INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

NORMATIVE TENSIONS IN DATA PROTECTION: PRIVACY RIGHGTS VERSUS STATE EXEMPTIONS UNDER GDPR AND DPDP ACT,2023

AUTHOR – NIVEDITA SINGH * & (DR) ANUPRIYA YADAV**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – NIVEDITA SINGH & (DR) ANUPRIYA YADAV, NORMATIVE TENSIONS IN DATA PROTECTION: PRIVACY RIGHGTS VERSUS STATE EXEMPTIONS UNDER GDPR AND DPDP Act,2023, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 640-650, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The growth of worlds has made personal data very valuable. This raises concerns about keeping our personal info private and how much power the government should have. This paper looks at the conflict between our right to privacy and the governments exceptions in data protection laws. It compares the European Unions General Data Protection Regulation (GDPR) and Indias Digital Personal Data Protection Act 2023 (DPDP Act). The GDPR is based on giving individuals rights and has limits on government interference. On the hand the DPDP Act gives the government a lot of freedom to decide what is best for national security and public order. This paper checks if the DPDP Act protects our right to privacy as stated in the Justice K.S. Puttaswamy v. Union of India case. It finds that Indias framework is a start but might not protect our privacy well because it has many exceptions and not enough safeguards. The study ends with suggestions to make Indias data protection laws better and more in line with standards while keeping our democracy accountable. The Digital Personal Data Protection Act, 2023 (DPDP Act) and data protection are key, to this. We need to ensure that the DPDP Act protects our privacy.

KEYWORDS: GDPR, DPDP Act, Executive Discretion, State Exemptions, Constitutional Law

Normative Foundations of Data Protection

When we talk about data protection, it's easy to jump straight into rules and compliance and

legal frameworks… but underneath all of that, there's something deeper going on. At its core, data protection is really about values. About what we, as a society, choose to protect and why. And in most modern democracies, that "why" almost always comes back to one idea—

privacy. Not just as a preference or a luxury, but as something far more essential.Privacy,

especially in the Indian context, took on a very different meaning after the landmark decision in Justice K.S. Puttaswamy v. Union of India. Before that, privacy sort of existed in fragments—recognized in bits and pieces, but never fully articulated as a standalone right.

The judgment changed that. It didn't just acknowledge privacy, it placed it right at the heart of the Constitution, linking it directly to life and personal liberty under Article 21.[1]And that shift… it matters. Because once something becomes a fundamental right, the way the State interacts with it has to change. The Court, interestingly, didn't stop at just declaring privacy as a right. It went further and laid down a kind of test—a way to evaluate when and how the State can step in and interfere. This three-part standard—legality, necessity, and

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

proportionality—now acts like a guiding compass. So, if the government wants to access or restrict personal data, it can't just do so casually. There has to be a law backing it (legality), the action must serve a genuine need (necessity), and even then, it must not go beyond what is required (proportionality). Sounds straightforward, but in practice… it's not always that

simple. Now, if we shift our focus a bit and look at the European Union's approach,

particularly the GDPR, you start to notice a different tone. The GDPR almost feels like it was written with a certain scepticism—like it doesn't fully trust either corporations or

governments with personal data. And maybe that's intentional. It builds its entire structure around the individual, placing strong emphasis on rights and protections.[2] Concepts like

fairness, transparency, and accountability are not just decorative terms; they actively shape how data is handled.For instance, the idea of purpose limitation ensures that data collected for one reason isn't casually reused for something else. Data minimization pushes entities to

collect only what is absolutely necessary, nothing more. And accountability… well, that's

where things get serious. Organizations are not just expected to follow the rules, they must be able to prove that they are following them. There's a certain strictness here, almost like the law is constantly asking: "Do you really need this data? And if yes, can you justify it?"What's also interesting is that the GDPR doesn't draw a sharp line between private entities and the

State. Both are held to high standards. Government access to data isn't left unchecked; it is tightly regulated, and often subject to independent oversight. This reflects a broader

philosophy—that power, regardless of who holds it, needs limits.

