Face Authentication and Access to Welfare Services

Kavita V. Nair[1]*

[1] University of Hyderabad, Hyderabad, India
* Correspondence: University of Hyderabad, Hyderabad, India.

https://doi.org/10.53104/curr.res.law.pract.2026.03002

Citation: Kavita V. N. (2026). Face Authentication and Access to Welfare Services. *Current Research in Law & Practice*, *4*(1), 11-17.

Abstract: Face authentication is becoming part of welfare service delivery in India through the Aadhaar system. It may help confirm identity, reduce paperwork, and support people who cannot easily use fingerprints or OTP-based verification. Yet welfare services are closely linked to basic needs such as food, pension, health care, subsidies, and cash support. When face authentication fails, the result may be more than a technical delay. It may stop an eligible person from receiving support. This paper examines face authentication from the perspective of welfare access, privacy, equality, and dignity. It argues that face authentication should remain one method of identity checking, not the only door to public benefits. A fair welfare system must provide backup methods, clear exception handling, simple complaint channels, and strict limits on data use. The main question is not only whether the technology can identify a person, but whether it helps eligible people receive welfare without fear, delay, or exclusion.

Keywords: face authentication; Aadhaar; welfare services; biometric identity; digital exclusion; privacy

1. Introduction

Face authentication has become an important part of digital identity use in India's welfare services (Unique Identification Authority of India, n.d.a; n.d.b). It is connected with the Aadhaar system, which is widely used to confirm identity when people receive public benefits. In official thinking, biometric authentication can help reduce false claims, identify the right beneficiary, and make welfare delivery faster. This makes the technology appear useful, especially in a large welfare system that serves many people across different regions.

Yet welfare services are not the same as ordinary online services. They often involve food rations, pensions, health support, subsidies, or cash benefits. For many people, these services are closely linked to daily survival (Totapally, S., Sonderegger, P., Rao, P., Gosselt, J., & Gupta, G., 2019; Khera, R., 2017). If face authentication works smoothly, it may save time. If it fails, the problem can become serious. A failed match may delay a pension payment, block access to food support, or force a person to visit an office again. For poor, elderly, disabled, or digitally less skilled users, this burden is not small.

The key issue is not only whether face authentication is accurate. The more important issue

is who suffers when the system does not work. A welfare beneficiary may not know why authentication has failed. The person may not have a smartphone, stable internet, updated records, or enough help from local officials. In such cases, technology does not simply check identity. It may become a gate that decides whether a person can receive a benefit.

2. Aadhaar-Based Welfare Delivery and the Role of Face Authentication

Aadhaar is a basic part of India's digital welfare system. It gives each enrolled resident a unique identity number and connects that identity with demographic and biometric information. In welfare delivery, Aadhaar is used to check whether the person asking for a benefit is the person recorded in the system. UIDAI describes Aadhaar as a tool for social and financial inclusion and for the delivery of subsidies, benefits, and services. This shows that Aadhaar is not only an identity document. It has also become part of public administration (Unique Identification Authority of India, n.d.a).

Face authentication works inside this larger system. It is not the same as Aadhaar itself. Aadhaar is the identity base. Authentication is the process of checking that identity. Face authentication is only one way to complete that check. UIDAI explains face authentication as a one-to-one match. The live facial image captured during authentication is compared with the facial image stored against the person's Aadhaar number. In this sense, face authentication does not create a new welfare right. It only decides whether a person can pass one step before receiving a service (Unique Identification Authority of India, n.d.b).

This difference is important. When Aadhaar is used in welfare delivery, the main goal should be to help the correct person receive the correct benefit. When face authentication is used, the goal should be the same. The technology should support access, not replace the welfare duty of the state. If officials treat face authentication as the only proof of identity, the system may become too narrow (Unique Identification Authority of India, 2016; 2021). A person may be legally entitled to a benefit but still face delay because the camera does not capture the face clearly or the system does not return a successful match.

Aadhaar-based authentication is also linked to requesting entities and service providers. These bodies use Aadhaar details to verify identity when people seek services, subsidies, or benefits. This makes face authentication more than a technical step. It becomes part of the relationship between the citizen, the state, and the service provider. The beneficiary is often in a weak position because the person needs the service and may not know how the system works. For this reason, face authentication should be understood as a welfare governance issue, not only as a digital identity tool.

