Periodical Part

Foresight brief / European Trade Union Institute, Foresight Unit ; 2020

Foresight Brief

The *Foresight Brief* is a publication from the European Trade Union Institute (ETUI) focused on strategic thinking about the future challenges for the world of work. It is produced by the ETUI's Foresight Unit, whose work concentrates on two priority areas: climate change adaptation and new technologies. The *Foresight Brief* is also available in French under the title *Notes de prospective*.

Labour in the age of AI: why regulation is needed to protect workers

Aída Ponce Del Castillo
Senior researcher, Foresight Unit

Superpowers, states and companies around the world are all pushing hard to win the AI race. Artificial intelligence (AI) is of strategic importance for the EU, with the European Commission recently stating that 'artificial intelligence with a purpose can make Europe a world leader'.

For this to happen, though, the EU needs to put in place the right ethical and legal framework. This Foresight Brief argues that such a framework must be solidly founded on regulation – which can be achieved by updating existing legislation – and that it must pay specific attention to the protection of workers. Workers are in a subordinate position in relation to their employers, and in the EU's eagerness to win the AI race, their rights may be overlooked. This is why a protective and enforceable legal framework must be developed, with the participation of social partners.

AI, along with other new technologies such as robotics, machine learning and blockchain, will disrupt life as we know it. If Europe develops regulation according to its values and, in particular, ensures the protection of workers, it can become a genuine global player and win the AI race while remaining faithful to its democratic identity.

#08 – February 2020
Editors of the Foresight Brief series: Christophe Degryse
Philippe Pochet
Aída Ponce Del Castillo

Editor of this issue:
Christophe Degryse,
cdegryse@etui.org

More information on
www.etui.org > Foresight Unit

ISSN 2507-1548

foresight unit

etui.

I. Why workers should care about AI

Artificial intelligence (AI) is a highly disruptive technology. This paper understands AI as giving machines the ability to interact with their environment and to make decisions: with a varying degree of autonomy, based on data collected or given to them, and in a manner which copies human thinking and can thus be considered as intelligent. Its impact on citizens, on companies, on public authorities and on society in general is the subject of much research but its impact on workers has been less of a focus. AI has the ability to affect the workforce in many ways, both as a standalone technology or when coupled with other technologies (robotics, machine learning, blockchain, etc.). This Foresight Brief therefore argues that a governance framework needs to be developed, and one preferably based on regulation rather than ethical guidelines, codes of conduct or standards.

Practically speaking, AI systems can impact workers in many different ways: trackers for Uber drivers, Deliveroo riders and lorry drivers; nurses connected with apps and tablets; technicians collaborating with robots in a production line; software deciding who should be promoted next, predicting outcomes and scheduling activities; etc. The impacts are many and diverse, but AI should not negatively affect workers' fundamental rights and conditions.

AI systems can impact workers in many different ways but this should not negatively affect workers' fundamental rights and conditions.

In companies, AI can be used to increase productivity, optimise processes or reduce costs. The technology has a symbiotic relationship with the humans working alongside it; although often invisible, it can be used to analyse behaviour, to recruit staff, to monitor workflows or to evaluate workers and their performance. In some instances, AI systems can even be used to fire workers: in an article in *The Verge*, Colin Lecher (2019) reported that Amazon's system tracks workers' productivity rate and 'automatically generates warnings or terminations regarding quality or productivity without input from supervisors'.

In light of the European Commission's future strategic work on AI, the objective of this Foresight Brief is to briefly describe possible regulatory and non-regulatory avenues for governing AI and other new and emerging technologies. This paper highlights seven essential dimensions that future regulation should address in order to protect workers:

1) safeguarding worker privacy and data protection
2) addressing surveillance, tracking and monitoring
3) making the purpose of AI algorithms transparent
4) ensuring the exercise of the 'right to explanation' regarding decisions made by algorithms or machine learning models
5) preserving the security and safety of workers in human–machine interactions
6) boosting workers' autonomy in human–machine interactions
7) enabling workers to become 'AI literate'

II. The new European Commission's focus on AI

In 2018, the Juncker Commission launched the Communication 'Artificial Intelligence for Europe' (2018a), which set out a European initiative on AI that ensures an appropriate ethical and legal framework, based on the

European Union's values and its Charter of Fundamental Rights. At the same time, countries around the globe announced national strategies to promote investment and research in, and the development and use of, artificial intelligence and other digital technologies.

