INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

AUTHORED BY - HARSHIT RANJAN SHRIVASTAVA

ABSTRACT

It was a huge stride forward for Indian constitutional law when the right to privacy was recognized as a basic right. In 2017, there was a case called Justice K.S. Puttaswamy (Retd.) v. Union of India. The Supreme Court said that Article 21, which is related to "Articles 14 and 19"[1], protects privacy as a basic right for life and freedom. This right safeguards, freedom and dignity in the digital era by giving people the right to make decisions, control information, and keep their bodies safe. Privacy is important for people's freedom, but it needs to be balanced with important state purposes like safety and welfare. This means that judges and lawmakers need to keep an eye on it.

KEYWORDS

Fundamental Rights, Article 21, Puttaswamy Case, Personal Liberty, Human Dignity, Informational Privacy, Decisional Autonomy, Aadhaar, Digital Age, and Data Protection.

INTRODUCTION

The right to privacy is one of the most important changes to India's law. It has changed the way people talk to the government. The Supreme Court unanimously decided in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) that "Article 21"[2], which protects life and personal freedom, also guarantees privacy. The Indian Constitution does not say this. This important decision changed history by emphasizing that privacy is fundamental for freedom, independence, and respect. It also changed earlier decisions that weren't as protective. The Court made it clear that privacy protects people's choices about their family, marriage, sexuality, and identity. It does this by protecting your right to privacy, your right to control your information, and your right to make your own choices. The constitution protects people from both the government and private parties using their personal information when privacy is seen as a basic right. This is especially important today since we live in the digital age, where new technologies like data collection and monitoring make us more worried. The Court did say

[1] Constitution of India 1950, art 14 & 19
[2] Constitution of India 1950, art 21

ISSN: 2582-6433

that privacy isn't always absolute and that it can be limited in ways that make sense for the safety, well-being, and order of the public. India has worked hard to find a middle ground between what people want and what businesses need. The new privacy law is an example of this because it fulfills international human rights standards.

HISTORICAL EVOLUTION

The Right to Privacy has meant many things to Indian judges over the years. The case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) makes this right a fundamental one. In M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of U.P. (1962), the Supreme Court declared that privacy was not a right protected by the Constitution. They contended the Constitution didn't make it plain. In Gobind v. State of M.P. (1975), however, the Court cautiously decided that Articles 19 and 21 do safeguard privacy, but only if it is limited in a fair fashion. After that, R. Rajagopal v. State of Tamil Nadu (1994) added informational autonomy to privacy. PUCL v. Union of India (1997) embraced privacy in communication by setting restrictions on phone tapping. Lastly, all nine judges in Puttaswamy agreed that privacy is a fundamental feature of people's freedom, respect, and independence. This was not what had been agreed upon before, and it brought Indian legislation in line with international human rights standards.

CASES RELATED TO HISTORICAL EVOLUTION

- **M.P. Sharma v. Satish Chandra[3]**

In India's first significant case, the Supreme Court examined whether the right to privacy was protected by the Constitution. The litigation started when the company's premises were subject to search warrants due to suspicions of fraud. The petitioners claimed that their privacy was breached by these searches. A panel of eight judges ruled that the Indian Constitution does not guarantee privacy as a fundamental right. The Court contrasted the U.S. and Indian constitutions, pointing out that whereas the U.S. Fourth Amendment expressly prohibits searches and seizures without a valid basis, India lacks a comparable provision. Therefore, no fundamental rights were violated by the legitimate authority to search and seize. This ruling set the standard for early Indian privacy law by categorically rejecting privacy as a right.

