International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

The Digital Dilemma: Protecting Human Rights in A Hyper-Connected World

Baibhaba Chinhara
2nd Year LLM Student, G.M. Law College, Sri Vihar, Puri-752003, India

***Abstract*— The rapid convergence of pervasive computing, artificial intelligence (AI), and mass data harvesting has inaugurated a transformative yet precarious era for global human rights. This "Digital Dilemma" represents a profound structural shift in how individual autonomy, state power, and corporate influence intersect. While digital technologies offer the potential to enhance information access and democratize civic engagement, they simultaneously risk eroding privacy, amplifying systemic discrimination, and normalizing mass surveillance. This paper conducts a comprehensive doctrinal and socio-legal analysis of the intersection between hyper-connectivity and human rights. It explores the emergence of the "digital welfare state," algorithmic bias, the weaponization of facial recognition technology (FRT), and the rise of digital authoritarianism. By evaluating global statutory frameworks—including the EU's General Data Protection Regulation (GDPR) and Artificial Intelligence Act (AIA)—alongside pivotal case laws, this paper argues that existing legal mechanisms are insufficient to combat the transnational asymmetries of digital power. The paper concludes by proposing a human-rights-centric regulatory paradigm grounded in established legal maxims to ensure that technological advancement does not eclipse fundamental human dignity.**

***Keywords*— Digital Rights, Artificial Intelligence, Digital Welfare State, Facial Recognition Technology, GDPR, Algorithmic Bias, Digital Authoritarianism.**

I. Introduction

Today's world is definitively digital, dissolving the traditional boundaries where human rights were exclusively protected by territorial laws. The digitalization of societal spheres has catalyzed the development of "digital rights"—an extension of universal human rights adapted to the needs of an information-based society. However, this hyper-connected reality has given rise to a "Digital Dilemma": the friction between the democratizing power of technology and its capacity for unprecedented surveillance and control. The internet, once heralded by cyber-utopians as a borderless realm of freedom, is increasingly becoming a highly regulated, surveilled, and corporatized space. Multinational technology companies act as digital sovereigns, wielding governance power that rivals nation-states.

Simultaneously, authoritarian and democratic regimes alike utilize digital tools to monitor citizens, suppress dissent, and automate essential public services. To safeguard the tenets of democracy and individual liberty, it is imperative to critically examine the sociotechnical forces shaping this epoch and robustly enforce international human rights law across the digital domain.

FIGURE I

II. The Emergence Of The Digital Welfare State

The digitalization of social security and public assistance has given rise to the "digital welfare state". Governments worldwide are automating welfare to increase efficiency and detect fraud; however, this transformation is often politically driven, concealing deep reductions in welfare budgets and the imposition of punitive conditionality. Philip Alston, the former UN Special Rapporteur on extreme poverty and human rights, warned that the digital welfare state risks becoming a "Trojan Horse for neoliberal hostility towards social protection". In these systems, automated technologies predict, monitor, and target the poor, fundamentally altering the relationship between the citizen and the state. The individual is no longer treated as a rights-holder entitled to an adequate standard of living, but rather as an applicant who must constantly prove their deservingness to a faceless algorithm. A striking example of this occurred in the Netherlands with the System Risk Indication (SyRI) tool, which used algorithmic data to predict the likelihood of individuals committing welfare fraud.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

The system selectively targeted low-income neighbourhoods for heightened scrutiny, inherently punishing the poor. Similarly, in India, the mandatory integration of the biometric Aadhaar identification system with food rationing led to starvation deaths when digital glitches or biometric mismatches denied vulnerable individuals their legal entitlements.

TABLE II
Harms of the Digital Welfare State

Mechanism	Impact on Human Rights	Example
Algorithmic Profiling	Discriminatory targeting of marginalized groups; violation of privacy.	SyRI system in the Netherlands targeting low-income areas.
Digital-by-Default	Exclusion of those lacking digital literacy or internet access, denying basic services.	Universal Credit system in the UK.
Biometric Mandates	Denial of life-saving aid due to technical errors; forced surrender of bodily data.	Aadhaar system in India.

