IDEMIA
PUBLIC
SECURITY

IDEMIA's recommendations for biometric technology in the identity domain

Governments are increasingly relying on biometrics (facial, iris or fingerprint recognition) in order to secure access to public services, whether online or in person. The main motivation of States with regard to setting up this type of system is generally to reduce the risk of identity fraud (for example, if a State distributes fertilizer to farmers for their crops, to prevent ineligible people from collecting the fertilizer and then selling it on to farmers).

The error rate for authentication using biometric technologies is considerably lower than that of other techniques, such as verifying a person's identity using the naked eye, based on a photo on an identity document. It is for this reason that the World Bank and USAID fund projects to set up biometric identity registers and e-IDs, particularly in Africa. They improve access to public services and the inclusion of citizens.

Certain precautions must be taken when rolling out biometric systems:

- When setting up the registers (biometric data acquisition phase), the system may erroneously - but with a low probability - consider that a person already exists ("false duplicate"). In such cases, an administrative inquiry is then normally carried out to rule out the risk of fraud, and to avoid biometric duplication. A person should not be excluded from registration solely on the basis of the detection of a duplicate.

- At the moment when the person wishes to access a service, it is possible that he or she might not be recognised, due to a degraded network access or for other technical reasons. Nevertheless, IDEMIA's technologies have a very low error rate (< 0.5% for fingerprint recognition, according to the latest NIST assessments). This error rate is higher for people with severely damaged fingers, but again remains very low. Demographic group has virtually no impact on the performance of IDEMIA's biometric identification and other algorithms, which are regularly rated as the fairest on the market.

Here too, IDEMIA recommends implementing a remediation procedure to enable access in another way, either using another type of biometrics (authentication by fingerprint or facial recognition), or reverting to the pre-biometrics method (in general, checking of a person's identity by an authorised agent on the basis of a photo in an identity document).

- The implementation of these systems should not have the effect of depriving part of the population of access to public services on a discriminatory or indirect basis.

- Digital identification should not be the only means of accessing basic goods and services, particularly when a lack of access due to technical error is likely to infringe upon the human rights of the people concerned or could cause them vital harm.

- Finally, insofar as these systems involve the collection and use of sensitive biometric data, IDEMIA recommends that the roll-out of such systems be preceded by an impact study in terms of confidentiality, data protection and human rights.

IDEMIA systematically promotes these recommendations to its customers and works actively to integrate them into the best practice guides and recommendations published by the working groups in which it participates.