

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Informational Privacy in South Asia: A Comparative Analysis of Justice K.S. Puttaswamy v. Union of India (2017) and Nepal's Landmark Supreme Court Decision No. 081-WO-0500

SUBRAT DHAKAL*

ABSTRACT

This article undertakes a comparative analysis of two judgments that, a decade apart and at very different institutional scales, established informational privacy as a judicially enforceable constraint on state data practices in South Asia. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge bench of the Supreme Court of India overruled M.P. Sharma and Kharak Singh to read a fundamental right to privacy into Article 21 of the Constitution, and articulated a three-fold test of legality, legitimate aim and proportionality for assessing state intrusions upon it. In Supreme Court of Nepal Decision No. 081-WO-0500, decided on a writ petition filed by a law student, Bivek Chaudhary, a Division Bench applied Nepal's express constitutional privacy guarantee under Article 28, read with the Individual Privacy Act, 2075, to hold that transport offices lacked statutory authority to publish examinees' citizenship numbers alongside driving-licence results, invoking the ultra vires doctrine governing public bodies and drawing directly on Puttaswamy itself. The article argues that despite sharp differences in constitutional text, institutional scale and remedial posture, a nationwide biometric-identity challenge decided by the country's largest possible bench as against a single administrative practice corrected by a two-judge bench, both courts converge on a common refusal to treat administrative convenience as a substitute for legal authorisation to disclose personal data. It concludes that this convergence, together with Nepal's explicit reliance on Indian precedent, offers a template of doctrinal economy and horizontal judicial dialogue for other South Asian jurisdictions confronting the privacy costs of state digitisation.

Keywords: *informational privacy, South Asian constitutional law, Article 21, Article 28, Aadhaar, ultra vires, comparative constitutional law, data protection, driving-licence results, citizenship number*

* Author is an Advocate and a Fellow Member of the Institute of Chartered Accountants of Nepal (ICAN).

I. INTRODUCTION

South Asia's constitutional courts spent the better part of the last decade catching up to a problem their drafters never anticipated: that the state's own record-keeping apparatus (biometric databases, examination boards, transport registries) could become the single greatest threat to a citizen's private life. The region's post-colonial constitutions were largely written against the memory of the colonial police state, and their privacy guarantees, where they exist at all, were built to answer searches, seizures and surveillance of a distinctly analogue kind. What neither the framers of India's 1950 Constitution nor Nepal's 2015 Constitution fully reckoned with was the administrative afterlife of personal data: the possibility that a government agency, acting entirely within its ordinary competence and with no malicious intent whatsoever, could strip a citizen of privacy simply by publishing a list.

Two judgments, a decade and a jurisdiction apart, forced this reckoning. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,¹ a nine-judge bench of the Supreme Court of India confronted the constitutionality of the Aadhaar biometric identification scheme and, in doing so, resolved a question the Court had left open for nearly seven decades, namely whether the Constitution protects a right to privacy at all. In Nepal, the Supreme Court's Decision No. 081-WO-0500,² delivered by a Division Bench on 18 Magh 2082 (1 February 2026), tackled a narrower but structurally identical problem: whether state transport offices could lawfully publish the citizenship numbers of driving-licence examinees alongside their examination results. The petition was filed by Bivek Chaudhary, a law student at Nepal Law Campus. What might, on its face, read as a modest administrative-law dispute about a licensing bureau's publication practices became, in the Court's hands, an occasion to articulate the constitutional and statutory architecture of informational privacy in Nepal and to apply the doctrine that public bodies possess only the powers a statute expressly confers on them.

II. THE INDIAN PARADIGM: *JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA* (2017)

A. The Aadhaar Litigation and Its Antecedents

The petition that eventually produced the 2017 judgment began life as a narrow challenge. Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, filed a writ petition contesting the Aadhaar scheme, a programme under which the Unique Identification Authority

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

² *Bivek Chaudhary v. Government of Nepal, Ministry of Physical Infrastructure and Transport*, Sup. Ct. Nepal, Writ No. 081-WO-0500 (decided 18 Magh 2082 B.S. / 1 Feb. 2026) (Nepal).

of India collected the biometric and demographic data of Indian residents and issued each a twelve-digit identification number, subsequently made a near-prerequisite for accessing welfare subsidies, opening bank accounts and filing tax returns. Successive petitions were tagged to Puttaswamy's, and by 2015 the matter had grown into a full-scale constitutional challenge to the state's authority to compel biometric enrolment at all.

