ÖAW AUSTRIAN ACADEMY OF SCIENCES

ITA – INSTITUTE OF TECHNOLOGY ASSESSMENT

ITA DOSSIER

BIOMETRICS: THE BODY AS UNIVERSAL ID?

IN BRIEF

- Biometric recognition is becoming more and more widespread in consumers' everyday lives and promises more security.
- Biometric procedures digitise characteristics of the body and can even remain unnoticed.
- In many cases, the processing of biometric data is opaque and difficult to control.
- Biometrics therefore poses risks for privacy, security, and fundamental rights.
- Regulatory measures can contribute to reduce some of the risks.

WHAT IS IT ABOUT?

The term biometrics refers to the automated recognition of individuals based on biological characteristics or behavioural patterns. Biometric data are generated from fingerprints, the face, iris, speech or movement patterns, amongst other things, and are already in use for a long time as, e.g., photo IDs. Biometrics are generally used to determine the identity of a person on the basis of certain characteristic features or for authentication. The range of applications for biometric methods has been increasing. The technology is no longer only used in the security sector, but also in the commercial sector.

Biometric recognition has found its way into consumers' everyday lives primarily as a "convenience technology", with processes such as fingerprint scanning or facial recognition increasingly being integrated into digital devices such as smartphones and computers.

Compared to a personal identification number (PIN) or a password, biometric procedures promise to ease login or unlocking of the devices. Furthermore, banks and financial service providers are increasingly making use of biometric procedures.

Consumers are thus becoming accustomed to biometrics in everyday life. Moreover, new and advanced methods for automated data analysis make it possible to process biometric data rapidly, even where large data sets are concerned. Common examples for this are, for instance, the comparison of fingerprints and voice or face recognition. Hence, processes that used to be restricted to the security domain are now also used in the commercial sector – and shape our everyday lives.

Fingerprints as a synonym for biometric features.

One critical aspect is that biometric data are often available on the internet without any form of protection. Persons the data originally relates to then have no way of recognising or controlling the processing of their biometric data. As a result, the body turns into a quasi-universal ID that is exposed to becoming regularly recorded or monitored without the knowledge or control of the person concerned. Biometrics therefore have a number of significant social implications, such as undetectable or invisible identification in public spaces or identity theft. This exacerbates the complex issue of surveillance and poses significant challenges to security, data protection, and democracy.

BASIC DATA

Project title:	The Body as Key?
Project team:	Schaber, F.; Strauß, S.; Peissl W.
Duration:	04/2020 – 11/2020
Funded by:	Federal Chamber of Labour

POTENTIAL DANGERS

Biometric recognition primarily entails advantages in terms of convenience and promises more security. However, its increasing use also involves new security risks. Biometric features are inextricably linked to the body and therefore cannot be altered or changed. As a result, biometric recognition has the potential to even reinforce threats such as identity theft. Biometric data are also not forgery-proof and can be copied by using simple means (e.g. adhesive strips for fingerprints or digital facial images) to trick security systems.

Photo: Alex Iby / Unsplash

Biometrics entail permanent risks for privacy.

Data security and secure transmission of biometric data are therefore essential. If the data are lost, they cannot simply be changed like a PIN or password because they are inextricably linked to the person captured. Third parties could misuse this data, identify people without their knowledge or penetrate systems. In practice, the level of protection for biometric procedures is often insufficient. Consequently, attacks on biometric systems are increasing. A further problem: biometric procedures are highly prone to errors; especially in case of facial recognition. The risk of false recognition is particularly high if only a few people are to be recognised amongst a large number of people. This can result in false suspicions or accusations, discrimination or racism. Numerous studies have shown bias in facial recognition. For example, people with non-white skin colour are up to 100 times more likely to be misidentified by certain algorithms than people with white skin colour. The subsequent analysis of existing data also poses enormous risks, e.g. facial images available on the internet can be analysed biometrically at any time, even long after their initial release. This allows for and reinforces ubiquitous, hidden surveillance. There are several grey areas when it comes to legal regulations, a problem exacerbated by insufficient and non-binding data protection and security standards. As a consequence, biometrics entail a permanent risk to privacy and the problem of hidden identification and surveillance aggravates significantly on a global scale. Specific regulations for biometric data are therefore necessary to reduce the risks.

WHAT TO DO?

The dangers of biometric applications intensify the need for more effective protection and governance:

- A clear ban on biometric methods in public spaces and especially on real-time surveillance based on biometrics and facial recognition should be considered. This should also include a ban on indirect surveillance, e.g., where of private and public biometric data are linked.
- More legal certainty and a clear distinction between authentication and identification should be created as biometrics blur the boundaries here. It is therefore necessary to regulate the use of biometrics more tightly to counteract the rampant commercialisation of biometric data.
- Facial images and voice recordings should generally be classified as biometric data and protected accordingly to limit risks of misuse.
- Data protection and security standards should be raised to limit the risks of biometric procedures. Higher and binding minimum standards for data security and transparency of biometric procedures are needed at national, European, and international level.
- The complex global problem makes it necessary to strive for harmonised regulation in the EU and subsequently also internationally.

FURTHER READING

Schaber, F.; Strauß, S; Peissl, W. (2020) Der Körper als Schlüssel - Biometrische Methoden für Konsument*innen; Final Report, No. ITA-2020-03, Vienna: Institute of Technology Assessment (ITA) in cooperation with the Federal Chamber of Labour
epub.oeaw.ac.at/ita/ita-project-reports/2020-03.pdf

CONTACT

Stefan Strauß
Email: *tamail@oeaw.ac.at*
Phone: +43 1 51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Apostelgasse 23, A-1030 Vienna; *www.oeaw.ac.at/ita/en*. | Frequency: The ITA Dossiers are published irregularly and publish the research results of the ITA. The ITA Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal "epub.oeaw": *epub.oeaw.ac.at/ita/ita-dossiers* | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: *creativecommons.org/licenses/by/4.0/* | ITA Dossier no. 55en April 2021 | *epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier055en.pdf*, Co-authors: Schaber, F., Peissl, W.