Algorithmic monitoring of workers in the context of the European standards for privacy and data protection

Ljupcho Grozdanovski
University of Liège

Structure

I. Algorithms changing the content of work and the structure of work relations

II. The Scope of the Right to Privacy in the Context of Algorithmic Monitoring

III. Data Protection Safeguards in the Context of Algorithmic Monitoring

IV. Concluding Remarks

I. Algorithms changing the content of work and the structure of work relations

A. General traits of the 4th industrial revolution

- Sophisticated new technologies (AI, Robotics, ICT…)
- **Autonomy** as a main feature of AI
- The concepts of **data mining** and **profiling**

B. Impact on labour and labour relations

- **Existing context**: issues raised by platform work and platform workers (*Uber* cases)
- **Future context**: algorithmic recruiting and monitoring of employees

Algorithmic Monitoring

Intelligent Systems with functionalities that allow for the measuring of one's daily activities and inferring one's levels of productivity.

Advantages

A step forward and away from the traditional, personal scrutiny of employers over their employees.

Risks

- Types of data that can be collected
- Accuracy of the assessment

Example of an employee monitoring algorithm - ISAAC

ISAAC is an intelligent system that, not only measures certain parameters relative to work performance (the most obvious being the time spent in front of a computer) but also builds a comprehensive image of the employees' profile.

ISAAC identifies the s.c. central workers, in charge with holding the network together; the knowledge brokers, perceived as critical connections to external knowledge, and the peripheral workers who are most likely of leaving their jobs.

Main issues with ISAAC

1°) Opacity

2°) Privacy and Data Protection issues

3°) Employee health and wellbeing

(cf. Article in *The Guardian*, 7 August 2019, available at: https://www.theguardian.com/technology/2019/apr/07/uk-businesses-using-artifical-intelligence-to-monitor-staff-activity (10.05.2019))

Main Legal Issues

1) **Privacy**: which limits deriving from the right to privacy can apply to algorithic monitoring?

2) **Data Protection**: which limits deriving from rules and principles on data protection can apply to algorithmic monitoring?

II. The Scope of the Right to Privacy in the Context of Algorithmic Monitoring

A. The Content of the Right to Privacy

Art. 8 ECHR

1. Everyone has the right to respect for his **private and family life, his home and his correspondence**.
2. There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law and is necessary in a democratic sociery in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or the protection of the rights and freedoms of others**.

Article 7, EU Charter of Fundamental Rights

Everyone has the right to respect for his or her **private and family life, home and communication.**

Article 8 EU Charter of Fundamental Rights

1. Everyone has the **right to the protection of personal data** concerning him or her.
2. Such data must be **processed fairly for specified purposes and on the basis of the consent of the person concerned** or some other **legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified**.
3. Compliance with these rules shall be subject to control by an independent authority.

Case law on the content of the right to privacy (focus on the right to privacy at work)

ECtHR, 16 December 1992, *Niemietz v. Germany*, App. N° 13710/88, para. 29: the notion of private life encompasses activities of professional and business nature.

Telephone, e-mail and Internet usage at work are covered by Article 8 ECHR

ECtHR, 25 June 1997, *Halford v. UK*, Appp. N° 20605/92,

ECtHR, 3 April 2007, *Copland v. UK*, App. N° 62617/00

B. Conditions for justified restrictions of the right to privacy

- **Legality**: a domestic law must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities (ECtHR, 4 May 2000, *Rotaru v. Romania*, App. N° 28341/95, para. 61)

- **Legitimate aims**: such as the prevention of crime through the disclosure of certain types of data (ECtHR, 28 January 2003, *Peck v. UK*, App. N° 44647/98).

- Necessity and Proportionality

ECtHR, 5 September 2017, *Barbulescu v. Romania*, App. N° 61496/08.

- An employee's electronic communication accessed by the employer cannot be grounds for the former's dismissal

ECtHR, 22 February 2018, *Libert v. France*, App. N° 588/13

- When the employer is habilitated to verify the employee's private use of a company's item (like a PC), she must not overstep the margin of appreciation available to her.

C. The 'Reasonable Expectations' Doctrine

Origins: *Katz v. United States*, 389 U.S. 347 (1967)

US Constitution, 4th Amendment

Constitutional protection over "what [a person] seeks to preserve as private, even in an area accessible to the public".

The case the **reasonable expectation of privacy test (key components)**:

- **an individual has exhibited an expectation of privacy**
- **the expectation is one that society is prepared to recognize as reasonable**

Reasonable expectations and algorithmic monitoring

Open issues?

- Can principles established in a pre-automated era on the right to privacy apply to modern, non-Human agents?
- Should there be a redefining of the right to privacy at work if the employee monitoring is automated?

