



Right to Privacy: The Legality of Biometric Surveillance Under Criminal Procedure

Muhammad Bilal Shahbaz khan

Visiting Lecturer, University Gillani Law College,

Bahauddin Zakariya University, Multan, Pakistan

Email: bilalshahbazkhan8888@gmail.com

Asmia Habib

Assistant professor, Nawab Allah Nawaz Law College,

Gomal University, Dera Ismail Khan, Pakistan

Email: asmiahabib6262@gmail.com

Tahmina Qamar

(LL.M) (D.F.S.L), Advocate High Court,

Lecturer, Shadab Law College, Pakistan

Email: tahminaqamar456@gmail.com

Abstract

Biometric surveillance is an important tool in present-day criminal investigation. New technologies such as fingerprinting, facial characteristics, iris scanning, voice recognition etc., make it easier to carry out identification and to help agents in serious cases to investigate an offense. Meanwhile, the technologies raise unique privacy issues based on the close association of biometric traits with the identity of the person and the fact that they can be kept, searched and re-used after they are first collected. The legal question is thus when does biometric surveillance leave the realm of legitimate investigative investigation and become the term of the excess: "a disturbing interference by the State in the life of citizens?"

The legal question is thus: when does biometric surveillance transcend into legitimate investigative investigation and when does it become a disproportionate state interference in the lives of citizens? The paper analyses the status and legal aspects of using biometric surveillance in the criminal procedure, focusing on the case of Pakistan and the progress made in other nations. It contends that biometric monitoring should be evaluated in the light of the criteria of legality, necessity, proportionality, accountability and effective remedy. The analysis shows that standard-police powers and the broad police surveillance provisions are not enough to comprehensively govern the entire life cycle of biometric data, especially the use of facial recognition tools in public places and the acquisition of information of people who are not suspected of Criminal offence. A significant patchwork of constitutional and statutory frameworks offers important foundations, but are out of sync with each other in Pakistan. The paper puts forward the need for and suggests a specific legal framework with statutory authorization, prior judicial authorization for intrusive surveillance, purpose limitation, data minimization, restriction on data retention, human verification, algorithmic accountability and effective remedies. It finds that while biometric surveillance has a legitimate role in the criminal justice, this role must not trump constitutional rights and due process.

Keywords: Biometric surveillance; right to privacy; facial recognition; criminal procedure; biometric data; proportionality; judicial oversight; Pakistan; artificial intelligence; data protection



Vol. 4 No. 2 (February) (2026)

1. Introduction and Research Framework

Biometric technologies have revolutionized the way in which a criminal investigation can be undertaken. New, more and more sophisticated digital systems can now collect, process and compare fingerprints, DNA profile, iris scan, voice recognition or facial recognition. The technologies can help law-enforcement agencies in identifying suspects, linking crime scenes and persons to criminal incidents and in investigating serious crimes. It makes sense that they'd be attractive: Biometric traits are hard to duplicate and can yield investigators valuable clues that other investigative techniques wouldn't normally yield. But biometrics are especially intrusive from a privacy standpoint, because they are useful for purposes of crime control (Smith & Miller, 2022a).

The difficulty with the law is apparent when biometric identification goes beyond comparing information about a known suspect and, rather, is used as a tool for identification generally. This could show up on conventional surveillance as someone being in one location. When that observation is made by biometric surveillance, it will become something that can be identified, searched and compared and saved. In particular, facial recognition technology allows an image captured from a public area to be used to convert the image to biometric information and subsequently compared to a reference database. The technology thus provides the possibility of changing normal public observation to systematic identification. This is also a recent development which has been termed an intensification of police surveillance, especially in its capacity to identify or to retrace people in public areas by using facial recognition (Sanchez-Graells, 2024a).

The consequences for the right to privacy thus go further than the traditional view of privacy. Recurring themes in the debate on privacy in the digital space are whether and to what extent a person can manage to keep reasonable control over information that concern identity, movements and personal relationship. Biometric data comes with its own special problem as it is intimately attached to the subject. But the face or fingerprint cannot normally be changed after illegal disclosure like a password or ID Number. The data can also potentially be utilized multiple times against future data once it is put into a biometric database. The gathering of biometric information therefore can result in a constant, as opposed to just ephemeral, interference with privacy (Robles, 2020).

The issue may become acute for example if there is biometric surveillance in public places. It is hard to argue that a citizen has no privacy interests in data that can be collected by the government about him in the public marketplace when the technology permits the government to track the movements of all people passing by a specific place. It is not just the fact that a picture has been acquired into the legal context, but is the added analytical step carried out on the picture. Facial recognition produces a novel representation of biometric data, based on the distinctive features of the face. For this reason, its legal evaluation can't be boiled down to the guidelines that govern traditional pictures or CCTV monitoring (Simmler & Canova, 2025a).