The role of face authentication should therefore remain limited and practical. It can help confirm identity in some situations. It can be useful when fingerprint authentication is difficult or when a field officer needs a quick identity check. Yet it should not become the only door to welfare services. In a welfare setting, the real test is not whether the system can produce a match. The real test is whether eligible people can still receive their benefits when the digital check does not work.

3. Why Face Authentication Appears Useful in Welfare Services

Face authentication appears useful because it gives welfare agencies another way to check identity. In many welfare settings, identity checking cannot depend on only one method. Fingerprint authentication may not work well for every person (Unique Identification Authority of India, n.d.c). Elderly people may have weak fingerprints. Manual workers may have worn fingers because of farm work, factory work, construction work, or other physical labour. Some people may also face difficulty because of injury, illness, or poor biometric quality. In these situations, face authentication can serve as an extra option.

Face authentication may also be easier for field-level delivery. A welfare worker may visit a village, a care centre, or a person's home. In such places, carrying

out a face check through a mobile device may be simpler than asking the person to travel to an office. This may matter for pensioners, disabled persons, or people living far from service centres. It may also help in health-related schemes where the person needs quick verification at the point of service.

The method may reduce some paperwork. In a paper-based process, the beneficiary may need to carry documents, submit copies, or wait for manual checking. These steps can delay access. They can also create room for mistakes. A face-based check may shorten part of this process if the system works well and if staff know how to use it properly. It can make the identity step faster, especially when the person's records are already linked with Aadhaar.

Face authentication may also help when OTP-based verification is difficult. Some beneficiaries do not have their own mobile phone. Some use a shared phone. Some numbers may not be updated in the system. Network problems can also stop an OTP from arriving on time. For such users, face authentication may offer another route. It should not replace all other methods, but it can reduce dependence on a single device, number, or document.

There is also a possible benefit in reducing local discretion. In some welfare settings, access may depend too much on the judgment of local officials or service agents. A clear identity check can reduce arbitrary decisions if it is used carefully. Yet this benefit has a limit. A digital check can also create new forms of control if officials refuse to use backup methods. The value of face authentication lies in making access easier, not in making welfare more conditional.

4. Authentication Failure and the Risk of Exclusion

Authentication failure may look like a technical problem, but in welfare services it can quickly become a problem of access. A face scan may fail because the camera is poor, the light is weak, or the internet connection is unstable. It may also fail because the person's Aadhaar photo is old or the face has changed because of age, illness, disability, injury, or hard living conditions. These are ordinary problems in real welfare settings. They should not be treated as signs that the person is not eligible.

The burden is often heavier for people who already depend on welfare support. A pensioner may not be able to visit the office many times. A daily wage worker may lose income if asked to return the next day. A person in a remote area may spend money on travel only to face another failed attempt. A person with low digital literacy may not understand what went wrong. For such users, repeated authentication is not a small inconvenience (Totapally, S., Sonderegger, P., Rao, P., Gosselt, J., & Gupta, G., 2019; Muralidharan, K., Niehaus, P., & Sukhtankar, S., 2025). It can become a real barrier to food, pension, health care, or cash support.

Face authentication can also create hidden inequality. The system may look neutral because it asks every person to pass the same digital check. Yet people do not stand in the same position before the system. Some have smartphones, stable internet, updated records, and family support. Others depend fully on local staff, service agents, or public offices. When the system fails, the second group has fewer ways to solve the problem. A rule that appears equal on the screen may affect vulnerable people more harshly in practice (Khera, R., 2017).

Local handling also matters. If an official treats a failed match as final proof that the person should not receive the benefit, the technology becomes a gatekeeping tool. The person may be told to update Aadhaar, come again later, or find another way to prove identity without clear help. This shifts the cost of system failure onto the beneficiary. A failed match should not become a failed right (Supreme Court of India, 2018). Welfare access should not depend on whether a machine gives a successful result at one moment.

Official rules already recognize the need for backup routes. UIDAI states that if an Aadhaar number has not been assigned, the person should be offered alternate and viable means of identification for receiving a subsidy, benefit, or service. It also notes that authentication failures may happen because of connectivity problems, biometric or demographic mismatch, OTP failure, device issues, or other

technical reasons. This means fallback methods are not an extra favour. They are part of fair welfare delivery.

For face authentication to be fair, every failed attempt should lead to a clear next step. The beneficiary should be told why the attempt failed, who can help, and what other proof can be used. Local staff should have the authority and duty to use exception handling. Paper identity, local verification, assisted verification, fingerprint, OTP, or other approved methods should remain available. The aim should be simple: no eligible person should lose welfare support only because face authentication did not work.

