



## Adapting constitution to technology: The evolution of rights across sovereign states

Venkatesh S

Joy University, Tirunelveli, Tamil Nadu, India

### Abstract

The evolution of Humankind started about 7 million years ago; however, the past 25 years' have been a witness of a newer evolution called the digital evolution. The digital evolution is characterized by artificial intelligence, surveillance technologies, social media platforms and cross border data sharing - which generates a new form of power, vulnerability and rights that challenges the constitutional orthodoxy. As the Sovereign states start to grapple with the restructuring of digital society, the traditional boundary between the state and the individual will be redrawn. Implementation of new digital rights rephrase the constitutional shift from static legal protection to dynamic technological oversight. This paper analyses the diverse pathways of constitutional adaptation across different sovereign states and explores the pioneering frameworks including "Digital Magna Carta" movements in various nations, the formal constitutional amendments in states like Portugal, Brazil, and Chile. Furthermore, the paper also discusses the deployment of these rights within the sovereign states for a dual function mechanism: first, to protect the individuals from intrusive capacities of both the state and dominant private monopolies and second, to assert legal sovereignty in a borderless cyberspace. The study concludes that formally recognizing digital rights as constitutional imperatives is essential to protect democratic freedom, it also argues that the effectiveness of the modern sovereign states now depends on the ability to adapt the idea of liberty into the digital realities of 21<sup>st</sup> century.

**Keywords:** Digital evolution, digital rights, digital magna carta, legal sovereignty

### Introduction

The principles of the state, the process and structure of the government, the fundamental rights and fundamental duties of a citizen in a supreme law that cannot be unilaterally validated by an ordinary legislative act is referred to as a constitution. Times back when the constitution is drafted in sovereign states, the humankind relied primarily on themselves, with mild or no dependence on technology. However, the situation is changing day by day and today most activities are impossible without relying on digital devices such as mobile phones and computers. In this situation an important question arises, "can the same traditionally written constitution effectively protect our rights in a digitally dependent community?". Therefore, the constitution must be amended or adapted to reflect the evolving realities of digital age. This paper examines the rights that sovereign states have adapted in this digital age. It explores how technological advancements have reshaped the traditional ideas of understanding the fundamental rights and state obligations. This study also highlights the significance of this adaptation in protecting the individuals and state sovereignty in this digital society.

### New Rights evolved in the digital age

As digital technologies become increasingly integrated into both private and public life, the importance of a human rights-based approach, guided by international norms and national constitutional law, cannot be overstated. These technologies, ranging from artificial intelligence (AI) to cloud computing, are transforming how societies function, how governments interact with citizens, who exercises influence and holds power over people's rights and freedoms, and how individuals conduct their daily lives. Thus technology has become part of everyone's life, let's see the new rights evolving from these technological life: 1. Right to data protection and privacy:

Technological advancements continuously reshape the digital landscape that creates a need for adaptive regulatory framework. The existing technologies such as the 5G-enabled hyper connectivity facilitates the collection of data with devices from the Internet of things, the processing of information through Big-data analytics and the reliance of Edge computing have significantly increased the volume of personal data flows. This intensification of data circulation increases the risk of individuals privacy and underscores the necessity of effective data protection mechanism. Individuals have the right to retain the control over their personal information and the right to determine who collects and stores their data. In this digital environment, the right to privacy is increasingly threatened by practices such as credential theft, unauthorized data harvesting and commercial exploitation of personal information. To overcome this, the global citizens seek for a new right to secure their personal data and digital privacy namely the right to data protection and privacy.

### Right to internet access and connectivity

The internet has become an indispensable cornerstone of modern society, fundamentally transforming how we live, work, learn, and interact. The pervasive integration of the internet into nearly every aspect of human life - from education and healthcare to economic participation and civic engagement - underscores its critical importance in our increasingly connected world. The internet has become more than just a tool; it is now a key enabler of numerous established human rights, including the rights to education, work, health, and freedom of expression. In this digital era, the digital connectivity is an integral part of everyone's life where the absence of internet access threatens to create a new form of disenfranchisement. Recognising the internet access as a constitutional right would provide a powerful framework for the adapting sovereign states.

