

INTERNATIONAL JOURNAL FOR
CONSTITUTION
& DEVELOPMENT OF LAW [IJCDL]

ISSN. 3049-3579 (ONLINE)

2026

VOLUME 2 ISSUE 1

This Article is brought to you for "free" and "open access" by the International Journal for Constitution and Development of Law. It has been accepted for inclusion in the Journal after due review.

To submit your Manuscript for Publication at International Journal for Constitution and Development of Law, kindly email your Manuscript at Ijcdl.official@gmail.com.

**CONSTITUTIONALISM IN THE DIGITAL AGE: PRIVACY,
ARTIFICIAL INTELLIGENCE, AND STATE SURVEILLANCE IN
COMPARATIVE PERSPECTIVE**

Shivam Shukla¹

ABSTRACT

Constitutions written for a world of paper files and physical borders are now being asked to govern facial recognition cameras, predictive risk scores, and bulk interception of communications. This article examines how constitutional courts in India, the United States, the United Kingdom, the European Union, and the Netherlands have adapted three classic guarantees, the right to privacy, freedom of expression, and due process, to the realities of computational government. Drawing principally on *Puttaswamy*, *Carpenter*, *Big Brother Watch*, *Bridges*, *Digital Rights Ireland*, *Schrems*, *SyRI*, and *Loomis*, it argues that a recognisable transnational doctrine is emerging: courts increasingly treat aggregation of data as a distinct constitutional harm, demand legislative rather than merely executive authorisation for surveillance, and insist that automated decision-making remain contestable by the person affected. The article concludes that the greatest doctrinal gap lies not in the recognition of rights but in remedies, and that data sovereignty claims, unless disciplined by proportionality, risk becoming a vehicle for surveillance rather than a shield against it.

Keywords: digital constitutionalism; privacy; surveillance; algorithmic decision-making; proportionality; data sovereignty; due process

INTRODUCTION

There is a familiar complaint that constitutional law always arrives late to a technological revolution. The complaint has some force. When the framers of the Indian Constitution debated Article 21 in 1948 and 1949, the state's capacity to watch its citizens was bounded by the number of policemen it could pay and the number of letters it could steam open. When the Fourth Amendment was drafted, the paradigm case of a search was a constable rummaging through a colonist's desk. Neither text says anything about metadata, machine learning, or a

¹ The author is a practicing advocate in Delhi.

camera that recognises a face in a crowd. Yet in the space of a single decade, constitutional courts on four continents have produced a body of case law that is far more coherent than the complaint would suggest. The purpose of this article is to map that case law, to identify the doctrinal moves that recur across jurisdictions, and to assess where the law remains unsettled.

The inquiry is organised around three constitutional guarantees that technology has placed under the greatest strain. The first is privacy, which has had to be reconceived as something that can be violated by the accumulation of individually innocuous data points. The second is due process, or the guarantee of fair and reasoned decision-making, which is threatened when the reasons for a decision are locked inside a proprietary or opaque model. The third is freedom of expression, which is chilled not by censorship in the traditional sense but by the knowledge that one is being watched. Cutting across all three is the question of what constitutional limits, if any, can be placed on the state's growing insistence that data generated within its borders be stored and governed there.

The method is comparative and doctrinal. The article does not survey every jurisdiction but selects decisions that have travelled, in the sense that they are cited by courts outside the system that produced them, and it is weighted towards apex courts because that is where the reconceptualisation of rights takes place.

PRIVACY RECONCEIVED: FROM TRESPASS TO AGGREGATION

A. The Indian Turning Point

For six decades the Supreme Court of India oscillated on whether privacy was a fundamental right at all. *M.P. Sharma* and *Kharak Singh* had both, in different ways, declined to locate such a right in Part III of the Constitution,² and although a line of later cases had quietly assumed its existence, the foundations remained contested. The nine-judge bench in *Justice K.S. Puttaswamy v. Union of India* settled the matter with a unanimity that was itself remarkable.³ Privacy, the Court held, is intrinsic to life and personal liberty under Article 21 and is woven through the other freedoms in Part III. What makes *Puttaswamy* significant for present purposes is not the recognition of the right but the structure of the test the Court adopted. Any infringement must satisfy a threefold requirement: there must be a law, the law must pursue a

² *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300; *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.

³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

legitimate state aim, and the means adopted must be proportionate to the object sought to be achieved.⁴ The plurality opinion also went out of its way to reject the argument that a person who shares information with a service provider thereby forfeits any constitutional interest in it, a point that would have been unremarkable in Europe but that placed India in tension with the American third-party doctrine at precisely the moment that doctrine was being reconsidered in Washington.