Coming back to India, the Digital Personal Data Protection Act, 2023… it feels like a work in progress. Not in a negative sense, but more like something that is still finding its balance. The Act does introduce important elements—consent-based processing, obligations for data fiduciaries, and certain rights for individuals (or data principals, as the law calls them).[5] These are all steps in the right direction, no doubt.But at the same time, there's a noticeable difference in how the law approaches power, especially State power. Unlike the GDPR, which seems cautious, the DPDP Act appears a bit more… accommodating. It creates space for the government to exempt itself or its agencies under broad grounds like national security or public order. Now again, these are valid concerns. Every State needs to protect its interests. But the issue is not the existence of these exemptions—it's their scope, and the lack of clearly defined limits. There's also this underlying shift in tone. While GDPR feels rights-driven, almost protective, the DPDP Act leans more towards regulation and governance. It sets up a framework, yes, but doesn't always anchor it firmly in the language of fundamental rights. And that can make a difference. Because when rights are not the central focus, they can sometimes become secondary… or negotiable. So, in a way, what we see here are two different approaches to the same problem. One starts with the individual and builds outward, placing checks on power. The other begins with regulation and tries to incorporate rights within it, while still leaving considerable room for the State to act. Neither approach is entirely perfect, but the tension between them is hard to ignore.[3]And maybe that's where the real conversation lies— not just in comparing laws, but in asking what kind of balance we are willing to accept. How much privacy are we ready to give up for security? And more importantly… who gets to make that decision?

State Exemptions: Scope and Justification

When we begin to look at data protection laws one thing becomes clear. No matter how strong the rights framework is there is always a point where the government steps in and says, "this is

where exceptions apply.". Maybe that's inevitable. Governments do have

responsibilities like security maintaining order and protecting sovereignty. The real issue is not whether exemptions exist. It's how far they go and who keeps them in check.

If we start with the GDPR the approach feels careful. It does allow for government

exemptions. They are not easily given. They are meant to be narrow, specific and justified.

The law doesn't just give power. Walk away. It places conditions around it. Any restriction

imposed by a government has to pass through the filters of necessity and proportionality. So, the government must show that the measure is genuinely required. Even then it cannot go

beyond what is strictly needed.

There's also something at play here. Scrutiny. Decisions taken under these exemptions are not final. They can be reviewed, challenged and tested before courts or independent authorities.

That makes a difference. Because when power is subject to review it behaves differently. It becomes measured more accountable.

Another important point is that when governments introduce their own restrictions they

cannot move too far away from the core values of the regulation. Fundamental rights still act like a line. So while flexibility exists it is not unlimited. There is always this underlying

reminder that privacy's not just a policy concern. It is a right that cannot be easily overridden.

Now when we turn to the DPDP Act, 2023 the picture starts to shift. The Act does provide for exemptions. The way they are framed feels broader. The Central Government is given the

authority to exempt its agencies on grounds like security, public order and sovereignty. These are aims.. The concern lies in how open-ended these categories can be.The language used is, at times quite wide. Terms like " order" or "security of the State" don't always come with

clear boundaries. That creates space for interpretation for discretion. Unlike the GDPR, where restrictions are closely tied to necessity and proportionality the DPDP Act doesn't always

make those limitations explicit.[4]There's also the question of oversight. Under the GDPR there are layers. Independent supervisory authorities, judicial remedies. In the framework those

checks feel less pronounced. The power to grant exemptions largely rests with the executive itself. And the mechanisms to review or challenge those decisions are not clearly

defined.[5]That's where the discomfort begins to build. Because when exemptions are broadly worded, discretionary in nature and not tightly monitored they start to shift the balance.

Privacy, which is supposed to be a right begins to feel conditional.[6]So what we are really

looking at here is a difference in approach. The GDPR treats exemptions as exceptions that must be justified and contained. The DPDP Act on the hand seems to treat them as necessary tools of governance. Giving the government an amount of trust, in deciding when and how to use them.[7]This difference might not seem dramatic at glance.. Its implications are significant. Because in the end it shapes how power is exercised.. How protected individuals actually are.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Comparative Analysis

Aspect	GDPR (European Union)	DPDP Act, 2023 (India)
Normative Foundation	Strongly rooted in fundamental rights, particularly privacy and data protection as core human rights within the EU legal order. Emphasizes dignity, autonomy, and individual control over personal data.	Primarily regulatory in nature with an emerging rights-based framework. Focuses on governance and digital economy needs while incorporating privacy protections in a developing form.
Philosophical Approach	Built on a rights-centric and precautionary model that reflects skepticism toward concentration of power, whether by the State or private entities.	Reflects a state-centric and trust- based model, where the executive is given broader authority with the assumption of responsible use.
State Exemptions	Narrowly defined and conditional. Must satisfy strict tests of necessity, proportionality, and legality. Exemptions are exceptional and not the norm.	Broadly framed exemptions available to the Central Government on grounds such as national security, sovereignty, and public order. These are discretionary and expansive in scope.
Scope of Executive Discretion	Limited executive discretion due to predefined legal thresholds and binding EU-wide standards.	Significant executive discretion, with the government empowered to notify exemptions without detailed statutory limitations.
Oversight Mechanisms	Independent Data Protection Authorities (DPAs) with strong enforcement powers. These bodies operate autonomously from government influence.	Data Protection Board functions under a framework where independence may be influenced by executive control, raising concerns about impartiality.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Judicial Safeguards	Robust judicial remedies available. Individuals can challenge violations before courts, and	Judicial remedies exist but lack detailed procedural clarity in the context of state exemptions,