## **Right to be forgotten or Right to erasure**

This Right to be forgotten provides right to individual to request for removal of his/her personal data floating around through Internet. The simple rule behind data erasure is that whoever is using the data has volunteer consent from the data owner. So, when the consent is withdrawn, the owner has a right to have his data erased. Also when the data controller has no legal right to process the data, the data should be erased.

## **Neuro-rights**

Expeditious development in neuroscience and neurotechnology are changing the stereotype of our present understanding and interaction with the human brain. In the coming decades, the technology once seemed like science fiction may now be able to read brain signals, improve human sense or alter human memory. While these advancements may benefit the society but also with some deeper ethical concerns, to overcome these concerns neuroright have been introduced. This right aims to protect the human brain and mental privacy. It ensures that data collected from the brain activity cannot be used or shared without the person's consent, thereby it safeguards individual's autonomy and dignity.

## **Adaptation of Digital Rights in the Sovereign states**

Digital rights ensures our basic human rights with regards to technology, fitting these rights in the states framework is a major challenge in the governance. While sovereign states have the power to frame there set of rules, but the rule must balance the states national security, public order, economic development and customary values. Lets discuss about some sovereign states adapted digital rights:

### **1. European Union**

The European Union's strategic evolution of digital rights represents a comprehensive "Digital Magtna Carta" which is codified through multiple framework such as General Data Protection Regulation (GDPR), the Digital Service Act (DSA), and the AI Act. These digital frameworks recalibrates basic human liberties such as privacy, espression and equality to fit into the complexities of the data driven society. The GDPR serves as the foundational pillar for restoring the individuals sovereignty over personal data through rights such as the right to erasure and right to data protection.

In the year 2019, an Austrian politician Eva Glawisching-Piesezek filed a suit against the Facebook Ireland limited, stating that she was subjected to a defamatory post posted by a facebook user which was went viral and she requested the facebook to remove the defamatory contents. Facebook removed the specific conetent but refused to remove the equivalent or identical contents. The Court of Justice of European Union held that, Once unlawful content is identified by court, a platform can require to remove the same or equivalent content without violating the EU law.

Furthermore, the European Union's vision extents to the principle of digital equality by addressing the digital divide through the "Digital decade" policy. The European Union treats the internet access and the digitral literacy not only as a utility but also as enabling right essential for the democratic participation, employment and education. The framework like Network and Information Security 2 (NIS2) integrates cybersecurity essential thing for the human dignity to fortify the digital infrastructure against the cyber

threats. By initiating these standards EU positioned it as the global architect of the digital governance and a leader in creating blueprints for the digital era ensuring an open, safe and equitable space in the digital society.

### **2. India**

In India the traditional constitutional rights are now interpreted in the digital context which gives rise to the new digital rights. The Supreme court of India have played a crucial role in expanding and recognizing the digital rights through constitutional interpretation and landmark judgements. India have adapted various frameworks namely Digital Personal Data Protection Act (2025), IT (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021) and the forthcoming Digital India Act (DIA) which is expected to replace the IT Act (2000) but still in draft. These new regulatory frameworks ensure that technology upholds and serves human dignity rather than eroding it.

In Justice K.S. Puttaswamy vs Union of India (2017) <sup>[1]</sup>, the Supreme Court of India recognised the right to privacy including the informational privacy as a fundamental right under Article 21. This case stand as a stepping stone for the Digital Personal Data Protection Act (2025), which grants rights such as consent, access, correction and erasure of personal data. In Anuradha bashin Vs Union of India (2020), the Supreme Court recognised the right to internet access as essential for exercising free speech and also begun protecting the digital identity, personal rights and freedom from excessive surveillance which signals a growth of digital right frameworks in India.

### **3. Russia**

The Russian civil code has acknowledged digital rights as legal objectives providing a framework for digital financial assets, smart contracts and tokens since 2019. The "dual track" system: the formulation of digital property rights alongside aggressive expansion of state surveillance and digital sovereignty clearly explains Russia's digital landscape. Moreover this enhancing digital growth is counterbalanced by strict rules and regulations. Between 2024 and 2026 the digital rules and management achieved a sovereign status. By 2025, a landmark law passed which criminalized the act of "knowingly" that is searching for extremist content, effectively outlawing curiosity and research into state- banned topics. But then Russian digital time faced a major downfall after the blocking of Apple's facetime, restrictions on whatsapp, telegram calls reasoned by unproven claims of the use in terrorism.