The new European Commission (EC) considers AI as a key priority: in her mission letters issued in September 2019, Commission President Ursula von der Leyen gave specific instructions to Margrethe Vestager, Executive Vice-President for 'A Europe Fit for the Digital Age', and to Thierry Breton, Commissioner for the Internal Market, tasking them with the coordination of a European strategy on data and artificial intelligence, including its human and ethical implications.

On 19 February 2020, the EC released a document entitled 'Structure for the White Paper on Artificial Intelligence – a European approach', which provides the basis for a balanced, values-based regulatory framework to promote Europe's innovation capacity. Based on a leaked version of that document (available at the time of writing this Foresight Brief), it appears that the EC identifies five options: (1) voluntary labelling for developers and users of AI; (2) sectoral requirements for public administration and a temporary ban on facial recognition in public spaces; (3) legally binding requirements that apply only to high-risk AI applications; (4) targeted amendments of the EU safety and liability legislation; and (5) an effective system of enforcement of the regulatory framework. In its conclusions, the Commission expresses a preference for a combination of options 3, 4 and 5, which would mean the creation of a horizontal instrument that sets transparency and accountability requirements, with specific amendments to the EU safety and liability legislation.

III. The governance of AI: possible approaches

1. Ethical guidelines and codes of conduct

Since AI systems can take decisions in an increasingly autonomous manner, it would seem logical to see regulators act to guarantee that they remain under legislative control and do not take decisions that are illegal or violate fundamental human rights. Instead, the whole regulatory debate has been taken over by an ethical narrative. The European Commission set up the High-Level Group on AI (HLG-AI), which eventually published the 'Ethics Guidelines for Trustworthy Artificial Intelligence'. This document is one of about 84 similar ethical guidelines developed by international organisations, multinational companies and other actors (see Algorithm Watch 2019, Jobin et al 2019). The multiplicity of texts raises questions about the lack of consistency and predictability of such an approach. In addition, ethical guidelines tend to be too broad and to focus on very general and aspirational aims: as Jobin et al report, 'these conceptual and procedural divergences reveal uncertainty as to which ethical principles should be prioritized and how conflicts between ethical principles should be resolved, and it may undermine attempts to develop a global agenda for ethical AI'. This can make such guidelines out of touch with the day-to-day issues that workers face when interacting with AI systems.

Codes of conduct are written to guide expected behaviour or to make promises regarding certain values. They are used by private corporations or international organisations as voluntary and self-regulatory instruments, and are therefore not legally binding (Biason 2018). When they are issued by international associations or organisations, they can or cannot be adopted by companies. Evidence shows that their impact is very limited, that companies using them have a limited ability to evaluate their success or implementation and that they are affected by a lack of independent monitoring (Auplat 2012,

Jenkins 2001). There are no means to enforce them and the lack of explicit sanctions for non-compliance is a concern (King, A. A., and Lenox, M. J. 2000). Revak (2011) even reports that there has not been any successful lawsuit against private corporations for violations of their codes.

As an example, the effectiveness of the 'Code of practice against disinformation' (2018), a self-regulatory standard signed by online platforms to fight against disinformation, is questionable. A report on its implementation shows that online platforms such as Google, Facebook and Twitter have failed in detecting threats and in providing metrics that elucidate the extent to which actions were taken to address the problem of disinformation (European Commission 2019).

The European Commission's (2008) 'Code of Conduct for Responsible Nanosciences and Nanotechnologies Research' was supposed to provide Member States, employers, research funders, researchers and more generally all individuals and civil society organisations involved or interested in nanosciences and nanotechnologies with guidelines favouring a responsible and open approach to research in this field. Auplat's (2012) analysis points out that this code has many drawbacks. It was designed as a voluntary, principle-based initiative and does not address technology risks or standards of performance, nor does it include evaluation schemes. All this makes it impossible to evaluate its efficiency. So far there has been no follow-up from the European Commission.