Biometric surveillance also begs questions about ends of police discretion. Criminal Procedure has always been at the center of balancing the interests of a state during a criminal investigation against personal rights. Gives guidance when officers are allowed to search, to seize, to interrogate and to gain evidence, to detain or obtain it. The current usage of biometric technologies brings these traditional classifications into question since people can be monitored without the need to actually interact with them and, in some cases, without any suspicion that foul play might be afoot. The information collected by a facial-recognition system at a public place could pertain to hundreds or thousands of people, including those having no connection to the investigation. It is then possible to



Vol. 4 No. 2 (February) (2026)

look beyond suspect-led identification using the technology to provide pre-crime population-level screening (Purshouse & Campbell, 2022a).

It can't only be a matter of privacy. Biometric dent for errors can have consequences for liberty and fairness of criminal proceedings. Misalignment might lead to police doubt against an innocent person and disparities in officer performance by group might have discriminatory effects. Furthermore, people aware that they are to be identified through biometrics in their movement and public life may change their otherwise legitimate actions. This can have a chilling effect on, inter alia, the exercise of the right to freedom of expression, association and peaceful assembly. The cases provide a perspective of the necessity to consider biometric surveillance as a matter of criminal procedure and constitutional governance, and not simply a matter of technological efficiency (Rezende, 2020).

This enquiry is relevant in the Pakistani context. The dignity of man and the privacy of home is inviolable as affirmed in Article 14 of the Constitution of Pakistan subject to law. The protection in the constitution is prior to the current biometric technologies, but it is not sensibly limited to the technologies of the times of its adoption. A significant digital and biometric infrastructure has also been developed in Pakistan and there is greater integration of surveillance technologies in law-enforcement and public-security sectors. Pakistani scholarship has recently pointed out the absence of significant legal safeguards for those who have their data collected and processed in regards to its rapid propagation through technology (Butt et al., 2024a).

In view of this, this paper explores the status of criminal procedure law regarding the constitutionality of the use of biometric surveillance system, and the development of related legislation in Pakistanis well as internationally. It queries about the adequacy of existing criminal procedure and privacy principles to support biometric surveillance and if not, the extent of current application of such principles and how these should be complemented to provide adequate safeguards. The core of the argument is that biometric monitoring is not, as some have suggested, a per-se illegitimate technique; its countervailing value to law enforcement is not, as others have argued, automatically legitimizing. Whether lawful or not should be contingent upon a clear legal basis, an investigative purpose that is legitimate and demonstrable necessity, procedural safeguards, independent oversight and an effective remedy against its misuse.

Hence, this paper has a right-based view of criminal procedure. It regards privacy as a constraint on how policing and investigative powers are to be exercised, rather than a problem for effective policing. It is based on a proposition that the more techno-capable the State is in identifying and monitoring people the more precise the legal controls need to be on that techno-equipment. It is, therefore, the goal to identify those circumstances regarding the use of biometric surveillance that is compatible with respect for privacy, due process and the rule of law.

2. Conceptualizing Biometric Surveillance and the Right to Privacy

Biometric surveillance is the regular gathering of individuals' biological or behavioral traits to identify, verify or monitor them. The most common examples are fingerprint, face and voice recognition or DNA profiling. While the techniques vary technically and legally, they share an important feature, they link a physical or behaviors; to a recognizable person. This link provides a perception of a particular legal nature to biometric information, and this puts questions in the forefront that, to a lesser extent, also exist with information that does not include biometrics.



Vol. 4 No. 2 (February) (2026)

The first distinction which should be made is the distinction that should be made between the biometric identification and ordinary observation. While a standard camera can capture a person's picture at a public area, biometric identification technology can turn that picture into an identifier to search. It's a big difference. An observation records an event, while the identification of an individual by its biometrics can identify it and link it with information in other databases. The repetition of the process may make it possible to reconstruct the individual's movements and association, where the process is repeated over time. The question at issue is thus not so much one of whether or not a state may view an individual in public but whether a state may systematically identify and catalogue that individual (Janjeva et al., 2023).

This distinction also calls into question the traditional conception of the public/private divide. Through the ages, privacy has been traditionally equated with the home, correspondence and other areas where individuals expect to enjoy privacy. Digital surveillance also shows how privacy can be violated with the collection and analysis of public-information. A pedestrian may be aware that he or she is subject to the view of others in a railway station or shopping area but may not be aware that he or she is being "automatically identified", "compared with images in a database" and being retained for a longer period of time. The extent of monitoring and its ability to analyze these data can turn what may otherwise be innocent monitoring practices into very informative personal data (Lynch, 2024).

Biometric Data are especially sensitive since they are about the individual and tend to be rather permanent. The identifier can be changed if the normal database with the username is hacked. A photo, fingerprint or pattern of the irises of the eyes may not normally be replaced or substituted. The repercussions of abusing them can then be far reaching from the initial investigation. This feature is conducive to affording a greater level of protection, especially in instances where biometric data is obtained from individuals not suspected of committing criminal offenses.