The test was applied within a year in the challenge to the Aadhaar biometric identity programme.⁵ The majority upheld the core of the scheme but struck down the provisions permitting private companies to demand Aadhaar authentication and the requirement of linking the number to bank accounts and mobile connections. Justice Chandrachud's dissent went further and would have invalidated the entire statute, in part because it had been passed as a money bill and in part because he regarded the architecture of a centralised biometric database as inherently capable of profiling.⁶ The dissent is worth noting because its emphasis on architecture rather than individual acts of access anticipates the aggregation reasoning that courts elsewhere would adopt.

B. The American Retreat from the Third-Party Doctrine

The Supreme Court of the United States reached a comparable point by a different route. For decades the third-party doctrine, derived from *Smith v. Maryland* and *United States v. Miller*, held that a person has no reasonable expectation of privacy in information voluntarily conveyed to another.⁷ Applied literally to the digital economy, the doctrine would have meant that almost nothing a citizen does online attracts Fourth Amendment protection, since almost everything is routed through a third party. The Court began to signal discomfort in *United States v. Jones*, where five Justices in two concurrences suggested that long-term GPS tracking implicated a reasonable expectation of privacy regardless of whether a physical trespass had occurred.⁸ Two years later, in *Riley v. California*, a unanimous Court held that police may not search a cell

⁴ *Id.* at 509–10 (Chandrachud, J., plurality opinion).

⁵ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar).

⁶ *Id.* ¶¶ 1153–1176 (Chandrachud, J., dissenting).

⁷ *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

⁸ *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment).

phone seized incident to arrest without a warrant, observing that the phone was less a container than a window into the whole of a person's life.⁹

The decisive step came in *Carpenter v. United States*.¹⁰ The government had obtained, without a warrant, 127 days of historical cell-site location information from the petitioner's wireless carriers. Chief Justice Roberts, writing for a five-Justice majority, declined to extend *Smith* and *Miller* to this "qualitatively different category" of records. The reasoning turned on two features: the comprehensiveness of the data, which provided "an all-encompassing record of the holder's whereabouts," and the involuntary nature of its generation, since carrying a phone is now practically compulsory for participation in modern life.¹¹ The majority insisted the decision was narrow, but its logic, that aggregated data can reveal what no single data point could, is not easily confined, and lower courts have since divided on its application to tower dumps, licence-plate readers, and pole cameras.

C. Europe: Bulk Interception and the Retention of Data

European courts were the first to articulate aggregation as a distinct harm, and they did so in the context of data retention. In *Digital Rights Ireland*, the Court of Justice of the European Union invalidated the Data Retention Directive in its entirety, holding that an obligation to retain the traffic and location data of the entire population for up to two years, without any link to a threat to public security, exceeded what was strictly necessary.¹² The Court observed that such data, taken as a whole, "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."¹³ The point was reinforced in *Tele2 Sverige*, which held that national laws imposing general and indiscriminate retention were likewise incompatible with the Charter,¹⁴ and in *La Quadrature du Net*, which permitted targeted or time-limited retention in response to a serious threat but maintained the prohibition on general retention as a default.¹⁵

⁹ *Riley v. California*, 573 U.S. 373, 393–97 (2014).

¹⁰ *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

¹¹ *Id.* at 2217–20.

¹² Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications*, ECLI:EU:C:2014:238, ¶¶ 56–69.

¹³ *Id.* ¶ 27.

¹⁴ Joined Cases C-203/15 & C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen*, ECLI:EU:C:2016:970.

¹⁵ Joined Cases C-511/18, C-512/18 & C-520/18, *La Quadrature du Net v. Premier ministre*, ECLI:EU:C:2020:791, ¶¶ 134–39, 168.