Aspect	GDPR (European Union)	DPDP Act, 2023 (India)
	decisions are subject to strict judicial scrutiny.	potentially limiting effective redress.
Accountability Framework	High level of accountability. Organizations must demonstrate compliance through documentation, audits, and impact assessments (e.g., DPIAs).	Accountability mechanisms are evolving. While obligations exist, enforcement structure and transparency requirements are still developing.
Transparency Requirements	Strong emphasis on transparency. Data subjects must be informed about data processing, and government actions are subject to disclosure norms.	Transparency obligations exist but may be diluted in cases involving government exemptions, where disclosure requirements are less स्पष्ट.
Balance Between Privacy & State Interest	Carefully calibrated balance with privacy as the default and state interference as an exception subject to strict safeguards.	Balance tends to tilt toward state interests in certain scenarios, particularly due to broad exemption provisions.
Enforcement Strength	Strong enforcement with heavy penalties for non-compliance, ensuring deterrence and compliance culture.	Enforcement mechanisms exist but are relatively new and may require strengthening for effective deterrence.

What stands out when looking at this comparison is the difference in attitude toward power. The GDPR seems to be cautious. It has checks, in place like it does not trust power. The DPDP Act seems trusting. It gives the executive some space to act. It seems to think that

power will be used responsibly.

This difference may seem small. It actually has big consequences. In data protection a law is strong not because of what it says. Also because of how well it stops people from misusing power. The GDPR and DPDP Act show two approaches. The GDPR has checks. The DPDP Act gives freedom. Both try to protect data. They do it in different ways.

Constitutional Concerns

When you start looking at the Digital Personal Data Protection Act, 2023 a little more closely... especially through a constitutional lens, some uneasy questions begin to surface. Not immediately, not in an obvious way, but gradually. On paper, the Act looks like a much-

needed step forward. India finally has a dedicated data protection law, and that in itself is

significant. But the real test of any such law isn't just whether it exists—it's whether it actually holds up against constitutional standards, particularly the right to privacy.Now, ever since the decision in Justice K.S. Puttaswamy v. Union of India, we have a fairly clear framework to assess this. The Court didn't just declare privacy as a fundamental right and

leave it at that. It laid down a structured way—almost like a checklist—to evaluate any state action that interferes with privacy.[8] And that checklist revolves around three key ideas:

legality, necessity, and proportionality. At first glance, the DPDP Act does seem to satisfy the requirement of legality. After all, the exemptions granted to the State are backed by statute.[9]There is a law in place, duly enacted, which authorizes the government to act in

certain situations. So in a technical sense, the first condition is met. But then again… legality alone was never meant to be enough. The Puttaswamy judgment made that very clear. A law can exist, and still be problematic if it allows too much unchecked power. This is where the

second requirement—necessity—starts to feel a bit uncertain. The Act allows the government to exempt its agencies on grounds like national security, public order, and sovereignty. These are important concerns, no doubt. But the issue is that these terms are often broadly defined, sometimes even vaguely worded.[10] And when standards are vague, it becomes difficult to assess whether a particular action is truly necessary or just convenient.There isn't always a

clear requirement for the State to demonstrate why a specific exemption is needed in a

specific situation. That lack of precision… it creates a kind of grey area. And in constitutional law, grey areas can be risky, because they leave room for interpretation—and sometimes, for overreach. Then comes proportionality, which is probably the most crucial part of the test, and also the most difficult to satisfy. Proportionality is not just about whether the State has a valid reason to act, but whether the way it acts is balanced and restrained. It asks a simple but powerful question: is the intrusion into privacy more than what is absolutely necessary?In the context of the DPDP Act, this is where concerns become sharper. The exemptions provided to the government are quite broad, and there are limited built-in safeguards to ensure that their