The most obvious current use of what is actually facial recognition is when you see it on the computer. The real-time facial recognition technology can match the images taken by the cameras with the reference database in nearly real time. Facial recognition can also be used to find faces in videos after an event has been recorded. With either form there is the potential for function creep. What might have been a good idea to gather for a specific purpose could later be applied for a different purpose. An infrastructure for routine monitoring could, for instance, be gradually developed from a system put in place to find persons wanted for more serious offences. However, the notion of purpose limitation is at the heart of the legitimate use of biometric monitoring (Jansen et al., 2021).

The functioning of AI adds to the intricacy of privacy issues. A biometric system is not simply a system that stores information but rather three that makes a probabilistic determination of identity. Image quality, database structure and algorithmic design and demographic characteristics can impact the result. Thus, a seemingly neutral technological contest can have an element of uncertainty. When the police response is inevitable based upon such a match, the implications for liberty as a result of technological mistakes can become issues for individuals (Smith & Miller, 2022b).

It is therefore important to take a view of the right to privacy as covering at least three related interests. The first is informational privacy related to the collection and applying of information related to an individual. The second is that of decisional and personal autonomy, which shields people from unduly intrusive interference by the state in their personal lives. The third is freedom from pervasive monitoring, an increasingly



Vol. 4 No. 2 (February) (2026)

significant issue where the surveillance can take place on an ongoing basis and even without being apparent.

The latter is particularly relevant to the area of criminal procedure: Traditionally, the police investigation starts with an offence, and then goes to establish who the perpetrator was. Mass biometric surveillance can turn these flows on its head, it can start by locating everyone in a specific place and then identify if some people match an investigative interest. This has constitutional implications as it alters the dynamics between suspicion and surveillance. Rather than justification for surveillance being suspicion, suspicion could be used as a justification for surveillance itself (Qandeel, 2024).

Not necessarily all biometric processing is incompatible with the concept of privacy. Fingerprints may have a proper evidence and identification use when taken with a lawful arrest of an individual for a serious offence. DNA comparison likewise may be upheld if its collection is allowed by law and is proportionate to the investigation. The difference, of great if not decisive, importance lies thus between targeted biometric investigation and generalized biometric surveillance. Both of these might be compatible with constitutional rights if regulated appropriately, but the latter one needs relatively greater justification (Murphy, 2022).

Throughout this paper, the underlying concept is therefore that biometric surveillance is a particular and unique form of interference in the right to privacy, allowing for the transformation of a person's presence into an identity that can be searched. Therefore, a scheme to assess its legality should reflect the sensitivity, longtermness, scale, and technological uncertainty of the processing of biometrics.

3. Legal Basis for Biometric Surveillance under Criminal Procedure

Legality of biometric surveillance starts with an evidential basis for powers of investigation. The state cannot limit freedom of expression on the grounds that a certain technology is beneficial for policing. These two things are different: the capacity to do work and the authority to do work. This distinction is especially crucial where biometric monitoring would enable the identification of a person, who does not otherwise undergo biometric monitoring, and is not suspected of a crime.

The principle of legality is that the relevant legal rule/matter must be open, transparent and capable of being foreseen. It should be possible for individuals to have an awareness, at least in broad terms, when their biometric information is being collected, by whom, for how long and for what purposes it is then to be used. The broad administrative discretion is a problem in that the practical limitations of surveillance are left to the agencies and not only publicly enacted laws. Legal specificity is a recurring element in the scholarship on the use of facial-recognition technology by the police (Galič & Stevens, 2023a).

A criminal procedure model should thus make a distinction between the various types of biometric surveillance. The selection of targeted collection from a person made up for and/materially differs from mass/indiscriminate identification in public places. Also, one-off evaluation after a particular crime event is less invasive than real time facial evaluation. The legal threshold to be applied should be commensurate with the interference (Raposo, 2024).

There is, of course, a very important measure: judicial authorization. In cases where biometric surveillance is especially intrusive, an independent judicial or other authority should consider the justification prior to initiating the surveillance. The list should include the nature of the offence being suspected, what exactly the investigation will be looking for, the technology to be used, the area and time to be monitored, the database used to match up biometrics and the desired storage time. These types of requirements



Vol. 4 No. 2 (February) (2026)

can help make sure that general authorizations remain general and do not create open-ended investigative powers (Mitsilegas et al., 2023).

In this regard, Pakistan's Investigation for Fair Trial Act 2013, which recognizes the significance of judicial control over particular innovative investigative strategies, is applicable. The bill proves that surveillance that impacts on the fundamental rights can also be made to have a warrant process. However, the use of biometric identification raises issues which can only partially be solved by a law principally dealing with the interception and the surveillance. For instance, in case of a facial-recognition search, the biometric processing of hundreds of uninvolved persons could be conducted without any communication being intercepted (Khan et al., 2025).

