

‘Open the pod bay doors, HAL’

Legal limitations on the use of biometric data for emotion detection in human-robot collaboration on the smart shop floor

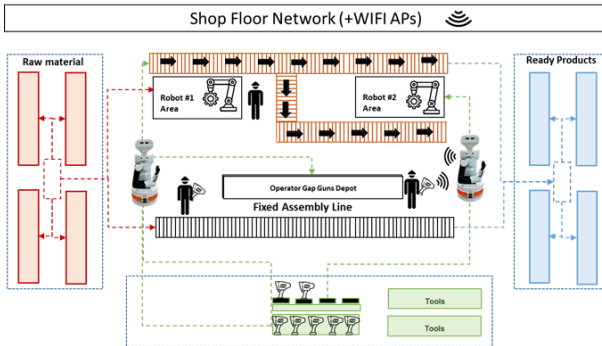


Ivo Emanuilov, Katerina Yordanova
Researchers

Robots in the smart factory



SeCoIIA Robotics (Mis)Use Cases



Cobots as 'means' of processing personal data

- EDPB Guidelines 07/2020 on the concepts of controller and processor

'Means' of processing

- 'Means' does not only refer to the technical ways of processing personal data, but also to the "how" of processing
- By determining the means and purposes of the processing of personal data, the employer who has decided to deploy cobots on the shop floor would undoubtedly qualify as a data controller

Biometric data++

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Conditions and additional measures in an employment context

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

Categories of data

Data revealing racial origin

- Distinction between data revealing racial origin and biometric data
- WP29, Opinion 02/2012 [4]:
the 'processing of biometric data could be used to determine [other] sensitive data, in particular those with visual cues such as race, ethnic group or perhaps a medical condition.'
- Potential additional obligations under Member State law
- What about a photograph? [6]

Categories of data

The metamorphoses of biometric data

- New category in GDPR: 'biometric data processed for the purpose of uniquely identifying a natural person'
- The only category of biometric data whose processing is considered sensitive [6]
- Narrow definition of biometric data in the GDPR: only the general regime under GDPR is applicable
- Quid 'specific technical processing'?

Categories of data

- (35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council ^(?) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Categories of data

Health data

- Health data processing to protect the vital interests of the data subject
- WP29, 2007, Working document on EHR [5]:
(...) processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment (...) where the data subject is not able to express his intentions.
- Narrow interpretation

Consent - a (very) bad idea?

- Imbalance of power also occurs in the employment context [1]
- Unlikely to be freely given [3]
- Power imbalance is even more obvious in the collaborative robotics use case since the worker would have little choice but to 'cooperate' with a machine that is part of their working environment

Legitimate interest

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
 - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
 - (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
 - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Legitimate interest (cont'd)

Facial recognition and emotion detection

- WP29 Opinion 02/2017 [3]
With the capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by automated means, to identify deviations from predefined movement patterns (e.g. factory context), and more. (...) disproportionate to the rights and freedoms of employees, and therefore, generally unlawful.
- Same stance by EDPS-EDPB on facial recognition in AI Act
- Proportionality to risks to the employer [2]

Prior analysis and identification of legitimate needs

- Systematically document how the deployment of cobots would enhance the productivity of humans on the shop floor and why they may lead to not only optimisation of business processes but may also bring safety gains
- Ethics of technology in the workplace

Data protection impact assessment

- (92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

Data protection impact assessment (cont'd)

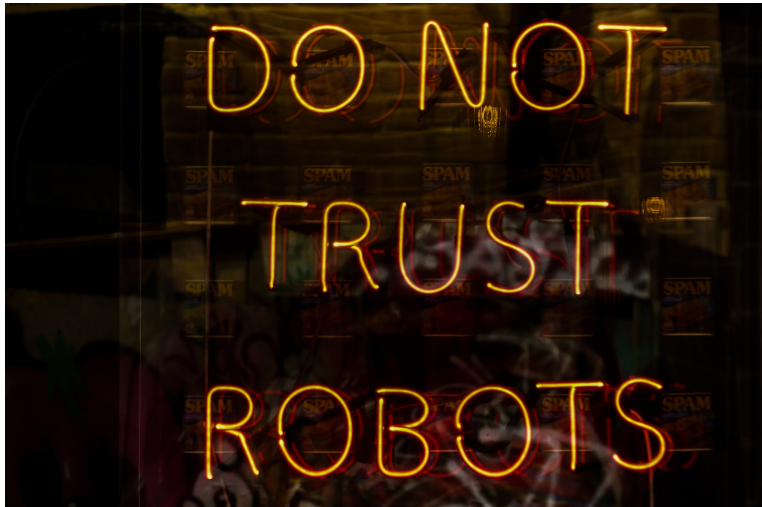
- Collective data protection impact assessment / collaborative human rights due diligence
- When would a DPIA be mandatory in this context?
- Quid industry-wide deployment of cobots to support a distributed process of manufacturing among several connected factories == 'large scale processing'?

Possible lawful grounds: Consent







- Experimental, early-stage deployment: consent? Possibly, but:
 - Employees are called upon to participate in early-stage deployment on a purely voluntary basis
 - Given the choice to participate in these trials on the same conditions
 - No discriminatory incentives for employees who choose to participate in the trials
- Explicit consent for each of the basic functions of the cobot which do not entail processing of special categories of data
- Distinction between the different categories of 'biometric data' crucial for transparency and consent reqs

Possible lawful grounds: Legitimate interest

- Security of manufacturing facilities and protection of vital interest? Possibly, but:
 - Narrowly defined security purposes
 - Context-dependent
 - Narrow interpretation of ‘how’ much processing is allowed
 - Legitimate interest assessment is subject to continuous re-evaluation
- Employee information and consultation procedures



References

-  Guidelines 05/2020 on consent under Regulation 2016/679
-  Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC
-  Opinion 2/2017 on data processing at work
-  Opinion 3/2012 on developments in biometric technologies
-  Working Document on the processing of personal data relating to health in electronic health records (EHR)
-  Kindt, E.J.: Having yes, using no? About the new legal regime for biometric data **34**(3), 523–538.
<https://doi.org/10/gdrhbt>

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

