THE RIGHT TO PRIVACY IN THE DIGITAL AGE: A COMPARATIVE ANALYSIS OF GLOBAL DATA PROTECTION REGIMES

Prof. Kamal Jeet Singh, Retired Professor of Law, HP University, Shimla,
Former Vice Chancellor, Madhusdan Law University, Cuttack, Odissa.

Ankit Raj Rajial, Ph.D. Scholar, Department of Law, HPU Shimla.

ABSTRACT

Privacy has gone from the realm of philosophical objectives to a set of fundamental rights that are now enforceable by law, and an area that has become a political battleground between the U.S.'s economy and society and those of eager competitors like China, India, and Russia. While the paper finds a common stance among people "when it comes to legal protection of personal data", it also observes a high level of divergence in legislation, which is rooted in different framings of state power, individual autonomy and notions of digital sovereignty. It also argues that the lack of a legally binding global data governance treaty leads to "structural asymmetries" disproportionately affecting developing States. The paper ends by arguing for a multi-lateral framework of data governance, anchored in the human right approach and therefore most principled, to the challenge of governing personal data in an interconnected world.

Keywords: Privacy, Data Protection, GDPR, DPDPA 2023, PIPL, Digital Sovereignty, International Law, Surveillance Capitalism.

I. INTRODUCTION

It is one of the oldest aspirations of human civilization and the most hot-button issue of the digital era: privacy. One hundred years later that small common law claim has spread to constitutional protections, treaty provisions, and a tangle of data-protection laws that now can be found on every inhabited continent of the world. Even while the normative consensus regarding "privacy as a human right" has grown, the capacity to secure 1:1 data protection has been undermined by technological forces of acceleration.

The international legal foundation for privacy is built on two pillars "Article 12 of the Universal Declaration of Human Rights 1948" and "Article 17 of the International Covenant on Civil and Political Rights 1966" that "both state that no one shall be subjected to "arbitrary or unlawful interference with his privacy, family, home or correspondence"." But the instruments are decades old, and provide only skeletal outlines for the governance of data concerning individuals, in platform mediated societies. Hence, it has been left up to regional and national legislatures to develop and make privacy protection real in the digital age, leading to a no-man's-land of regulatory models diverging hugely in normatively oriented ways.

This paper is divided into 6 sections. Part II looks at the historical and theoretical developments of the right to privacy, the way it has been first founded on natural law, second recognised on constitutional terms and third made into an entitlement in data protection. Part III covers the key international data protection laws and documents. In part IV, each of the four major regulatory regimes will be compared. Part V examines the challenges that artificial intelligence, 'surveillance capitalism' and cross-border data flows present. In Part VI, a framework for a more coherent international approach is offered, followed by a summary of the key arguments of the paper.

II. HISTORICAL AND THEORETICAL EVOLUTION OF THE RIGHT TO PRIVACY

A. Natural Law and Liberal Foundations

There are philosophical precursors to privacy in the Enlightenment liberalism, especially in the understanding of John Locke of the self having "natural dominion" over body and mind, or the Immanuel Kant's categorical imperative that privileges human dignity based on the ability to act rationally as an autonomous agent. From this intellectual framework Warren and Brandeis

sought the normatively informed legal conceptualization of their influential defense of the need for a legally cognisable right to privacy—one that could be asserted through the common law of tort, given the increasing power of the press and photography to intrude into domestic life.

The first constitutional mention of privacy, in Justice Brandeis' dissent in Olmstead v United States favoring the Fourteenth Amendment, was recognition that the framers of the Constitution had desired to guard against governmental intrusions in belief, thought, emotion or sensation.

B. From Privacy to Data Protection: The European Contribution

Enduring the evolution from a "liberty-based approach" to a "data-protection based approach" to privacy was an essentially European success. The experimental results were then presented to the "Council of Europe in the Convention 108 of 1981" which lays down fundamental rules of fairness and purpose limitation and of data quality.

Finally, the European trajectory led to the GDPR 2016 which superseded the "Data Protection Directive 95/46/EC", and introduced up to the date the highest level of data-protection yet enacted, with the greatest applied extraterritorial scope of any such legislation passed anywhere in the world. The GDPR's rethinking of the nature of personal data put it on an equal footing with the dignity and autonomy of the person, and with those values as a green-ray. It is this normative shift, transforming data protection from a regulatory tool into a primary right which has subsequently impacted the legislative trajectory in Asia, Latin America, and Africa.

III. INTERNATIONAL LEGAL INSTRUMENTS AND INSTITUTIONS

The General Assembly had statements made in Resolution 68/167 earlier, that reiterated that unlawful or arbitrary monitoring is in breach of international human rights law.