The Code of Criminal Procedure 1898 also provides the underlying procedural parameters to criminal investigation but comes in a technological landscape very different from the current digital landscape. Traditional wording of provisions regarding investigation, search and evidence do not explicitly provide rules for automated biometric identification and algorithmic matching and large-scale biometric databases. Thus, a reliance on general investigative power brings uncertainty about the nature of police power.

The Prevention of Electronic Crimes Act 2016 offers another applicable Act, though with the main focus on electronic offences and capabilities grounded on investigation of electronic offences. The end consequence is a fragmented legal landscape in which certain laws are used to govern specific activities, but fail to create a comprehensive system for the entire life cycle of biometric data (Fussey & Webster, 2023).

At least four stages in the system of management should be regulated by law: collection, processing, retention and disclosure. Lawful authority should be needed to make the collection. There needs to be a specified investigation purpose for processing. Document retention should only be maintained for reasonable periods as long as necessary for that purpose. There should be a legal basis for disclosure / transfer. If these stages are not separated and treated as a single police power there would be great possibilities of secondary use and institutional abuse.

Private surveillance systems should also be subject to the right of legality. The constitutional safeguards should never be taken away because of the disconnection between the fact that a private entity was the first to collect biometric information and the subsequent receipt of that information by the law-enforcement agencies. No governmental processing of information that follows the initial sharing should be beyond the bounds of public authorities' accountability.

Lastly, work within the legal boundaries along with a great remedy. People need to be able to contest any unlawful collection or use of biometric data in some way. In the absence of remedies, statutory limitations run the risk, becoming merely declaratory. Meaningful consequences for an unlawful surveillance, such as judicial review, deletion orders and correction of inaccurate records of biometric information or exclusion of evidence illicitly acquired or appropriate compensation can be provided.

he proper legal angle therefore is to regard the same as regulated permissibility of the law. Biometric surveillance should be allowed in the criminal procedure if there is an investigative need but cannot be a substitute for statutory authority given the presence of technology. Brighter the capability to monitor, tighter the law should be and vice versa.

4. Necessity, Proportionality and Procedural Safeguards

The very fact that there is a legitimate authority to use biometric surveillance is insufficient to make every use of the power legitimate. There is a second stage analysis



Vol. 4 No. 2 (February) (2026)

needed: whether the specific use of biometric technology is “necessary and proportionate to the investigation.” This is very important in the field of constitutional criminal proceeding as a criminal measure can be taken for a legitimate cause yet still be a too great burden on individual freedoms. As facial recognition systems are becoming more sophisticated, it has become even more crucial of an assessment (Murray, 2024).

Just showing that biometric surveillance might help an investigation isn't enough. Police must determine that the technology is reasonably needed to accomplish a legitimate investigation and that alternative methods not as intrusive exist that can still allow a legitimate investigation to be achieved. An important police authority should not therefore use large scale facial recognition, simply because it is more efficient and quicker to deploy than traditional investigations. That question should be whether in specific situations there is a need for further interference with privacy. Recent research into retrospective facial recognition has rightly focused on exactly this challenge, while this technology can significantly extend investigative possibilities, it also presents a greater difficulty in assuring that it is actually necessary for surveillance (Sanchez-Graells, 2024b).

When assessing proportionality, the seriousness of the suspected offence, the nature of the biometric technique, the number of people affected, the duration of the surveillance and the consequences of possible error have to be taken into consideration. A one-to-one facial recognition of someone who is reasonably suspected of a serious crime is not the same as a “blanket” system wherein a person is scanned every time they make an appearance at all four corners of a public gathering spot. The latter could conceivably impact thousands of people not involved in the inquiry, and for whom there should be a much greater standard of proof.

This assessment should take account of the principle of data minimization. The law-enforcement authorities must only obtain the necessary biometric information which is relevant to the investigation. If everyone is targeted, this can open the door for a criminal investigation to be degenerated and become generalized ‘population surveillance’. The laws and regulations should therefore differentiate among the data of suspects, witnesses and persons who are incidentally captured by monitoring. Normally, the information about persons, who are not important in the investigation, should be deleted after a defined time period.

A similar issue is retention. The privacy interference does not come to an end when the biometric information is first collected. They can be continuously stored for future searches and potential other uses. The retention period should also, therefore, be related to the purpose of the information obtained. If a person is no longer a suspect, they should not be held any longer unless for a specific, lawfully reviewable reason. It would be hard to make a permanent database with biometric data of all the civilian people who are innocent justifiable.