III. Algorithmic Bias And AI Decision-Making

Artificial Intelligence (AI) and automated decision-making systems are highly reliant on massive datasets. However, because these datasets reflect historical and societal inequalities, algorithms frequently replicate and amplify existing human biases. This phenomenon, known as algorithmic bias, manifests across critical sectors including criminal justice, healthcare, and employment. In the criminal justice system, predictive policing and risk assessment algorithms—such as COMPAS in the United States—have been heavily criticized for generating racially disparate outcomes, predicting higher recidivism risks for minorities despite neutral variables. In healthcare, algorithms designed to predict medical needs have been found to heavily favor wealthy populations over marginalized groups, utilizing past healthcare expenditure as a proxy for health needs. Furthermore, AI hiring tools often exhibit gender and racial bias, systematically filtering out qualified candidates from underrepresented backgrounds. The opacity of these "black-box" algorithmic systems impedes accountability and redress. Victims of algorithmic discrimination rarely understand why a decision was made against them, violating the principles of due process and the right to a fair trial.

IV. Mass Surveillance, FRT, And The "Great Scrape"

The deployment of Artificial Intelligence has exponentially enhanced the surveillance capabilities of both states and private corporations. Facial Recognition Technology (FRT) represents one of the most severe threats to the right to privacy and the ability to maintain anonymity in public spaces. The foundation of modern FRT relies on the "Great Scrape"—the automated, mass extraction of personal data and billions of images from the internet. Companies like Clearview AI have scraped billions of publicly available images from social media to create searchable "faceprints" without the knowledge or consent of the data subjects. Scraping obliterates the traditional concept of informed consent and contextual integrity; just because an individual posts an image for a specific audience does not imply consent for inclusion in a global surveillance database.

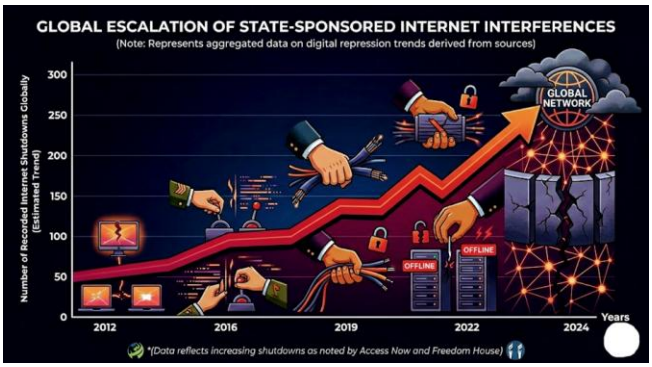

FIGURE 2

V. Digital Authoritarianism And The Contraction Of Civic Space

Digital technologies have empowered authoritarian regimes to exert unprecedented control over information and civic organizing. "Digital authoritarianism" involves the use of the internet, AI, and surveillance technology to control, repress, and manipulate domestic and foreign populations. A primary tool of digital authoritarianism is the internet shutdown. States routinely disconnect networks during elections, protests, or periods of instability to stifle dissent, block the documentation of human rights abuses, and sever transnational advocacy networks. In Myanmar, following the 2021 military coup, the junta utilized internet blackouts and telecommunications disruptions to stifle democratic resistance.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

Similarly, the Iranian government has repeatedly employed network shutdowns to crush protests and isolate activists from the global community. Furthermore, authoritarian regimes utilize sophisticated spyware, such as Pegasus, to conduct transnational repression. By infecting the digital devices of journalists, human rights defenders (HRDs), and political dissidents, regimes can monitor communications across borders, inducing a chilling effect on the freedom of expression and the right to political participation.

VI. Statutory Provisions And International Frameworks

To address the digital dilemma, various jurisdictions have enacted statutory provisions, though their effectiveness remains fragmented.

A. The European Union (EU)

The EU leads the global landscape with a rights-centered approach.

1. General Data Protection Regulation (GDPR):

Article 6 requires a lawful basis for processing personal data, while Article 17 guarantees the "right to erasure" (right to be forgotten). Crucially, Article 22 grants individuals the right not to be subject to a decision based solely on automated processing (profiling) that significantly affects them.

2. Digital Services Act (DSA):

Regulates intermediary service providers and Very Large Online Platforms (VLOPs), imposing strict transparency obligations and banning advertising based on special categories of sensitive data.

3. Artificial Intelligence Act (AIA):

Adopts a risk-based approach, outright banning "unacceptable risk" AI practices (like mass biometric surveillance and social scoring) and imposing rigorous human rights impact assessments on "high-risk" systems.

