

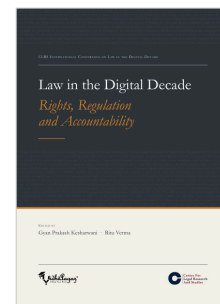
CHAPTER 19

“You Can Reset a Password, But Not Your Biometrics”: The Problem of Irreversible Biometric Data

Aakriti Jain and Shreya Agarwala

in *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma (VidhiAagaz 2026), pp. 227–237

DOI <https://doi.org/10.63108/VAB.LDD.1.19>



CITATIONS

BLUEBOOK (21ST ED.)

Aakriti Jain & Shreya Agarwala, “*You Can Reset a Password, But Not Your Biometrics*”: *The Problem of Irreversible Biometric Data*, in *LAW IN THE DIGITAL DECADE: RIGHTS, REGULATION AND ACCOUNTABILITY* 227 (Gyan Prakash Kesharwani & Ritu Verma eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Aakriti Jain and Shreya Agarwala, “‘You Can Reset a Password, But Not Your Biometrics’: The Problem of Irreversible Biometric Data’ in Gyan Prakash Kesharwani and Ritu Verma (eds), *Law in the Digital Decade: Rights, Regulation and Accountability* (VidhiAagaz 2026) 227.

CHICAGO (17TH ED.)

Jain, Aakriti, and Shreya Agarwala. “‘You Can Reset a Password, But Not Your Biometrics’: The Problem of Irreversible Biometric Data.” In *Law in the Digital Decade: Rights, Regulation and Accountability*, edited by Gyan Prakash Kesharwani and Ritu Verma, 227–237. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.1.19>.

APA (7TH ED.)

Jain, A., & Agarwala, S. (2026). “You can reset a password, but not your biometrics”: The problem of irreversible biometric data. In G. P. Kesharwani & R. Verma (Eds.), *Law in the digital decade: Rights, regulation and accountability* (pp. 227–237). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.1.19>

SOURCE

<https://doi.org/10.63108/VAB.LDD.1.19>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 19

“You Can Reset a Password, But Not Your Biometrics”: The Problem of Irreversible Biometric Data

AAKRITI JAIN* AND SHREYA AGARWALA**

Traditionally, passwords have been used as the first-line guardian of digital identity, but they have proven rather fragile, as users tend to use either predictable passwords that can be easily hacked or passwords that are difficult to remember. These consistent drawbacks have pushed us towards developing new methods of verification that are much faster, convenient and safer to use. Biometric authentication (fingerprinting, facial recognition, iris scanning, voice recognition) is the first thing that springs to mind in this scenario. While there have been numerous studies on the effectiveness and convenience of biometrics in the past, one important issue that needs to be answered is whether the existing legal framework is prepared for the unique challenge presented by irreversibility. A legal, doctrinal and comparative approach has been applied in this paper in analysing data protection laws, judicial decisions and guidelines from selected jurisdictions to assess whether the current remedy framework sufficiently accounts for the enduring nature of biometric damage. It argues that the issue of irreversibility requires a unique approach to regulate, i.e., an approach based on proactive precautionary measures instead of reactive ones and ends with suggestions for how this could be done.

Keywords: Biometric authentication, irreversibility, data protection law, privacy, biometric damage, digital identity

1 INTRODUCTION

A password is a matter of fact about what an individual remembers while the biometric identifier is a matter of what an individual is. The difference may be somewhat academic, but it serves as the point of departure for this paper. Passwords can never be right as they can only work or fail. Indeed, passwords are constantly failing and are being reset. Breach alerts typically conclude with an instruction to reset the password, no matter how often that process has already been undergone by the victim. In contrast, once the fingerprint, the iris pattern, the facial geometry or the voiceprint has been captured and stored, it can never be changed again in one's lifetime, and possibly much longer than that.

The ease of use of biometrics for authentication is not under contention here and is already widely accepted as it is faster than entering a password and it is impossible to forget in the same sense as a PIN can be and most importantly it protects against the most rudimentary form of credential sharing and phishing attacks. Indeed, governments have invested so heavily in national identity frameworks based on biometrics, like India's Aadhaar program, the largest of its kind in the world. Likewise, private sector platforms have integrated fingerprinting and facial recognition into the basic experience of mobile device use. The issue that has been lagging behind all of this is the legal understanding of what happens once the template itself is breached. Data protection laws were built upon an architecture that assumes that

* Student at Unitedworld School of Law, Karnavati University, Gandhinagar, Gujarat, India.

