Page 1187 - 1203 **DOI:** *https://doij.org/10.10000/IJLMH.118351*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 5

2024

Constitutional Protections for Digital Privacy: A Comparative Study of Estonia and India

ADITYA PRATAP SINGH[1]

ABSTRACT

Digital identity verification systems are a very vital part of modern governance and business activities. Being safe, convenient, and accessible, they can offer maximum advantages in relation to other identification methods. Focusing on Estonia's e-Residency and India's Aadhaar-the two best-known digital identity verification systems -is the comprehensive aim of a comparative study. Estonia's e-Residency was launched in 2014. Non-Estonians can access Estonia's digital infrastructure and the EU market using a government-issued smart ID card. Such a program is customized for entrepreneurs, freelancers, and digital nomads, whereby an online, streamlined business management also encompasses the formation of a company, accounts in a bank, and filing of taxes. The advantages include the global reach, easy setup of businesses, and high level of security measures in the form of two-factor authentication and blockchain technology. The disadvantage of it being highly dependant on user's digital literacy and non-global awareness.

India's Aadhaar, launched in 2009, looks for issuing a unique identification number to every resident of India, a number that would cover more than 1.3 billion people. It assimilates vast biometric and demographic data, allowing one to verify his or her identity so as to use various services such as banking, telecommunications, public distributions, and direct benefits transfer. The strength of the system lies in being all-inclusive with a biometric authentication process, hence very broad in application, as it entails full savings in government welfare schemes. However, Aadhaar, despite its low-cash delivery model, has pointed out high-profile breaches on account of its lack of privacy and security, with possible misuse of personal information, besides operational challenges such as technical glitches and exclusion of vulnerable populations. A comparison of these two systems will highlight distinct approaches to digital identity verification.

Estonia has its e-Residency that aims to deliver a secure, effective digital infrastructure for the global entrepreneur using the most advanced technologies that assure the security and integrity of data. India's Aadhaar project on the other hand, aims at identity verification on a scale never done before, targeting an unprecedented all-inclusive delivery of benefits to a vast population but still afflicted with enormous problems around privacy and security

[1] Author is a student at Amity University, Noida, India.

 [ISSN 2581-5369]

concerns as well as practical problems. Both systems offer clues as to how such systems can be implemented and managed, making interesting trade-offs between scale, inclusiveness, security, and technological dependence. This comparison will be about the individual assumptions in their specific needs: tailoring an appropriate digital identity solution to national contexts and users, along with continuous negotiations of new challenges related to data privacy and security.

I. INTRODUCTION

Even amid today's rapid technological advancement, governments see individual privacy as a critical issue. Despite our various cultures and histories, we must recognize that privacy is important for both individual dignity autonomy and freedom, especially now that we are in a time of data without borders. Therefore, we should consider countries like Estonia and India.

Owing to its technological proficiency, Estonia is one of the most recognizable countries. Upon its independence from the Soviet Union in 1991, Estonia has made information technologies a central concern in both governance and infrastructure. A basic value deeply embedded in both law and society is information privacy. The Estonian Constitution forbids unjustified intrusions into privacy, while Estonia's compliance with the EU's General Data Protection Regulation (GDPR)governs individual data processing. Estonians are eligible for several rights, which come together as access, the ability to correct data, the right to delete it, and information concerning its use. The digital identity system developed by Estonia aligns with yet another ambition for secure privacy-friendly e-services.

There was a complicated and circuitous path for India to recognize privacy as an essential right. This led to a final point with the noteworthy judgment of Justice K.S. Puttaswamy v Union of India 2017, the year when the Supreme Court ruled affirmed that privacy was an essential part of Article 21. The decision was one of the leading decisions in Indian privacy law about the consequences of emerging technology. Since that judgment, India has developed data protection laws, especially including the Information Technology Act, 2000, the IT Rules, 2011 and Digital Personal Data Protection Act, 2023. Estonia and India, in both cases, have emphasized the right to privacy as crucial to safeguarding the freedom of an individual in this increasingly interconnected and data-driven world.