use remains proportionate. There's no strong requirement for independent oversight before or after such powers are exercised. Nor is there always a clear mechanism for individuals to

challenge these actions effectively. And that absence… it matters. Because proportionality is not something that can be assumed—it needs to be demonstrated, monitored, and, if required, corrected. Without that, even well-intentioned powers can become excessive over

time.Another issue that quietly sits beneath all of this is the lack of detailed procedural

safeguards. The Act does not always specify how decisions regarding exemptions are to be made, what standards must be followed, or how transparency is to be ensured. This procedural gap can weaken accountability. It creates a situation where the exercise of power depends more on discretion than on clearly defined rules.[11]Put all of this together, and you

begin to see the larger picture. The DPDP Act does make an effort to align with constitutional principles, but the alignment isn't always complete. It meets the basic threshold of legality

but struggles with the deeper requirements of necessity and proportionality. And because of that, there remains a real possibility that the balance between privacy and State power could

tilt too far in one direction.[12]So, while the Act is definitely a step forward, it may not yet fully live up to the constitutional vision of privacy laid down in Puttaswamy. And that gap…

however small it may seem now, is something that needs careful attention going forward.

Normative Tension: Rights vs State Power

There is a struggle at the heart of any law that protects data. It is like a balance scale that

never quite finds its balance. On one side you have the individual and their rights. They want to be left alone and have control over their life. On the side you have the State with its need to keep people safe and maintain order. Both of these things are important and necessary. The problem starts when it becomes hard to tell where one ends and the other begins.

Privacy is a deal especially after the court case of Justice K.S. Puttaswamy v. Union of India.

It is no longer something that can be ignored. Privacy is closely tied to being treated with dignity and being able to make your choices. In a country that values freedom, like a

democracy privacy is essential. So if someone interferes with your privacy they need to have a good reason. At the same time the State cannot do its job without some information. It

needs to be able to act to keep people safe and protect the country.

The question is not whether the State should have some power. It should. The question is how much power is much. This is where things get tricky. When you start making exceptions for good reasons it can be hard to draw the line. Sometimes things do not go back to the way they were before. If the State has much power to make decisions it can start to overstep its bounds. What starts as a way to help the government do its job can become a way to spy on people.

[13]Take surveillance for example. It is supposed to help keep people safe. If there are no clear rules it can become too much. It can go from watching a people to watching everyone. When that happens, people start to feel like they are being watched all the time. This can make

people change their behaviour. They might not say what they think or do what they want

because they are afraid of being watched. There is also the issue of freedoms like the right to say what you think and associate with who you want. These freedoms are closely tied to

privacy. When privacy is not protected these freedoms start to disappear. It does not happen at once but it can happen slowly. If you compromise on privacy a little and a little there

eventually people will have less freedom. What makes this even more of a concern is that it can affect how well the government is held accountable. In a system where the State has a lot of control over data it is essential to be transparent. If decisions about data are made without being checked it can be hard to question them. This is a problem because in a democracy the ability to question the government is crucial. When you look at how different countries

handle this balance you can see some differences. The GDPR for instance acknowledges the tension between rights and State power. It sets boundaries. Makes sure that any actions taken by the State are proportionate. It also creates groups to oversee how power is used. The goal is to make sure that when the State interferes it does so in a way that is fair and follows the

rules.[14]The DPDP Act, 2023 on the hand seems to approach this balance differently. It

recognizes the importance of privacy. It also gives the State a lot of room to make decisions. The rules that are supposed to limit the States power are not always clear or strong. It is like the law is trying to do two things at once: protect privacy and make sure the State can do its job.[15]This is where the struggle becomes most apparent. When a system relies much on trust

it can overlook the need for rules to prevent abuse. Trust is important. In a country that values freedom it is not enough on its own.In the end this is not a legal issue. It is a question about how we view power and how much we're willing to give up in exchange, for safety. The

balance is delicate. Is never fully resolved. What matters is how carefully we maintain this balance and whether we have a system that can correct itself when things start to go far.

Recommendations

1. Narrowing Exemptions

At present, the scope of state exemptions under the Digital Personal Data Protection Act, 2023 feels… a little too wide, almost open-ended in parts. While grounds like national

security or public order are undeniably important, the way they are framed leaves significant room for interpretation. And that's where the risk lies. When legal language is broad, it tends to stretch—sometimes beyond what was originally intended. So, what really needs to happen is a move toward clarity. The law should define these grounds more precisely, maybe even

include illustrative situations or thresholds that justify their use. This would not only limit arbitrary application but also create a clearer boundary for the exercise of power. In a way, it's about shifting from "trust us" to "here's exactly when and why we act." That small shift can make a big difference in how rights are protected.