5. Consent, Privacy and the Unequal Position of Welfare Beneficiaries

UIDAI states that face authentication is consent based. It also explains that the live face image is matched with the facial image stored against the Aadhaar number. On paper, this means the user agrees before the face check takes place. In welfare services, consent is more difficult than this. A person who needs food ration, pension, health support, or subsidy may not feel free to refuse. The person may think that refusal will delay the benefit or lead to denial. In this situation, consent may exist in form, but it may not feel like a real choice.

The position of the welfare beneficiary is not equal to the position of an ordinary user in a private digital service. A private app user may leave the service if the terms seem unfair. A welfare beneficiary often cannot do that. The person may depend on the benefit for daily needs. The person may also depend on local officials, service agents, or field workers to complete the process. If the official says face authentication is needed, the beneficiary may accept it without asking questions. This makes the meaning of consent weaker.

Face data also needs careful treatment because it is linked to the body and identity (Ministry of Electronics and Information Technology, 2023). A password can be changed. A face cannot be changed in the same way. If face data or authentication records are used beyond the welfare purpose, the risk becomes serious. The user may not know who has access to the record, how long it is stored, or whether it may be used for another service later. For this reason, face authentication should be limited to the specific welfare purpose for which it is collected.

Privacy concerns are not only about data theft. They are also about control. A person receiving welfare support should not feel that the state can watch or track every service use through biometric records. Authentication should only confirm identity at the point where identity is needed. It should not become a way to build a wider record of movement, behaviour, or dependence on public support. The poor should not have to give up privacy in order to receive basic benefits.

The risk of wider use is not imaginary. In 2025, the Indian government announced rules that allow both government and non-government entities to use Aadhaar authentication for public-interest services, after approval. The stated purposes include ease of living and better access to services. This may support service delivery, but it also makes purpose limitation more important. If more bodies can seek Aadhaar authentication, the line between welfare access, service convenience, and identity tracking may become less clear.

A fair welfare system should treat consent as more than a button, a form, or a spoken yes. The beneficiary should be told why face authentication is being used, what data is being captured, whether another method is available, and what will happen if the person refuses. Consent should not be valid when refusal leads to silent exclusion. A person should be able to choose another approved method without fear of losing the benefit.

6. Constitutional and Legal Concerns

Face authentication in welfare services raises legal concerns because it connects biometric identity with access to basic benefits. In India, Aadhaar has been accepted as part of welfare delivery, but this acceptance is not without limits. Section 7 of the Aadhaar Act deals with the use of Aadhaar for subsidies, benefits, and services funded by the state. It also says that when an Aadhaar number has not

been assigned, the person should be offered alternate and viable means of identification. This point is important. Welfare access should not depend on only one identity method.

The Supreme Court of India's Aadhaar judgment in 2018 also shows this limited acceptance. The Court did not reject Aadhaar as a whole. It allowed Aadhaar use for welfare benefits under Section 7, but the judgment also placed Aadhaar within the wider concerns of privacy, legality, and proportionality. This means face authentication cannot be judged only by administrative convenience. It must also be judged by whether it respects basic constitutional values.

Privacy is the most direct concern. Face authentication uses biometric identity. A face is not like a password or a card. It is part of the person's body. If facial data or authentication records are used too widely, the person may lose control over personal identity information. Privacy protection should cover collection, use, storage, sharing, and deletion of data. The welfare purpose should remain clear and limited.

Equality is also involved. A system may use the same rule for every beneficiary, but the effect may not be the same for every person. Elderly persons, manual workers, disabled persons, people in remote areas, and people with poor digital access may face more difficulty in passing authentication. If these groups are more likely to face failure, the system may become unequal in practice. Equal treatment cannot mean forcing every person through the same digital gate when their real conditions are different.

Dignity is another concern. A person who receives welfare support should not be treated as suspicious by default. The state may verify identity to prevent fraud, but verification should not become humiliating or harsh. A beneficiary should not have to prove the same identity again and again only because a machine does not return a match. The process should respect the person's time, body, and need for basic support.

Fair procedure is also necessary. If face authentication fails, the person should receive a clear reason and a real chance to use another method. There should be no silent denial. A local officer should not be able to say only that "the system failed" and close the matter. The beneficiary should know where to go, what document to show, and how the benefit can still be received. Without this, face authentication may weaken the legal protection that welfare rights need.