B. The United States (US)

The US follows a highly fragmented, market-driven model.

1. Computer Fraud and Abuse Act (CFAA):

The primary statute regarding unauthorized computer access, highly debated regarding its applicability to data scraping.

2. Biometric Information Privacy Act (BIPA):

An Illinois state law providing robust protections for biometric data, requiring informed opt-in consent before the collection of faceprints, and frequently used to litigate against FRT companies.

C. International Human Rights Law

1. ICCPR & UDHR:

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR) protect the right to privacy. Article 19 of both instruments protects the freedom of expression.

2. UN Guiding Principles on Business and Human Rights (UNGPs):

Mandates that technology companies conduct Human Rights Due Diligence (HRDD) to identify, prevent, and mitigate human rights abuses linked to their operations, products, and downstream end-use.

VII. Landmark Case Laws

Judicial systems globally are grappling with the digital dilemma. The following landmark cases illustrate the tension between digital expansion and fundamental rights:

A. Van Buren V. United States, 593 U.S. 374 (2021)

The US Supreme Court ruled that liability under the CFAA relies on a "gates-up-or-down" inquiry. Access is unauthorized only if an individual bypasses a technical barrier or "digital gate," thereby validating the legality of scraping public data not hidden behind passwords.

B. HIQ LABS, INC. V. LINKEDIN CORP., 31 F.4TH 1180 (9TH CIR. 2022)

The Ninth Circuit held that scraping publicly accessible profile data does not violate the CFAA, prioritizing the scraper's business interests over the privacy interests of users.

C. Carpenter V. United States, 585 U.S. 296 (2018)

The US Supreme Court ruled that the government's acquisition of cell-site location information (CSLI) constitutes a search under the Fourth Amendment. The Court recognized an "anti-aggregation principle," acknowledging that persistent digital tracking violates an individual's reasonable expectation of privacy, setting a precedent applicable to FRT surveillance.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

D. SOSA V. ONFIDO, INC., 600 F. SUPP. 3D 859 (N.D. ILL. 2022)

In litigation under Illinois' BIPA, a federal court held that extracting facial geometry using FRT software from images does not constitute protected "speech" under the First Amendment, thus allowing privacy regulations against private FRT companies to proceed.

E. Justice K.S. Puttaswamy (RETD.) V. Union Of India (2017) 10 Scc 1

The Supreme Court of India unanimously affirmed that the right to privacy is a fundamental, inalienable human right guaranteed under Article 21 of the Indian Constitution, deeply impacting global data protection discourse and digital sovereignty.

VIII. Legal Maxims in the Context of Digital Rights

To effectively navigate the digital dilemma, jurisprudence must return to foundational legal maxims that prioritize human dignity over technological determinism:

A. Salus Populi Suprema Lex Esto (The Health/Welfare Of The People Should Be The Supreme Law)

Corporate profit models and the "Great Scrape" must not supersede the collective privacy and security of the public.

B. UBI JUS, IBI Remedium (Where There Is A Right, There Is A Remedy)

The opacity of algorithms and the lack of transparency in digital welfare states actively violate this maxim. Individuals harmed by AI bias or digital tracking must be afforded a clear, actionable right to private redress.

C. Nemo Commodum Capere Potest De Injuria Sua Propria (No One Can Obtain An Advantage By His Own Wrong)

Tech platforms utilizing deceptive design ("dark patterns") or bypassing informed consent to harvest data for AI training must not be legally permitted to profit from this unlawful extraction.

IX. Core Challenges Of Digital Technologies

A. Algorithmic Bias And The Amplification Of Inequality

Algorithmic decision-making systems are frequently marketed as objective, yet they systematically reflect and reproduce the structural inequalities embedded in their training data. This phenomenon, known as algorithmic bias, acts as a digital gatekeeper, disproportionately harming marginalized communities across multiple sectors:

1. Criminal Justice:

Predictive policing and risk assessment algorithms, such as the COMPAS system used in the United States, have been shown to falsely flag African American defendants at significantly higher rates than white defendants, creating a feedback loop of over-policing and disproportionate incarceration.

2. Healthcare:

Healthcare algorithms designed to predict medical needs have exhibited severe racial bias by using healthcare expenditures as a proxy for illness, resulting in equally sick Black patients receiving significantly less additional care than white patients.