[3] M.P. Sharma vs. Satish Chandra AIR 1954 SC 300

ISSN: 2582-6433

- **Kharak Singh v. State of Uttar Pradesh[4]**

It said that the police kept an eye on persons they felt were up to no good. Kharak Singh, the person who filed the suit, didn't like the Uttar Pradesh Police Regulations that allowed them to spy on people, even traveling to their homes at night. He stated that these measures violated his basic rights, which the Constitution protects. There were six judges, and they couldn't agree on a decision. Most of the people who voiced out assumed that overnight house visits were against the law because they violated "personal liberty" under Article 21. The Constitution didn't contain anything about privacy rights, though. The Court made it clear that freedom meant not letting anyone into your home or personal life without a solid reason. Even while privacy wasn't seen as a separate basic right, the decision was essential since it connected it to personal freedom. Justice Subba Rao went even further in his renowned ruling and argued that everyone has the right to privacy.

- **Gobind v. State of Madhya Pradesh[5]**

It was one of the earliest Indian Supreme Court cases to touch upon the right to privacy. The petitioner challenged police regulations that permitted surveillance of individuals with prior criminal records, arguing that such measures violated his fundamental rights under Articles 19(1)(d) and 21 of the Constitution. The Court, while upholding the regulations, acknowledged that privacy is a constitutional value implicit in the right to life and personal liberty. However, it emphasized that privacy is not absolute and can be curtailed by compelling state interests such as public order and security. This cautious recognition of privacy laid the foundation for later jurisprudence, balancing individual liberty against the needs of state surveillance.

- **Justice K.S. Puttaswamy v. Union of India[6]**

It was a landmark nine-judge bench decision that firmly established privacy as a fundamental right under Article 21. The case arose from a challenge to the Aadhaar scheme, where Justice Puttaswamy argued that compulsory biometric identification violated personal liberty. The Court unanimously held that privacy is intrinsic to life and liberty, encompassing autonomy over personal choices, bodily integrity, and informational privacy. It overruled earlier precedents such as M.P. Sharma and Kharak Singh, which had denied privacy as a fundamental right. The judgment transformed Indian constitutional law, ensuring that privacy protections

[4] Kharak Singh vs. State of Uttar Pradesh AIR 1963 SC 1295
[5] Gobind vs. State of Madhya Pradesh AIR 1975 SC 1378
[6] Justice K.S. Puttaswamy vs. Union of India AIR 2017 SC 4161

ISSN: 2582-6433

extend to digital data, surveillance, and personal freedoms, thereby shaping the legal framework for individual rights in the modern era.

IS PRIVACY A FUNDAMENTAL RIGHT??

It wasn't always obvious in the Indian Constitution that "privacy" was a basic right. The Supreme Court said that the government could safeguard the peace by watching over people a lot in the first few years of freedom. But as technology got better and the government learned more about people's lives, it became more and more vital to have unambiguous legal protection. Nine judges made the landmark Puttaswamy decision in 2017, which ruled that all Indians have the right to privacy.

The Court made it clear that privacy is not a separate or "extra" right, but rather a vital part of the rights we already have. Article 21 says that everyone has the right to be free and live. The courts say that you can't genuinely have "liberty" or "dignity" if you can't keep your things and data safe. The government can't stop you from doing what you want, loving who you want, or living your life the way you want.

You can do what you want, but that doesn't mean you can. The government can still invade individual's privacy if it needs to in order to keep the country safe or stop people from committing crimes. For this to happen, the government needs to follow three steps: there must be a clear rule that lets it happen, there must be a true need for it, and the action must be "proportional," which means the government shouldn't get more information than it needs. With smartphones and digital tracking being so common these days, this right is a very crucial safety net. It makes sure that the law protects our area.

PRIVACY AND THE DIGITAL WORLD??

In our digital age, practically everything we do online leaves a "digital footprint" that displays private information about us. As soon as we open our phones, a lot of firms, such as data brokers, social networking sites, and mobile apps, start gathering a lot of personal information. This data clearly shows our names, phone numbers, and email addresses. But it also has a lot more private "metadata." This includes our current location on GPS, our browsing history, the goods we buy, and even the "likes" and "shares" that reveal our political and religious opinions. Social media businesses, in particular, utilize intricate algorithms to look at this data in order

ISSN: 2582-6433

to develop detailed psychological profiles of us so they can offer us focused advertisements or influence how we behave on their platforms.