The threshold obstacle was doctrinal rather than factual. Two earlier decisions stood in the challengers' way. In *M.P. Sharma v. Satish Chandra*,³ an eight-judge bench had held, in the course of considering search-and-seizure powers, that the Indian Constitution contains no right analogous to the American Fourth Amendment, and that privacy could not therefore be read into it. In *Kharak Singh v. State of U.P.*,⁴ a six-judge bench addressing police surveillance regulations had similarly concluded, notwithstanding its invalidation of nocturnal domiciliary visits on other grounds, that privacy was not a right the Constitution guaranteed. Because both decisions issued from benches larger than any that had subsequently entertained privacy claims, a three-judge bench hearing the Aadhaar matter in 2015 referred the constitutional question to a bench of appropriate strength, ultimately convened as a bench of nine.

B. Overruling *M.P. Sharma* and *Kharak Singh*

The lead opinion, authored by Dr. D.Y. Chandrachud, J. (writing for himself, then Chief Justice Khehar, and Agrawal and Nazeer, JJ.), dismantled both precedents on textual and structural grounds rather than by simple disagreement. *M.P. Sharma*, the Court reasoned, had answered a narrower question than the one later attributed to it, namely whether Article 20(3)'s protection against self-incrimination imported a Fourth Amendment-style warrant requirement, and had never actually adjudicated whether privacy might be located elsewhere in Part III, including Article 21's guarantee of life and personal liberty. Its broader pronouncement that privacy enjoyed no constitutional protection was, in Chandrachud, J.'s framing, dictum unmoored from the question actually before that bench. *Kharak Singh* fared little better: the Court found its invalidation of nightly domiciliary visits to be an implicit recognition of privacy interests even as its express holding denied that any such right existed, an internal contradiction compounded by the fact that *Kharak Singh*'s reasoning rested on the since-overruled *A.K. Gopalan*⁵ approach to fundamental rights, an approach *Rustom Cavasjee Cooper*⁶ and *Maneka Gandhi*⁷ had long

³ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

⁴ *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).

⁵ *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27 (India).

⁶ *Rustom Cavasjee Cooper v. Union of India*, (1970) 1 SCC 248 (India).

⁷ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

since displaced in favour of reading Part III rights as an interlocking, mutually reinforcing scheme rather than isolated silos.

Six separate opinions issued, from Chandrachud, Nariman, Chelameswar, Bobde, Sapre and Kaul, JJ., each reaching the same destination by a distinct doctrinal route. Nariman, J. traced privacy through the "sub-species" of liberty and dignity protected by Article 21 read with Articles 14 and 19. Chelameswar, J. grounded a version of privacy directly in Article 21's guarantee against deprivation of life or personal liberty "except according to procedure established by law," while resisting any suggestion that privacy was an unenumerated right requiring separate discovery. Kaul, J.'s opinion is perhaps the most instructive for present purposes: it devoted sustained attention to comparative and international materials, the EU's General Data Protection Regulation, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the report of the Justice A.P. Shah Committee on a national privacy framework, treating informational privacy as a distinct, and distinctly urgent, facet of the broader right.

C. The Three-Fold Test: Legality, Legitimate Aim, Proportionality

The Court's summary of conclusions, appended to Chandrachud, J.'s opinion and adopted in the Order of the Court, did more than declare privacy fundamental; it supplied the doctrinal machinery for adjudicating future claims. Privacy, the Court held, is "not an absolute right," and any law encroaching on it must satisfy a three-part standard: first, legality, meaning that the encroachment must be traceable to an existing law rather than executive fiat; second, need, meaning that the law must serve a legitimate state aim (national security, crime prevention, the efficient delivery of welfare benefits and similar objectives were offered as illustrations, not as an exhaustive list); and third, proportionality, meaning that a rational nexus must exist between the objective pursued and the means the law adopts to pursue it. The Court coupled this with a further, less remarked-upon proposition: that privacy carries both negative content, restraining state intrusion, and positive content, obliging the state actively to safeguard the privacy interests of its citizens, a formulation with obvious relevance to a state agency's affirmative choice to publish, rather than withhold, sensitive identifiers.

