

Biometrics Institute Concepts and Solutions Report

The future of responsible biometrics

February 2025



9. Facephi: The future of responsible biometrics: Trends and solutions

Biometrics have transformed the way in which we interact with digital technologies, allowing speedy, accurate identity verification. However, as its adoption expands, key questions are emerging about how to ensure its ethical and responsible use. Aspects such as privacy, data security, equity and inclusivity are the main focus of the debate.

Current trends in responsible biometrics

Privacy as a priority

Regulations like the General Data Protection Regulation (GDPR) in Europe and growing interest in similar laws in other regions have led companies to adopt privacy-first approaches by design. The use of anonymisation techniques, advanced encryption and secure storage of biometric data is now standard practice.

Solutions based on the "on-device" model (processing on the user's device) are gaining ground. This approach minimises the transfer of sensitive data, reducing risks and aligning with user demand to allow greater control over their personal information.

Bias mitigation in biometric algorithms

Bias in biometric algorithms has been widely documented, especially in facial recognition technologies. Institutions and developers are working to create more inclusive models, trained with data sets representative of global diversity. Generative AI is taking on a crucial role in this area, facilitating the creation of synthetic identities and the augmentation of images in underrepresented groups. Furthermore, certification and validation by bodies such as the National Institute of Standards and Technology (NIST) have established themselves as guarantors of the standardisation and robustness of these technologies. What's more, practices such as continuous auditing and inclusive design are crucial in order to minimise any discrepancies in error rates between different demographic groups and to promote the responsible adoption of biometrics.

Transparency and explainability

The rise of AI in biometric systems has generated the need to promote an understanding of how these systems work and about how they impact users.

Transparency in biometric processes allows users to trust the technology and understand how their data are processed. Furthermore, compliance with regulations such as the European Union Artificial Intelligence Act (AI Act) is crucial for building trust in these solutions.

Focus on accessibility and inclusive design

Ensuring that biometric technologies are accessible to all users, regardless of their skills, age or level of technological experience, is a challenge that has become a priority. This includes the design of intuitive interfaces, the reduction of technical complexity and the incorporation of visual and tactile elements adapted to different needs.

Emerging solutions for a responsible future

Decentralised processing and data protection

Decentralised biometric processing can mitigate certain cybersecurity risks, such as attacks on centralised databases, and strengthen user privacy. This falls in line with the trend towards self-sovereign identity, allowing sensitive data to remain under the control of the users themselves.

On-device biometrics also contribute to this aim, although it is essential to strengthen security measures on the devices themselves. It is not always feasible to delegate full responsibility for protection to users, as many are not aware of the threats.

Significant advances are being made in hashing and cryptography techniques, including solutions such as homomorphic encryption, allowing operations to be performed on data without the need for decryption. However, their adoption still faces technical challenges.

Concurrently with the advancement of Synthetic Data techniques and generative AI, it is crucial in sectors that handle sensitive data, such as healthcare or identity verification, to explore Federated Learning techniques that allow the training of algorithms without centralising information.

Continuous audit and ethical standards

Algorithm auditing is essential for detecting and correcting any potential biases. These evaluations include demographic impact analyses and periodic reviews of the algorithms to adapt them to new data.

Assessments such as those performed by the NIST (Facial Recognition, Presentation Attacks etc.), are commonplace in the industry, but it is crucial to add new standards and assessments for new challenges such as Deepfakes or Injection Attacks.

Informed consent and user education

Ensuring informed consent is a mainstay of responsible biometrics. This includes providing users with clear information about how their data are collected and processed, as well as consent withdrawal options.

Concurrently, education plays a key role in training users in how to interact with biometric technologies safely and consciously.

Responsible and ethical use cases

The design and implementation of biometric solutions must always consider their impact on real life, especially in sensitive sectors.

Key examples of responsible apps include:

- **Banking and digital payments:** Biometric systems in banking allow for faster and more secure processes, but they must ensure that they do not exclude vulnerable populations
- **Border control and security:** Biometric technologies used at airports and border crossings must strike a balance between security and privacy. The use of bias-free algorithms reduces discrimination risks and ensures fair treatment for all travellers.
- **Medical care:** Biometrics in the healthcare sector can facilitate secure access to medical records and protect sensitive patient information.

The future of responsible biometrics

The future of biometrics lies not only in its expansion, but also in the way it is adopted ethically and transparently. Organisations have the responsibility to align their technological developments with the principles of privacy, security and equity.

To ensure responsible and sustainable solutions, it is essential for there to be a continued commitment to audit, regulation and inclusive design, balancing technological innovation with ethics to deliver fair and equitable benefits to all users.

Organisation: [Facephi](#)

Contact: Javier Barrachina, R&D Director, jbarrachina@facephi.com