II. PURPOSE AND IMPORTANCE OF PRIVACY RIGHTS IN THE DIGITAL AGE

The international community has identified the right to privacy as a basic human right that serves as the basis for several other rights. Privacy, as a right, is recognised in the Universal

Declaration of Human Rights (UDHR), 1948, and the International Covenant on Civil and Political Rights (ICCPR), 1966. Article 12 of the UDHR and Article 17 of the ICCPR provides legal protection to persons against 'arbitrary interference 'with one's privacy, family, correspondence, home, reputation, and honour.[2]

The importance of privacy rights has been similar to that of protecting democratic values and civil rights. The context of digital information and the extraordinary influence that institutions of government and businesses have over personal data make these freedoms an important threat for potential misuse or exploitation. Thorough privacy protections prevent these violations and halt unauthorized surveillance or discrimination of individuals who might, otherwise, face these situations.

Privacy is additionally an important component of nurturing innovation and expansion in the economy. Technologies driven by data are fundamental to a variety of industries; having clear and applicable standards on privacy results in a level playing field among organizations. Businesses create innovations in a responsible manner, as they know they will have to answer for any infractions toward consumer privacy through legal or market reputational penalties. For this reason, consumer trust is developed which will be key to the success of new digital services.

At last, privacy rights provide authority to individuals by letting them govern information associated with their identity. Every day, the gathering and processing of data makes it empowering for individuals to have some level of authority over their own information. It provides an individual with the ability to be conscious and can ultimately lead to making educated decisions about their online behaviour and protecting potential risks - ensuring that, consequently, privacy rights afford much more than protection, but truly facilitate empowerment and personal autonomy in this online communication age.

III. ESTONIA'S E-RESIDENCY PROGRAMME

On December 1st, 2014, Estonia started the e-Residency program as an element of its extensive initiative addressing the global digital economy. Through this uncommon program, people from all corners of the world may become "e-residents" of Estonia, via accessing a digital identity, without the obligation of having a physical presence in Estonia. The concept behind the initiative drew on Estonia's deep tradition of innovation in information technology since the 1990s.[3]

2 Oishika Banerji, Different aspects of Right to Privacy under Article 21 - iPleaders, (Dec. 6, 2021), https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/.

3 What is Estonian e-Residency and how to take advantage of it?, Xolo. https://www.xolo.io/zz-en/e-residency.

Having achieved independence from the Soviet Union in 1991, Estonia was obliged to start from zero in its economy and governance architecture redevelopment. The country took a confident step by substantially investing in its digital infrastructure, devoid of traditional models. The country completely understood that it was possible to harness technology as a top opportunity for modernizing public services and the economy. This vision set up e-governance systems, took on digital identity cards, and presented online voting, along with various other e-services that are now fundamental to the digital community in Estonia.

The idea of digital transformation was the backbone of E-Residency. It was the brainchild and propagator of Taavi Kotka, who formerly held the position of Estonia's Chief Information Officer. Embracing the notion of sharing the benefits of Estonia's digital ecosystem with people outside its jurisdiction became a priority for Kotka, along with other Estonian leaders. We will create a virtual residency to serve non-residential individuals in launching and overseeing businesses from anywhere around the world.

The concept was to enable global entrepreneurs, freelancers, and digital nomads to use this platform for streamlined business activities within the confines of the European Union. Estonia was visible as a foundation for digital entrepreneurship that stressed both digital security and ease of usability along with simplicity in the digital framework. This nurtured both global economic relationships and established the principle from which Estonia can advance towards becoming an innovator in global digital practices.[4]

IV. INDIA'S AADHAR POLICY

The Aadhaar system, as well as the Supreme Court ruling over it, had shaped, moulded, and is still shaping India's legal and social landscape and represents the complexity and challenge in attempting to reconcile state interests with individual rights in the digital age.

The Aadhaar project is the result of the Indian government's initiative since 2009, aiming to become a unique identification number for every resident in India. This is all-encompassing proof of identity, using biometric and demographic data that gain access to services from both the public and private sectors for the client. It was to develop, launch, and then operate the Aadhaar system. In just a very brief span, it became one of the world's largest biometric databases.