Although not binding for the world as a whole, modernised Convention 108+ (2018 Protocol) of the Council of Europe has been ratified and/or opened for accession by states outside Europe, so this presents the closest approximation of a universal treaty standard for data protection. In 2023, Graham Greenleaf's political analysis of data privacy laws and bills around the world found 162 laws and bills, an amazing increase from 14 laws from 1990.

While mainly focusing on criminal law harmonisation, the Budapest Convention on

Cybercrime includes provisions with an impact on privacy-related issues about the lawful interception of information and the jurisdiction of states in cyberspace. The OECD Privacy Guidelines (1980, revised 2013) provide 8 widely-shared principles of data protection which have inspired national legislation in the OECD countries, but have no binding force on national laws. Collectively, these instruments form an international "norm" that is a threshold of international acceptance for appropriate behavior, rather than a firm rule, by actors of a certain kind.

IV. COMPARATIVE ANALYSIS OF MAJOR DATA PROTECTION REGIMES

A. The European Union: The GDPR Model

The GDPR's impact around the world is significant, as Anu Bradford has described in a paper she wrote, the 'Brussels Effect': EU GDPR substantive requirements have been carried over to laws of many African countries, South Korea, Japan, India and even Brazil, despite not being legally bound to comply with EU GDPR standards. But the critics argue that the complexity and costs of compliance with GDPR impose a disproportionate burden on small businesses and civil society organizations, while the apparent consent mechanisms in fact have become meaningless in practice, given the power imbalance between citizens and large scale platforms.

B. The United States: Sectoral Fragmentation and State-Level Innovation

In the United States, the regulatory vision is very different, based on a constitutional tradition that sees the privacy as a liberty interest against state interference and which expects competition in the markets to police corporate actions. Currently, federal data protection law is sectoral legislation: Health Insurance Portability and Accountability Act 1996 (HIPAA), Children's Online Privacy Protection Act 1998 (COPPA), and Gramm-Leach-Bliley Act 1999 (GLBA) provide protection to health data, data collected from children and financial data, respectively; and there is no omnibus federal privacy law.

C. India: Constitutional Recognition and Legislative Codification

After this, the journey of jurisprudential evolution pertaining to privacy, in India, reached the grand finale with the unanimous verdict of the constitution bench of the Supreme Court, in "Justice K.S. Puttaswamy (Retd.) v Union of India, 2017", in which the court held that "the right to privacy is a fundamental right under article 21 of the Constitution and overruled the

two Judge Bench Supreme Court verdicts to the contrary". In the lead judgment of Justice D.Y. Chandrachud, privacy was found to be part and parcel of human dignity and autonomy and control of personal information was part of it.

It took a long time for the legislation to follow the Puttaswamy judgment. After the Justice Srikrishna Committee Report (2018), the "Personal Data Protection Bill 2019" was introduced in Parliament where it was extensively discussed in the "Joint Parliamentary Committee, and ultimately withdrawn in 2022". Instead, the enacted "Digital Personal Data Protection Act 2023" (DPDPA) is India's first-ever complete data protection law.

Chinmayi Arun has contended that the surveillance provisions of the Act violate the rights framework framed in the Puttaswamy judgment, because the manner in which it is framed, prioritizes the interests of the state and the corporations over the protection of the rights.

D. China: Data Protection within a State-Centric Paradigm

China has implemented a complex data-governance regime which includes the Cybersecurity Law of 2017, the Data Security Law of 2021, and the Personal Information Protection Law of 2021. The Cybersecurity Law includes provisions on data localisation. Structurally similar to the GDPR, the "Personal Information Protection Law" (PIPL) provides for legal bases of consent and necessity for processing, grants data subject rights, and also requires obligations to be placed upon personal information processors.

It has been argued that there lies a fundamental contradiction in the Chinese approach while the law is formally rights-protective; most claims of Party-State on data access for national security and social governance are overarching. Jeremy Daum's analysis notes that, while the PIPL is imposing strong limits on the private sector, it is largely off-limits for public security organs and the state. As China exports its specific model of data based authoritarianism via the Digital Silk Road Initiative, which provides surveillance systems and data-governance frameworks to partner countries, many questions arise about the export of its model of data-centric governance.

V. EMERGING CHALLENGES: AI, SURVEILLANCE CAPITALISM, AND CROSS-BORDER DATA FLOWS

A. Surveillance Capitalism and the Commodification of Personal Data

“Surveillance capitalism" is a concept introduced by Shoshana Zuboff, which refers to a new economy making its way that turns the human experience into "free raw material" freely taken to turn into behavioural data and processed to be sold as 'behavioural futures' to advertising markets. Under this analysis, the formal consent requirements in data protection law – notice, choice, opt-out – lack a fundamental capacity to regulate an economic system which is built on the assumption that it can, at scale, extract personal data asymmetrically. What is at stake for law is not just in regulating certain practices, but in challenging the ground rules of an architecture of the economy that views privacy as an externality to be surmounted.