** Student at Unitedworld School of Law, Karnavati University, Gandhinagar, Gujarat, India.

any given data could be easily renewed, superseded or become obsolete through the simple process of issuing a new one. Biometric data is an exception to this rule.

2 RESEARCH METHODOLOGY

2.1 Research Questions and Methodology

The two guiding research questions for the analysis include:

- firstly, whether the irreversibility of biometric identifiers raises a novel legal risk that cannot be sufficiently covered by traditional breach and remedy approaches; and
- secondly, whether biometric-specific preventive measures ought to be required under Indian data protection law, instead of imposing onerous horizontal obligations as to all personal data.

The paper uses a comparative method based on doctrinal research and compares Indian constitutional privacy law to the Digital Personal Data Protection system, along with the EU special-category approach and Illinois biometrics legislation.¹

2.2 Research Gap and Contribution

Past literature related to biometrics often tends to be centred on themes like surveillance, consent, accuracy, discrimination and cybersecurity. However, in this paper, the gap has been identified in terms of doctrine, specifically the clash between the nature of the biometric identifier's permanence and the remedy-oriented approach that takes for granted containment of the compromised information. The primary contribution of this research is the formulation of an "irreversibility principle", which holds that when the data principal cannot reasonably replace the compromised biometric identifier, the duty of protection should rest with the entity that decides to capture, store, and use that identifier.²

3 IRREVERSIBILITY AS A UNIQUE LEGAL HARM

3.1 The Unique Character of Compromise of a Biometric Identifier

Earlier, laws designed for data protection have been constructed on the presumption derived from the fields of financial and identification security, that of replacing an identifier in case of its breach. For instance, a credit card number, once revealed, is cancelled and replaced; similarly, passwords, once revealed, are reset by the system and even Social Security and Aadhaar numbers, which are very hard to recover once leaked can still be flagged, monitored and eventually reissued and/or supplemented with further means of verification. Biometric identifiers fall outside of the scope of this paradigm. A person only has a finite set of ten fingerprints, two irises, one face and one voice. In case the template of any of those is compromised, a replacement cannot be made as in the case of passwords and the same identifier will keep being used indefinitely even for the rest of a person's lifetime and across different systems unaware of this breach.

¹ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4–7; Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 9, 2016 O.J. (L 119) 1, 38–39 (2016).

² Regulation (EU) 2016/679 of the European Parliament and of the Council, arts. 5, 32, 2016 O.J. (L 119) 1, 35, 51–52 (2016); Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/5(c), 15(a)–(b) (2024).

This is the exact rationale behind the passage of the Biometric Information Privacy Act (BIPA) by the Illinois legislature in 2008 which is one of the very first and most significant biometrics-specific laws ever passed in the world. The findings in the law itself recognise the distinction between biometric identifiers and other unique identifiers because of the simple reason that while a Social Security number can be altered after it is compromised, there is no way for a biometric identifier to be altered since it is biologically determined.³

The doctrinal importance of this legislative holding is that it changes the nature of the injury. In any traditional data breach claim, the act of exposure is wrongful, while the actual injury arises from its misuse. This principle is codified in the standing doctrine used by courts of law across many jurisdictions, including the United States, in determining the viability of any data breach claims when plaintiffs usually must establish an appreciable risk of the future misuse of their personal information, rather than its actual exposure. The Illinois courts' approach to interpreting BIPA is quite different, however, since the very act of collecting biometric data without notifying the individual in writing about his/her rights and obtaining his/her written consent constitutes a violation of the privacy right. The body of BIPA case law on this topic culminates in *Rogers v. BNSF Railway Co.* and similar lawsuits in which the court has ruled against a rail operator for its reckless or intentional violation of BIPA by fingerprinting thousands of truckers without written, informed consent.⁴

3.2 Irreversibility Accumulates over Time and Across Other Systems

The second aspect that makes the breach of biometrics stand out from a regular data breach is the ability of the compromise to accumulate. While a password can no longer be used in any other place after a reset, if the user takes care of this problem, a compromised biometric template could potentially have found its way into multiple systems: a mobile phone, a company security system, a countrywide identification system, customer identification at a bank, an investigative database in a state police force, all of which would independently collect the same physical trait from the person.