Relying on a multiplicity of ethical guidelines, codes of conduct or other similar voluntary initiatives to govern AI is not effective, it does not guarantee adequate workers' protection and it can easily open the door to 'ethics washing'. Moreover, trustworthiness is a quality of human beings, not of the technology (Metzinger 2019). Therefore, democratic participation, rule of law and respect of human rights must prevail in the governance of AI. This Foresight Brief suggests that the provisions of the General Data Protection Regulation (GDPR) are a useful tool which, when coupled with a governance framework, would be able to (re) act when unpredictable events occur and create a beneficial environment not only for European industry but also for society and workers. It will be interesting to see how Member States adopt national laws or promote the adoption of collective agreements that contribute to achieving this goal.

Relying on a multiplicity of ethical guidelines, codes of conduct or other similar voluntary initiatives to govern AI is not effective, it does not guarantee adequate workers' protection and it can easily open the door to 'ethics washing'.

2. Standards

In addition to ethical guidelines and codes of conduct, another kind of self-regulatory initiative that some stakeholders are pushing forward are standards. Standardisation organisations such as the International Standards Organisation or the IEEE Standards Association (IEEE SA) are consensus-building organisations, open mainly to (paying) members who create the standards. The IEEE has established 14 working groups to develop what they call 'human' standards, as part of their 'Global Initiative on Ethics of Autonomous and Intelligent Systems', which also includes an 'Ethics Certification Program for Autonomous and Intelligent Systems' (ECPAIS) (Winfield 2019). To engage in the standardisation process, technical expertise, financial resources and institutional knowledge are all required (Cihon 2019).

This publication argues that standards should be used to deal with the technical aspects of AI, rather than with human behaviour. Creating a standard on ethics presents several drawbacks. Firstly, it is questionable whether ethics or wellbeing can be standardised or subject to a certification, as a product is. Furthermore, should certification bodies have a say about what is the right ethical framework to apply to society? Another issue of concern is that standards are consensus-based documents drafted by a limited number of individuals, which means they escape the democratic legislative process.

3. Updating existing legislation

In 2018, the Juncker Commission proposed several legislative and non-legislative actions, which included: a 'Coordinated Plan on the Development of Artificial Intelligence in Europe'; the appointment of 52 experts to the High-Level Group on Artificial Intelligence (see 'Ethical guidelines' above); the creation of the Expert Group on Liability and New Technologies to assist the Commission in providing guidance on the implementation of the Product Liability Directive; and the formulation of policy responses to the challenges posed by AI in the fields of liability, safety, the Internet of Things (IoT), robotics, algorithmic awareness, and consumer and data protection.

With numerous stakeholders having signalled that concrete rules are needed to ensure that human rights, safety and security are preserved, the Commission has set up specific groups to consider whether existing regulations are 'fit for purpose' and compatible with AI technologies. The Commission will also open a public consultation process from which concrete legislative proposals might emerge.

Developing a regulatory strategy on AI and new technologies involves dealing with numerous intertwined and connected aspects of the law, which touch upon areas as diverse as the conception of the technology, transparent and accountable design, building and deploying the technology, and civil law liability rules for determining who is responsible and liable. This Foresight Brief argues that to guarantee adequate workers' protection from the impact of AI, existing EU legislation needs to be updated in order to cover possible gaps.

Below is a summary of the legislative areas that are relevant for worker protection and in which existing laws require an update.