Handling this information is often like using a blade with two edges. Apps on our phones make our lives easier by using our private information. For example, an exercise app needs to know about our health to keep track of our progress, and a meal delivery service needs to know where we are to find restaurants nearby. But there is an issue when this information is not handled in a transparent way. A lot of consumers "accept" large and complicated Terms and Conditions without knowing that they can be granting an app access to their whole contact list, private images, or microphone. Companies and marketers often buy this information or get it for free. Then they follow us around on numerous websites. It feels like there are always digital eyes on us because of this.

The law is changing so that it can cope with these issues. The Digital Personal Data Protection (DPDP) Act 2023 in India encourages businesses to be a lot more careful today. They need to be honest with people about what data they are gathering and why. Justice K.S. Puttaswamy also said that our "informational privacy," or the right to own our own digital names, is a basic right that is safeguarded. This means that platforms can't treat our data like it's their own anymore. It's still challenging to establish a balance between the good things that technology can do for us and the need to safeguard our personal space, even if we live in the age of AI and big data. Keeping things private isn't enough to secure our digital privacy anymore. We also need to defend our freedom and make sure that our private lives don't become things that anyone may buy and sell around the world.

THE GOVERNMENT'S POWER VS. YOUR PRIVACY??

In constitutional democracies, there is a fine line between the rights of individuals and the power of the state. The Indian Supreme Court says that privacy is a basic right, but not an absolute one. The government can only legally intercept, monitor, or gather personal data in certain situations and following rigorous legal rules.

1. **Privacy is Not Absolute**

In basic law, there is no such thing as an unlimited right. The government wouldn't be able to fight crime, collect taxes, or keep people safe if everyone had the right to privacy. In the Puttaswamy case, the Supreme Court made it plain that privacy is a "qualified" right. There

ISSN: 2582-6433

may be times when other people's rights or the safety of the country are more vital than the Constitution's protection of your private life. Law students should realize that the right to privacy can't be utilized to cover illicit acts. People have the right to privacy, but the law also knows that privacy is social and that the demands of the group may come before those of one person.

2. The "Three-Fold Test"

In any privacy matter, this is the most critical thing that the law states must happen. The Court adopted this rule so that the government can't spy on people for "national security" purposes. Legality indicates that the government must follow a rule that the legislative created. An executive order by itself is not enough. Second, Legitimate Need makes sure that the government has a valid reason to exist, such keeping people safe or healthy. Third, you can utilize proportionality as a test for "rational nexus." It checks to see if the government's strategy is the best approach to attain the goal. The authorities can't watch over an entire city and capture a burglar with only one phone call.

3. National Security and Sovereignty

When it comes to national security, the state has the strongest justification for violating privacy. In an era of global terrorism and cyberwarfare, the government must be able to decipher encrypted communications in order to prevent attacks. “Section 69 of the IT Act”[7] permits the federal government to intercept any digital data if it is required for India's "sovereignty and integrity." This is the most potent weapon, but it is also the most contentious, as demonstrated by the debates around software like Pegasus. Determining the boundary between "national security" and "political surveillance" is the legal problem here. This is to ensure that the authority to protect the nation is not used to stifle opposition.

4. Prevention and Investigation of Crime

Privacy shouldn't get in the way of law and order. If the police have a reasonable reason to believe that someone is breaking the law, they can search residences and take digital information. This principle is particularly crucial for your work with the Bharatiya Nagarik Suraksha Sanhita (BNSS). To get to the bottom of things, the authorities should be able to look at the victims' private texts. The "Code of Criminal Procedure" (and now the BNSS) says that

[7] Information Technology Act 2000 (India), s 69

ISSN: 2582-6433

searches must be done with warrants or unambiguous written orders. This is to make sure that they are not done for no cause or to harass someone.