Accuracy is another key thing to look at. No Biometric identification is infallible determination of identity; it is a technologically based assessment, and as such, could potentially be wrong. If there is a wrong match an innocent person will be the target of police. In particular, this risk is grave in situations where consequences of an interaction with the criminal legal system are based on biometric information, such as arrests, searches or coercive action. The academic literature to this end has, therefore, been focused on recognizing automated recognition as an investigative aid - rather than a determination of identity that should be accepted as the right answer (Purshouse & Campbell, 2022b).

This concern is what prompted the need for human verification. Before coercive action is



Vol. 4 No. 2 (February) (2026)

taken an automated match should normally be independently evaluated by a trained officer and, as required, backed up by further evidence. Technology error is not precluded by this requirement, but renders an algorithmic output not the 'silver bullet' replacement of human judgement. It also upholds the traditional criminal-procedure rule that state coercion can only rely on some sort of evidentiary basis that can be challenged. There's an additional layer of proportionality that is algorithmic bias. If the biometric system functions differently for different groups of people, it may increase the risk of particularly disadvantaged groups if it is put in place. Thus, the legal assessment should include testing for accuracy before and while in use to determine differential error rates. The issue goes beyond a purely technical one. Algorithms with a systematic tendency to lead to a higher rate of false investigatory algorithms on the investigation of certain individuals can also raise equality and non-discrimination concerns in addition to privacy concerns (Smith & Miller, 2022c).

Transparency would also be an aspect of procedural safeguards. Subject of biometric supervision shall be granted in case of disclosure which takes into account the investigation, the opportunity to challenge the legality and reliability of the biometric supervision process. When in a criminal process any biometric evidence is outlined, the stage should be set for the Defense to put questions regarding how the image or sample was acquired, the reliability of the system and the potential for error. There should be no automatic evidential value given to an opaque, technological process simply because it's called "AI."

Independent oversight must therefore be provided. Internal police rules can give the operational rules for conducting the surveillance but they are not enough if there are serious constitutional risks arising from the surveillance system itself. Authorization and a supervisory authority that is independent from the deployment of the biometric system should be granted to audit the system, ensure compliance, investigate complaints, and force corrective action. Continuous supervision should also involve regular evaluations on the continued need for the technology to serve the intended goal it was designed for (Manojlovic et al., 2025).

Lastly, there needs to be real as opposed to symbolic repercussions for illegal biometric monitoring. The right for people to ask for the deletion or correction of information that was illegally processed and/or, if applicable, judicial relief or compensation. However, courts should also be given sufficient authority to remedy non-compliant evidence obtained after serious infringements of statutory and/or constitutional guarantees of fair treatment in a criminal process.

Thus, it's controlled necessity. The intrusiveness and scale of biometric surveillance must be proportionate and lawfully justified by law enforcement so that the more intrusive and on a larger scale, the greater the justification required. This will maintain the intrinsic worth of biometric technology without allowing technological effectiveness to stand alone as a reason for its increased power.

5. Comparative Legal Perspectives

As comparative experience shows, biometric surveillance is more being recognized as a specific regulatory issue than merely a new method of police surveillance. Despite the variety of legal structures of the constitution there are three common principles in legal systems relating to biometric surveillance which could be deduced: a legal basis for its use needs to be sufficiently precise; biometric surveillance should be necessary and proportionate; and mechanisms for protecting against potential error or misuse are to be given to citizens in the course of its processing.



Vol. 4 No. 2 (February) (2026)

Looking at the European approach, it's a good example. Biometric data, (data used to identify a person uniquely), is notably covered by the European data-protection legislation as particularly sensitive data. This method mirrors an understanding that biometric processing generates a new type of personal information and not simply to aid investigators in analyzing the information they already have. Moreover, fundamental rights can be affected by the use of facial-recognition technology at each stage of the process: from the acquisition of the image to the creation of the biometric template to the comparison and for this reason, it was recently argued that the use of the technology should be properly regulated by law (Simmler & Canova, 2025b).

The European experience also shows how crucial it is to differentiate the existence of a technology and the legal basis on which to use it. Not only is facial recognition technically possible, but it is not yet legal grounds for police to use. Regulation needs to set the schedule as to when and for what purpose, against whom and with what safeguards, the technology can be applied. The new European framework therefore focuses more and more on risk classification and basic rights and restrictions for highly intrusive applications of biometric technologies.

Yet another example is United Kingdom. But the use of police facial recognition has been the subject of much academic study, which has raised concerns about the ease with which the technology could be used to limit the use of certain technologies capable of quickly recognizing a person over a large area, and the draconian implications of using general policing and surveillance powers for such regulation. This experience evidence shows that using an existing statutory framework created for the traditional way of surveillance might not be enough to give the targets sufficient clarity on automated biometric identification (Purshouse & Campbell, 2022c). The overarching message for Pakistan is that legislation needs to have in mind the capabilities of biometric technology; they should not be expected to follow along with general police powers, which can – and have so far – adapted to technological change.

