Safety and Data Security in the workplace: the impacts of the general decision issued by the Italian Data Protection Authority on the implementation of Biometric Technologies.

Massimiliano Pappalardo

In Italy, one of the most critical areas for the data privacy is the processing of personal data of the employees in the workplace. Over the past weeks, the Italian Parliament and the Italian Data Protection Authority ("IDPA") have approved new provisions that will have a considerable impact on the existing legal framework.

Indeed, the Italian Parliament has recently voted a bill, named "Jobs Act", whereby it has empowered the Government to review the rules that any organization shall have to comply with, in order to lawfully implement remote monitoring systems in the workplace, limiting the existing burdens for the employers, in particular, with regard to the remote monitoring of the corporate electronic systems.

Furthermore, on November 12, 2014, the Italian Data Protection Authority issued a general decision, along with a set of guidelines, in order to regulate biometric technologies and their application.

In the workplace, biometric data are often used in automated and identification procedures, in particular, for the control of entry to both physical and virtual areas (e.g. access to particular electronic systems or services).

Among the points that may have a practical impact for a number of organizations: (i) the obligation to notify the IDPA of any data breach affecting biometrics and (ii) the measures to be implemented in order to avoid a prior checking procedure before the IDPA.

In this respect, the prior checking before the IDPA will not be needed with regard to specific kinds of data processings:

- automated authentication;

- control of access to physical "sensitive" areas and/or to dangerous equipment.

With regard to the last point, "sensitive targets" can be considered:

- areas aimed at hosting secret operations;
- areas where high value goods are stored;
- checkpoint areas for dangerous manufacturing operations;
- dangerous machineries.

In addition to the above, such an exemption will be subject to specific requirements, including:

- the authentication/control system shall be based on fingerprints or hand topography;
- raw biometric data shall be automatically deleted;
- the transmission of biometric data in the course of the authentication/control process shall be encrypted;
- two different set of security measures shall be implemented, depending on the solution for the storage of biometrics chosen by the employer: (i) on smart cards or mobile devices under the direct control of the employee or (ii) on the biometric readers of the employer.

In the other cases, the use of biometrics in the workplace will need a prior authorization of the IDPA.

Companies will have 180 days (starting from the publication of the general decision of the IDPA on the "*Gazzetta Ufficiale"*) to comply with the new provisions.

@Max_Pappalardo