Welcome to the Datafied Workplace
risks and opportunities of the new surveillance through AI and IoT

18 January 2022
4pm CET - online
Mini-lectures series on cybersecurity
Michele Molè, PhD Candidate
University of Groningen, Faculty of Law
table of contents

01. workplaces: a matter of surveillance

02. 'datafied' workplaces and the new surveillance through AI and IoT

03. fundamental labour rights, risks and opportunities

04. privacy as enabler?

05. privacy, economic freedoms, security

06. explainability and understanding of 21st century surveillance
workplaces: a matter of surveillance
workplaces through the industrial revolutions
over three centuries of tech at work, one common thread: surveillance
surveillance as **social control** became the necessary paradigm towards the new industrialised working society

three steps:

- **macro surveillance** (First Industrial Revolution: establishment of large industrial plants);
- **micro surveillance** (Second Industrial Revolution: Scientific Management, assembly lines);
- **surrounding surveillance** (Post Second Industrial Revolution, Fordism: private life is corporate life)
workplaces were born as databases (and still are today)
'datafied' workplaces and the new surveillance
'datafied' workplace

refers to employee monitoring software, performance assessment tools, productivity analytics, cybersecurity tools. Refers to the increasing possibility of collecting data and information on workplaces and employees, making them manageable and controllable through technology [Sánchez-Monedero, J, Dencik, L (2019) The datafication of the workplace]

new surveillance

In the Concise Oxford Dictionary surveillance is defined as "close observation, especially of a suspected person". Yet today many of the new surveillance technologies are not "especially" applied to "a suspected person". They are commonly applied categorically. (...) In a striking innovation, surveillance is also applied to contexts (geographical places and spaces, particular time periods, networks, systems and categories of person), not just to a particular person whose identity is known beforehand. [Marx G.T. (2002), What’s New About the “New Surveillance”? Classifying for Change and Continuity, Surveillance & Society 1(1): 9-29]
unforeseen capabilities for workplace and employees surveillance

- **Surveillance capabilities today determine corporate structures**: data and informations are essential assets;
- Monitoring as contractual prerogative: protecting company property, implementing company policies, optimising the organisation or implementing Occupational Safety and Health Administration policies;
Artificial Intelligence and the Internet of Things

TWO TECHNOLOGIES EXPANDING IN ANY WORKING-RELATED (AND NOT) PURPOSE

- I refer to Artificial Intelligence as a system based on data-rich inputs and computational techniques to make predictions or choices. These are tools built on large amounts of data from which it is possible to deduce patterns or predict outcomes applied to a variety of cases (Calo 2017);
- The Internet of Things (IoT) can be defined as network of physical objects or environments – ‘things’ – that are sensor-embedded. It enables people, objects or spaces to be digitally present in cyberspace, so that they can communicate with each other independently of human intervention; objects and spaces can be used to monitor changes in the human body, physical states or inter-personal relationships (such in the case of wearables at work), going far beyond simple monitoring by the well-known GPS geolocation technology-
whether for management purposes, worker safety or cybersecurity, the so-called new surveillance in 'datafied' workplaces is a potentially constant presence inside and outside workplaces and working hours;

I therefore find all encompassing the taxonomy offered by Kelloggs et alii (2020) of the purposes of new surveillance at work: recommending, restricting, recording, rating, replacing, rewarding;

It makes it possible to focus less on contractual prerogatives and to highlight its instantaneousness and comprehensiveness

Some examples
risk management, (cyber)security and safety, productivity assessment, hiring and recruiting, mental health and well being, predict accidents, reskilling, health check and social distancing, workers and customer relations

Little Tech is Coming for Workers (2021), coworker.org
Teramind, Controllo (Monitoring for labour management and maintaining cybersecurity standards):

An employee monitoring software tracks all user activity for apps, websites, emails, network etc. while at work. In addition to basic employee monitoring, Teramind’s PC monitoring software also includes insider threat detection, third-party vendor monitoring, data loss prevention, risk management, legal and compliance features as part of their monitoring suite.

Kronos, SAP Workforce Forecasting and Scheduling, GoBridgit, IBM Watson Talent Insights:

Workforce forecasting consists of using historical and forward looking workforce data to predict, identify trends. Which worker performs best on a specific project? Which workers are going to quit? Who is more promising for a position?

Ameyo, Activtrack, Cogito, Genome, Rescue Time:

Quality monitoring of call centres workforces (cordiality, reactiveness). Study and evaluation of time for particular tasks, reduction of distractions.

Amazon wrist band haptic feedback system

Thompson Reuters CLEAR, InterGuard, HubStaff, FlexiSpy, Oracle Retail XBRI Loss Prevention Cloud Service:

AIs which, by collecting data from the devices used by the users, makes it possible to record any type of data entering or leaving the smartphone, smartwatch, laptop or tablet.

Affectiva, Human, Microsoft Wellness Insight:

Tracking worker involvement, any symptoms of stress, emotional states, job retention, satisfaction.