5. Digital Evidence Collection under BSA

The Bharatiya Sakshya Adhiniyam (BSA) has modified how Indian judges look at evidence. Digital data, such as emails, WhatsApp chats, and server logs, is now the major evidence, so the government can "compel" people to give them up. This helps police prove modern crimes like cyberfraud or online harassment, but it also raises a privacy issue: how much information can they get? People keep all of their information on their phones and laptops, which is what the law says. This means that you need to be specific about what kind of proof you want to collect. You can't take additional personal things with you if you only need one email for the case. You also can't take the complete laptop.

6. Maintenance of Public Order

"Public order" involves keeping rioting, carnage, or disorder from erupting in one place. The government may utilize data to find "troublemakers" or keep an eye on the spread of "fake news" that could lead to violence when there is trouble in the neighborhood or a disturbance in the peace. In certain regions, this could involve "internet shutdowns" or watching what people say on social media. Even though these acts are nasty, courts usually let them happen if they are only for a short time and are meant to save lives. The difficulty is making sure that these skills aren't exploited to hinder peaceful protests. People have the right to demonstrate, according to Article 19. This right is the same as the right to privacy.

7. Legitimate Use under the DPDP Act, 2023

The Digital Personal Data Protection Act brought up the idea of "certain legitimate uses." This means that the government can utilize your private information for public purposes without your permission. For instance, the government can already check your information against databases that are already in existence if you want a passport or a government grant. The state can also look into someone's health records if they are sick and can't provide consent. This is supposed to help the government do its job better so that the "right to privacy" doesn't come in the way of providing critical services.

8. Surveillance Safeguards and Oversight

There are administrative steps in place to make sure that the government doesn't turn into an

ISSN: 2582-6433

all-powerful "Big Brother." In India, for example, the union home secretary or a state home secretary has to sign orders for phone tapping. Then, a "Review Committee" directed by the Cabinet Secretary looks over these orders. Some people say this is "government checking itself," but it does make things more responsible. A legal researcher would do well to look into whether these protections are "sufficient." The judiciary has often contended that to ensure comprehensive justice, "judicial oversight" where a judge authorizes the warrant should complement "executive oversight."

9. The Role of Judicial Review

The Constitution calls the court the "sentinel on the qui vive," which means "watchful guardian." If you don't like the way the government is collecting your personal information, you can go to court and submit a Writ Petition under Article 32 or 226. If a legislation or action by the government doesn't pass the three-part privacy standard, the courts can "strike it down." This guarantees that the government will always follow the law. Even if a law authorizes the government obtain information, the Supreme Court can nonetheless find it is unlawful. This can happen if the law is overly vague or provides the police too much "unbridled" power.

10. Preventing a Surveillance State

Privacy rules are meant to keep the country from turning into a place where everyone feels like they are being watched. As a result, people are afraid to say what they think, read certain books, or meet certain people. This is called the "chilling effect." The Supreme Court made it clear that privacy is important for "individual dignity." Limiting the power of the state, the law guards each person's "inner sphere" even when the state is strong. A democracy is different from an authoritarian one because of this balance. People get help from the government, not the other way around in a democracy.

PROTECTION OF PERSONAL DATA (THE DPDP ACT)

India has enacted its first full law to protect people's private information. The name of the law is the Digital Personal Data Protection (DPDP) Act, 2023.

1. The Concept of the "Data Principal" and "Data Fiduciary"

The Act makes some formal names actual. That's you, the person whose information is being gathered. The Data Fiduciary is the business, hospital, or government entity that decides how and why to use your data. Because of this, it is evident that the fiduciary must take care of the

ISSN: 2582-6433

principal by law. This regulation makes sure that the user still "owns" their digital identity and that the firm is simply a guardian.

2. The Requirement of Clear and Affirmative Consent

Under the DPDP Act, "implied consent" is no longer enough. Before a fiduciary may take your data, they have to tell you in straightforward, simple language. You can write this notification in English or any of the 22 languages listed in the 8th Schedule of the Constitution. To agree, your answer must be clear and positive. You can easily change your mind about this agreement at any time for your peace of mind. The company has to stop using your data right away if you take back your authorization.

