Finding the right regulatory formula

\[(\text{workers} + \text{data}) \times \text{AI} \div \text{uncertainty} = ?\]

Aida Ponce del Castillo
European Trade Union Institute
Foresight Unit
The overall EU Digital Strategy, the White Paper on AI and the Data Strategy should contain legal provisions about the specific situation of workers, the risks they face, the unbalanced power relationship they have vis-à-vis employers.
Finding the right regulatory framework: a proposal
5 key aspects:

- Enforcement existing legal framework
- Lessons from other pieces of legislation
- Role of standardization
- Role of soft law
- Filling Regulatory gaps/weaknesses
1. Enforcing existing legal framework

**International:**
- autonomy
- justice
- beneficence
- non-maleficence

**European:**

**New tech at work:**

**Safety:**
- General Product Safety Dir.
- Reg on Medical Devices.
- Dir Use of Work Equipment.
- OHS ‘Framework’ Dir.
- Machinery Dir.
- Radio Equipment Dir.

**Privacy and data protection:**
- e-Privacy Dir (forthcoming Reg)
- GDPR

**Liability:**
- Product Liability Directive
- EC’s Report 2020

**Cybersecurity:**
- Dir on the Security of Network and Information Systems.
- EU Cybersecurity Act 2019

Aida Ponce Del Castillo © etui (2020)
2. Lessons from other pieces of legislation

Can help in building **anticipatory governance for AI:**

- Examples of ex ante solutions in other Regulations and Directives

- Consider scientific uncertainty

- **Incorporate:**
  - Technology risk assessment.
  - Risk assessment at the workplace.
  - Data Protection Impact Assessment.
  - Anticipation of misuse.
2. Lessons from other pieces of legislation - ex ante solutions

(new) Medical Devices Reg.

- Prioritise safety assessment.
- Enable capacity of oversight (algorithms).
- Reinforcement of the responsibility of manufacturers, importers and other actors involved in marketing.
- Anticipate and monitor potential unintended use/misuse.

GDPR

Art. 5- Principles of data processing

Accountability: Obligation of data controllers to apply the DPIA.

’Right of explanation’: To provide a clear and understandable explanation of automated decisions.
# 3. Role of standardization

<table>
<thead>
<tr>
<th>ISO/IEC JTC 1 SC 42</th>
<th>IEEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>WG 2: Bid data</td>
<td>P7002: Data Privacy Process</td>
</tr>
<tr>
<td></td>
<td>P7010: Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems.</td>
</tr>
</tbody>
</table>

Aida Ponce Del Castillo © etui (2020)
4. Role of soft law

**OECD** Principles on AI (2019)

**EU- HLWG on AI**
Ethics Guidelines for Trustworthy Artificial Intelligence (2019)

Voluntary labelling system.

**Advisory bodies** need to have an appropriate multidisciplinary expertise for constructive assessment.
5. Filling regulatory gaps

There is a need to distinguish AI applications and its risks in the employment context vs other contexts: 7 concrete proposals:
GDPR Art. 88 and Art 9 need specific Guidelines by EDPS:
• Quality check
• Access to see what kind of data is collected about workers.
• Ability to supervise data and correct data.
• Monitoring and profiling (H&M case).

GDPR Art 5: principles of processing:
Transparency
Purpose limitation
Data minimisation
Autonomy, “right to disconnect”.

GDPR Article 9.1. Biometrics and FRT
Surveillance dehumanizes the employment relationship.

Case law of the European Court of Human Rights on the protection of the privacy and personal data of employees.

**GDPR Art 88.** EDPB need to issue guidance on workplace surveillance.
Digital control of employees

COVID-19 intensifies surveillance in the workplace

In the pandemic, digital tools for controlling employees are springing up like mushrooms. What means do we have to prevent permanent invasion of privacy?

May 8th, 2020 at 8:00 a.m.- Guest post, Aida Ponce Del Castillo - in data protection - 4 additions
Remote monitoring technology

How comfortable would you feel with your employer using each of the following types of technology to manage employees working remotely?