The European Court of Human Rights has been more accommodating of bulk interception but has surrounded it with procedural conditions. In *Big Brother Watch v. United Kingdom*, the Grand Chamber accepted that bulk interception is not per se incompatible with Article 8 of the Convention, given the nature of contemporary threats, but held that the United Kingdom's regime violated the Convention because it lacked independent authorisation at the outset, did not require the categories of selectors to be specified in the warrant, and did not subject selectors linked to identifiable individuals to prior internal authorisation.¹⁶ The Court described these as "end-to-end safeguards" and made clear that the assessment of proportionality had to be made at each stage of the process, from authorisation to retention and use. The companion judgment in *Centrum för rättvisa v. Sweden* applied the same framework and found a violation on narrower grounds.¹⁷

D. Convergence

Three jurisdictions, three textual starting points, and yet a common destination. Each court has moved away from a model in which privacy is infringed only by a discrete intrusion into a protected space, and towards a model in which the constitutional harm lies in the state's capacity to assemble a profile. Each has also concluded that the source of authorisation matters. *Puttaswamy* demands a law. *Carpenter* demands a warrant. *Big Brother Watch* demands independent authorisation and specified selectors. The proposition that the executive may not license itself to watch the population is now, if not universal, at least widely shared.

FACIAL RECOGNITION AND PREDICTIVE POLICING: THE NEWER BATTLEGROUND

The retention cases concerned data the state passively collected. The newer disputes concern data the state actively generates through automated systems deployed in public space. The leading common-law decision is *R (Bridges) v. Chief Constable of South Wales Police*, in which the Court of Appeal of England and Wales held that the police's use of live automated facial recognition was unlawful.¹⁸ The Divisional Court had found the deployment lawful, and the Court of Appeal did not dispute that facial recognition could in principle be justified. What it found fatal was the breadth of the discretion left to individual officers to decide who would

¹⁶ *Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15, ¶¶ 350–61, 424–27 (Eur. Ct. H.R. May 25, 2021) (Grand Chamber).

¹⁷ *Centrum för rättvisa v. Sweden*, App. No. 35252/08 (Eur. Ct. H.R. May 25, 2021) (Grand Chamber).

¹⁸ *R (Bridges) v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

be placed on a watchlist and where the cameras would be deployed. The legal framework, the court held, left "too much discretion" to be compatible with the requirement that an interference be "in accordance with the law."¹⁹ The court also held that the force had failed to discharge its public sector equality duty because it had not taken reasonable steps to determine whether the software produced biased results by race or sex.²⁰ That second holding is significant because it converts an anti-discrimination obligation into a due diligence requirement that attaches before deployment, not merely a remedy that becomes available after harm.

The Dutch decision in the *SyRI* litigation addressed a different technology with a similar result.²¹ The System Risk Indication was a legislative scheme allowing government agencies to pool data and apply a risk model to detect welfare fraud, deployed disproportionately in low-income neighbourhoods. The Hague District Court held that the legislation violated Article 8 of the Convention because the risk model was not transparent, the affected individuals could not know that they had been flagged, and the scheme failed the requirement of a fair balance between the objective and the interference. The court was careful not to hold that risk profiling was impermissible as such; its objection was to the absence of any mechanism by which the profiled could understand or contest the model.²²

Indian courts have not yet produced an equivalent ruling, though the deployment of facial recognition by police forces in Delhi, Hyderabad, and elsewhere has proceeded largely without statutory backing. On the reasoning of *Puttaswamy*, an interference with privacy that rests on executive procurement decisions rather than on a law would appear to fail at the first stage of the test, and the Aadhaar judgment's insistence on legislative authorisation reinforces the point.²³ The gap between doctrine and practice is, however, considerable, and it is a recurring theme of this field that the announcement of a constitutional standard does little unless someone with standing is prepared to litigate it.

¹⁹ *Id.* ¶¶ 90–94.

²⁰ *Id.* ¶¶ 176–201.

²¹ *NJCM v. De Staat der Nederlanden* (SyRI), Rb. Den Haag 5 Feb. 2020, ECLI:NL:RBDHA:2020:865 (Neth.).

²² *Id.* ¶¶ 6.49–6.59, 6.86–6.95.

²³ *Puttaswamy* (Aadhaar), (2019) 1 SCC 1, ¶¶ 285–300.

ALGORITHMIC DECISION-MAKING AND THE CONTENT OF DUE PROCESS

A. The Problem Stated

Due process, in whichever textual form a constitution expresses it, has always assumed that a decision-maker exists who can be asked for reasons. Machine learning systems disrupt that assumption in two ways. First, the model may be proprietary, so that the reasons exist but cannot be inspected. Second, the model may be genuinely opaque, in that its outputs are the product of statistical correlations that no human being, including its designer, can articulate as a chain of reasoning. Constitutional courts have so far encountered the first problem more often than the second.

