, https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer. Accessed 29 June 2024

[17] Wolford, Ben. "What is GDPR, the EU's new data protection law? - GDPR.eu." *GDPR compliance*, https://gdpr.eu/what-is-gdpr/. Accessed 29 June 2024.

may face fines of up to $7,500 per willful offense and $2,500 for unintentional violations.[18]

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)[19]- Canada's federal privacy law, PIPEDA, was passed in 2000. It applies to private-sector entities in Canada that use, collect, or disclose personal data for commercial purposes. According to PIPEDA, a commercial activity is any transaction, conduct, or act that is commercial in nature, such as leasing, trading, or selling membership, donor, or fundraising lists. PIPEDA defines personal information as any subjective or factual information concerning an identified person, whether recorded or not. This includes age, income, name, blood type, personnel records, opinions, and disciplinary actions. Companies must follow the ten fair information principles to comply with PIPEDA: Accountability, Identifying purposes, Consent, Limitations on data acquisition, Limited use, disclosure, and retention, Accuracy, Safeguards, Openness, Individual access Organizations may be fined up to $100,000 Canadian for each violation.

The China Personal Information Protection Law[20] (PIPL) is China's new data privacy law, aimed at protecting personal information and addressing issues related to data leaking. On October 13, 2020, the first PIPL draft was submitted to the National People's Congress, and on October 21, 2020, it was published and opened for public comment. The PIPL applies to companies and persons who process personally identifiable information (PII) in China, as well as those that process PII of Chinese nationals outside of China. Although the current draft version is likely to be altered before it is approved, certain substantial implications for organizations may already be predicted. More tighter data transfer standards, mandated security measures and data localization requirements, and greater penalties and fines for firms that violate them are all projected.

European Digital Rights (EDRi)[21] defines facial recognition technology as a sort of biometric

[18] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General." *California Department of Justice*, 13 March 2024, https://oag.ca.gov/privacy/ccpa. Accessed 29 June 2024.

[19] Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5

[20] The PRC Personal Information Protection Law (Final): A Full Translation." *China Briefing*, 24 August 2021, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/. Accessed 29 June 2024

[21] European Digital Rights." *MacArthur Foundation*, https://www.macfound.org/grantee/european-digital-rights-10115695/. Accessed 29 June 2024

identification that "uses statistical analysis and algorithmic predictions to automatically measure and identify people's faces to make an assessment or decision." However, EDRi warns that facial recognition technology has been criticized for reflecting social biases, leading in racial profiling and the formation of assumptions about sexual orientation and gender identity.

THE IMPACT OF HUMAN RIGHT VIOLATIONS IN DIGITAL AGE

Over the previous decade, the global number of internet users has more than doubled. As of January 2020, the digital population was 4.54 billion. The Internet has become an essential part of most people's daily lives. It allows us to work, communicate, and access essential services. Increasingly, technology is a vital facilitator for the exercise and enjoyment of numerous human rights, in particular the right to freedom of expression and information. However, a lack of adequate infrastructure or connectivity usually leaves behind the poorest communities, and the digital divide shows its discriminatory effects in all its strength.[22] The internet has made it possible for everyone with an internet connection to share information and ideas, transforming the way people communicate. This has significantly impacted the exercise and protection of information rights, including privacy, freedom of expression, and access to information. The United Nations Human Rights Council's (UNHRC) 2016 Resolution[23] on the promotion, protection, and enjoyment of human rights on the internet confirmed that these rights permit a wide range of other fundamental rights. When these rights are advanced and practised online, they should be protected in the same way that they are promoted offline. The internet has the potential to empower democracy, yet it is often undercut by authoritarian ideologies. Globally, clear themes have arisen, with all internet users experiencing similar possibilities, problems, threats, and human rights violations, albeit to varied degrees. The contradictions between human rights and freedoms, as well as the increase in limits on access to online spaces, will continue. Restoring the internet to a dynamic environment that fosters innovation and human potential will be challenging due to political polarization and non-state actors' seemingly unlimited power. The ultimate goal is to maintain and establish online environments in which human rights can be protected, respected, and promoted. Fortunately, there are effective remedies to restrictive rules and a growing number of innovative solutions to address these

[22] "UN: Human Rights Council adopts resolution on human rights on the Internet - ARTICLE 19." *Article 19*, 15 July 2021, https://www.article19.org/resources/un-human-rights-council-adopts-resolution-on-human-rights-on-the-internet/. Accessed 29 June 2024.

[23] A/HRC/RES/32/13

issues.