2. Judicial Oversight

One of the most effective ways to ensure that power does not go unchecked is to subject it to independent review. Right now, the framework does not strongly mandate judicial scrutiny for the exercise of state exemptions, and that absence can feel… concerning. Introducing a

system where government actions—especially those involving access to or restriction of personal data—are subject to prior or subsequent judicial review would add an important layer of accountability. It doesn't mean slowing down governance or creating unnecessary

hurdles; rather, it ensures that decisions are justified and defensible. Courts, after all, play a crucial role in maintaining constitutional balance, particularly in light of the standards laid down in Justice K.S. Puttaswamy v. Union of India. Embedding judicial oversight into the process would reinforce the idea that privacy is not just a statutory concern, but a

constitutional one.

3. Independent Data Protection Authority

The effectiveness of any data protection law depends heavily on the strength and

independence of its enforcement body. While the DPDP Act establishes a Data Protection

Board, questions remain about how independent it truly is from executive influence. And that matters… perhaps more than it seems at first. An authority that operates under significant

government control may find it difficult to act against the very entity that oversees it. What is needed, therefore, is a genuinely autonomous institution—one with financial, functional, and administrative independence. Its members should be appointed through a transparent and

balanced process, and its decisions should be free from external pressure. Only then can it act as a real watchdog, capable of holding both private entities and the State accountable.

4. Transparency Requirements

Transparency is one of those principles that sounds simple but carries immense weight. When the State exercises its power, especially in areas as sensitive as personal data, there needs to

be some level of openness about it. Currently, the DPDP Act does not fully ensure that

instances of exemptions or government access to data are disclosed in a meaningful way. And without that visibility, it becomes difficult for citizens to even know when their rights might

be affected. Introducing clear transparency requirements—such as periodic reports, disclosure of exemption orders (with necessary safeguards), or even anonymized data on government

requests—can help bridge this gap. It's not about compromising security, but about ensuring that power is not exercised in complete opacity. A little light, even if filtered, goes a long way in building trust.

5. Incorporation of Proportionality Test

Perhaps one of the most important reforms would be to explicitly incorporate the principle of proportionality into the text of the law itself. While this standard has already been established constitutionally through Justice K.S. Puttaswamy v. Union of India, it is not clearly codified within the DPDP Act. And that creates a gap between constitutional theory and statutory

practice. By embedding proportionality directly into the Act—requiring that any restriction on privacy must be necessary, appropriate, and the least restrictive option available—the law can align more closely with constitutional expectations. It also provides clearer guidance to authorities, helping them make decisions that are not just legally valid, but also fair and

balanced. In a sense, it brings structure to discretion, ensuring that power is exercised with restraint rather than assumption.

Conclusion

If you step back and look at the larger picture, the Digital Personal Data Protection Act, 2023 does feel like an important moment in India's legal journey… almost like a long-awaited arrival. For years, there was talk about the need for a comprehensive data protection law,

especially after the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy

v. Union of India. And now that the law is finally here, it does signal progress. It shows that privacy is no longer being treated as an abstract idea, but as something that needs structure, rules, and actual enforcement.But at the same time… there's a certain hesitation you can't

quite ignore. Because having a law is one thing, and having a law that truly protects people is something else entirely. The real challenge for the DPDP Act lies in how it manages that

delicate, ongoing tension between individual rights and state power. It's not an easy balance to strike. On one side, there's the need to protect personal data, to ensure dignity and

autonomy. On the other, there's governance—security concerns, administrative efficiency, public order. Both are valid, both matter… but they don't always sit comfortably together.

When you compare this with the GDPR, the contrast becomes clearer. The GDPR feels settled, almost confident in its approach. It places the individual at the center and builds

protections outward from there. There's a kind of firmness in how it treats power—it allows intervention, but only within clearly defined limits, and always with oversight. The DPDP Act, in contrast, feels more cautious, maybe even a little unsure. It takes steps toward

protecting privacy, but at the same time, it leaves space—quite a bit of space—for the State to step in when it deems necessary. And that space… is where the concern lies. Because without strong safeguards, without clearly defined limits, that space can expand. Executive discretion, if left unchecked, tends to grow over time. Not always intentionally, not always in bad faith, but simply because the structure allows it. And when that happens, the balance slowly shifts. Privacy, which is supposed to be a right, starts to feel conditional—something that exists until it becomes inconvenient. That's why the conversation cannot end with the enactment of the law. In many ways, this is just the beginning. The DPDP Act needs to evolve, to be tested,