Informational privacy was expressly carved out as "a facet of the right to privacy," with the Court noting that dangers to it "can originate not only from the state but from non-state actors as well," and directing the Union Government towards the data-protection legislative process then underway under Justice B.N. Srikrishna's committee. The Aadhaar Act itself was left for a separate constitution bench to test against this newly minted standard, a task completed the

following year in *Puttaswamy (Aadhaar-5J.)*,⁸ which upheld the scheme's core architecture while striking down its extension into private commercial transactions.

III. THE NEPALI FRONTIER: SUPREME COURT DECISION NO. 081-WO-0500

A. Case Background

Bivek Chaudhary, a resident of Mahalaxmi Municipality, Lalitpur, at that time studying law in the fifth semester of the B.A. LL.B. programme at Nepal Law Campus, filed writ petition 081-WO-0500 against Nepal's Ministry of Physical Infrastructure and Transport, the Department of Transport Management, the Bagmati Province Ministry of Labour, Employment and Transport, and four district transport management offices (Ekantakuna, Thulo Bharyang, Chabahil and Radhe Radhe, Bhaktapur). His grievance was precise: the transport offices, in publishing the results of the written and practical examinations for driving licences, were listing not only each candidate's roll number and name but also their citizenship certificate number (*nagarikta* number), a unique national identifier, on office noticeboards and, in several instances, on the offices' official Facebook pages.

Chaudhary's petition invoked Articles 16, 28, 46 and 133(2) and (3) of the Constitution of Nepal, and rested on a specific statutory hook: Section 19 of the Individual Privacy Act, 2075 (2018), which grants every person a right to confidentiality over personal information held in electronic form, and Section 2(ga)(4), which expressly enumerates a citizenship certificate, passport, national identity card, driving licence and voter identification card as categories of "personal information" (*byaktigat suchana*). He argued, further, that the governing procedural directive, the Driving Licence Examination Operating Procedure Directive, 2077 (2020), required only that passing candidates' roll numbers and names be published, not their citizenship numbers, and that the respondent offices, as statutory bodies, possessed no independent authority to publish information the governing directive did not require.

An application for interim relief was declined on 26 Kartik 2081, the Court reasoning that the substantive question would be resolved on final hearing, though the petition was granted priority listing under Rule 73 of the Supreme Court Rules, 2074. The respondent offices' written replies were largely uniform: no law affirmatively prohibited publishing citizenship numbers, the practice assisted in distinguishing candidates who shared identical names, and the format tracked the architecture of the Department's Nepal Electronic Driving Licence and Vehicle Registration System (NEDLVRS), which the individual offices had no discretion to alter. The Ministry of Physical Infrastructure and Transport, for its part, disclaimed any operational role

⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.)*, (2019) 1 SCC 1 (India).

in the matter, arguing that examination administration and result publication fell entirely to the provincial transport offices and that it had been joined as a respondent without cause.

B. The Court's Reasoning: Privacy Under Article 28 and the *Ultra Vires* Doctrine

The Division Bench of the Supreme Court of Nepal, comprising Justice Dr. Manoj Kumar Sharma and Justice Meghraj Pokharel, structured its analysis around a single question: did publishing citizenship numbers alongside examination results infringe the constitutional right to privacy? Its answer proceeded on two mutually reinforcing tracks.