The USA has a more disjointed approach. Besides state-level biometric privacy laws, constitutional safeguards on searches or governmental surveillance also exist. Academic studies have focused on the potential of facial recognition that generates a novel form of surveillance, that can monitor, track and identify people across interacting cameras and databases (Urquhart & Miranda, 2022). The essence of this is the exercise of force of nature of the ordinary doctrine of constitution: it can be even more adapting to the rapid pace of technological development than the prior legal categories.

Comparative scholarship also reveals the need for the regulation of algorithmic systems of decision-making. With facial recognition is not just the sensing of the information, there is also an assessment made regarding identity. Thus, issues of accuracy, transparency and discriminatory impact are a concern in the legal analysis. More recent scholarship suggests that systems utilizing biometric data can pose challenges to criminal-procedure rights due to automated systems that can shape investigations and impact criminalized people without offering them sufficient means to understand or question the process (Bass, 2022).

Another comparative lesson deals with the balance between privacy and public security. Good investigation should never be viewed as conflicting with the need for privacy protection. Finding a way to adequately control biometric identification can help investigations, minimize subjective identification and even save from an incorrect accusation. The challenge comes when such a technology is used without discrimination or held longer than the lawful use of the technology. Comparative regulation thus increasingly is inclined towards a risk-based approach than towards either unrestricted



Vol. 4 No. 2 (February) (2026)

deployment or prohibition.

Comparative experience indicates that there are three key reforms for Pakistan. First, and most obvious, there should be a more specific legal reference to biometric surveillance, rather than to more general investigation powers. Secondly, previously approved use of intrusive biometric techniques, with evidence to demonstrate the need, should be required. Third, the legislation ought to deal with the complete life cycle of the information – from its collection stage to its processing, storage, disclosure, and deletion (Rana & Iqbal, 2025).

Overall, the comparative class is a lesson in adaptation of the law. Criminal procedure should not be technologically neutral (in the sense of differences between technologies). There is a level of intrusion involved in consolidating a fingerprint of an identified suspect and a retrospective facial search of CCTV footage compared to real-time facial recognition as people come into a public area. These differences should be respected in law and safeguards should be respected proportionately to the capability and risk of the various techniques.

6. Biometric Surveillance under Pakistani Law and Proposed Reforms

While the constitutional structure of Pakistan increasingly forms a basis for privacy protection, there is no yet very detailed regime of biometric surveillance. The dignity of man and privacy of the home is guaranteed by Article 14 of the Constitution and legality, liberty and equality is strengthened by Article 4, 9 and 25 of the Constitution. The problem is that today's biometric surveillance is done much more through the informational and technological process and not through the traditional physical intrusion. This means that a modern understanding of privacy needs to acknowledge that any collecting, identification, storage, and automated processing of biometric data can impact individual rights, even without physical searches (Butt et al., 2024b).

The system of laws in Pakistan is still disjointed. Investigation for Fair Trial Act 2013 is an important piece of legislation that regulates certain types of surveillance with judicial approval and the Prevention of Electronic Crimes Act 2016 is legislation which covers electronic crimes and powers of investigation. Both laws however, fail to provide an all-encompassing regulatory framework for the entire life cycle of biometric identification. The fact that there is no provision to ensure that biometric information is only collected from those suspected of committing a crime is especially important as this information can be collected from people who are not suspected of an offence and retained or searched for other crime investigations. A large disconnect between the increasing surveillance infrastructure and lack of a cohesive legal framework on the collection, retention, sharing, and judicial oversight of such data has also been noted in recent research conducted in Pakistan (Haq, 2024).

The Personal Data Protection framework proposed is relevant, but it cannot be considered a full solution to the problem of criminal procedure. Data protection covers the use of information while criminal procedure covers the use of investigative power. These functions overlap but differs in some aspect. For a police biometric search to be legal, there must then be a valid criminal-investigative purpose as well as the appropriate data-governance protections. Comparative studies have shown that a lack of coordination between the criminal procedure and data protection can result in gaps in oversight and uncertainty about what is the relevant standard of law (Galič & Stevens, 2023b).

Pakistan should therefore have a separate law enforcing biometric monitoring system. First, the law must specify what kinds of biometric surveillance are allowed, and clearly differentiate between a person being identified and the general monitoring of public



Vol. 4 No. 2 (February) (2026)

spaces. Secondly, the intrusive surveillance should be, in the ordinary, subject to a prior judicial authorization. The suspected offense, purpose of the investigation, geographic and/or temporal boundaries, and the technology used and planned retention period should be identified in the application (Domingo Jaramillo, 2025).

Thirdly, the purpose limitation and data minimization principle should be made part of the law. Biometric information should only be taken where there is some reasonably necessary criminal-investigative purpose. Normally the information related to persons eliminated from suspicion should be deleted and not stored indefinitely. Second use should be subject of independent legal justification (Galič & Stevens, 2023c).