B. *Loomis* and the Limits of the Warning Label

The best-known decision is *State v. Loomis*, in which the Wisconsin Supreme Court upheld the use of the COMPAS recidivism risk score at sentencing.²⁴ The defendant argued that because the algorithm was a trade secret he could not challenge its accuracy, and that its use of gender as a variable violated due process. The court rejected both arguments, reasoning that the score was one factor among many, that the defendant had access to the inputs even if not to the weights, and that a sentencing court retained discretion. It did, however, require that any pre-sentence report containing a COMPAS score be accompanied by written cautions about the tool's limitations, including that it had not been validated for the Wisconsin population and that studies had raised concerns about racial disparities.²⁵ The decision has been widely criticised, and the criticism is largely justified. A warning label is a poor substitute for the ability to test the instrument, and the assumption that a judge presented with a numerical score will discount it appropriately is contradicted by a substantial literature on automation bias. Nevertheless *Loomis* is instructive because it shows a court trying to preserve the form of individualised judgment while conceding the substance to a machine.

C. Europe's Structural Answer

The European approach has been to legislate a right rather than to adjudicate one case at a time. Article 22 of the General Data Protection Regulation confers a right not to be subject to a

²⁴ *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017).

²⁵ *Id.* at 769–70.

decision based solely on automated processing that produces legal or similarly significant effects, subject to exceptions, and where an exception applies requires suitable safeguards including the right to obtain human intervention and to contest the decision.²⁶ The Court of Justice gave the provision teeth in *SCHUFA*, holding that a credit-scoring agency's generation of a probability value constituted an automated decision within Article 22 where a third party drew strongly on that value in deciding whether to contract with the person.²⁷ The significance of *SCHUFA* lies in its refusal to allow the formal location of the decision to defeat the right: if the score is decisive in practice, the scoring is the decision.

The Artificial Intelligence Act builds on this by classifying systems used in law enforcement, migration, the administration of justice, and access to essential public services as high-risk and subjecting them to conformity assessment, human oversight, and logging requirements before they may be placed on the market.²⁸ The Act also prohibits certain uses outright, including real-time remote biometric identification in public spaces for law enforcement, subject to narrowly drawn exceptions.²⁹ Whether these prohibitions will be enforced against member state security agencies with the rigour their text suggests is an open question, given the national security carve-out in Article 2(3).

D. Judicial Decision-Making Itself

The use of algorithms within courts raises a distinct constitutional concern, because the judiciary is the institution whose reasoning is supposed to be public. The Constitutional Court of Colombia has gone further than most in reflecting on the question, holding in a 2024 decision that a trial judge's use of a large language model to draft parts of a judgment was not in itself unconstitutional but had to be disclosed, verified, and confined so that the judge remained the author of the reasoning.³⁰ The principle that emerges, and it is one that ought to be uncontroversial, is that whatever assistance a court accepts, the duty to give reasons that a litigant can understand and appeal is non-delegable.

²⁶ Regulation (EU) 2016/679, art. 22, 2016 O.J. (L 119) 1.

²⁷ Case C-634/21, *OQ v. Land Hessen* (*SCHUFA Holding AG*), ECLI:EU:C:2023:957, ¶¶ 43–50, 73.

²⁸ Regulation (EU) 2024/1689, arts. 6, 14, 26 & annex III, 2024 O.J. (L 1689) 1.

²⁹ *Id.* art. 5(1)(h).

³⁰ Corte Constitucional [C.C.] [Constitutional Court], agosto 2, 2024, Sentencia T-323/24 (Colom.).

SURVEILLANCE AND THE CHILLING OF EXPRESSION

The relationship between surveillance and free speech has received less judicial attention than the relationship between surveillance and privacy, but it is arguably the more important of the two for constitutional democracy. The point was put well by Justice Sotomayor in *Jones*: awareness that the government may be watching "chills associational and expressive freedoms."³¹ The difficulty for litigants has been standing. In *Clapper v. Amnesty International*, the Supreme Court held that lawyers and journalists who reasonably feared that their communications with foreign contacts were being intercepted under section 702 of the Foreign Intelligence Surveillance Act lacked standing because their injury was speculative.³² The decision has the practical effect of insulating a secret programme from constitutional review unless and until the government chooses to disclose that a particular person was targeted. European courts have been more willing to recognise that the mere existence of a regime of secret surveillance may itself interfere with Convention rights, a position the Strasbourg court has held since *Klass v. Germany* and reaffirmed in *Roman Zakharov v. Russia*.³³

The Indian Supreme Court's response to the Pegasus spyware allegations occupies a middle ground. In *Manohar Lal Sharma v. Union of India*, the Court declined to accept the government's refusal to confirm or deny use of the spyware on national security grounds, observing that the state cannot obtain a "free pass" merely by invoking that phrase, and appointed a technical committee under a retired judge to investigate.³⁴ The Court explicitly framed the concern in terms of the chilling effect on the press and on the freedom of expression under Article 19(1)(a). The committee's eventual report was inconclusive, and the episode illustrates both the willingness of courts to assert jurisdiction over surveillance and the limits of what they can find out.