Ronald Deibert has also pointed out that the commercial internet is now part of a surveillance system, funneling data into the hands of state security services and also into those of corporate profilers, resulting in a vicious cycle of private data-gathering and state surveillance. The critique does not stop there however: Morozov sets his sight on a 'solutionist' impulse, which sees data collection and algorithmic optimisation as necessarily good, while regulation is always bad. These Copernican takes collectively argue that mere opt-out fulfilment of data-protection standards, like the creation of privacy notices, consent banners and data subject access, may not be enough if there is no structural change to the platforms whose business relies on privacy degradation.

B. Artificial Intelligence and Automated Decision-Making

Inherent features of artificial intelligence systems are problematic in terms of privacy; current data-protection mechanisms are less capable of addressing these challenges. Large-scale, personalized-data sets are used to train machine-learning models; the models themselves are opaque, making it hard to hold them accountable; and the models can be trained on patterns that represent discrimination in the data set. UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) does stress the need to respect the right of privacy and data protection as a key principle of ethical AI, thus calling for privacy by design, explainability of algorithms and human oversight for algorithmic systems.

The European Union's AI Act 2024 is the first global legislation of its kind, which is binding on artificial intelligence and takes a risk-based approach, where certain applications are banned (mass biometric surveillance use in public spaces and social scoring) and high-risk AI systems require transparency, human oversight and data governance requirements. A live issue for regulators is how the AI Act interacts with the GDPR in general, and how in particular the

purpose limitation principle of GDPR fits with the data-hungry needs of machine learning. Moving beyond the necessity of minimising data, Paul Bernal has suggested that privacy in the age of AI can only have a positive quality, ensuring that individuals are properly informed and can challenge against automatic decisions which impact them.

C. Cross-Border Data Flows and Digital Sovereignty

Cross-border transfers of personal data are now one of the most controversial aspects of digital geopolitics. States are hopefully pushed in two different directions between two imperatives: economic imperative of maintaining free data flows to enable digital trade and cloud-computing services and security and sovereignty imperative of wanting to keep data within the national jurisdiction. Data localisation measures such as those outlined in China's Cybersecurity Law and those proposed in India's framework, and which have become a feature of the sectoral legislation of many States, run headlong against the ‘free-flow' principles of the WTO General Agreement on Trade in Services and a suite of digital trade chapters.

EU–US data transfer deals based on distinct models of state authority, rights and how much intelligence is too much – Safe Harbour, Privacy Shield and the ongoing litigation of the Data Privacy Framework – all failed. In her report on the first decade of the GDPR, Lokke Moerel observes that the GDPR's adequacy decision system – whereby the European Commission recognises third countries as providing an equivalent level of protection has emerged as an important mechanism of regulatory power that is inconsistently applied.

VI. TOWARDS A GLOBAL DATA PROTECTION FRAMEWORK

While diverse national schemes of protection are a reflection of legitimate differences in constitutional history, political economies and capacities of regulators, they have produced structural inequalities that are harmful to the people and the state capacities of the Global South. MNCs relocate activities and data-processing operations to countries with the laxest safeguards to provide services to users across the world, known as regulatory arbitrage. As a result, the subsequent 'race to the bottom' casts doubt on the dignity-profazying purpose of privacy as human right.

The answer can only be a principled one, with the development of a binding multilateral measure on personal data protection which is grounded in international human rights law and

which sets minimum standards that no law, anywhere, could mark as chronically under-met. It could be based on the material principles of Convention 108+, the implementation model of the GDPR and the development sensitivity elements under the various bilateral agreement frameworks for digital partnerships. It would have to solve three fundamental problems: question of jurisdiction, which state's law is applicable to the data processing which takes place across the borders; question of enforcement, how and from where to compel non-compliant actors; and question of sovereignty, how to reconcile legitimate security interests of the countries with privacy interests of individuals.

This is because there is an opportunity and risk in the newly emerging global data governance discussions, in the UN Ad Hoc Committee to combat cybercrime and also in the ITU. There is an opportunity to establish universal minimum standards and provide capacity-building mechanisms so the developing states can effectively enact and enforce their data-protection regimes. The danger is if the negotiating process is to be sold domestically and internationally as a means of digital sovereignty, which states, and especially authoritarian ones, would want to present as a tool for mass surveillance and cross-border exfiltration of data; doing so, by international instruments, could sell domestically repressive practices as digital sovereignty.