The cumulative quality of such a problem is precisely the reason why the argument developed within this paper separates the issue of irreversibility from a question of degree. An approach which is geared towards addressing the possibility that, for example, an email address might be collected for the purpose of spamming cannot be properly balanced to address the problem of an irreversibility that is cumulative, cross-situational and cannot be fixed once achieved. Any legal mechanism which attempts to respond mainly through post-fact notification and monetary compensation will necessarily treat the wrong as a transitory rather than permanent one.

4 COMPARATIVE ANALYSIS

4.1 European Union: Biometric Data as a Special Category

The General Data Protection Regulation (GDPR) is perhaps the most complex regulation of the three regimes that have been discussed in this paper since it categorises biometric data in an entirely unique manner. According to Article 9 of the GDPR, biometric data used for uniquely identifying a natural person belongs to a closed list of “special categories” of personal data. Along with information about the

³ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/5(c) (2024).

⁴ *Rogers v. BNSF Ry. Co.*, 680 F. Supp. 3d 1027, 1032–34 (N.D. Ill. 2023).

health status of a person, genetic data, racial or ethnic origin of the individual and some other categories of personal information, which present a particularly high risk in case of processing, biometric data is subject to certain restrictions. Processing biometric data is prohibited by default and allowed in specific instances described in Article 9(2).⁵

The doctrine of a special-category approach, as far as the irreversibility argument put forward here is concerned, consists of the fact that it introduces an element of asymmetry into the very beginnings of the regulatory regime instead of depending only on the remedy stage. The data controller wanting to process biometric data according to the requirements of the GDPR has to comply with a higher standard of compliance before the very possibility of collecting it and the very reason why a higher standard is required lies precisely in the increased danger posed to the individual by the processing of such data and a danger which as has been suggested earlier is essentially irreversibility-based. While this model alone does not resolve the irreversibility dilemma since a special category can be broken through and the danger would remain unresolved nonetheless, it does something that reactive measures cannot. It structurally discourages collecting biometric data in the first place, since what has never been collected cannot be irreversibly damaged.

4.2 The United States: Sectoral Differences, Partially Remedied by State Law

In the United States, there is no broad federal data protection legislation like the GDPR, nor does biometric data receive any form of federal protection. Instead, a select few states, including Illinois, Texas, and Washington State (with the latter two lacking a private right of action) have their own independent biometric privacy laws. BIPA's structure is instructive precisely because it appears to have been drafted with irreversibility as its central premise rather than an incidental concern. Under the statute, the private entity must have a publicly accessible written policy on retention and destruction in place before collection, obtain informed, written consent before collection and destroy the biometric data after the initial purpose of its collection is served or within a statutory time period, whichever is sooner.⁶ Most importantly, BIPA provides a private right of action with an already determined sum of money for each breach, thus eliminating the proof-of-loss issue in many instances.

The potential magnitude of exposure that this liability model could create for the non-compliant organisation has been illustrated through *Rogers v. BNSF Railway Co.*, wherein a jury awarded damages against the defendant for thousands of statutory violations committed due to the unwitting fingerprinting of truckers as they entered its rail yards, yielding an initial judgment of \$228 million that was modified based on subsequent guidance from the Illinois Supreme Court on the accumulation and discretionary nature of statutory damages. Regardless of any assessment regarding the magnitude of this exposure, the liability model deserves consideration on its own merits. BIPA does not require proof that the compromised fingerprint subsequently led to a fraud perpetrated upon the person. Rather, the liability is in place due to the fact that the individual's inability to ever change their compromised fingerprint creates the complete harm itself. This is exactly the kind of front-loaded and non-discretionary form of liability that a regime sensitive to irreversibility needs, despite the limited geographical scope of the statute and the fact that few American states provide similar protections.⁷

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 9, 2016 O.J. (L 119) 1, 38–39 (2016).

⁶ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15(a)–(b) (2024).

⁷ *Rogers v. BNSF Ry. Co.*, 680 F. Supp. 3d 1027, 1032–34 (N.D. Ill. 2023).