Overview of AIs and IoT as surveillance tools
The pandemic has accelerated the development and use of surveillance through AI and IoT

- Little Tech database (from CoWorker.org) analysed over 550 workplace surveillance tools: 1/3 were developed in 2020/2021, 2/3 from 2018 onwards;
- European Company Survey (Eurofound 2020): 51% of 21.869 companies in EU27 and UK report the use of data analytics; especially, data analytics for employees surveillance in transports, manufacturing, retail, financial services.
- Sharp increase in the demand for workplace surveillance tools. The global market of these products is expected to reach 3.84$ billion dollars in 2023 (Panel for the Future od Science and Technology STOA, 2020)
ENISA Threat Landscape 2021

- **Companies are more exposed and vulnerable**: Cybercriminals go where money and knowledge is!
- **Social engineering** remains the most prevalent attack technique (tapping into emotions that drive action from recipient's side)
- New strong trend of **tailored attacks against employees working from home** (COVID19); The pandemic revealed unpatched and newly discovered vulnerabilities as well as initial access via compromised credentials;
- Patch and vulnerability management are a new priority both for SME and multinational companies; **a strong issue on IT infrastructure outsourcing**;
- Multiple extortion methods: ransomware + public shaming websites; media amplification of their victims; reaching out companies boards, investors, stakeholders, customers disclosing info about the attack; calling and harassing employees.
03. fundamental labour rights, risks and opportunities
WHICH RISKS FOR FUNDAMENTAL LABOUR RIGHTS?

- privacy and data protection
- freedom of thought
- freedom of assembly & association
- prohibition of forced labour

CFREU, ECHR, ESC, CCFSRW
WHICH RISKS FOR FUNDAMENTAL LABOUR RIGHTS?

EDPB and FRA (2020 and 2018): processing personal data of employees on the basis of consent it is problematic, being "unlikely to be freely given", even more so in the context of greater connectivity of the internet of things (IoT)
WHICH RISKS FOR FUNDAMENTAL LABOUR RIGHTS?

Surveillance at work - regardless of management or security purposes - through digital technologies might have a "chilling effect on the fundamental rights of the employees to organise, set up workers' meetings and to communicate confidentially" (WP 29, 2017)
WHICH RISKS FOR FUNDAMENTAL LABOUR RIGHTS?

- Percepyx, Worktango, Littler Mendelson: profiling to predict unionising
- Thomson Reuter CLEAR: hard-to-find data for investigations on "organised labour"
WHICH RISKS FOR FUNDAMENTAL LABOUR RIGHTS?

Kronos, SAP workforce, Affectiva, Cogito, Fama AI: surveillance for management or prevention enforces the 'function creep' of data collection, opening the door to unequal treatment in performance evaluation, access to bonuses or benefits, promotions, health status (alcohol and drugs abuse, disabilities), reputation scoring, background check.
04. privacy as enabler?
expansion of surveillance means blurring the lines between workplaces and private life (or better: individual autonomy)
privacy as enabler

Some literature claims the fundamental right to data protection and privacy (art. 7, 8 CFREU, art. 8 ECHR) as rights ‘enabling’ the information symmetry (Berendt 2019, Elrick 2020), thus opening ‘black boxes’ in workplaces, safeguarding trade union freedoms, equal treatment and protection against forced labour conditions under articles 4, 9-11 ECHR (Ebert, Wildhaber, Adam-Prassl 2021)
privacy as enabler

Nevertheless, European jurisprudence focussed on workplace surveillance under art. 8 ECHR is divided. The jurisprudence ranges from identifying requirements of legitimacy, legality, necessity and proportionality with a duty of notification on employers under art. 8 ECHR (ECtHR, Bărbulescu v. România), to denying that duty as a necessary condition for workplace surveillance (ECtHR, Lopez Ribalda v. Spain) thus emphasising the employer's free economic initiative (Collins P. 2020).
05. privacy, economic freedoms, security
a complex compromise...

implementing economic freedoms, the need to protect corporate assets and the fundamental rights of workers requires addressing several common goods of society:

- Privacy can conflict with security needs and other civil liberties
- Privacy can ensure security
- Without security there's no liberty: data security is crucial to realise data protection
...requires an holistic approach

Fundamental labour rights application by the European Courts of articles 4, 8-11 ECHR should pave the way for a holistic approach on workers' rights under this kind of surveillance, through duties to explain and make understandable the impact on fundamental freedoms of newly developed technologies
explainability and understanding of 21st century surveillance
explaining and understanding towards substance

Demir and Baykara v Turkey and Enervi Yapi-Yol Sen v Turkey and other ECtHR case law define fundamental collective labour rights as the means to adjust power inequalities in subordinate employment: the Court ‘does not accept restrictions that affect the essential elements of trade union freedom, without which that freedom would be devoid of substance’ (Demir para 144).
explain and understand towards information symmetry

workers must not simply be informed or listened to, but put in a position to have a say in workplace measures that significantly influences them (ECtHR, National Union of Belgian Police v. Belgium).

this should pave the way on a more unanimous interpretation of the GDPR
explain and understand involve: employees, employers, providers

the Strasbourg Court already recognises a negative and positive duty imposed on states (respectively, to refrain from interferences and promote fundamental labour rights) to ensure the enjoyment of fundamental freedoms at work, applicable also over third parties (ECtHR, Wilson and Palmer v. UK) – i.e. over employers and nowadays also service providers, being often embedded in the corporate structure.
explain and understand to establish social dialogue

ECtHR should provide a firm basis on which to build principles of explainability and understanding of workplace surveillance. Therefore, the premise for effective right to privacy and private life, trade union freedoms, equal treatment, prevention of forced labour conditions. And, finally, to negotiate the algorithm (digital skills, social dialogue, codetermination)
Thank you!

m.mole@rug.nl