3.1 Two fundamental overarching dimensions: the precautionary principle and human rights

Precautionary Principle

Applying the fundamental **legal precautionary principle** as defined in the Treaty on the Functioning of the European Union (TFEU, Art. 191), rather than the so-called 'innovation principle' (for which there is no treaty provision), is key to achieving the kind of innovation which benefits everyone. The innovation principle is a concept which was invented in 2013 by various CEOs as a lobbying/deregulatory tool and which does not have a legal basis. It is not found in EU treaties, secondary legislation, case law or the national constitutional traditions of any Member State (Garnett et al 2018; Garnett 2019). The term was coined by the European Risk Forum (ERF), a lobby platform for chemical, tobacco and fossil fuel industries, who asked Manuel Barroso, former President of the European Commission, Herman Van Rompuy, former President of the European Council, and Martin Schulz, former President of the European Parliament, to adopt it formally (Letter from

12 CEOs, 2013). As a result of intense lobbying, it is now referred to in several texts and policy documents from the EU institutions (Garnett et al 2018). The European Commission (2019b) defines it as 'a tool to help achieve EU policy objectives by ensuring that legislation is designed in a way that creates the best possible conditions for innovation to flourish'. It is often invoked in relation to four aims: (1) to keep products on the market with the fewest possible restrictions and regulations, (2) to attack the precautionary principle, (3) to seek deregulation and (4) to use the impact assessment phase (before drafting new or revised rules) to claim harm to innovation (Corporate Europe Observatory 2018).

Applying the fundamental legal precautionary principle as defined in the Treaty on the Functioning of the European Union (TFEU, Art. 191), is key to achieving the kind of innovation which benefits everyone.

Contrary to this, the precautionary principle emanates from international environmental law. It is an 'early warning' system that 'enables decision-makers to adopt precautionary measures when scientific evidence about an environmental or human health hazard is uncertain and the stakes are high' (European Parliament 2015). The concept was developed in the 1980s but was more formally adopted at the United Nations Rio de Janeiro Conference on Environment and Development and in the United Nations Biodiversity Convention, both of which took place in 1992. It is enshrined in the TFEU in Article 191 and in European Court of Justice case law (Sandoz Case 1983 provides an assessment of the principle).

This Foresight Brief suggests that the precautionary principle is an essential principle that must be at the heart of technological development. It can sustain such development, give direction to innovation and, in the case of AI, help to (1) build a governance based on social dialogue and which involves relevant societal actors; (2) provide a framework conducive to the explicability and accountability of algorithmic decision-making; (3) contribute to ensuring that technological innovations are safe for society (Ponce del Castillo 2017).

Human rights

Decisions taken by artificial intelligence systems can have real and serious consequences for the human rights of individuals, namely discrimination and inequality. There is evidence that workplace discrimination, for example, can be facilitated by AI (AccessNow 2018). Human rights frameworks should not only be enforced but also incorporated into AI governance systems. In this sense, the current Council of Europe Commissioner for Human Rights, Dunja Mijatović, stated that it is the responsibility of states to reinforce the monitoring of human rights compliance by AI systems and to act when there is an infringement. To achieve this, states should ensure and strengthen independent oversight and empower national human rights structures (Mijatović 2019).

Future actions on these matters will be made public at the end of May 2020 by the Council of Europe's Ad Hoc Committee on Artificial Intelligence (CAHAI). This committee was set up to 'examine the feasibility and potential elements, on the basis of broad multi-stakeholder consultations, of a legal framework for the development, design and application of artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law' (Council of Europe 2019).

In assessing artificial intelligence, the Council of Europe also stated that it should be regulated internationally and be operationalised in 'a legal framework that sets out a procedure for public authorities to carry out human rights impact assessments', that evaluates the potential impact of AI systems

on human rights, taking into account the nature, context, scope and purpose of such systems, and with a mechanism to mitigate such risks (Council of Europe 2019).

3.2 Safety

The **General Product Safety Directive** lays down rules that products must conform to. It currently requires producers to carry out a safety assessment only at the moment of their placing on the market. It does not address the risks linked to the evolution of products incorporating machine learning, for instance in a work process. The EC will release proposals for a revision of the Directive in 2020, through targeted amendments. As new technologies, including AI, transform the characteristics of many products, the challenges to be solved concern pre-market surveillance, products with integrated software (which need to be secure and up-to-date), as well as the set-up of traceability systems for such products.