The legal test should be simple. The state may use technology to improve welfare delivery. Yet the method must be lawful, limited, necessary, and fair. Face authentication should not collect more data than needed. It should not be used for purposes beyond welfare access. It should not deny benefits when a less harmful method can confirm identity. In welfare services, constitutional protection has meaning only when the person can still receive support after the digital check fails.

7. Safeguards for Fair Use of Face Authentication

Face authentication should be used as an option, not as the only method of identity checking. In welfare services, the main aim is to make sure that eligible people receive support. The method used to check identity should serve this aim. It should not become more important than the benefit itself. If face authentication is treated as the only door to welfare access, a technical failure may turn into denial of support.

Other methods should remain available. Fingerprint authentication, OTP verification, paper identity, local verification, and assisted verification should all have a place in the system. Different people face different difficulties. Some may not pass fingerprint checks. Some may not receive OTP messages. Some may not be able to complete face authentication because of age, illness, disability, poor lighting, weak internet, or device problems. A fair system needs more than one route.

No person should be denied welfare only because face authentication fails. A failed match should lead to help, not punishment. The local officer or service provider should explain what happened in simple language. The person should be told what can be done next. The next step should be practical. It

should not require long travel, repeated visits, or extra cost unless there is no other way.

Exception handling should be clear. Local officials should know when and how to use backup methods. They should not be afraid to approve another form of verification when the person is clearly eligible. Rules that exist only on paper are not enough. Staff at ration shops, pension offices, health centres, and local service points need simple instructions. They should also know that welfare cannot be stopped only because the machine fails.

There should be a written record when a benefit is delayed or denied after authentication failure. The record should state the reason, the date, the officer or service point involved, and the next action required. This protects the beneficiary. It also protects honest officials. Without a record, denial can become silent. The person may leave without knowing whether the benefit is delayed, rejected, or still pending.

Beneficiaries also need a simple complaint channel. The complaint process should not depend only on online forms or mobile apps. Many welfare users may not be comfortable with digital systems. They should be able to complain at a local office, through a help desk, by phone, or through an assisted service point. The complaint should receive a clear response within a fixed time. A person who depends on food, pension, or health support cannot wait for an unclear process.

Data protection is also necessary. Face authentication should be used only for the stated welfare purpose. The data should not be used for tracking, profiling, or unrelated services. Only the minimum information needed for authentication should be collected. Access to records should be limited. Storage should also be limited. The beneficiary should know why the face check is being used and whether another method is available.

Independent checks can help identify hidden problems. The system should review whether authentication failures are affecting some groups more than others. Elderly persons, disabled persons, manual workers, women in remote areas, and people with poor digital access may face greater difficulty. If these groups face more failed attempts or delayed benefits, the system should be corrected. It is not enough to say that the technology works in general. It must work fairly for the people who need welfare most.

The success of face authentication should not be measured only by the number of successful digital transactions. A high number of matches does not prove that the system is fair. The better measure is whether eligible people actually receive their benefits without fear, delay, or humiliation. Face authentication can support welfare delivery in India only when it remains a bridge to access, not a gate that the poor must pass before receiving what they are already entitled to.

References

Khera, R. (2017). Impact of Aadhaar on welfare programmes. *Economic and Political Weekly*, *52*(50), 61–70.

Ministry of Electronics and Information Technology. (2023). *The Digital Personal Data Protection Act, 2023*. Government of India.

Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2025). Identity verification standards in welfare programs: Experimental evidence from India. *The Review of Economics and Statistics, 107*(2), 372–392.

Supreme Court of India. (2018). *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, W.P. (C) No. 494 of 2012.

Totapally, S., Sonderegger, P., Rao, P., Gosselt, J., & Gupta, G. (2019). *State of Aadhaar Report 2019*. Dalberg.

Unique Identification Authority of India. (2016). *The Aadhaar Act, 2016, as amended*. UIDAI.

Unique Identification Authority of India. (2021). *The Aadhaar Authentication and Offline Verification Regulations, 2021*. UIDAI.

Unique Identification Authority of India. (n.d.a). *About your Aadhaar*. UIDAI.

Unique Identification Authority of India. (n.d.b). *Authentication: Frequently asked questions*. UIDAI.
Unique Identification Authority of India. (n.d.c). *Authentication devices and documents*. UIDAI.