Aadhaar was introduced mainly as an instrument that would make the delivery of public services, particularly welfare programs, more efficient. It would help in ridding ghost or fake

[4] *Just a moment...*, https://www.researchgate.net/publication/358812544_ESTONIAN_E-RESIDENCY_AND_CONCEPTIONS_OF_PLATFORM-BASED_STATE-INDIVIDUAL_RELATIONSHIP.

 [ISSN 2581-5369]

identities so the fraud incidence lessened and subsidies and other benefits reached the right recipients. Over time, it gradually covered an extremely wide spectrum, and governments made its use mandatory for a few more purposes like opening a bank account, submitting one's taxes, and even admitting children to schools.

Even the somewhat scattershot process of its infiltration in the last five to six years rang alarm bells concerning privacy, data security, and the reach of state surveillance. Indeed, such gargantuan centralisation of such a huge base of individual data is fraught with grave risks - particularly so when there is no comprehensive legislation on data protection. The resultant case filings before the courts led to a landmark judgment of the Supreme Court in the K.S. Puttaswamy v. Union of India[5].

V. COMPARATIVE ANALYSIS OF PROTECTIONS FOR DIGITAL PRIVACY: ESTONIA & INDIA

(A) Estonia:

Estonia has an extremely advanced digital society, and strong rights of citizens about digital privacy are guaranteed both at the national and the EU level. The main protection areas include.

1. Constitutional Right to Privacy

The Estonian Constitution guarantees the fundamental right of privacy, under which one's data is protected. This is the legal basis for the country's rights to digital privacy.

2. General Data Protection Regulation (GDPR)

Estonia is also part of the European Union and falls within the scope of the most rigorous data protection laws in the world, GDPR. The rights of GDPR include the following:

Right to Access: Users will be entitled to access their data held by organisations.[6]

Right to Rectification: They may rectify data that appears to be incorrect.

Right to Erasure ("Right to be Forgotten"): They may request erasure of their personal data under certain situations.[7]

Right to Erasure: An individual has the right to request his data to be erased.

Right to Restrict Processing: An individual has the right to limit how his data is processed.

[5] (Sept. 27, 2018), https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.
[6] *Right of Access*, General Data Protection Regulation (GDPR) https://gdpr-info.eu/issues/right-of-access/.
[7] *Right to be Forgotten*, General Data Protection Regulation (GDPR) https://gdpr-info.eu/issues/right-to-be-forgotten/.

Data Portability: The citizen has the right to transfer his data from one service provider to another.

Consent: Organizations have to be very sure about having explicit consent before the collection of any personal data.[8]

3. Estonian Personal Data Protection Act

It is the national law that supplements the GDPR and gives more specific information on how data protection is carried out in Estonia. It outlines the rights of individuals regarding their data as well as the mandates of the organizations handling personal data.[9]

4. X-Road and Digital Identity

The Estonian X-Road is a decentralized data exchange that ensures citizens retain control over their data. Every citizen of Estonia has an e-ID that is their digital identity unique electronic ID that enables them to access public and private e-services securely. All operations related to the digital identity of the citizen are logged so that citizens can, at any point in time, see who accessed their data, thus controlling who would have access at any point.[10]

5. Digital Transparency and Accountability

Estonia makes privacy in the use of personal data visible. All that the government does about citizens' data can be checked and authority can also be held liable using public registers and audit trails.

Collectively, all these protections ensure that Estonian citizens have very solid digital privacy rights that make Estonia one of the most securely and transparently digitally developed countries in the world.

6. Transparency in Data Processing

Estonians have a central e-portal where they can see all that is happening with regard to their personal data, who and which government agency or private organisation accessed, when and for what.

7. Judiciary Procedures

Citizens can bring cases to courts if they believe that their right to digital privacy has been violated. They can also appeal to the Estonian Data Protection Inspectorate or to the European

[8] *Consent*, General Data Protection Regulation (GDPR) https://gdpr-info.eu/issues/consent/.
[9] *Personal Data Protection Act–Riigi Teataja*, https://www.riigiteataja.ee/en/eli/523012019001/consolide.
[10] Sander Nõmmik, *X-Road – interoperability services*, E-Estonia (June 10, 2024), https://e-estonia.com/solutions/x-road-interoperability-services/x-road/.