A successful international system would require institutional undergirding—a truly independent international supervisory body, a copiously funded body, and a body with the power to update technical standards and draw on them to respond to technological developments. It would have to do more than just ensure data protection in the strictest sense, but seek to tackle wider structural issues like platform concentration, surveillance capitalism, and AI opacity that make it hard to exercise formal rights in reality. In brief, it would have to take seriously the suggestion of Bernal that privacy in a digital age is not just about controlling the flow of information and data, but about maintaining conditions of autonomy and dignity of human kind in an algorithmically mediated environment.

VII. CONCLUSION

The right to privacy has come a long way over the century-plus since it was coined in Warren and Brandeis's seminal article and is now not simply a common law curiosity, but a constitutional fundamental right, and one that has morphed from a right of individual liberty to a global regulatory enterprise unlike anything seen before, and far more complex. The four regulatory systems explored in this paper—the GDPR, the US sectoral model, DPDPA (India),

and PIPL (China)—represent a whole new set of normative visions of the interactions between actors (individual and collectives), data, states, and markets. However, they cannot just be harmonised through technical standard setting; their differences are, at their heart, political and philosophical.

But purely national solutions are no longer sufficient for the globalisation of the data flows. The personal information of one citizen of Gurugram, captured by a server in Oregon and pushed through an algorithm trained in Shenzhen and monetised in Frankfurt is not sufficiently shielded by any one law. So, setting up an effective international data-protection system represents not one of these technical hopes, but one of the most pressing needs of global justice. This should be based on human rights principles, take developmental asymmetries into account, not be susceptible to ‘state capture', and adaptive enough to follow technological advances.

But the biggest challenge is that the right to privacy not be the rhetorical flourish of a system that structurally bars its actualisation, as Morozov feared all digital rights to be. The devolution formal legal protections, and the attainment of substantive data sovereignty are the main problems of digital governance in the current age, and one that can be solved by neither states, nor corporations, nor individuals alone.

BIBLIOGRAPHY

A. Table of Cases

Data Protection Commissioner v Facebook Ireland Ltd (Case C-311/18) EU:C:2020:559

Dobbs v Jackson Women's Health Organization 597 US 215 (2022)

Griswold v Connecticut 381 US 479 (1965)

Internet & Mobile Association of India v Union of India (2019) SCC Online Del 8494

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

Olmstead v United States 277 US 438 (1928)

Roe v Wade 410 US 113 (1973)

Schrems v Data Protection Commissioner (Case C-362/14) EU:C:2015:650

B. Table of Legislation and International Instruments

Budapest Convention on Cybercrime (CETS No 185) 2001

California Consumer Privacy Act 2018, Cal Civ Code §§ 1798.100–1798.199

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Convention 108, Council of Europe)

Cybersecurity Law of the People's Republic of China 2017

Digital Personal Data Protection Act 2023 (India), No 22 of 2023

EU AI Act, Regulation (EU) 2024/1689

General Data Protection Regulation (EU) 2016/679

International Covenant on Civil and Political Rights 1966, Art 17

Personal Information Protection Law (PIPL), People's Republic of China 2021

Universal Declaration of Human Rights 1948, Art 12

C. Books

Bradford A, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020)

Bernal P, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge University Press 2014)

Deibert R, Reset: Reclaiming the Internet for Civil Society (House of Anansi Press 2020)

Hillman JE, The Digital Silk Road: China's Quest to Wire the World and Win the Future (Profile Books 2021)

Morozov E, To Save Everything, Click Here: The Folly of Technological Solutionism (PublicAffairs 2013)

Zuboff S, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019)

D. Articles and Chapters

Arun C, 'India's Privacy Law is Inadequate' (2023) 93 Harvard Law Review Forum 118

Beydoun K, 'Privacy in the Age of Algorithmic Discrimination' (2022) 72 Duke Law Journal 1201

Daum J, 'China's PIPL — Who Does it Actually Protect?' (2021) 44 China Law Translate 7

Finnemore M and Sikkink K, 'International Norm Dynamics and Political Change' (1998) 52 International Organisation 887

Greenleaf G, 'Global Data Privacy Laws 2023: 162 National Laws & Bills' (2023) 181 Privacy Laws & Business International Report 1

Moerel L, 'GDPR Ten Years On — Taking Stock' (2025) 62 Common Market Law Review 243

Schwartz PM and Peifer K-N, 'Transatlantic Data Privacy Law' (2017) 106 Georgetown Law Journal 115

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 193

E. Other Sources

European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' (2020)

UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (2021)

UN Human Rights Council, 'The Right to Privacy in the Digital Age' UN Doc A/HRC/27/37 (2014)

UNGA Resolution 68/167, 'Right to Privacy in the Digital Age' (18 December 2013)