The **Regulation on Medical Devices** lays down rules concerning the placing or making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU. The increased use of AI systems in the medical sector is creating several challenges. In a Joint Research Centre report, Holder et al. (2019) identify challenges related to AI that is incorporated in software in medical devices. The producer has to provide a safe product and ensure data protection is built into the design. The roles of the producer and the operator require further clarification. Another challenge is related to the application of the Regulation to mobile apps and the access and sharing of data, which might be addressed in the forthcoming Commission strategy on the topic.

The **Machinery Directive** sets safety requirements that manufacturers must meet to place machinery on the EU market. It is currently under revision and a new Directive or Regulation is expected by 2021. The revision will consider whether the Directive is fit to cover: (smart) robotics; interdependence and human–machine collaboration in environments where robots and humans share the operating space; the Internet of Things; and artificial intelligence. The aspects that need proper assessment are related to the multiplicity of interconnected systems, and particularly the interaction of AI systems with physical systems, and predictive maintenance, including cybersecurity and machine learning.

> When AI becomes embedded in work equipment, working conditions change and companies need to make sure workers understand the technology and its impact, as well as ensure that they are safe.

The **Radio Equipment Directive** establishes a regulatory framework for placing radio equipment on the market. It sets requirements for software and equipment capable of taking different configurations. The Directive was open to consultation until November 2019, during which time the EC requested contributions to a data collection exercise on the protection of personal data and privacy and on the protection from fraud in internet-connected radio equipment and wearable radio equipment. The important issues for labour are related to: the ultra-connectivity of devices; the Internet of Things; privacy and security requirements for

connected products that aim to protect people from cyber risks and ensure the security of data; the security of the 5G network; and products that are interconnected and likely to be hackable.

The **Directive on the Use of Work Equipment** lays down minimum safety and health requirements for the use of work equipment, defined as any machine, apparatus, tool or installation used at work. In selecting work equipment, the employer is required to pay attention to the specific working conditions and to any hazards posed by the use of the work equipment. Working with AI-augmented 'cobots' (collaborative robots designed to work in direct cooperation with a human), exoskeletons or wearables, for example, can trigger new safety, security or psychosocial risk factors, and even possibly decrease workers' autonomy. When AI becomes embedded in work equipment, working conditions change and companies need to make sure workers understand the technology and its impact, as well as ensure that they are safe.

3.3 Liability

The **Product Liability Directive** offers a liability framework, but the biggest challenge is establishing the causal link between a product alleged to be defective and the alleged damage, as well as clarifying how the software works and whether it is a product. Both the European Commission's evaluation (2018) and its report from the 'Expert Group on Liability and New Technologies – New Technologies Formation (NTF)' (2019) confirm 'the need to pursue the reflection on the future of the Directive in order to ensure legal certainty'.

Key findings of the report show that some characteristics of new technologies, such as their complexity, opacity and limited predictability, make it difficult for victims to make claims or the allocation of liability may be unfair or inefficient. Specific challenges related to the world of work that need to be addressed are: (1) making a distinction between high-risk and low-risk applications, something that can be relative depending on what benefits whom; (2) the fact that this Directive is intertwined with product design and with issues related to learning software; (3) sectoral liability, as is the case in the transport sector, which has its own specific liability rules; (4) the fact that there are other potentially liable parties, such as data providers (Dheu 2020).

Proposals from stakeholders such as the European Economic and Social Committee related to compensation funds and the insurance of AI (EESC 2019) do not provide clarity as to how those issues can be solved.

3.4 Privacy and data protection

GDPR Article 88 should be revised or the European Data Protection Board should provide guidelines to enlarge its scope, given the fact that processing workers' data is becoming increasingly complex.

The **General Data Protection Regulation** (GDPR) outlines regulatory requirements to the collection, process, and storage of personal data, and to do so, it outlines seven key principles: (1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimisation, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality and (7) accountability. GDPR aims at redressing the imbalances between those who have the ability to collect data and the data subjects. Therefore, since data is the key element of AI and other technologies, GDPR requires the 'privacy by design' and 'privacy by default' principles to be embedded in software and systems dealing with personal data.