3. Purpose Limitation and Data Minimization

These are the two "golden rules" for being safe online. "Purpose limitation" means that a corporation can't use your information to construct a credit score profile of you if they receive it to deliver you a pizza. Data minimization means that a corporation should only collect the least amount of information it needs to do its function. For example, a calculator app doesn't really need to view your contact list or GPS location to work.

4. Accuracy and Erasure of Data

The Act gives you the "Right to Correct" and the "Right to Erasure." The data fiduciary must repair your data if it is wrong or out of date if you ask them to. The Right to Erasure, commonly known as the "Right to be Forgotten," permits you to tell a firm to delete your information once it has been used for its intended purpose. When you remove your account, social media applications shouldn't keep your information on their computers.

5. Protection of Children’s Data

The DPDP Act is pretty tough on kids under 18. Companies can't utilize kids' information without receiving consent from their parents first. They can't additionally watch or record what youngsters do or show them ads that are only for them and could "harm" their health. This is a huge step toward keeping the information of the next generation of internet users protected.

6. Duties and Obligations of Data Fiduciaries

The business is in charge of safety. To stop data breaches, they need to put in place "reasonable security safeguards." If there is a breach, the fiduciary must now legally alert the Data

ISSN: 2582-6433

Protection Board of India and the people who were hurt. People won't be able to hide data leaks from the public. They also need to engage a Data Protection Officer (DPO) to handle complaints and make sure the company meets the rules.

7. The Data Protection Board of India (DPBI)

The Act grants the DPBI the most power to make rules. It works like a "referee" on the web. It can investigate into issues, bring in firm officials, and fine them a lot of money for not obeying the rules. The Board is a separate entity that makes sure that even the biggest tech companies are held accountable if they break the rules governing Indian people' privacy.

8. Significant Data Fiduciaries (SDFs)

The government can name some corporations "Significant Data Fiduciaries. " These are companies like Google, Meta, or huge banks that handle a lot of sensitive data. These SDFs also need to conduct the Data Protection Impact Assessments (DPIA) that are required. They should also have outside auditors check on them from time to time to make sure they aren't putting people's privacy at risk.

9. Financial Penalties for Non-Compliance

The DPDP Act works because it punishes people who breach the law extremely severely. Companies that don't protect their information could be penalized up to ₹250 crore. Fines used to be only for show, but today they are designed to be "deterrent." This implies that corporations will lose more money if they disobey the regulation than if they respect it. Companies need to start doing their work in a way that doesn't invade people's privacy.

10. Exemptions for Government and "Legitimate Uses"

The Act doesn't require permission for some actions. While the government gives individuals money, benefits, or licenses, that's an example of a "legitimate use." You must also observe this guideline while you're sick, in a disaster, or at work. Some individuals think these exclusions are overly broad, but their role is to make sure that the right to privacy doesn't stand in the way of critical or life-saving government services.

PRIVACY IN MODERN TECHNOLOGY (AI AND FINGERPRINTS)

Biometric indicators, such as fingerprints, alter the parameters of personal privacy when integrated with artificial intelligence (AI). Our real bodies and our online selves are now always

ISSN: 2582-6433

connected. People don't just use fingerprints to get into their phones nowadays. They are also made into digital "templates" that are used for many purposes, like keeping track of who is at the office and keeping banking safe. This is incredibly useful; however, the biggest difficulty is that fingerprints last forever. If someone takes your fingerprint or shares it with someone else, you can't change it. If someone sneaks into a database that has these digital maps, they will take the person's name and make it impossible to get it back. In other words, the law says that it is highly necessary to keep this information protected.

There are more concerns now that smart technologies may "infer" data from other data. AI systems can utilize fingerprints or facial patterns to predict facts about a person that they didn't plan to divulge, such as their race, genetic history, or even their mental condition. "Surveillance by Inference" works even if you don't notify anyone. An AI only needs to be smart enough to figure it out. AI-based surveillance in public settings may also keep a close eye on what people do, which takes away their "right to be anonymous" in a crowd.