 [ISSN 2581-5369]

Data Protection Board.

(B) India:

India's approach to digital privacy is evolving, with several key legal frameworks and judicial rulings providing protections for citizens' digital privacy. Below is an overview of the protections guaranteed to Indian citizens:

Hey, just a heads up, here's a summary of stuff you ought to keep in mind about digital privacy in India:

1. **Constitutional Right to Privacy**

The Supreme Court of India, through the judgment passed in the month of August 2017, recognized the Right to Privacy as a fundamental right. The right has been made applicable in cases via Article 21[11] of the Indian Constitution, which talks about the right to life and personal liberty.

2. **Information Technology Act, 2000**

The IT Act is the leading legislation on cybercrime and digital privacy. It includes provisions like insisting that businesses take security measures for the protection of sensitive personal data and penalising private images and the transmission or capture without authorization.[12]

3. **Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act, 2023: This is a statutory law that includes the legal protection of personal data with respect to privacy, consent, and legitimate processing. It prescribes the obligations placed on Indian and foreign entities engaged in processing data related to individuals in India. The Act places data security and transparency duties as well as liabilities with corresponding penalties in cases of non-compliance. The Act also states an exemption for the government in matters related to national security or public order. The Act will increasingly and certainly alter the practices in handling data across various industries with the help of regulations and court interpretations.[13]

4. **Aadhaar Act, 2016**

The Aadhaar Act manages the use of the Aadhaar biometric identification system that includes

[11] *Law & Justice2.pmd*, (Jan. 7, 2009), https://www.indiacode.nic.in/bitstream/123456789/15240/1/constitution_of_india.pdf.
[12] *Cyber Law In India: IT Act 2000*, https://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html.
[13] *Salient Features of the Digital Personal Data Protection Bill, 2023*, (Aug. 9, 2023), https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264.

 [ISSN 2581-5369]

provisions for data security, limited sharing, and prohibition of unauthorized disclosure of Aadhaar data.[14]

5. **Cyber Security Measures**

India has also put in place the framework for cybersecurity through the National Cyber Security Policy and through agencies such as the Indian Computer Emergency Response Team, (CERT-In) in order to curb cyber attacks on citizens' data.

6. **Judicial Remedies**

Citizens have a right to approach judicial remedies in case their right to digital privacy has been infringed. This can be done through writing petitions in the higher courts or claiming compensation for data breaches.

VI. ESTONIA'S JUDICIAL PRECEDENTES

Estonia, like many countries in the European Union, has a legal system that is influenced significantly by both domestic and European Union law. Although the Estonian legal system is relatively young, having been re-established after independence from the Soviet Union in 1991, it has developed several significant judicial precedents, particularly in the area of digital privacy, data protection, and e-governance. Here are some notable judicial precedents in Estonia:

1. Right to Digital Privacy and Data Protection- Riigikohus (Estonian Supreme Court) Decision on Data Retention (2014) [15]

The principle of the Riigikohus ruling on data retention from 2014 emanates from the fact that Estonia's data retention laws were incompatible with a key provision relating to a person's privacy rights. In Estonia, like all other European Union member states, there existed laws retaining telecommunication data, such as call records, SMS, and internet usage, for a specific amount of time. This aligns with the 2006 EU Data Retention Directive, which requires telecommunications companies to retain data for law enforcement and national security purposes.

Estonian law would ensure that communications service providers store communications service metadata-who communicated, when, where, and for how long information for at least six months. It is aimed to be useful in the investigation of more serious crimes, like terrorism

[14] *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services Act), 2016*, BYJU'S (Nov. 4, 2016), https://byjus.com/free-ias-prep/aadhaar-targeted-delivery-financial-subsidies-benefits-services-act-2016/.