3. Employment and Credit:

Automated hiring tools have penalized female candidates by replicating historical, male-dominated industry data. In the financial sector, algorithmically driven lending systematically charges Black and Latinx borrowers' higher interest rates, perpetuating economic disparities and engaging in "algorithmic redlining".

B. The Rise Of The Punitive "Digital Welfare State"

Governments globally are automating social protection systems, giving rise to the "digital welfare state". According to Philip Alston, the former UN Special Rapporteur on extreme poverty and human rights, these systems frequently serve as a "Trojan Horse for neoliberal hostility towards social protection," utilizing digital tools to surveil, target, and punish the poor.

1. Dehumanization and Exclusion:

Automation shifts the state-citizen relationship, treating vulnerable individuals not as rights-holders, but as applicants who must constantly prove their eligibility to rigid, faceless algorithms.

2. Punitive Surveillance:

Systems like the SyRI fraud detection tool in the Netherlands intentionally target low-income neighborhoods for heightened scrutiny, while mechanisms in Australia have issued arbitrary "robo-debts" to welfare recipients.

3. Fatal Errors:

The mandatory linkage of welfare to biometric digital ID systems, such as India's Aadhaar, has led to catastrophic outcomes, including starvation deaths when individuals were denied food rations due to fingerprint recognition failures.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

C. Mass Surveillance And Digital Authoritarianism

The proliferation of AI and mass data extraction has equipped both states and corporations with the infrastructure to obliterate public anonymity.

1. The "Great Scrape" and Facial Recognition:

Companies like Clearview AI have scraped billions of images from the internet without consent to build vast facial recognition technology (FRT) databases. This dragnet data collection violates fundamental privacy principles and subjects the public to a perpetual, unregulated police lineup.

2. State Repression and Internet Shutdowns:

Authoritarian regimes employ "digital authoritarianism" to manipulate populations and suppress dissent through internet shutdowns, deep packet inspection, and localized network blackouts during protests or elections.

3. Transnational Repression:

The deployment of commercial spyware, such as Pegasus, enables governments to infiltrate the devices of human rights defenders (HRDs) and journalists globally, facilitating cross-border intimidation and physical violence.

X. Recommendations For Safeguarding Human Rights

To mitigate these challenges, interventions must shift from reactive troubleshooting to systemic, rights-based governance. The following recommendations provide a framework for action:

A. Enforce Robust, Risk-Based Regulatory Frameworks

The international community must harmonize regulations to prevent a fragmented landscape where technology companies exploit legal loopholes.

1. Adopt Risk-Based Legislation:

Policymakers should look to models like the European Union's Artificial Intelligence Act (AIA), which categorizes AI by risk. AI systems presenting "unacceptable risks"—such as real-time biometric surveillance in public spaces and social scoring—must be outright banned.

2. Regulate Data Extraction:

Laws must conceptualize the mass scraping of personal data as a form of surveillance. Regulations should require a legitimate, public-interest basis for data collection and mandate that public availability does not equate to a forfeiture of privacy rights.

B. Mandate Human Rights Due Diligence (Hrdd) For Corporations

Technology companies and investors must be held accountable for the real-world impacts of their products, aligning with the UN Guiding Principles on Business and Human Rights (UNGPs).

1. Lifecycle Impact Assessments:

Businesses must conduct comprehensive algorithmic and human rights impact assessments prior to the deployment of any digital system, actively evaluating potential harms to equality, privacy, and marginalized groups.

2. Accountability for End-Use:

Companies must exercise leverage over the "downstream" application of their technologies, refusing to supply software or hardware to state or private actors who utilize it for unlawful surveillance, discrimination, or transnational repression.

3. Accessible Grievance Mechanisms:

Corporations and states must establish transparent, operational-level grievance mechanisms, ensuring that victims of algorithmic harm or data misuse have a clear and effective path to legal remedy and redress.

C. Implement Algorithmic Transparency And Participatory Design

To combat the opacity of algorithmic "black boxes," governance frameworks must enforce transparency and democratize the design process.

1. Explainability and Auditing:

Algorithms used in high-stakes domains (welfare, justice, employment) must be subject to mandatory, independent third-party data audits to test for bias and ensure decisions are explainable to the individuals affected by them.

2. Participatory and Inclusive Design:

Digital systems must be co-designed with the meaningful inclusion of the communities they are intended to serve, particularly vulnerable populations, to ensure that the technology reflects real-world needs and avoids encoding systemic prejudices.