DATA SOVEREIGNTY: SHIELD OR SWORD?

Data sovereignty, the claim that data about a state's residents should be stored, processed, and governed within its territory, has become a central plank of technology policy in India, China, Russia, and increasingly in Europe. Its constitutional character is ambiguous. On one view it is

³¹ *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

³² *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409–14 (2013).

³³ *Klass v. Germany*, 28 Eur. Ct. H.R. (ser. A) ¶¶ 34–38 (1978); *Roman Zakharov v. Russia*, App. No. 47143/06, ¶¶ 171–79 (Eur. Ct. H.R. Dec. 4, 2015) (Grand Chamber).

³⁴ *Manohar Lal Sharma v. Union of India*, (2023) 5 SCC 1, ¶¶ 42–49, 61.

a means of vindicating rights: data held domestically is subject to domestic constitutional constraints and domestic courts. On another it is a means of extending surveillance: data held domestically is accessible to domestic agencies without the friction of mutual legal assistance.

The European Court of Justice's decisions in *Schrems I* and *Schrems II* are usually read as data protection cases, but they are better understood as decisions about the extraterritorial reach of constitutional guarantees.³⁵ In each, the Court invalidated an adequacy arrangement permitting transfers to the United States because American surveillance law did not confine access to what was strictly necessary and did not provide the data subject with an effective remedy before an independent body. The Court's insistence that the level of protection must be "essentially equivalent" to that guaranteed within the Union is a demand that the Charter follow the data. This is sovereignty in the service of rights.

India's Digital Personal Data Protection Act 2023 takes a different path. It permits cross-border transfers except to countries notified by the central government, and it exempts state instrumentalities from many of its obligations on grounds including sovereignty, security, and public order.³⁶ Whether the exemptions survive the *Puttaswamy* proportionality test is a question that has not yet been litigated, but the breadth of the exemption for the state is difficult to reconcile with the principle that any interference must be necessary and proportionate. The contrast with the European model is instructive. A localisation mandate that keeps data within reach of a domestic executive that is itself exempt from the governing statute does not enhance constitutional protection; it removes the last practical obstacle to its erosion.

ASSESSMENT AND CONCLUSION

Three conclusions may be drawn from this survey. The first is that the recognition of rights has proceeded faster than the development of remedies. Courts in every jurisdiction examined have accepted that aggregated data engages privacy, that automated decisions engage due process, and that secret surveillance engages expression. What they have been less able to do is give the affected person something useful. *Loomis* offers a warning label. *Clapper* offers nothing. *Big Brother Watch* offers a procedure, but one that operates inside the intelligence services and is invisible to the person watched. The Dutch *SyRI* court came closest to a substantive remedy by

³⁵ Case C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650; Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.*, ECLI:EU:C:2020:559.

³⁶ Digital Personal Data Protection Act, No. 22 of 2023, §§ 16, 17(2)(a), India Code (2023).

requiring that the profiled be able to know and contest, and it is that model, of contestability as the irreducible minimum of due process, that deserves to travel.

The second is that legislative authorisation has become the hinge of the analysis. This is a healthy development, because it returns the question of how much surveillance a society will tolerate to the institution that is accountable for answering it. It also carries a risk, illustrated by the Indian data protection statute, that a legislature will authorise everything and exempt the state from the rest. Proportionality review is the only safeguard against that outcome, and it is a safeguard that depends on the willingness of courts to apply the test with rigour to statutes as well as to executive action.

The third is that the constitutional significance of artificial intelligence lies less in the novelty of the technology than in its effect on the distribution of knowledge between the citizen and the state. A constitution assumes that the governed can understand what is being done to them and by whom. A state that knows its citizens comprehensively while its own reasoning remains inscrutable has inverted that assumption. The doctrinal resources to correct the inversion already exist: the requirement of law, the requirement of proportionality, the requirement of reasons, and the requirement of a remedy. The task of the next decade is not to invent new rights but to make the old ones operational against a new kind of power.