[15] (Mar. 6, 2016), https://privacyinternational.org/sites/default/files/2017-12/HRC_estonia-2.pdf.

and organized crime. Because it requires the storage of information about information regarding people suspected of no crime whatsoever, the law is most likely to infringe on individuals' rights to privacy and protection of their data.

Judgment:

Indeed, it was the judgment of the Court of Justice of the European Union (CJEU) in the case of Digital Rights Ireland Ltd. v. Minister for Communications, decided on April 8, 2014, that the Estonian Supreme Court further assimilated during the same year. Therein, it held that the EU Data Retention Directive was violative of the fundamental rights to privacy and data protection as enshrined in the EU Charter of Fundamental Rights.

In the Estonian case, the Supreme Court held that data retention laws in the country were unconstitutional because they put a disproportionate burden on privacy.[16]

2. Personal Data and Consent- Riigikohus Decision on Personal Data Processing (2016):[17]

This case involved a dispute over the processing of personal data by a private company without the explicit consent of the individuals involved. The company argued that the data processing was necessary for the performance of a contract.

Judgment:

The Supreme Court ruled that personal data processing without explicit consent could only be justified under specific, narrowly defined circumstances. The decision reinforced the importance of obtaining clear and informed consent from individuals before processing their data, in line with both Estonian and EU data protection laws.[18]

3. Surveillance And Privacy- Riigikohus (Estonian Supreme Court) Decision on Surveillance Powers (2019)[19]

In 2019, the Estonian Supreme Court (Riigikohus) was asked to review the surveillance powers of the Estonian Internal Security Service (Kaitsepolitsei) under Estonian law. The case arose

[16] (Mar. 6, 2016), https://privacyinternational.org/sites/default/files/2017-12/HRC_estonia-2.pdf.
[17] *Independent Supervision for Protection Personal Data Processed by the Courts in the Republic of Bulgaria for the Purposes of Discharging Their Judicial Functions*, Yearbook of Estonian Courts (June 10, 2021), https://aastaraamat.riigikohus.ee/en/independent-supervision-for-protection-personal-data-processed-by-the-courts-in-the-republic-of-bulgaria-for-the-purposes-of-discharging-their-judicial-functions/.
[18] *Independent Supervision for Protection Personal Data Processed by the Courts in the Republic of Bulgaria for the Purposes of Discharging Their Judicial Functions*, Yearbook of Estonian Courts (June 10, 2021), https://aastaraamat.riigikohus.ee/en/independent-supervision-for-protection-personal-data-processed-by-the-courts-in-the-republic-of-bulgaria-for-the-purposes-of-discharging-their-judicial-functions/.
[19] *Constitutional judgment 3-4-1-42-13*, https://privacylibrary.ccgnlud.org/case/constitutional-judgment-3-4-1-42-13.

from concerns that the broad surveillance powers granted to the security services infringed on individuals' right to privacy, particularly in the context of digital communications and data interception.

The central argument against the surveillance laws was that they allowed for extensive monitoring and data collection without adequate safeguards or oversight, potentially violating the right to privacy enshrined in both the Estonian Constitution and the European Convention on Human Rights (ECHR). Privacy advocates argued that digital surveillance practices lacked sufficient legal constraints, allowing for potential abuse and unwarranted intrusion into citizens' private lives.

The Internal Security Service justified its actions on grounds of national security, arguing that digital surveillance was crucial for protecting the state from serious threats such as terrorism, espionage, and cyberattacks. However, the plaintiffs contended that these surveillance practices needed to be balanced against the right to privacy and required stricter legal safeguards to prevent misuse.

Judgment:

The Estonian Supreme Court ruled that while surveillance is indeed necessary to ensure national security, it must be conducted in a manner that respects individual privacy and is proportionate to the threat being addressed. The Court emphasized the following key points:

- **Proportionality and Necessity:**

Surveillance measures must be proportionate, meaning that they should only be used when necessary and to the extent required for addressing a specific national security threat. Blanket or excessive surveillance that is disproportionate to the risk would be unconstitutional.