Right to Access Information -Access to the internet has grown dramatically during the previous decade. Unfortunately, limits on accessing information have risen. Internet users face several threats, including shutdowns, content filtering, social media levies, censorship,and DDoS attacks. In 2019, India experienced approximately 100 internet shutdowns, including the longest documented shutdown in history in Kashmir.[24] In late 2019, India's Supreme Court declared that indefinite internet shutdowns violate free speech and expression. As a result, the government must now announce the causes and duration of any future shutdowns.[25] The growing tendency of internet shutdowns suggests that governments may continue to use them in the future, particularly during times of public unrest or elections. Recent jurisprudential advances in India may raise civic consciousness and defend individuals' right to access information.

Registration of Bloggers

Bloggers, who self-publish online and can write informally, semi-professionally, or professionally, play an important role in disseminating information and exercising their right to free expression. Bloggers and journalists have many similarities, thus legal rules should protect both groups. The United Nations General Comment 34 to the International Covenant on Civil and Political Rights[26] (ICCPR) evaluates journalism, including bloggers. Restricting the operation of websites, blogs, or other internet-based systems contradicts the right to free expression. (USD). Human Rights Watch has criticized the plan to make blogging without a license a criminal offense.[27] The license charge restricts freedom of expression and information sharing. Bloggers are being forced to pay unreasonably large fees. offline. The new criminal charges levied against bloggers are also cause for alarm. Several instance where bloggers have been mistreated and imprisoned.[28] Threats to both professional and informal journalism are

[24] BBC, 'Why India shuts down the internet more than any other democracy' (2019) (accessible at https://www.bbc.com/news/world-asia-india-50819905).

[25] Time, 'India's Supreme Court Orders a Review of Internet Shutdown in Kashmir. But For Now, It Continues' (2020) (accessible at https://time.com/5762751/internet-kashmir-supreme- court/).

[26] Human Rights Committee, General Comment no. 34." *Ohchr.org*, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf. Accessed 29 June 2024.Human Rights Committee 102nd session Geneva, 11-29 July 2011

[27] The Right to Blog - 2013." *Article 19,* https://www.article19.org/wp-content/uploads/2018/02/Right-to-Blog-EN-WEB.pdf. Accessed 29 June 2024. [28] In 2019, the Daily Maverick reported that Zimbabwean bloggers were routinely imprisoned and mistreated. One blogger was charged with cybercrime but ultimately acquitted

increasing, with little evidence of meaningful efforts to solve them. If states do not respect and safeguard their international human rights duties, imposing burdensome obligations on bloggers and journalists may become common practice.

Blocking and filtering content

Censorship has increased during the past decade. The most common form of censorship is the barring and filtering of certain content on social media. Blocking is the process of preventing access to a website, domain, or IP address. Filtering technology restricts access to specified sites based on their qualities. Blocking and filtering may violate Article 19 of the Universal Declaration of Human Rights (UDHR), which states that everyone has the right to seek, receive, and share information and ideas regardless of borders. Internet shutdowns differ from blocking and filtering in that the former causes complete loss of access, while the latter allows for partial or affected access.

Increased accessibility and the need for digital literacy and safeguards.

ICTs play a crucial role in promoting economic development. By doing so, they can help realize socioeconomic goals and dreams. To achieve these objectives, adequate access to ICTs and digital literacy are necessary. Internet access will surely increase. Inadequate digital literacy can lead to ongoing and potentially worsening online harms, particularly for vulnerable sections of society.

The intersection of net neutrality and zero-rated content

Net neutrality,[28] the theory that strives to ensure that access to content is open, free-flowing, fair, and equal, may be threatened by the zero-rating approach, which seeks to direct internet traffic. According to the Electronic Frontier Foundation (EFF), net neutrality plays a crucial role in maintaining unfettered access to information and ideas across our information society. In contrast, zero-rating has the potential to skew both content consumption and market access. Some multinational firms argue that zero-rating can promote universal internet access. The EFF and other digital rights activists reject the idea that some access is preferable to no access. Some claim that zero-rating allows new internet gatekeepers to control access. The debate over net neutrality and zero-rating fluctuates based on current state positions. In 2015[29] and 2016,

[28] "Net Neutrality." *Federal Communications Commission*, https://www.fcc.gov/net-neutrality. Accessed 29 June 2024

[29] (MANKOTIA)MANKOTIA, ANANDITA SINGH. "Airtel Zero plan prima facie violates the principle of net

the India-Facebook-Airtel debate centered on Facebook and Airtel's differential pricing for certain material and free access to other items. The Indian Telecom Regulatory Authority has rejected Facebook's reported intention to guarantee ubiquitous internet access, citing public uproar. India has since implemented strict net neutrality legislation.

