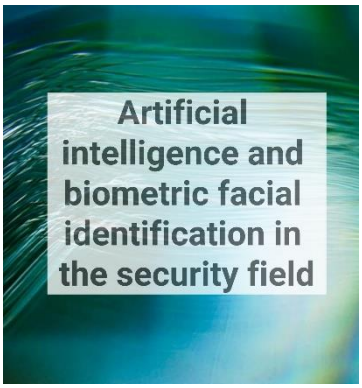
Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ARTIFICIAL INTELLIGENCE AND BIOMETRIC FACIAL IDENTIFICATION IN THE SECURITY FIELD

Javier Dorado / School of Prevention and Integral Safety and security / 2024

ABSTRACT



The use of biometric facial identification technologies in public and private institutions for security purposes is a reality. Examples are detection and prevention within access control, or the identification of suspects or wanted persons. Nonetheless, the use of these techniques that operate with artificial intelligence and automated decisions presents several problems, not only in terms of regulatory legitimacy from the point of view of the protection of fundamental rights, but also from an operational perspective. In this sense, biometric identification must be approached from a dual analysis: the technical-operational and the legal-regulatory, as both dimensions can entail risks for the organisation and the physical integrity of individuals.

Link to ISO 31000

Parts from ISO 31000 referenced in this article – Risk Assessment, Risk Treatment, Monitoring, and Review.

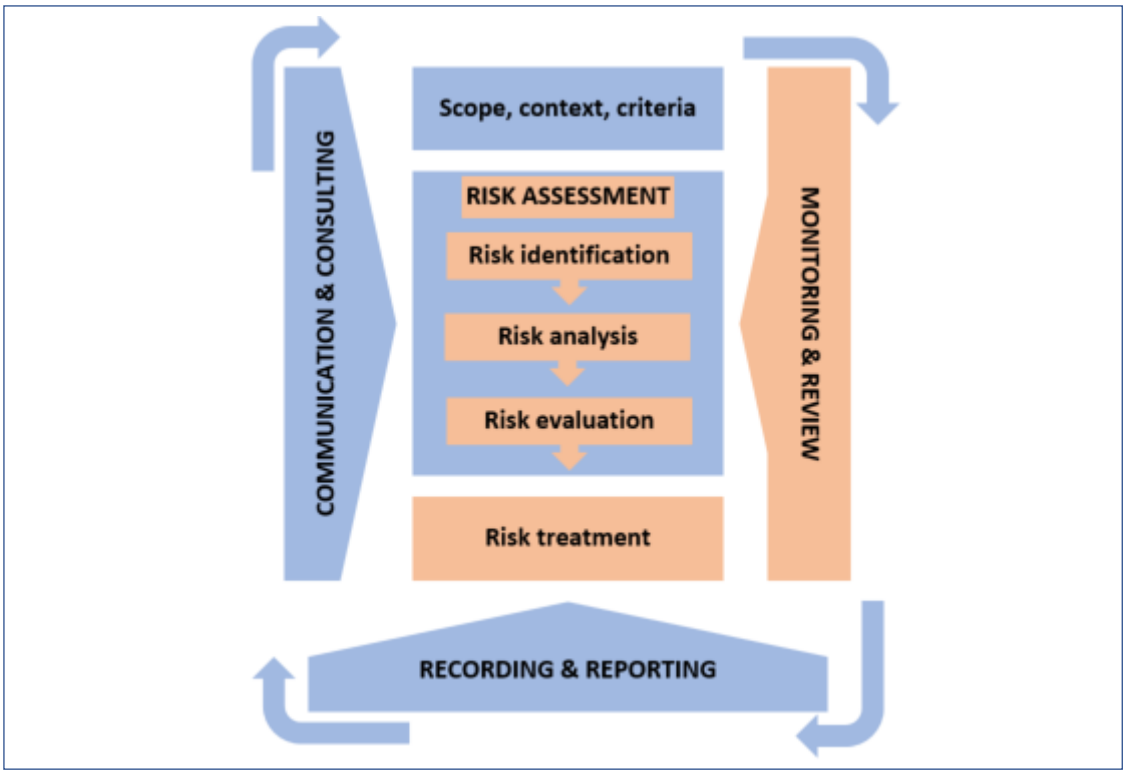


Figure no. 1. Risk management process (adapted from ISO 31000:2018), Risk assessment, risk treatment, monitoring, and review.