- **Judicial Oversight:**

The Court reinforced the principle that all surveillance activities, particularly those involving digital communications, must be subject to strict judicial oversight. This means that any request for surveillance must be reviewed and authorized by an independent judicial body to ensure that the actions are justified and by the law.

- **Legal Safeguards:**

Surveillance powers must be accompanied by sufficient legal safeguards to protect individual rights. The Court highlighted the importance of mechanisms such as due process, transparency (to the extent possible), and accountability to prevent the abuse of surveillance powers.

 [ISSN 2581-5369]

- **Targeted Surveillance:**

The Court held that surveillance should be targeted and not applied broadly or indiscriminately. Digital surveillance, in particular, should focus on individuals or groups who are reasonably suspected of posing a threat to national security, rather than the general population.[20]

VII. INDIA'S JUDICIAL PRECEDENTES

1. K.S. Puttaswamy v. Union of India[21]

K.S. Puttaswamy v. Union of India, a case dealt with in 2017, is the most important landmark in Indian constitutional law. It was brought by Justice K.S. Puttaswamy who retired as a judge. He moved for the mandatory linking of Aadhaar with welfare schemes because it invaded the right to privacy. The Supreme Court had a central question before it: whether or not the right to privacy was a part of the Indian Constitution's fundamental rights.

On 24th August, a nine-judge bench of the Supreme Court declared by a unanimous verdict that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution. The court held that privacy was a fundamental right, now protected by the Constitution's framework, and could not be infringed except by the law. It was a judgment of immense significance because it established privacy as one of the basic rights and went on to have an important impact on later legal developments in India.

For yet another time, the Aadhaar system faced a significant challenge in its path by the Court. In a subsequent judgment in 2018, a five-judge bench of the Supreme Court ruled that Aadhaar was constitutionally valid but placed several restrictions on it. The Court ruled that while Aadhaar could be used for purposes of delivery of government welfare schemes, it could not be made mandatory for obtaining services like bank accounts mobile connections or admission to schools. The court further emphasized robust measures for the protection of data and reiterated that the government should provide security and ensure the privacy of Aadhaar data.

2. Justice K.S. Puttaswamy (Retd.) v. Union of India (2018) – The Aadhaar Judgment[22]

After the landmark right-to-privacy ruling in 2017, the Aadhaar scheme faced further challenges. The petitioners argued that the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, which mandated the use of Aadhaar for accessing

[20] *Constitutional judgment 3-4-1-42-13*, https://privacylibrary.ccgnlud.org/case/constitutional-judgment-3-4-1-42-13.
[21] (Aug. 24, 2017), https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
[22] *Justice K.S. Puttaswamy and Anr. vs. Union of India (UOI) and Ors.*, https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-and-ors-vs-union-of-india-uoi-and-ors.

 [ISSN 2581-5369]

government services and subsidies, violated the right to privacy.

The petitioners contended that Aadhaar's requirement of collecting biometric and demographic data infringed upon privacy rights and allowed for potential mass surveillance by the state. Additionally, they argued that linking Aadhaar to essential services such as banking, taxation (PAN cards), and mobile numbers was unconstitutional and led to an invasion of personal privacy.

Judgment:

In 2018, a five-judge Constitution Bench of the Supreme Court delivered its verdict. The judgment upheld the constitutionality of Aadhaar but imposed several important restrictions on its use:

- **Aadhaar's Validity:**

The Court upheld the validity of Aadhaar for certain purposes, such as availing government subsidies, stating that it was constitutionally permissible as it aimed to streamline the distribution of government benefits and reduce fraud.

- **Proportionality and Legitimate Aim:**

The Court found that Aadhaar was designed to serve a legitimate state interest—ensuring that benefits and subsidies reached the intended beneficiaries—and that it met the test of proportionality.

- **Restrictions on Mandatory Use:**

The Court ruled that Aadhaar cannot be made mandatory for services not related to welfare subsidies, such as opening bank accounts, obtaining mobile phone connections, or admissions to schools.

- **Linking Aadhaar to PAN (Permanent Account Number):**

The Court upheld the mandatory linking of Aadhaar to PAN cards, stating it was necessary to prevent tax evasion.