Fourth, there should be technical and institutional auditing of biometric system. Authorities shall evaluate the accuracy, demographic performance, false-match rates and the security and retention of databases. The mere occurrence of an algorithmic match should not be deemed to be an adequate reason for arrest or other coercive measures. There must be still a need for human verification and corroborating evidence (Urzenitzok, 2025).

Fifthly, the framework must be accompanied by effective remedies. Persons should have the right to contest any illegal collection, the right to correct or delete any inaccurate biometric information and the right to seek a court order to stop any use of surveillance beyond the power of the statute. In the context of criminal proceedings, courts should have powers to deal with the use of unlawfully obtained biometric evidence. (Omid & Soren, 2025).

Lastly, there needs to be parliamentary and independent control over the operations in addition to operational regulation. Records of deployment, authorization, search and retention of data should be kept by the agencies using biometric technologies. Independent review would allow the idea of the technology first being used for exceptional criminal investigations to become a routine matter of population surveillance to be identified.

The goal should not be to dissuade legitimate technological innovation. Biometric identification can be of real value in the process of criminal identification, especially in serious offences, where the traditional means of identification are not satisfactory. The goal, rather, is to make sure technological capability is kept in subservient position to constitutional legality. Recent scholarship from Pakistan shows that there should be legal protections in place to match the fast-paced development of biometric identification and surveillance, and not merely piecemeal regulations.

The focus in Pakistan should therefore be to shift from an implicit model where perhaps the general investigative powers may suffice to justify the use of biometric surveillance to an express model based upon legality, necessity, proportionality, judicial oversight, accountability and remedy. This kind of reform will safeguard privacy rights without taking any lawful investigation techniques away from law-enforcement agencies.

7. Conclusion

Using powerful identification technologies without turning the legitimate investigation process into one of indiscriminate monitoring is a hard, but necessary, legal question for the criminal justice today. The solution cannot be a full ban on technology, or an unlimited discretion for the police. Biometric technologies can be used in a legitimate way in the detection and investigation of crime, however, must be subject to constitutional and procedural limitations.

This paper's main thesis is that biometric surveillance represents a very special form of interference with privacy as it turns the physical attributes into data that can be searched



Vol. 4 No. 2 (February) (2026)

and stored over a prolonged period. Presuming the presence of a person in a public place is not alone sufficient reason for unrestricted biometric identification. The purpose, extent, duration and impact of the surveillance should be taken into account when assessing whether it is legal.

Five principles are of major importance as far as criminal procedure is concerned. There must be clear statutory authority to be legitimate. The need must be for a genuine investigation. Proportionality imposes the obligation for the level of intrusiveness of the surveillance to reflect the gravity of the crime and the purpose of the investigation. Judicial and independent oversight are needed to ensure accountability. Remedy demands that people have a real way to contest collection and use of their data if it is illegal.

Although there are some foundations to these principles in Pakistan's current legal system, it is disjointed. A unified constitutional protection of privacy, surveillance legislation and electronic-crime regulation should be used to create a regulatory framework specifically for biometric investigation. Targeted use of biometric identification should be differentiated from mass surveillance, judicial oversight should be put in place for intrusive uses, retention and secondary use should be limited and there should be human verification of algorithmic matches and effective remedies.

The end goal should be to make sure technological advancement isn't a means of runaway government. Legitimacy of a democratic criminal-justice system is not just a function of its ability to identify criminals. It should also show that the measures taken to ensure security are compatible with respect for privacy and dignity, and equality and the rule of law. This means that although biometric surveillance might be compatible with criminal procedure, it must be done in accordance with the law and not in violation of it.

References:

- Bass, A. (2022). Smile! You're on Camera: Police Departments' Use of Facial Recognition Technology & the Fourth Amendment. *Loy. LAL Rev.*, 55, 1053.
- Butt, M. F., Saleem, H. A. R., Hashmi, M. A. I., & Bano, N. (2024a). THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN. *ASSAJ*, 2(4), 1449–1458.
- Butt, M. F., Saleem, H. A. R., Hashmi, M. A. I., & Bano, N. (2024b). THE RIGHT TO PRIVACY IN THE AGE OF SURVEILLANCE: LEGAL PROTECTIONS IN PAKISTAN. *ASSAJ*, 2(4), 1449–1458.
- Domingo Jaramillo, C. (2025). *Risks of remote biometric identification systems in public places for law enforcement purposes under the AI Act regulation*.
- Fussey, P., & Webster, C. W. R. (2023). Independent report on changes to the functions of the Biometrics and Surveillance Camera Commissioner arising from the Data Protection and Digital Information Bill. *Home Office*, 6.
- Galič, M., & Stevens, L. (2023a). Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law. *New Journal of European Criminal Law*, 14(4), 459–478.
- Galič, M., & Stevens, L. (2023b). Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law. *New Journal of European Criminal Law*, 14(4), 459–478.
- Galič, M., & Stevens, L. (2023c). Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law. *New Journal of European Criminal Law*, 14(4), 459–478.
- Haq, A. H. U. (2024). The right to privacy & personal data protection: An analysis of