Furthermore the state Duma (lower house of Russia's bicameral parliament) granted the Federal Security Service of Russian Federation (FSB) more powers to command nationwide internet shutdowns in the early 2026, while the government provide domestic alternatives like the "Max" platform. While the NGO's like Roskomsvoboda continue to challenge these measures but the judiciary overwhelmingly favors state security over individuals privacy. Conclusively, Russia's digital framework concentrate more in "digital gulag" where the state prioritize states security over the protection of civil liberties.

### **4. China**

The digital transformation and its governance in China shows a strategical shift from fragmented regulation towards

a comprehensive, flexible and sovereignty oriented legal framework. In the year 2016, China chose a strategical approach that balances national security concerns with economic openness and geopolitical realities. China's digital governance played a vital role in the year 2016, where it came with the enactment of Cyber Security Laws (CSL). This law mandated security assessments for trans-national data transfer and also introduced the principle of data localization by critical information operators. The idea of data localization marked China's first formal assertion of "Cyber – Sovereignty", where the data generated within the state was considered as national resource which is subject to state control. In 2021, after larger experiments and global uncertainty, China made the enactment of Data Security Law (DSL) and Personal Information Protection Law (PIPL). The enactment of these laws made the state governance to systematic national framework.

The DSL classifies data according to its importance to national security and public interest, while the PIPL established rules for personal data protection and interstate data transfers. These both laws are introduced to regulate overseas data processing activities that affect Chinese citizens or national interests.

China's digital governance approach was not only focused on state control but also on regulatory diversification. Later in 2024, regulatory frameworks were made for cross border data flows provisions (2024), which made the terms unambiguous providing the vague concepts clear and also narrowed down the scope of mandatory security reviews.

## 5. Chile

Chile is spearheading a digital revolution in Latin America, it became the first nation to grant constitutional protection to neurorights which gives a fundamental human right by protecting the brain data to safeguard mental privacy and free will from technological manipulation. Beyond neurorights, the 2024 Data Protection Law aligns Chile with GDPR standards by establishing a specialized agency to enforce the rights of Access, Rectification, Cancellation and Opposition (ARCO rights). Internet access also have been codified as public utility that ensures the universal equity which supports the right to internet access. With the establishment of the National Cybersecurity Agency in 2025, Chile is balancing rapid innovation with some ethical safeguards. The newer frameworks implemented in Chile sets a sophisticated global precedent for digital sovereignty and human-centered technological rights.

## 6. Spain

Spain has launched the Digital Rights Observatory (ODD) to safeguard security, equity and transparency in the digital age. The objective of launching this observatory focus on four pillars that is citizen empowerment, oversight of the digital rights charter, ethical technology research and international cooperation.

## Conclusion

The digital rights between the sovereign states reveals a divergence in the constitutional priorities. The European Union and Chile are pioneering in the human-centered framework by establishing the rights like "Right to be forgotten" and "Neuro-rights" as a essential safeguard for personal sovereignty. If we see on the other hand, the

frameworks seen in Russia and China highlight the tension between the technological improvements and state sovereignty by establishing "cyber-sovereignty" which mostly prioritize the national security and surveillance over individuals rights. Meanwhile, sovereign state like India is finding the middle path by balancing both individual and states liberties where it utilize the judicial activism to bridge the gap between the traditional states and modern digital realities. The true strength of state's constitution in the digital age not lies in the complexity of technology, but by its ability to ensure that technology remains a tool for human welfare rather than a means of domination. As digital governance continues to evolve, the idea of "Digital Magna Carta" is gradually taking a new shape. The choices made by sovereign states today will determine whether future digital societies promote freedom, equality and empowerment or enable widespread of surveillance and control. If a constitution should remains as a "supreme law", it must evolve as living document capable of addressing new digital challenges by creating rights that protect human dignity and state's sovereignty.