3. Pursue "Algorithmic Greenlining":

Rather than merely aiming for "neutral" algorithms—which often preserve the discriminatory status quo—developers should optimize systems for equity.

"Algorithmic greenlining" involves explicitly designing automated systems to correct historical disadvantages, promote racial and economic justice, and drive investments into vulnerable communities.

XI. Conclusion

The "Digital Dilemma" demands a profound reconceptualization of human rights in the 21st century. The unrestricted harvesting of personal data, the implementation of biased algorithms, and the rise of the digital welfare state all demonstrate that technology is not inherently neutral; it is a mechanism that amplifies the power of those who wield it. To protect human rights in a hyper-connected world, the international community must move beyond fragmented, reactive legislation. It is imperative to enforce universal, rights-centered regulatory frameworks that impose strict Human Rights Due Diligence (HRDD) on corporate actors, mandate algorithmic transparency, and outright ban technologies that pose unacceptable risks to human dignity, such as mass biometric surveillance and unregulated commercial spyware. Ultimately, preserving democracy in the digital age requires institutionalizing accountability so that the digital revolution serves to elevate the human spirit rather than automate its subjugation.

REFERENCES

[1] Alston, P. (2019). World stumbling zombie-like into a digital welfare dystopia. Third World Network.

[2] Access Now. (2024). Lives on hold: internet shutdowns in 2024. Access Now.

[3] American Bar Association. (2024). Ensuring Trust in Artificial Intelligence by Understanding the Role and Importance of Economic Justice. ABA Civil Rights and Social Justice Section.

[4] Amnesty International. (2025). Breaking up with Big Tech: Briefing on Big Tech monopolies and human rights. Amnesty International.

[5] B-Tech Project. (2019). UN Human Rights Business and Human Rights in Technology Project (B-Tech): Applying the UN Guiding Principles on Business and Human Rights to digital technologies. Office of the High Commissioner for Human Rights.

[6] Carpenter v. United States, 585 U.S. 296 (2018).

[7] Council of the European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. Official Journal of the European Union.

[8] Council of the European Union. (2022). Digital Services Act (DSA). Regulation (EU) 2022/2065. Official Journal of the European Union.

[9] Council of the European Union. (2024). Artificial Intelligence Act (AIA). Regulation (EU) 2024/1689. Official Journal of the European Union.

[10] Electronic Frontier Foundation (EFF). (2026). OHCHR Protection of HRDs in the Digital Age: EFF Submission.

[11] Geneva Academy. (2026). Guiding Principles for Businesses on Protecting Human Rights Throughout the Neurotechnology Lifecycle. Geneva Academy of International Humanitarian Law and Human Rights.

[12] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022).

[13] Human Rights Watch. (2025). A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making. Human Rights Watch.

[14] International Bar Association. (2020). Digital transformation and human rights. Global Insight.

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017).

[16] Lendvai, G. F., & Gosztonyi, G. (2025). Algorithmic Bias as a Core Legal Dilemma in the Age of Artificial Intelligence: Conceptual Basis and the Current State of Regulation. Laws, 14(3), 41. https://doi.org/10.3390/laws14030041

[17] New America. (2023). Governing the Digital Future. Planetary Politics Initiative.

[18] Pajuste, T. (Ed.). (2025). Human Rights in the Digital Domain: Core Questions. Cambridge University Press. https://doi.org/10.1017/9781009606295.017

[19] Public Citizen. (n.d.). Racism In, Racism Out: Algorithmic Racism. Public Citizen.

[20] Solove, D. J., & Hartzog, W. (2025). The Great Scrape: The Clash Between Scraping and Privacy. California Law Review.

[21] Sosa v. Onfido, Inc., 600 F. Supp. 3d 859 (N.D. Ill. 2022).

[22] Suar, L. (n.d.). The Digital Dilemma: Protecting Human Rights in a Hyper-Connected World. G.M. Law College, Puri.

[23] Tomain, J. A. (2025). Facial Recognition Technology and the First Amendment. Michigan Technology Law Review, 32(1).

[24] United Nations Special Rapporteur on Counter-Terrorism. (2025). Protecting Human Rights while Using Artificial Intelligence to Counter Terrorism: Position Paper. UN OHCHR.

[25] Van Buren v. United States, 593 U.S. 374 (2021).