The first was textual and statutory. The Court walked through the governing transport statutes, the Vehicle and Transport Management Act, 2049 (1993), and its 2054 (1997) regulations, the Bagmati Province Vehicle and Transport Management Act, 2075, and the 2077 Directive, and found that each spoke only to a requirement that applicants submit a copy of their citizenship certificate with their application; none authorised, still less required, that a citizenship number be disclosed upon publication of results. From this textual absence the Court drew a doctrinal conclusion rooted in the *ultra vires* principle governing statutory bodies: under Section 42(6) (cha) of the National Civil Code, 2074, a legal person (*kanuni byakti*) may act only within the bounds a statute expressly confers. The Bench reinforced this with comparative authority, invoking the House of Lords' holding in *Hazell v. Hammersmith and Fulham London Borough Council*⁹ that a public body's powers are confined to what a statute or its constitutive instrument expressly permits, and that what is not authorised is, correspondingly, prohibited. Since no governing instrument authorised disclosure of citizenship numbers, the respondent offices had, in the Court's assessment, acted outside their lawful authority in doing so.

The second track was substantive and constitutional. Article 28 of the Constitution of Nepal, 2072 (2015), Nepal's privacy clause, provides that the privacy of any person's body, residence, property, documents, data, correspondence and character shall be inviolable "except as provided by law." The Court read this alongside Section 2(ga) of the Individual Privacy Act, which folds citizenship certificates into its definition of personal information, and Section 11(1) and (2)(ga) of the same Act, which recognises an individual right to confidentiality over one's own personal documents and specifically designates the citizenship document as such. It further drew on Section 28(1) of the Right to Information Act, 2064 (2007), obliging public bodies to protect personal information from unauthorised disclosure, and Section 298(1) of the National Penal Code, 2074, which criminalises breach of the confidentiality of electronically held or transmitted information. The Bench characterised the citizenship certificate as the "primary

⁹ *Hazell v. Hammersmith and Fulham London Borough Council*, [1992] 2 AC 1 (HL) (UK).

document of personal identity," noting that it is a constitutionally guaranteed entitlement under Article 10, that it embeds sensitive biographical data such as name, date of birth, address and parentage, and that its number, once exposed, meaningfully lowers the cost of identity-linked fraud for anyone inclined to exploit it.

What is striking, for a comparative reader, is how far afield the Bench travelled for reinforcement of a fairly narrow administrative-law point. It invoked Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, together with the U.N. Human Rights Committee's General Comment No. 16 on Article 17's obligations regarding electronically held personal data. It surveyed the EU's Charter of Fundamental Rights (Article 8), the Treaty on the Functioning of the European Union (Article 16), the General Data Protection Regulation, and its national transpositions in the United Kingdom, Italy and Spain, alongside the OECD's Use Limitation Principle. And, most tellingly, it engaged directly with *Puttaswamy*, citing the Indian Supreme Court's holding that privacy "is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21," together with India's Digital Personal Data Protection Act, 2023, and two of Nepal's own precedents: *Adv. Baburam Aryal v. Government of Nepal*,¹⁰ on the obligation of data-holding institutions to safeguard collected information absent express statutory authorisation for disclosure, and *Adv. Bhaktiram Ghimire v. Government of Nepal*,¹¹ concerning the outsourcing of smart-card driving-licence production, in which the Court had earlier articulated that citizens' personal particulars "must remain wholly confidential."

C. Disposition

The Bench concluded that the respondent offices' practice of publishing citizenship numbers on noticeboards and, more pointedly, on their official Facebook pages infringed the examinees' right to informational privacy, notwithstanding that privacy is not, in the Court's own words, an "absolute right." A writ of mandamus issued directing the respondent transport offices henceforth to publish driving-licence examination results without citizenship numbers. The Court declined, however, to issue a writ of certiorari quashing any specific prior administrative decision, on the ground that Chaudhary's petition had not identified which particular decision it sought to have annulled, a narrow but telling reminder that Nepali writ practice, like its Indian counterpart, still polices the line between a generalised grievance and a decision capable of judicial annulment.

¹⁰ *Adv. Baburam Aryal v. Government of Nepal*, NKP 2074, vol. 1, Decision No. 9740 (Nepal).

¹¹ *Adv. Bhaktiram Ghimire v. Government of Nepal*, NKP 2079, vol. 12, Decision No. 11003 (Nepal).