4.3 India: Constitutional Acknowledgement Without a Statutory Special Category

India offers the best example for this paper's claim due to the unusual discrepancy between constitutional law and statutory provisions. The 2017 Supreme Court judgment made in a case of nine judges through Justice K.S. Puttaswamy v. Union of India declared that the right to privacy is a fundamental right and it constitutes an integral part of the Right to Life and Personal Liberty guaranteed under Article 21 of the Constitution according to the constitutional law theory.⁸ On the other hand, the 2018 five-judge bench case of Justice K.S. Puttaswamy (Ret'd) v. Union of India (Aadhaar), where the constitutionality of India's national biometric ID scheme based on the proportionality test was considered, stated the objective of Aadhaar as delivering welfare benefits as justifiable, and the scheme thus passed the proportionality test. Nonetheless, Justice D.Y. Chandrachud's dissenting opinion is doctrinally relevant in this context insofar as he has regarded the privacy right of an individual with respect to his biometric data as particularly important due to the permanence and association with bodily integrity of the data in question, in view of the fact that the compromise of the biometric database cannot be corrected as other kinds of compromised information can.⁹

4.3.1 *Digital Personal Data Protection Act, 2023: Protection of Irreversible Biometric Identifiers*

The Digital Personal Data Protection Act, 2023 (DPDP Act), which was assented to by the President of India in August 2023, and whose Rules were notified on 13 November 2025 and which provides for gradual enforcement, including many of its main operative provisions eighteen months after notification, has intentionally diverged from the special category approach of the GDPR and previous Indian draft data protection laws. The DPDP Act does not have any special category of sensitive personal data and biometric data is governed by precisely the same horizontal standards of notice, consent or one of nine other exceptions to consent, purpose limitation and security as the person's name and address.¹⁰ The Act does not refer to biometric data at all.

This is not a mere question of drafting differences, but a real regulatory gap. In the light of the DPDP Act regime, any organisation which processes fingerprints or face data, whether for purposes of work attendance or building entry, stands subject to more or less similar threshold obligations as compared to those organisations that process email IDs for a newsletter, even though the November 2025 Rules have imposed special obligations such as the appointment of Data Protection Officers and periodic audits on Significant Data Fiduciaries, which are organisations that qualify as such because of the nature or scale of processing, though in practice these will include biometric processors too.¹¹

The end result is thus of a state whose Supreme Court has acknowledged, in terms of constitutional theory, the special vulnerability associated with biometric information, yet whose main data protection law has failed to incorporate this insight into a unique rule for collection, a deadline for destruction, or a template protection requirement akin to those contained in BIPA as a matter of private enforcement, and/or in the GDPR as an exception category.¹² It is in this way, the present paper argues, that the gap

⁸ Justice K.S. Puttaswamy (Ret'd) v. Union of India, (2017) 10 SCC 1, 260–62 (India); INDIA CONST. art. 21.

⁹ K.S. Puttaswamy (Ret'd) v. Union of India (Aadhaar), (2019) 1 SCC 1, 1026–27, 1400–01 (India) (Chandrachud, J., dissenting).

¹⁰ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4–7.

¹¹ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 10.

¹² Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4–8; Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15; Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 9, 2016 O.J. (L 119) 1, 38–39 (2016).

between the rationale of the Aadhaar dissent and the design of the DPDP Act can be most clearly articulated.

Thus, the fundamental problem is not the lack of privacy laws in India, but the lack of a regulatory trigger for biometric data which is distinct from other types of personal information. Even in the presence of a horizontal regime governing the collection and use of biometric data, it will fail to account for the fact that the risk associated with an error is very high since there is no way for the data subject to get a replacement face, fingerprint, iris, or voice. India should thus distinguish regular personal data and data whose misuse results in an irreversibly changed status with respect to the safety of the data subject.

4.3.2 *Right to Information Act, 2005: Transparency Versus Biometric Privacy*

The Right to Information Act of 2005 becomes equally significant in relation to the governance of biometric information of individuals that is held by public authorities. Since biometric information needs to have strict privacy protection because of the fact that once the fingerprint, facial geometry, iris pattern or voiceprint becomes compromised, it cannot usually be replaced, the process of collecting, processing and storing of such information needs to remain transparent. Therefore, in the context of biometric databases, the RTI framework can become a complementary tool, which will allow citizens to obtain information about the policies and procedures of handling, retention and securing of biometric information, as well as about the mechanisms of its governance. However, the right to information is not an unlimited right to access any kind of personal or sensitive information. The exemptions listed in Section 8(1)(j) of the RTI Act, especially those relating to security issues and information that involves personal privacy, help balance governmental transparency with the protection of individuals from unnecessary disclosure.¹³ This distinction becomes even more important for biometric databases like the Aadhaar database: public institutions need to be answerable about how biometric data is managed, without making individuals' biometric identifiers publicly available. In this respect, the RTI can complement the precautionary principle that has been suggested in this paper.