interpreted, and, where necessary, refined. It needs stronger oversight, clearer boundaries, and a more explicit alignment with constitutional principles. Because a right, especially one as

personal as privacy, cannot rely solely on trust—it needs protection that is visible, enforceable, and consistent. In the end, what really matters is not how well the law reads, but how it works in

practice. Does it make people feel secure about their data? Does it give them confidence that their information won't be misused or accessed without justification? These are the questions that define success, not just compliance. So yes, the DPDP Act is a step forward. But it is not the final step. Bridging the gap between recognition and real

protection—that's where the real work lies. Because privacy, if it is to mean anything at all, has to be more than just a constitutional promise. It has to be something people can actually rely on… every day, without even thinking about it.

Bibliography

Primary Legal Sources

1. **General Data Protection Regulation (GDPR), Regulation (EU) 2016/679**, Official Journal of the European Union, L119/1, 4 May 2016.
2. **Digital Personal Data Protection Act, 2023**, Gazette of India, Ministry of Electronics & IT, Government of India, 2023.
3. **Justice K.S. Puttaswamy v. Union of India**, (2017) 10 SCC 1, Supreme Court of

India.

4. **Constitution of India, 1950**, Articles 21 and 19(1)(a).

Books and Monographs

5. Cate, Fred H., and Viktor Mayer-Schönberger. *Data Protection Principles in the Digital Age*. Oxford University Press, 2019.
6. Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford University

Press, 2014.

7. Solove, Daniel J., and Paul M. Schwartz. *Information Privacy Law*. 6th Edition,

Wolters Kluwer, 2020.

8. Reidenberg, Joel R. *Privacy in the Information Age*. Law Journal Press, 2000.

Journal Articles and Papers

9. Greenleaf, Graham. "Global Data Privacy Laws 2021: 149 Countries, with European Standards Leading." *Privacy Laws & Business International Report*, 2021, Issue 169,

pp. 10–13.

10. Singh, R., & Sharma, A. "Balancing Privacy and State Power: A Comparative Study of GDPR and DPDP Act, 2023." *Indian Journal of Law and Technology*, Vol. 18,

2023, pp. 45–67.

11. Kuner, Christopher. "The GDPR as a Template for Global Data Protection Regulation." *International Data Privacy Law*, 2017, Vol. 7(1), pp. 3–15.
12. Bhatia, P. "Privacy and Surveillance in India: Examining the DPDP Act, 2023."

Journal of Indian Constitutional Law, 2024, Vol. 12(2), pp. 75–92.

Reports and Working Papers

13. European Commission. *Data Protection in the EU: Guide to GDPR Implementation*,

2020.

14. Ministry of Electronics and Information Technology, Government of India. *Digital Personal Data Protection Act, 2023: Official Guide and Commentary*, 2023.
15. Privacy International. *Government Surveillance and Data Privacy in India: Challenges under the DPDP Act*, 2023.

Online Resources

16. Information Commissioner's Office (UK). "Guide to GDPR." Available at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general- data-protection-regulation-gdpr/

17. Data Security Council of India. "DPDP Act, 2023 – Key Features and Analysis." Available at: https://www.dsci.in/dpdp-act-2023-analysis
18. European Union Agency for Fundamental Rights (FRA). *Handbook on European*

Data Protection, 2018.

Case Commentaries and Analysis

19. Bhat, V. *Puttaswamy Judgment: The Right to Privacy in India – A Critical Commentary*, Legal Eagles Publications, 2018.

20. Kuner, Christopher, and Giovanni Comandé. "The EU GDPR: A Legal Analysis."

Computer Law Review International, 2019, Vol. 20(2), pp. 42–55.

ENDNOTES

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

2 Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 5.

3 Digital Personal Data Protection Act, 2023 (India).

4 GDPR, Art. 23.

5 GDPR, Art. 77–79.

6 DPDP Act, 2023, Sec. 17.

7 DPDP Act, 2023.

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

9 Digital Personal Data Protection Act, 2023.

10 DPDP Act, 2023, Sec. 17.

11 Justice K.S. Puttaswamy v. Union of India.

12 Digital Personal Data Protection Act, 2023.

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

14 Digital Personal Data Protection Act, 2023

15 GDPR, Arts. 5, 23