GDPR includes only one article dedicated to employment, Article 88, which focuses on the processing of personal data in the context of employment, allowing Member States to enact more specific rules to ensure the protection of employees' rights and freedoms. When GDPR was being negotiated, Article 88 was supposed to be a standalone piece of legislation but the EU Commission eventually decided against this idea.

This Foresight Brief argues that Article 88 should be revised or that the European Data Protection Board should provide guidelines to enlarge its scope, given the fact that processing workers' data is becoming increasingly complex and given the development of technologies that can analyse not only physical traits and biometric data, but also perform facial recognition and even detect emotions or behaviours (CPDP 2020).

3.5 Cybersecurity

Cybersecurity is a relevant issue as workplaces have increased their online connectivity, making them vulnerable to cyberattacks. In its annual Global Risk Report 2020, the World Economic Forum ranks cybersecurity as one of the world's most critical risks, along with environmental degradation (World Economic Forum 2020).

The **Directive on the Security of Network and Information Systems** ('NIS Directive') entered into force in August 2016 and is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to achieve a high common level of security in network and information systems.

The **EU Cybersecurity Act** entered into force in 2019 and aims at achieving a high level of cybersecurity, cyber resilience and trust in the EU. It lays down a framework for the establishment of European cybersecurity certification schemes, with the aim of ensuring cybersecurity for ICT products, services and processes in the EU. It also aims to avoid the fragmentation of the internal market with regard to cybersecurity certification schemes in the EU. It identifies the objectives and tasks of the European Union Agency for Cybersecurity (ENISA).

In the workplace, cybersecurity implies preserving the security of company assets and of workers, who can be targeted and are often seen as vulnerable or weak links. However, cybersecurity can also be used as an excuse to deny workers access to information about the AI tools the company uses or as a means to exercise more workplace surveillance. EU governance should address this risk and also the risk of workers' personal data being compromised by cyberattackers. ENISA should issue further guidance and adopt a broader stance, beyond the issue of skills and cyber 'hygiene'.

The legal instruments listed above should be updated, to take new technologies into consideration, particularly AI. In doing so, this Foresight Brief argues that the following seven key dimensions should be addressed.

IV. Seven key dimensions that future AI regulation should address

The governance of artificial intelligence and similar new technologies cannot be entrusted to only a limited number of actors. Europe can only become a global digital leader if it remains faithful to its fundamental rights, social dialogue and tripartite participation, which is why workers, through trade unions, have to be at the negotiating table and contribute to the co-creation of both national and European AI strategies.

Besides real opportunities to create new business models and new types of jobs, and to employ people with hybrid skills or qualifications, the

The governance of artificial intelligence and similar new technologies cannot be entrusted to only a limited number of actors. Europe can only become a global digital leader if it remains faithful to its fundamental rights, social dialogue and tripartite participation.

development of AI also raises the risk of the opposite happening. Trade unions have made demands to be involved in the shaping of new technologies and in negotiations related to the introduction of artificial intelligent systems, automation, machine learning and robotics at the workplace (ETUC 2016, 2020; TUAC 2017; IG METALL 2019; UNI EUROPA ICTS 2019,). The agreements which result from such negotiations are not only an effective means of producing high-quality legislation exactly where it is needed (Tricart 2019), they also help in rebalancing power and distributing the gains from technology among workers.

Seven dimensions to future regulation, which should be discussed when such negotiations take place. These are relevant in several sectors and not fully covered by other legal instruments:

1. Safeguarding worker privacy and data protection

There is a need to ensure that workers know how to exercise their privacy rights. The application of Article 88 of GDPR can be insufficient for some practical workplace situations. New provisions are thus needed to respond to demands from workers about access to their analysed data and how such data is used, stored or shared outside the employment relationship. Additionally, trade unions at the national level should be able to cooperate with national data protection authorities, provide them with advice about the specific situations of workers, and encourage them to develop guidelines on data protection and privacy at the workplace.

2. Addressing surveillance, tracking and monitoring

In certain contexts, workers interact with technologies, apps, software, tracking devices, social media or devices in vehicles, which monitor their health, biomedical data, communications and interactions with others, as well as their levels of engagement and concentration or their behaviour.