1. Introduction

A company entrusts you with the task of analysing the risks involved in implementing a biometric identification camera for access control purposes on its premises. However, they are not only concerned about the potential failures that this technology might generate, which could endanger private security purposes, but also about the possible administrative sanctions that this could entail within the framework of data protection.

With regard to technical-operational issues, the company needs to detect a number of persons who have previously been convicted of theft or burglary. For these persons, the company has biometric facial identification templates. However, the company has concerns about the possibility of incidents (false positives or false negatives) with this technology.

In terms of regulatory issues, the company is unclear to what extent and under what conditions it can use this technology without incurring a data protection infringement.

2. Case

The company in question is a jewelry shop and, as mentioned above. It has a database with the facial templates of people (15 in total) who have been previously convicted by the criminal courts in the last three years, specifically for theft or burglary in the establishments of this business.

The manager of the jewelry shop explains that the biometric identification camera, if positive, will inform the state security forces and bodies, so that they can go and arrest those identified, as they have a restraining order against the establishments, issued by the criminal jurisdiction.

However, the manager knows that this type of technology sometimes fails, either because of false positives (mistaken identifications) or false negatives (failure to detect the reported person in the database). In the first case, the company does not want to have problems with customers, as a false positive could lead to a complicated situation, as the system is designed to alert the police, when, in this case, the person identified has no criminal record. In the second case, on the contrary, if the identification fails, there would be a potential risk to the physical integrity of the employees, and/or to the company's assets, depending on whether the individuals in question are punished for robbery with violence or theft, respectively.

Furthermore, it is not clear to the company whether they can use this type of technology legally or whether there are risks of sanctions, which could lead to financial problems for the company.

For all these reasons, you are entrusted with the task of issuing a report with a dual perspective: a) a technical-operational report on the risks and advantages that the use of biometric identification cameras for access control purposes may entail; and b) a regulatory report on the conditions under which this technology can be used without violating data protection regulations.

3. Best practices

3.1 Technical-operational risks: a) False positives; b) False negatives

3.1.1 Identification and analysis of risks

The main risks to be reported to the company are indeed the possibility of occurrence failure of the technology such as false positives or false negatives.

3.1.2 Risk assessment

In the first case, it is important that the company providing this technology informs us of the probability of its software generating this type of failure. Once this point has been clarified, and considering that the bug cannot be neutralised, a two-step protocol should be put in place, in order to ensure that no one who does not meet the requirements is stopped. In this regard, it is recommended that a switchboard should filter out suspicious positives, i.e., those where there is doubt as to the identification of suspects.

In the case of false negatives, it is clear that it is difficult to implement an ex-ante access control process, as it is precisely this that has failed. Therefore, again, human verification is needed. If artificial intelligence fails, human intelligence can make up for it. This could be done by training employees, so that they can appeal to the competent public authority when they suspect that a customer's behaviour is inappropriate and may pose a risk to the physical integrity of employees or the company's assets.

3.2 Regulatory risks: GDPR sanctions

3.2.1 Identification and analysis of risks

On the legal-regulatory level, the company's assignment presents even more problems. The first thing we need to make clear to the company is that Art. 9 GDPR establishes a prohibitive rule regarding the use of "biometric data intended to uniquely identify a natural person". This prohibitive rule is accompanied by a series of assumptions that legitimise the use of personal data through these technologies. These assumptions include a) explicit consent; b) vital interests of the data subject or another natural person; c) exercise of legal actions; d) essential public interest.

3.2.2 Risk assessment

Regarding consent, it can hardly be given, in the terms of the GDPR (art. 7), in the context of the establishment. We cannot ask for explicit, specific consent, for the purposes of processing, from every single customer entering the establishment. As for the essential public interest, we must rule it out, as we are in the field of private security.

On the other hand, the other two enabling grounds (vital interests and legal action) can lift the ban on the processing of biometric data for access control purposes.

However, considering the millions of administrative penalties that would result from unlawful use of such data without respecting the principle of lawfulness (Art. 83.5 GDPR: administrative fines of up to EUR 20 000 000 or, in the case of a company, an amount equivalent to up to 4% of the total annual global turnover of the previous financial year), we recommend that a consultation with the national data protection agency be carried out. In the meantime, we recommend that the company

do not make use of these technologies, as the enabling grounds that may legitimise the use of these technologies may not be sufficient to make a fully lawful use of them.

References

ISO 31000 Risk management. In: ManagementMania.com [online]. Wilmington (DE) 2011-2023, 11/11/2016 [cit. 05/30/2023]. Available at: https://managementmania.com/en/iso-31000-risk-management

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.