5 FROM REACTIVE REMEDY TO PROACTIVE DESIGN

5.1 Comparative Synthesis

The comparison gives rise to regulatory instincts: the GDPR increases the level of lawfulness of data processing, BIPA transforms duties specific to biometrics into legal obligations protected through a private remedy and India's DPDP regime offers a horizontal baseline but fails to address the particularity of the biometric issue.¹⁴ For India, the lesson is not to emulate either system in toto; instead, it needs to integrate the notion of front-end cautioning alongside the recognition that capturing biometric data illegally is in itself an actionable wrong.

This comparative analysis leads to a more focused proposition than the general one regarding stricter penalties. The issue is not that the penalties are insufficient but the problem is that the entire framework of remedies – notice of breach, mitigation and compensation tied to actual loss – assumes a harm which

¹³ Right to Information Act, 2005, § 8(1)(j), No. 22, Acts of Parliament, 2005 (India).

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 9, 2016 O.J. (L 119) 1, 38 (2016); Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15, 20 (2024); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4–8.

is finite and, at least in part, reversible. If the harm is irreversible, by definition it is not something which can be reversed: by the time the legal system intervenes in response to the breach, it is already too late for this type of data, regardless of whether the breach occurred accidentally or on purpose. This is not to argue that biometric authentication should not be used as its benefits in comparison to passwords are undeniable. The point, however, is the need to reframe biometric regulation around precaution rather than remedy.¹⁵

5.2 Template Protection Is Mandatory

One issue raised frequently in the technical literature regarding security issues relating to biometric systems is the difference between storing a raw biometric image and storing an irreversible and non-reversible cryptographic template based on that raw image. Techniques classified under ‘cancellable biometrics’ and ‘biometric template protection’ were introduced specifically so that, if compromised, the stored template can be invalidated and a new template can be created by applying a new transformation to the underlying physical feature, which creates an analogous ability to reset the biometric to the same degree as an ordinary credential. There are standards documents produced by the US National Institute of Standards and Technology outlining this very category of technique for over ten years, yet very few data protection laws mandate its use.¹⁶

A precautionary approach to regulation would demand by statute that an organisation using biometrics for identification store only biometric templates which cannot be reversed and which have been created using such processes, but not using any raw image or matchable biometric feature sets and would make the legitimacy of the collection process dependent upon demonstrable adherence to a recognised technical standard.

5.3 Purpose-Based and Time-Limited Retention as a General Rule by Default

The provision under BIPA that a private entity must have a written retention and destruction policy before the collection of biometric information and the deletion of biometric information after the satisfaction of the intended purpose or the expiry of a statutory period (whichever is earlier) is a prudent design that should be considered for adoption outside of Illinois and beyond the private sector. While the principle of limitation of processing on grounds of purpose under the DPDP Act limits data usage after the intended purpose is achieved, there is no maximum limit for biometrics and the practice of implementation follows the complaint-based approach of the DPDP Act.¹⁷

A ceiling on retention specific to biometric identifiers, such as a hard-coded maximum duration unless there is a valid ongoing consent or statutory mandate, would lower the number of vulnerable records at any one time and therefore, the scope of any potential breach incident, which is precisely what the precautionary approach would seek to mitigate, since the harm resulting from its triggering cannot subsequently be mitigated.

¹⁵ *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1206–07 (Ill. 2019); *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶¶ 20–27 (Ill. 2023).

¹⁶ NIST Special Publication 800-63B, § 5.2.3.

¹⁷ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15(a) (2024); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 8, 12.