D. Legal Principles Established in Decision No. 081-WO-0500

The Supreme Court's decision in Case No. 081-WO-0500 significantly strengthened the constitutional protection of informational privacy by recognising that a person's citizenship number constitutes sensitive personal information and that public authorities cannot disclose such information without express legal authorisation. The Court reaffirmed fundamental principles of administrative law, emphasising that statutory authorities may exercise only those powers expressly conferred upon them by law and that any action beyond those powers is unlawful. The judgment has consequently become a leading precedent on informational privacy and the limits of administrative discretion in Nepal.

The principles established by the decision include the following.

- Protection of personal information, although not an absolute right, is indispensable in ordinary circumstances as an integral aspect of the constitutional right to privacy.¹²
- Administrative authorities must act strictly within the scope of the powers conferred upon them by law and by applicable directives. They cannot exercise powers that have not been expressly granted.¹³
- Although the competent authority may publish the results of licensing examinations, it has no legal authority to publish the citizenship numbers of examinees unless such disclosure is expressly authorised by law.¹⁴
- The unauthorised publication of citizenship numbers exposes individuals to significant privacy risks, as hackers or other malicious actors may use such information to obtain and misuse additional personal data.¹⁵
- A citizenship number is a unique personal identifier and constitutes highly sensitive personal information because it is directly linked to an individual's identity.¹⁶
- A citizenship certificate contains intimate personal information, including a person's name, date of birth, permanent address and parental details, all of which deserve legal protection against unauthorised disclosure.¹⁷
- A citizenship certificate is the primary legal document establishing an individual's identity and therefore warrants the highest degree of protection.¹⁸

¹² *Bivek Chaudhary, supra* note 2, at para. 25.

¹³ *Id.* at para. 25.

¹⁴ *Id.* at para. 25.

¹⁵ *Bivek Chaudhary, supra* note 2, at para. 18.

¹⁶ *Bivek Chaudhary, supra* note 2, at para. 16.

¹⁷ *Id.* at para. 16.

¹⁸ *Id.* at para. 16.

- Legal persons, including statutory and public authorities, may do only what the law expressly permits. They possess no inherent powers, and any action beyond the authority conferred by statute is *ultra vires* and unlawful.¹⁹

IV. COMPARATIVE ANALYSIS: DIVERGENCES AND CONVERGENCES

A. Convergences

Both courts arrived at a common insistence: that informational privacy is not merely an incident of some other right but a standalone interest deserving direct constitutional protection. *Puttaswamy* did this at the level of grand constitutional theory, tracing privacy through dignity, autonomy and the interlocking structure of Part III. Decision No. 081-WO-0500 did it at the level of a single transport office's Facebook page, but the underlying commitment is identical, that a citizen's identifying data does not become fair game for disclosure simply because a government body finds it administratively convenient to disclose it.

Both courts, too, rejected what might be called the efficiency defence: the argument, made in both cases by state respondents, that disclosure served a legitimate administrative purpose, deduplication of Aadhaar enrolment and prevention of welfare leakage in India, disambiguation of same-named examinees and prevention of impersonation in Nepal, and should therefore survive scrutiny on that basis alone. Neither court treated administrative convenience as self-legitimizing. *Puttaswamy* subjected it to the discipline of its three-fold test; the Nepali Bench subjected it to the discipline of the *ultra vires* doctrine, asking not whether the disclosure served some plausible public purpose but whether any law had actually authorised it.

Finally, both judgments reach for the same external scaffolding: the ICCPR, the UDHR, the OECD Guidelines and, in Nepal's case explicitly, *Puttaswamy* itself. This is not incidental. It signals that South Asian courts confronting first-generation informational-privacy questions are, consciously, building on each other's reasoning rather than working in doctrinal isolation, and that Indian constitutional jurisprudence functions as persuasive, if not binding, authority for its neighbours in ways that mirror the older common-law tradition of cross-citation among Commonwealth courts.

B. Divergences

The structural point of departure is textual. Article 21 of the Indian Constitution says nothing about privacy; the right had to be implied from "life" and "personal liberty," a process that required overruling two precedents and convening a bench of nine. Article 28 of Nepal's

¹⁹ Bivek Chaudhary, *supra* note 2, at para. 15.