<table>
<thead>
<tr>
<th>Technology</th>
<th>% Very comfortable</th>
<th>% Fairly comfortable</th>
<th>% Very uncomfortable</th>
<th>% Fairly uncomfortable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keystroke – tracking how often and quickly you are using your keyboard</td>
<td>50</td>
<td>10</td>
<td>40</td>
<td>10</td>
</tr>
<tr>
<td>Camera – recording when you are sat in front of your home computer</td>
<td>30</td>
<td>20</td>
<td>50</td>
<td>10</td>
</tr>
<tr>
<td>Electronic tracking – wearable devices to monitor where you are</td>
<td>10</td>
<td>20</td>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>Automated hiring/promotions – software that will determine who gets hired or promoted</td>
<td>10</td>
<td>20</td>
<td>60</td>
<td>10</td>
</tr>
</tbody>
</table>

Source: YouGov Polling/Prospect, Sept 2020
Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre

The Hamburg Commissioner for Data Protection and Freedom of Information imposes a 35.3 Million Euro Fine for Data Protection Violations in H&M's Service Center

In a case concerning the monitoring of several hundred employees of the H&M Service Center in Nuremberg by its management, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) has issued a fine of 35,258,707.95 Euros against H&M Hennes & Mauritz Online Shop A.B. & Co KG.

The company is registered in Hamburg and operates a service center in Nuremberg. Since at least 2014, parts of the workforce have been subject to extensive recording of details about their private lives. Corresponding notes were permanently stored on a network drive. After absences such as vacations and sick leave - even short absences - the supervising team leaders conducted so-called Welcome Back Talks with their employees. After these talks, in many cases not only the employees' concrete vacation experiences were recorded, but also symptoms of illness and diagnoses. In addition, some supervisors acquired a broad knowledge of their employees' private lives through personal and floor talks, ranging from rather harmless details to family issues and religious beliefs. Some of this knowledge was recorded, digitally stored and partly readable by up to 50 other managers throughout the company. The recordings were sometimes made with a high level of detail and recorded over greater periods of time documenting the development of these issues. In addition to a meticulous evaluation of individual work performance, the data collected in this way was used, among other things, to obtain a detailed profile of employees for measures and decisions regarding their employment. The combination of collecting details about their private lives and the recording of their activities led to a particularly intensive encroachment on employees' civil rights.

This data collection was made known by the fact that the data became accessible company-wide for several hours in October 2019 due to a configuration error. After the Hamburg Commissioner for Data Protection and Freedom of Information was informed about the data collection through press reports, he first ordered the contents of the network drive to be "frozen" and then demanded it to be handed over. The company complied and submitted a data record of around 60 gigabytes for evaluation. Interrogations of numerous witnesses confirmed the documented practices after analyzing the data.

The discovery of the serious violations has prompted those responsible to take various corrective measures. The HmbBfDI was presented with a
Making the purpose of AI algorithms transparent

\[ \text{info + explicability + accountability} \Rightarrow \text{transparency} \]

- Data collection
- Data selection
- Decision system

How do algorithms work? and for what?

Origin
- Quality
- Correlation
Building on Articles 13-15 and Recital 71 of GDPR:

Information GDPR Art 12 \[
\begin{array}{c}
\text{Understandable} \\
\text{Meaningful} \\
\text{Actionable}
\end{array}
\] =

(a) understand the significance and consequences of an automated decision;
(b) obtain an explanation of an automated decision;
(c) **challenge** the decision.
Extrapolating GDPR’s requirement of ‘privacy by design’ & ‘privacy by default’ to the employment context

- detecting a human presence and outlining the workspace for the worker vs for the machine.
- avoiding collision.
- flexibility and adaptability of human-robot collaboration.
- integrating feedback from workers in the work process.
- provisions outlining cyber-security risks.

Preserving the security and safety of workers in human-machine interactions
Autonomy is key when joint human/machine problem-solving takes place.

Example: preserving the workforce’s tacit knowledge and supporting the transfer of that knowledge into the machine, whether it is a cooperative robot or a software.
Digital skills are not enough.

A new role for workers’ representatives would be:

- to flag up digitally related new risks,
- to assess the uncertainty of invisible technologies,
- to find new ways of integrating tacit knowledge into the workflow and work process.

**AI literacy:** workers need to be able to critically understand AI’s role, its impact on their work and anticipate how it will transform their work.
Labour in the age of AI

7 dimensions that regulation can protect workers

Find out more!

#AI4workers etui.

Thank you