5.4 Non-Contingent Liability Calibrated to Incentivise Collection Prevention and Not Misuse

The most instructive element of the American experience, when viewed from a structural perspective, is that a liability regime requiring a plaintiff to demonstrate the misuse, financial harm, or risk of future identity theft of a biometric data identifier before awarding any form of compensation asks too much of the injured party. The difficulty inherent in such a requirement derives from the reality that misuse of a captured biometric may take place several years down the road via entirely unconnected means. Thus, while Illinois' Biometric Information Privacy Act's model of statutory liquidated damages, based on unlawful capture rather than actual misuse, does not solve the problem of irreversibility, it recognises this difficulty by making it an intrinsic part of its liability formula: a biometric data capturer takes the risk that capturing such data without a lawful process will come at a cost.¹⁸

India is an example of a jurisdiction that currently relies on the administration of penalties via the Data Protection Board in the DPDP Act and not the creation of an individual enforceable private right of action in order to enforce the Act.¹⁹ It would be necessary for this jurisdiction to balance the cost of creating the private right of action against the precautionary principle of incentive alignment.

5.5 Consent as a Threshold Gate and Not as a Liability Shield

Lastly, it is essential for a precautionary approach to avoid seeing the act of obtaining consent as a sufficient response to the problem of irreversibility. The consent mechanisms within all three regimes mentioned earlier serve their purpose quite effectively as a gate into collecting biometric information; however, they fail to solve the question of how to deal with the consequences of the data becoming vulnerable without any further involvement of the data principal in the process. The person who consented to having his fingerprint scanned for gaining entry to a facility did not consent to the risk of that information becoming public due to the vendor's breach of security in another context. It follows that in a precautionary regime, consent is only necessary but not sufficient: where collection is legal in terms of the justification for collecting data, there should be safeguards both technological and in terms of retaining data regardless of whether or not the consent is legally obtained.²⁰

TABLE 1. *Treatment of biometric data under the GDPR, BIPA and the DPDP Act*

Issue	GDPR	BIPA	India (DPDP)
Regulatory Treatment	Special Category/ High Bar	Biometric-Specific Law	Horizontal Personal Data Law
Collection	Prohibited unless Article 9 condition satisfied	Written notice and informed consent	Lawful purposes within DPDP regime
Retention	Principle of storage limitation	Written retention/destruction policy	Broad principles; no specific biometric retention limit

¹⁸ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/20 (2024); *Cotbron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶¶ 20–27 (Ill. 2023).

¹⁹ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 27–33.

²⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 9(2)(a), 2016 O.J. (L 119) 1, 38–39 (2016); Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15(b) (2024); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 6.

Issue	GDPR	BIPA	India (DPDP)
Remedy	Administrative/judicial remedies	Private cause of action and statutory damages	Admin enforcement through Board regime
Basic Message	Prevent unnecessary data collection	Illegal data collection must have independent consequences	Add biometric-specific duties

6 OBJECTIONS AND LIMITATIONS

Five objections are posed against the proposal:

- First, there could be improvement in the security and ease of access through biometric authentication and restrictive measures might drive organisations to go for less secure methods. The regulation would thus focus on the conditions of use instead of prohibiting biometrics.
- Second, no method of template protection will make biometric authentication completely safe. It is rather an issue of risk reduction and legal management and not technology.²¹
- Third, compulsory template protection architecture, fixed retention limits and independent certification requirements will incur unavoidable compliance costs, which will unfairly burden small data fiduciaries and new entrants in the market and may even cement the position of incumbent firms who can better bear these compliance costs compared to small firms, which could offer services such as biometric attendance or access control solutions. In any event, this is an unavoidable trade-off rather than an argument against adopting a precautionary design, since a differentiated compliance regime, depending on either the amount of processing or the sensitivity of the use case, as in the GDPR's proportionality principle, would alleviate some of the burden.
- Fourth, detaching recovery from actual harm results in disproportionate litigation. The ruling in *Cothron v. White Castle System, Inc.*, by the Supreme Court of Illinois, whereby the Illinois Supreme Court ruled that there is a violation of the BIPA every time biometric data is captured and transmitted, rather than once per collection, turned normal timekeeping into a potential basis for statutory liability and led to the Illinois legislature capping damages for such violations shortly thereafter. In adopting the non-contingent approach of BIPA, an alternative jurisdiction needs to incorporate the fine-tuning that the Illinois legislature failed to include in the statute, either by setting statutory damages on the basis of one accrual of liability per incident for each data subject, or by instituting a proportionality rule.²²
- Fifth, making the consent gate tougher will create conflict for those who rely on biometric authentication systems, especially those based on Aadhaar to gain access to various welfare benefits and essential services and for whom refusal of consent does not actually represent a viable alternative. A precautionary principle intended to shield people from irremediable damage should not be applied in such a way that exacerbates the exclusion of the very group it intends to help. Such conflict can be better handled using the other parts of the above proposal, namely retention and deletion and liability provisions without recourse to consent procedures.