III. Data Protection Safeguards in the Context of Algorithmic Monitoring

A. Structure and Fundamental Principles

GDPR (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 , OJ L 119, 4.5.2016, p. 1)

General Principles on Personal Data Protection

Art. 5

1. Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**')

(b) Collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…)

(c) Adequate, relevant and limited to what is necessary to the purposes for which they are processed ('**data minimisation**')

d) Accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (…) **('accuracy')**

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…) **('storage limitation')**

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing (…) ('**intengrity and confidentiality**')

Operative concepts (Art. 4 GDPR)

- **Data processing**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- **Data controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
- **Data processor**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Basic Safeguards and Requirements in the GDPR

Art. 13, par. 1, GDPR

Where personal data relating to a data subject are collected from a data subject, the controller shall, at the time when personal data are obtained, **provide the data subject with all of the following information**:

a) The **identity and the contact details of the controller** and, where applicable, of the controller's representative;

b) The **contact details of the processing** for which the personal data are intended as well as the **legal basis for the processing**;

c) The **purposes of the processing** for which the personal data are intended as well as the legal basis for the processing;

d) Where the processing is based on point (f) of Article 6(1), the **legitimate interests pursued by the controller** or by a third party;

e) The **recipients or categories of recipients of the personal data**, if any;

f) Where applicable, the fact that the controller **intends to transfer personal data to a third country or international organization** and the existence or absence of an adequacy decision by the Commission (…)

Article 14, 'Information to be provided where personal data haven't been obtained from the data subject' (…)

Article 15, 'Right of acces by the data subject'

Par. 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the personal information:

a) The **purposes of the processing**;

b) The **categories of personal data concerned**;

c) The recipients or categories of recipients to whom the personal data have been or will be disclosed (…)

d) Where possible, the **envisaged period** for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) The existence of the **right to request from the controller rectification or erasure** or personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) The right to **lodge a complaint** with a supervisory authority;

g) Where the personal data are not collected from the data subject, any available information as to their source;

h) The existence of **automated decision-making**, including profiling (…) and, at least in those cases, **meaningful information about the logic invoved, as well as the significance and the envisaged consequences of such processing for the data subject.**

B. Safeguards and principles in automated decisions

Main issue: is algorithmic monitoring 'automated decision making'?

Algorithmic monitoring can *prima facie* be qualified as an automated decision within the meaning of **Art. 22(1)** if employees are profiled **solely by the algorithm *i.e.* without Human intervention**. It is, indeed, stated in this provision that "the data subject shall have the right not to be subject to a **decision based solely on automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".

The interpretation of the term ‘solely’ remains unclear.

Cf **Veale, Edwards, “*Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*,” 34 Comp. L. & Sec. Rev. (2018), 398-404, at 40**: “many automated systems produce significant outputs about individuals e.g. relating to criminal bail, welfare benefits or potential for employment, but few do so without what is often described as a ‘human in the loop’ - in other words they act as decision support systems, rather than autonomously making decisions (…) if Human involvement at all is allowed, through literal interpretation, to exclude a system from the ambit of Article 22, then its reach will be small indeed. Worse still, it would be easy to introduce a nominal human into the loop, ‘rubber stamping’ automated decisions in order to knock out art 22 rights.”

Article 22 GDPR

1. The data subject shall have the **right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significanlty affects him or her**.

2. Paragraph 1 shall not apply if the decison:

a) is necessary for **entering into, or performance of, a contract** between the data subject and a data controller;

b) is **authorised by Union or Member State law to which the controller is subject** and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data **subject's explicit consent**.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement **suitable measures to safeguard the data subject's rights and freedoms and legitimate interests**, at least **the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.**

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in **Article 9(1), unless point (a) or (g) of Article 9(2)** applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 22 GDPR creates two obligations for the employer:

- an **obligation *ex ante*** to inform the employees of the nature of the algorithmic monitoring and provide an explanation on the functionality of the HR algorithm;
- an **obligation *ex post*** of explanation and human intervention, aimed at revealing the rationale behind a specific decision, and an obligation to process personal data in compliance with Union law, which of course includes the EU Non-Discrimination Principle

(*cf.* **Watcher, Floridi, Mittelstadt, "*Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation*," 2 Int'l Data Privacy Law (2017), 1-25, at 3**: "an *ex ante* explanation can logically address only system functionality, as the rationale of a specific decision cannot be known before the decision is made."

IV. Concluding Remarks

Employers and software developers: must take into account the limits stemming from the right to privacy and the requirements pertaining to data protection.

Lawyers and Courts: it remains to be seen how insturments like the ECHR, the EU Charter and the GDPR will apply to cases of algorithmic monitoring. It is reasonable to assume that in automated contexts, provisions on fundamental rights protection will increasingly be interpreted in relation to, and in light of the rules and standards on data protection.