Constitution, by contrast, names privacy explicitly, extending it in terms to a person's "body, residence, property, documents, data, correspondence and character." Nepal's courts have never had to fight the interpretive battle India's did; their task is calibrating the scope of an acknowledged right rather than establishing its existence in the first place. This is a genuine jurisprudential head start, though it comes with its own cost: because Article 28's guarantee runs "except as provided by law," Nepali courts must do correspondingly more work parsing whether a particular statute or directive does or does not constitute the "law" required to displace the presumption of confidentiality, precisely the interpretive labour the Bench performed here.

The procedural paths could hardly have been more different. *Puttaswamy* was the product of a decade-long, multi-petitioner constitutional marathon, ultimately requiring the country's largest possible bench and producing six opinions running to several hundred printed pages. Decision No. 081-WO-0500 was resolved by a two-judge Division Bench, on a single writ petition filed by an individual law student contesting a comparatively contained administrative practice, and disposed of with a single order of some dozen paragraphs. That asymmetry reflects less a difference in the seriousness of the underlying privacy interest than the sheer institutional scale of Aadhaar as a nationwide biometric infrastructure touching over a billion residents, as against a discrete practice confined to a handful of provincial transport offices.

The remedial architecture differs as well. India's judgment operated in declaratory mode, establishing a constitutional standard against which a since-enacted data-protection statute and the surviving portions of the Aadhaar Act would later be tested by subsequent benches. Nepal's judgment operated in the more immediate register of administrative-law relief, mandamus directing a specific, concrete change in publication practice, with no occasion, and no request, to develop a general data-protection standard beyond the facts before it. One court built a constitutional framework for future litigation; the other applied Nepal's existing framework to correct an identified administrative overreach.

V. TOWARDS A SOUTH ASIAN JURISPRUDENCE OF PRIVACY

Taken together, these decisions suggest something of value to courts elsewhere in the region, in Bangladesh, Sri Lanka, Pakistan and beyond, that have yet to confront the informational-privacy question with comparable rigour. The first lesson is doctrinal economy: a jurisdiction whose constitution, like Nepal's, expressly names privacy need not import India's interpretive machinery wholesale; it need only develop a coherent standard for testing when a "law" genuinely displaces the constitutional default of confidentiality, a task closer to ordinary statutory interpretation than to grand constitutional theory. The second is institutional: Nepal's

experience demonstrates that meaningful privacy jurisprudence need not await a decade-long, multi-petitioner mobilisation of the kind Aadhaar produced. A single, well-prepared writ petition, filed in this instance by a law student still completing his professional training, proved sufficient to secure a considered judicial articulation of the *ultra vires* limits on administrative data practices, coupled with concrete relief.

The third lesson concerns the layering of authority itself. The Nepali Bench's willingness to cite *Puttaswamy* directly, alongside its own domestic precedents in *Baburam Aryal* and *Bhaktiram Ghimire*, models a form of horizontal judicial dialogue increasingly common among South Asian apex courts confronting shared legal problems inherited from broadly similar administrative-law and constitutional traditions. As governments across the region digitise identification, licensing and welfare-delivery systems along lines resembling India's Aadhaar architecture, the interpretive labour *Puttaswamy* performed, distinguishing legitimate state need from mere administrative convenience, is available for reuse, and Decision No. 081-WO-0500 shows a court doing exactly that reuse in miniature.

VI. CONCLUSION

Neither judgment treats privacy as a relic of an analogue age to be politely retired in the face of administrative digitisation; both treat it as a right whose content must expand precisely because the means of violating it have expanded. The Indian Supreme Court did this by overruling seven decades of contrary authority and constructing, from six separate opinions across a nine-judge bench, a single workable test. Nepal's Supreme Court did it by holding four transport offices to the plain text of their own governing directives and declining to let administrative habit substitute for statutory authorisation. What unites them is a shared refusal to let the state's bureaucratic convenience masquerade as legal entitlement, and a reminder, evident in Chaudhary's petition as much as in the Aadhaar litigation, that the boundary between citizen and surveilled subject in South Asia is still being drawn, one case at a time, by petitioners willing to test it and courts willing to hold the line.