²¹ NIST Special Publication 800-63B, § 5.2.3.

²² *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶¶ 1, 20–27 (Ill. 2023).

7 IMPLEMENTATION

An irreversibility-sensitive system would regulate the circumstances under which biometrics can be used and not ban biometrics. These regulations embody the normative principle contained in the paper in actionable legal obligations:

7.1 Necessity Analysis Before Collection

The data fiduciary must state why biometric authentication is necessary, why less invasive identifiers are insufficient and an alternative that was considered. Processing of high-risk information requires a documented risk analysis.²³

7.2 Template-First System Architecture

Raw biometric images must not be stored whenever possible when authentication may be performed using protected templates. Compliance must be independently verifiable.²⁴

7.3 Retention and Deletion Control Mechanisms

Each biometric system must have a defined purpose, maximum retention period, deletion controls and an established process for retention exceptions where required by law.²⁵

7.4 Irreversible Breach Response Mechanism

The biometric breach response should not only include notification but also contain containment, forensic examination, downstream processor identification, enhanced authentication methods and appropriate reporting to regulators.²⁶

7.5 Remedies and Accountability

Unlawful collection or retention of biometrics should be able to attract an appropriate remedy regardless of whether downstream identity theft occurs in all cases. There must be an established means through which people can complain.²⁷

7.6 Technical Standards Independent of the Legislation

The regulator should establish or adopt minimum standards for the protection of templates, encryption, access controls, key management, proof of destruction and auditing of processes.²⁸

²³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 4–8; Regulation (EU) 2016/679 of the European Parliament and of the Council, arts. 5, 25, 35, 2016 O.J. (L 119) 1, 35, 39, 56 (2016).

²⁴ NIST Special Publication 800-63B, § 5.2.3.

²⁵ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15(a) (2024); Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 5(1)(e), 2016 O.J. (L 119) 1, 35 (2016).

²⁶ Regulation (EU) 2016/679, *supra* note 1, arts. 33–34, 2016 O.J. (L 119) 1, 51–52 (2016); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 8(5)–(6).

²⁷ Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/20 (2022); *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004, ¶¶ 20–27 (Ill. 2023).

²⁸ NIST Special Publication 800-63B, § 5.2.3.

8 CONCLUSION

Biometric authentication addresses a genuine vulnerability associated with passwords, but this paper does not dispute the use of biometrics. What the paper disputes is that the laws constructed to govern the use of biometrics were, for the most part, constructed on an entirely different set of assumptions about data – namely data which could be reissued, substituted and managed after a breach. The special category approach of the EU increases the bar to collection of such data, but no more. Among the various models proposed in the sectoral approach to biometrics regulation, the American one, illustrated by BIPA in Illinois, represents the most precautionary one because liability is triggered simply upon the fact of unconsented collection as opposed to demonstrable damage downstream, but still suffers from the geographic and institutional fragmentation. India provides the most vivid example of the chasm highlighted throughout this paper: the biometric-specific constitutional jurisprudence, especially that of Justice Chandrachud in his dissenting opinion in the Aadhaar case, which recognises biometric data as uniquely and irreversibly vulnerable data, coexisting with a newly implemented statutory regime which fails to incorporate this understanding into a biometric-specific standard of collection and retention. This can be achieved without entirely discarding the principle-based horizontal approach established in the DPDP Act, and only requires adding biometric-specific protections, in terms of template protection standards and strict ceilings on retention, as well as a more precautionary liability rule. Any rule of law which only reacts after irreversible damage has occurred fails to provide protection for the individual because it is reactive in nature.²⁹

* * *

²⁹ NIST Special Publication 800-63B, *supra* note 16, § 5.2.3; Regulation (EU) 2016/679, art. 9; Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15, 20 (2022); K.S. Puttaswamy (Ret'd) v. Union of India (Aadhaar), (2019) 1 SCC 1, 1026–27 (India) (Chandrachud, J., dissenting).