The increase in cybercrime and cyberattacks

Cybercrime is changing faster than response methods, resulting in greater complexity and risk. Attacks against individuals, businesses, civil society organizations, and governments are becoming more common. Hackers are expected to launch an attack every 39 seconds, for a total of around 2200 each day. Cybercrime is expected to cost $3 trillion (USD) by 2020, causing major economic worries. The expansion of stringent cybersecurity measures endangers human rights, in addition to the problem of cybercrime. Cybersecurity began as a global trend in 2014, and it has since evolved into a lucrative industry. Despite legitimate security concerns, cybercrime laws frequently violate the fundamental human rights of internet users. Legislation aimed at preventing cybercrime may fail to effectively safeguard fundamental human rights, making internet users vulnerable to both the crime and harsh punishment. Cybercrime is expected to continue surpassing cybersecurity measures.

The Right to Free Expression

Criminalizing online speech poses the greatest threat to freedom of expression, according to recent trends. Governments use vague and sweeping regulations to criminalize specific types of online expression. The spread of disinformation in the digital space poses a significant threat to freedom of expression as governments tighten controls.

AI Violations on human rights

The development of artificial intelligence in the digital age has accelerated globally. The new AI has supplanted people by taking over their duties across all areas. With recent AI tools like chatGPT and openAI, its use has become irreplaceable in the near future, but at the expense of increasing the risk of cybercrime, intellectual property issues, job loss, data protection and privacy issues, liability for damage, cybersecurity and lack of accountability, legal personhood issues, and discrimination. The AI has badly violated individuals' human rights, which are

neutrality, says Trai." *The Economic Times*, 16 April 2015, https://economictimes.indiatimes.com/tech/internet/airtel-zero-plan-prima-facie-violates-the-principle-of-net-neutrality-says-trai/articleshow/46938313.cms?from=mdr. Accessed 29 June 2024.

critical for their personal growth, including the right to privacy and security, which the state has a key responsibility to protect. The AI has failed to ensure human rights protections, notably for the most marginalized and ethnic minorities. The risks of employing artificial intelligence technologies like fraud detection systems and face recognition technology for social control, mass monitoring, and discrimination. One of the most serious challenges in AI is 'informational privacy', and there is concern about disclosing sensitive information. Artificial intelligence (AI) has been connected to both aggression and abuse. For example, using AI-assisted applications and tools to produce so-called 'deep fake' images, as demonstrated in Image-Based Abuse, a person's face can be digitally blended into existing pornographic pictures or movies. Fake sexual images may still be immensely destructive to women since we live in a society where women's value and appropriateness as workers, parents, or friends are still related to outdated notions of sexual repute or character. Furthermore, while language processing techniques are intended to detect abusive language, they may be used by abusers who employ veiled or antagonistic language that, on its own, may not look serious enough to warrant reporting to police. On a communal level, automated content assessments and the spread of misinformation and disinformation exacerbate gender inequality and intolerance. These decisions are frequently affected by advertising income or engagement figures, which contributes to the normalisation of sexism, misogyny, and other inequities in online platforms.[30]

CONCLUSION

With the continued expansion of the digital rights, the tension between digital rights and human rights is becoming more visible as technology becomes more fundamental to our daily lives and societal functioning. Due to lack of strong Data Protection rules provides Tech corporations with a society primed for digital exploitation. With minimal oversight or responsibility, these firms brazenly intrude into residents' lives and progressively violate human rights. More of digital rights has paved way for a threat to equal protection, economic rights, and basic freedoms, ranging from discrimination to invasive surveillance activities. To reverse these trends, appropriate legal standards must be enacted in our digitally evolving communities. Digital rights should be promoted through investments in public awareness and education projects that assist communities in learning and digital literacy should be promoted, but also its impact on our daily lives. Unless appropriate steps are implemented to protect the interests

[30] **Technology's Role in Addressing Violence Against Women by Anastasia Powell**-This article is based on a panel presentation delivered at the event 'AI for Impact: Social Justice in the Digital Age', hosted by The Equality Institute during Melbourne Connect's Innovation Week

of human society, the future of human rights in this technological age remains questionable. The Indian government should promptly enact laws to regulate the use of AI tools and its violation in india. Digital rights such as right to access internet is considered as a fundamental right However, despite recent advancements in new technology, the government and other agencies in India continue to infringe many of human beings' digital rights. However, as the use of digital technologies has risen, a number of individuals' human rights have been abused and infringed

This legal issue may pose national security risks if an entity has a connection to the central government. The privacy of children, women and minorities tend to especially in this digital age and they have become frequent targets of exploitation. In the digital age AI has spawned new kinds of annoyance impersonating someone's else's identity for financial gain -each of which has the effect of impinging of one’s privacy.

Another suggestion is to integrate Constitutional Artificial Intelligence that will operates at the boundary of AI-driven technological developments and the imperatives for integrating them with fundamental human rights and values by embedding ethical-juridical perceptions in their techno-architectural structure to ensure a just, fair, and non-discriminatory AI decision making. The states have to connect a the digital gap by "adopting national Internet-related public policies that have at their main objective of universal access" and thereby "applying a comprehensive human rights-based approach in providing and expanding access to ICT."