The Digital Personal Data Protection (DPDP) Act, 2023, controls these gadgets in India. Sharing genetic information is against the law. Businesses and the government should adopt "privacy by design" and make sure that fingerprints are only used for the purpose they were taken for. As AI gets smarter, it's hard for lawyers to make sure that it keeps us secure without using our unique physical qualities to monitor or profile us without our permission.

CHALLENGES IN PROTECTING PRIVACY TODAY??

In 2026, keeping secrets is just one part of protecting your privacy. It also means dealing with a complicated web of hidden data collecting, powerful AI, and difficult legal problems. As the digital era goes on, a number of "new-age" challenges have made it harder for people and the government to keep an eye on their personal information.

These are the main issues that make it hard to safeguard privacy in today's world:

1. **The "Black Box" of Artificial Intelligence**

AI is a unique threat to privacy since it learns from data instead of just keeping it. When you provide an AI your personal information, it is stored in a "black box," which is a convoluted math model that even the people who built it can't find or remove information about a single individual. This brings up the issue of "data inference," which means that AI can tell what your religion, sexuality, or health problems are merely by looking at what you buy or listen to. Long-

ISSN: 2582-6433

standing consent norms don't always keep you safe because the AI "guesses" this information instead of acquiring it from you.

2. Dark Patterns and Manipulative Design

People often lose their privacy not by force, but by lying. "Dark patterns" are ways that user interfaces are designed to get you to make decisions that are better for the firm than for your privacy. It's evident that an app is trying to trick you when it hides the "Reject" or "Manage Settings" button in three pages of small, dark text but makes the "Accept All" button big and easy to click. Companies gain "consent" that is morally wrong but legal by playing on our desire for ease and grasp of the law. This is because the person gave out their information after being deceived.

3. Surveillance Normalization and the Chilling Effect

More and more people live in and near towns and residences that have smart cameras, GPS tracking, and facial recognition. This is known as "normalizing surveillance." People get scared when they think they're being monitored all the time. People may cease going to peaceful protests, reading books that are controversial, or speaking out because they think they are being filmed and that the footage could be used against them in the future. This makes privacy a political issue instead of a personal one. A society that is always being observed is one that is afraid to be different.

4. Data Localization and Cross-Border Transfers

These days, everything you need doesn't stay in one place for very long. When you use a worldwide app, people in India, Ireland, and the US may all work together to handle and store your personal information. When it comes to "jurisdiction," the law is terribly wrong about this. The DPDP Act won't require a corporation to respect the laws if it is based in a country that doesn't care much about privacy. This "legal fragmentation" can change your digital rights if your data is kept on a computer in several places.

5. The Rise of the Metaverse and Biometric Tracking

We need "high-stakes" data for the next wave of technology, such as the metaverse and virtual reality (VR). These devices keep track of your heart rate, how your eyes move, and even how you walk, which is not the same as what you post on social media. This is called "biometric data," and the bad news is that it never goes away. You can change your password if someone

ISSN: 2582-6433

gets it, but you can't alter your body if a corporation gives out your biometric "fingerprint" or eye scan. It's more crucial than ever to secure your privacy because a breach could lead to identity theft that lasts your whole life.

CONCLUSION

The momentous *Puttaswamy* verdict in 2017 raised everyone's right to privacy in India from a secondary idea to a basic one. The Supreme Court says that privacy is important for life and freedom under Article 21 since it protects a person's right to control their own body, information, and dignity. This privilege may be limited for valid reasons, such as national security. However, any government action must now pass a strict three-part test of need, proportionality, and legality. The Digital Personal Data Protection Act of 2023 makes "data fiduciaries" responsible for collecting and using personal data. This rule makes the protection even stronger in the digital age.

REFERENCES

BOOKS

Indian Constitutional Law by M P Jain.

Constitutional Law of India by Dr. J.N. Pandey.

V.N. Shukla's Constitution of India.

BARE ACT

The Constitution of India

WEBSITE

https://www.indiacode.nic.in/bitstream/123456789/19150/1/constitution_of_india.pdf

https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/

https://indiankanoon.org/doc/1199182/