Courts have on several occasions ruled in favour of workers who have been the victims of undue tracking and monitoring. In one example, Barbulescu v. Romania (2017), the Grand Chamber of the European Court of Human Rights ruled against an employer who had prohibited all personal use of work IT equipment and thereafter dismissed an employee for being in breach of that rule. The court decided that an employer could not, by way of instructions or policy, completely eliminate private social life in the workplace.

In a second example, Antovic and Mirkovic v. Montenegro (2017), the ECHR was asked to rule on the situation of two professors who claimed their employer had breached their right to private life in the workplace, because this employer had installed video surveillance systems in university lecture theatres where they taught. The court ruled that such surveillance had violated the provisions of domestic law and that video surveillance at work is an intrusion into an employee's private life.

As surveillance technologies can lead to violations of human dignity and workers' rights, monitoring and tracking policies need to be clearly justified and discussed on a case-by-case basis. This must cover such aspects as what is possible, what the limits are, and where and how the data collected

from the workforce comes from (for instance, private email, social media posts or offline activity). Moreover, the right to disconnect or the right to be unavailable should be respected across the board, as is already the case in some EU countries such as France.

3. Making the purpose of AI algorithms transparent

What is the point of having a 'fair' or transparent algorithm if it does not respect labour standards? Making algorithms transparent usually refers to unveiling the code, which in some cases might be subject of confidential business information. Often, having the mathematical code is not enough to understand the purpose behind the algorithm. Even if Uber algorithms were fair and transparent, the business model could still treat workers as commodities, disregarding their rights and their need for social protection. Making algorithms 'fair' should not be the ultimate goal, as this would be little more than ticking a box to claim to have met an ethical requirement.

Algorithmic fairness at the workplace implies designing algorithms while taking into account social implications such as: who are the targeted individuals; what are the tradeoffs made in the input of values and variables, like race, gender or socieoeconomic status; or how do algorithms make calculations or predictions. Knowing this can help to identify possible risks and avoid harm.

4. Ensuring the exercise of the 'right to explanation' for decisions made by algorithms or machine learning models

Automated decisions can impact workers negatively: incorrect performance assessment, the allocation of tasks based on the analysis of reputational data, or profiling. Moreover, algorithmic decisions can have a bias that manifests itself in many forms (in the design, data, infrastructure, or misuse of the model), all influencing the results. In such situations, the 'right to explanation' is essential. Building on Articles 13-15 and Recital 71 of GDPR, mechanisms and frameworks should be created so that workers can exercise this right. In practice, this means obtaining information that is simultaneously understandable, meaningful and actionable (GDPR Art 12) and makes it possible to: (a) understand the significance and consequences of an automated decision; (b) obtain an explanation of an automated decision; and (c) challenge the decision. In sum, the complexity of a machine learning system should not be an excuse to undermine workers' rights.

5. Preserving the security and safety of workers in human–machine interactions

This point concerns industrial and collaborative robots, which need to respect the safety and security aspects and the physical or ergonomic needs of workers. It also involves integrating the requirements concerning 'privacy by design' and 'privacy by default' into machines and work processes. Provisions for safe and secure cognitive systems should include aspects related to: detecting a human presence and outlining the workspace for the worker and the workspace for the machine; avoiding collision; flexibility and adaptability of human–robot collaboration; integrating feedback from workers in the work process; and provisions outlining cyber-security risks.

6. Boosting workers' autonomy in human–machine interactions

This means that workers make the final decision, using the input provided by a machine. This is particularly important when joint (human/machine) problem-solving takes place. Boosting workers' autonomy also means preserving the workforce's tacit knowledge and supporting the transfer of that knowledge into the machine, whether it is a cooperative robot or a piece of software (something that is particularly pertinent in processes that require testing, quality control or diagnosis).