- **Private Companies:**

The Court struck down provisions that allowed private companies (such as telecom operators and banks) to use Aadhaar for identity verification, citing privacy concerns. Aadhaar could not be used for commercial purposes or by private entities.

- **Data Protection and Security:**

 [ISSN 2581-5369]

The judgment emphasized the need for strong data protection measures to safeguard the sensitive biometric data collected by Aadhaar. It directed the government to introduce a robust data protection law to ensure that personal information is securely handled.

3. Anuradha Bhasin v. Union of India (2020) – Internet Shutdown and Digital Rights[23]

The case was filed in the wake of the internet shutdown in Jammu and Kashmir following the abrogation of Article 370 in August 2019. It was pleaded that the prolonged suspension of the internet interfered with the right to freedom of speech and expression and the right to privacy, as access to the internet was basic to the conduct of daily activities and for freedom of information in a modern digital society.

Judgment:

It has been held by the Supreme Court that access to the internet is freedom under Article 19 of the Indian Constitution, subject to reasonable restrictions.

Any restrictions imposed on the Internet can only be pursuant to the doctrine of proportionality and must be necessary, and for compelling reasons such as national security, but cannot be arbitrarily altogether.

The Court declared indefinite shutdowns of the internet unconstitutional and suspension orders must be reviewed at intervals in order to continue holding justification.

- **Importance:**

Even though this is not strictly a case about privacy, this judgment recognized the basic role digital access plays in present life and impacted privacy issues of collection of data as well as rights to online information access.

4. Shreya Singhal v. Union of India (2015) – Online Speech and Privacy[24]

A landmark judgment was Shreya Singhal v. Union of India, which dealt majorly with the constitutionality of Section 66A of the Information Technology Act, 2000. Section 66A made it criminal to send any message or information via a computer or communication device that was "grossly offensive," "menacing," or caused "annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will."

It was attacked as being too vague and too sweeping in its language, which everybody has

[23] (July 4, 2020), https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf.
[24] *A background to Section 66A of the IT Act, 2000*, https://prsindia.org/theprsblog/a-background-to-section-66a-of-the-it-act-2000.

proceeded to misuse during periods of popularity and notoriety of sham sainthood.

Many people were arrested under this section who posted criticizing remarks about politicians, government actions or other public figures online.

The petitioners claimed that the provision was vague and arbitrary and was violative of freedoms of speech, privacy, and the right to life under Articles 19 and 21.

Judgment:

It was on this basis that the Supreme Court ruled Section 66A to be unconstitutional and grossly overbroad, vague, and violative of the right to free speech.

While the case was, at its core, a freedom of speech case, the judgment had strong implications for digital privacy. It clarified the Court's basic concern about vague and excessive restrictions on online activities because they invaded both freedom of expression and privacy.

Although the case ostensibly was a matter of free speech, the Court's decision had significant implications for digital privacy as well. Convicting speech online on seemingly vague grounds may foreseeably result in surveillance or excessive government control over private online communications.

Although the judgment did not extensively address privacy, the court recognized that the sweeping authority of the government to monitor or penalize online speech threatened not only freedom of expression but also the right to privacy. Implicitly, the Court endorsed the idea that online communication should be free from unwarranted intrusion by the state.

- **Impact:**

It is actually a major win for digital freedom in India. For the first time, a judgment has protected persons digitally who have been using this medium to exercise freedom of speech and expression so that broad or vague laws could not be used to suppress dissent or criticism of the government.

This judgment reinforced the argument that just as freedom of speech is crucially important in the analogue space, it remains so in the digital space and cannot be curtailed by arbitrary laws.

While free speech has been the core theme of the case, the judgment must reach a balance between the right of privacy and control of the government over online communication, thereby indirectly contributing towards the larger conversation of digital privacy in India.

VIII. CONCLUSION

In the digital world, where governments are increasingly moving towards integrating

technology with governance and service delivery, such protection of privacy is highly crucial. Estonia and India have certainly made big steps in this direction with the programme of e-Estonia in Estonia and the Aadhaar Act of India, which has shown how technology can drive national development. As the digital revolution continues, so is the right to digital privacy one of the most important issues requiring legal safeguarding to protect citizens from data misuse.