## References

1. Justice KS Puttaswamy (Retd.) Vs. Union of India, (2017) 10 SCC 1 (India), 2017.
2. Shreya Singhal Vs. Union of India, (2015) 5 SCC 1 (India), 2015.
3. Google Spain SL v. Agencia Espanola de Proteccion de Datos (AEPD), Case C-131/12, Court of Justice of European Union, 2014.
4. Auradha Bhasin V. Union of India, (2020) 3 SCC 637 (India), 2020.
5. Dicey AV. Introduction to the study of the law of the constitution. Macmillan, London.
6. General Data Protection Regulation (EU) 2016/679 (GDPR), 2016.
7. Kuner C. European Data Protection Law. Oxford University Press, 2020.
8. Digital rights essential in the internet age. Iberdrola. <https://www.iberdrola.com/about-us/our-innovation-model/what-are-digitalrights#:~:text=Freedom%20of%20expression%2C%20information%20and,Protection%20of%20minors>
9. The Peril and Potential of GDPR. Centre for international governance innovation. [https://www.cigionline.org/articles/peril-and-potentialgdpr/?utm\\_source=google\\_ads&utm\\_medium=grant&gad\\_source=1&gad\\_campaignid=1716904719&gbraid=0AAAAADsVJifF42dgbotYk1d0kTVuwK2J&gclid=Cj0KCCQiAhOfLBhCCARIsAJPiopNYOpKh6QDB7kwBoe56eEHn0sH-8\\_k\\_wRGJV9NZewNn-DurKdmdhPYaAkzDEALw\\_wcB](https://www.cigionline.org/articles/peril-and-potentialgdpr/?utm_source=google_ads&utm_medium=grant&gad_source=1&gad_campaignid=1716904719&gbraid=0AAAAADsVJifF42dgbotYk1d0kTVuwK2J&gclid=Cj0KCCQiAhOfLBhCCARIsAJPiopNYOpKh6QDB7kwBoe56eEHn0sH-8_k_wRGJV9NZewNn-DurKdmdhPYaAkzDEALw_wcB)
10. Miralles DZ. Chile's draft constitution looks to the future: digital rights as fundamental rights. Constitutionnet, 2022. <https://constitutionnet.org/news/chiles-draft-constitution-looks-future-digital-rightsfundamentalrights#:~:text=Every%20person%20has%20the%20right,digital%20space%20free%20of%20violence.%E2%80%9D>
11. Chile's – Information Technologies. International Trade Administration, 2025. <https://www.trade.gov/country-commercial-guides/chile-informationtechnologies#:~:text=Furthermore%2C%20>

- initiatives%20like%20the%20public,report%20incident  
s%20to%20the%20ANCI
12. Digital rights, Fundamental rights: Spain launches the digital rights observatory. Fundacionhermes, 2025. <https://fundacionhermes.org/en-gb/digital-rightsfundamental-rights-spain-launches-the-digital-rightsobservatory/#:~:text=The%20initiative%2C%20led%20by%20Red,in%20Spain%20and%20across%20Europe>
  13. Charter of Digital rights. OECD Digital Policy Platform, 2021. <https://depp.oecd.org/policies/ESP2472>
  14. From Digital rights to International Human rights: the emerging right to human decision maker. University of Oxford, 2023. <https://www.oxfordaiethics.ox.ac.uk/blog/digital-rights-international-human-rights-emerging-right-human-decisionmaker#:~:text=The%20US%20Blueprint%20for%20an,human%20rights%20and%20fundamental%20freedoms>
  15. A Digital Magna Carta? The European Declaration of Digital rights. Morrison & forester LLP, 2022. <https://www.mofo.com/resources/insights/220207digital-magna-carta>
  16. Rosen J. The Right to be Forgotten. Stanford Law Review, 2012.
  17. Thibault H. China's new identity system boosts the government's control over citizens online. Le Monde, 2025. [https://www.lemonde.fr/en/international/article/2025/07/18/in-china-a-new-digitalidentity-has-increased-the-government-s-control-over-citizens-onlineactivities\\_6743473\\_4.html](https://www.lemonde.fr/en/international/article/2025/07/18/in-china-a-new-digitalidentity-has-increased-the-government-s-control-over-citizens-onlineactivities_6743473_4.html)