Vol. 4 No. 2 (February) (2026)

- Pakistan's proposed personal data protection bill. *UCP Journal of Law & Legal Education*, 2(2), 01–27.
- Janjeva, A., Calder, M., & Oswald, M. (2023). *Privacy Intrusion and National Security in the Age of AI: Assessing proportionality of automated analytics*.
- Jansen, F., Sánchez-Monedero, J., & Dencik, L. (2021). Biometric identity systems in law enforcement and the politics of (voice) recognition: The case of SiiP. *Big Data & Society*, 8(2), 20539517211063604.
- Khan, S. M., Yaqoob, A., Khokhar, J. A., & Malik, F. (2025). An examining the legal framework for criminal investigations in Pakistan: Gaps and reform needs. *The Critical Review of Social Sciences Studies*, 3(1), 1957–1969.
- Lynch, N. (2024). Facial recognition technology in policing and security—Case studies in regulation. *Laws*, 13(3), 35.
- Manojlovic, D., Lazic, D., & Deckovic, S. (2025). POLICE SURVEILLANCE UNDER THE DRAFT INTERNAL AFFAIRS LAW: FULL ENVIRONMENTAL SURVEILLANCE-GENERAL SUSPICION OF CITIZENS OR SUSPECTS. *Economic and Social Development in Bipolar and Multipolar Environment (Book of Proceedings)*, 106.
- Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2023). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, 29(1–2), 176–211.
- Murphy, E. (2022). Conceptions of consent, family and jurisdiction in forensic genetic genealogical searches. *Law, Practice and Politics of Forensic DNA Profiling: Forensic Genetics and Their Technological Worlds*, 143.
- Murray, D. (2024). Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of the human rights law framework. *The Modern Law Review*, 87(4), 833–863.
- Omid, P., & Soren, F. (2025). The digital double: Data privacy, security, and consent in AI implants. *Digit J Eng Sci Technol*, 2(1), 105.
- Purshouse, J., & Campbell, L. (2022a). Automated facial recognition and policing: A Bridge too far? *Legal Studies*, 42(2), 209–227.
- Purshouse, J., & Campbell, L. (2022b). Automated facial recognition and policing: A Bridge too far? *Legal Studies*, 42(2), 209–227.
- Purshouse, J., & Campbell, L. (2022c). Automated facial recognition and policing: A Bridge too far? *Legal Studies*, 42(2), 209–227.
- Qandeel, M. (2024). Facial recognition technology: Regulations, rights and the rule of law. *Frontiers in Big Data*, 7, 1354659.
- Rana, A., & Iqbal, A. (2025). Privacy and Surveillance: Legal and Technical Perspectives. *UCP Journal of Law & Legal Education*, 3(2), 01–28.
- Raposo, V. L. (2024). 'Look at the camera and say cheese': The existing European legal framework for facial recognition technology in criminal investigations. *Information & Communications Technology Law*, 33(1), 1–20.
- Rezende, I. N. (2020). Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, 11(3), 375–389.
- Robles, J. (2020). Patel v. Facebook, Inc.: The collection, storage, and use of biometric data as a concrete injury under BIPA. *Golden Gate UL Rev.*, 50, 61.
- Sanchez-Graells, A. (2024a). Responsibly buying artificial intelligence: A 'regulatory hallucination.' *Current Legal Problems*, 77(1), 81–126.
- Sanchez-Graells, A. (2024b). Responsibly buying artificial intelligence: A 'regulatory



Vol. 4 No. 2 (February) (2026)

- hallucination.’ *Current Legal Problems*, 77(1), 81–126.
- Simmler, M., & Canova, G. (2025a). Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*, 56, 106092.
- Simmler, M., & Canova, G. (2025b). Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*, 56, 106092.
- Smith, M., & Miller, S. (2022a). The ethical application of biometric facial recognition technology. *AI & SOCIETY*, 37(1), 167–175. <https://doi.org/10.1007/s00146-021-01199-9>
- Smith, M., & Miller, S. (2022b). The ethical application of biometric facial recognition technology. *Ai & Society*, 37(1), 167–175.
- Smith, M., & Miller, S. (2022c). The ethical application of biometric facial recognition technology. *Ai & Society*, 37(1), 167–175.
- Urquhart, L., & Miranda, D. (2022). Policing faces: The present and future of intelligent facial surveillance. *Information & Communications Technology Law*, 31(2), 194–219.
- Urzenitzok, P. (2025). Algorithmic Accountability in Facial Recognition Technology: Addressing Bias and Transparency in European Law Enforcement Applications. *SPLITLAW*, 381.