E-Estonia positions the country strategically from other emerging global leaders in e-governance and, consequently, digital identity. Through e-Residency and X-Road, the citizens and e-residents of this country can access services in these governments and financial, and educational services over the internet with security. They ensure that people's data is safe, transparent, and controlled. As a country that follows the General Data Protection Regulation by the European Union, personal data is more monitored. While the citizens and the e-residents both make use of digital identities, Estonia's law ensuring their safety in a digital world remains sound. For example, in the 2014 Riigikohus ruling on data retention, emphasis is put on the fact that Estonia focuses on ensuring there is consent before such retention and puts its trust in judicial review in cases of infringement; hence, how such strong protection of privacy can integrate with technological development.

Significantly, the provisions of India's Aadhaar Act created a humongous digital infrastructure for more than a billion individuals to get unique biometric identities through which they could access government services and other ways of financial inclusion. Digital privacy and security concerns remain; if Aadhaar is mandatorily made use of, then there is indeed no comprehensive data protection law in force. The two key judgments were that of Justice K.S. Puttaswamy declaring privacy as a constitutional right, and the 2018 Aadhaar judgment, which, although granted constitutionality to Aadhaar, interpreted it with drastic restrictions-including its prohibition to being used in public affairs and insistence on more robust data protection. Such key judgments on issues of surveillance, data abuse, and questions of consent are still lacking in the current jurisprudence. In Estonia and India, the right to digital privacy is not merely a legal principle but rather an important supporting factor in exercising public trust in digital governance. Estonia is a shining example of how strong privacy protections can foster an innovative culture, build trust, and fuel economic growth. The experience with Aadhaar gives a strong feel for balancing state objectives against individual rights. In the future, as India continues on the path to digital transformation, it will have to take several other steps to further strengthen its digital privacy framework:

(A) Enact a Comprehensive Data Protection Law:

 [ISSN 2581-5369]

The Digital Personal Data Protection Act, of 2023 establishes an all-rounded framework for the protection of personal data which can be looked at by relating to privacy, consent-based processing, and lawful use. It, however, creates pertinent issues of state powers about surveillance and the exemptions of state entities in the process that might impede its effectiveness. Indian businesses need to change attitudes regarding the handling of data concerning the provisions of this Act. The Data Protection Board, with judicial interpretations that follow, will also clarify matters for the Act.

(B) Strengthen consent mechanisms:

Data collection should on Estonia's model be on a consent basis in India. The personal information should remain totally under the individual's control. Consent should be well-informed, explicit, and revocable at will so that a person can opt out of services without being denied access to more important services.

(C) Provide an Independent Data Protection Authority:

India requires a well-funded, independent Data Protection Authority that oversees the enforcement of data protection laws, investigates data breaches, and makes entities liable for misusing personal information.

(D) Improve Cyber Security Infrastructure:

Cyber attacks and data breaches are quickly becoming widespread fear in India, and a strong, appropriate framework for cyber security has to be developed and appropriately strengthened. It will certainly suffice if regular audits are performed on government databases, sensitive data is encrypted, and the best international practice is followed in the sphere of digital security.

(E) Judicial Control of Surveillance:

In this way, surveillance activities must be strictly set in the control of the judiciary to prevent misuse. Indeed it would be right to say that activity for surveillance must be necessary for national security, yet it could hardly be proportionate, targeted, and transparent in character, or otherwise clear safeguards of individual privacy.

The increasingly greater areas of life more and more controlled by technology will always need to have privacy as a matter of vigilant oversight. Indeed, the Estonian case exemplifies how innovative e-governance can evolve with strict privacy requirements, while the Aadhaar scheme in India illustrates how national goals must be weighed against individual rights. It will be a great starting point for India to achieve a comprehensive legal framework, strengthen cybersecurity, and bring people more empowered about being in control of their data to build a

digital future where growth will not only be the hallmark but respect and protection towards citizens' privacy.

*****

 [ISSN 2581-5369]