7. Enabling workers to become 'AI literate'

With the development of AI, companies are looking after their own interests by upskilling or reskilling their employees. For workers, acquiring technical skills, although necessary, is not enough. They need to become 'AI literate', which is understood as being able to critically understand AI's role and its impact on their work. This means learning to work alongside AI and to anticipate how AI will transform their career and role at work. Passively using AI systems or tools does not benefit the workers themselves; a certain distance needs to be established for them to see AI's overall impact and influence (Ponce del Castillo 2018).

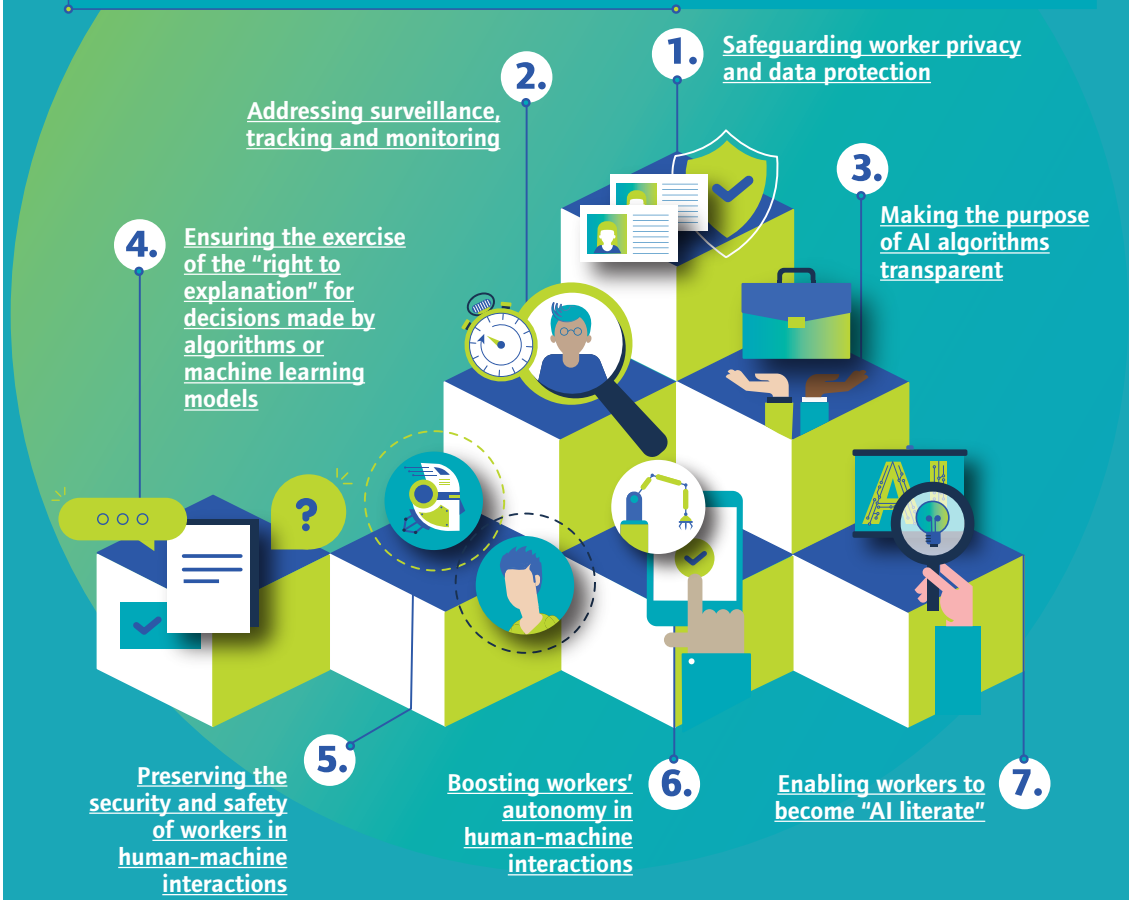
Schools and social partners have a role to play, along with other actors, in rethinking adult education in environments where some jobs may disappear. AI literacy involves understanding if and how the workforce is going to be affected by technology implementation. There is scope here for a new role for workers' representatives to flag up digitally related (new) risks and interactions, to assess the uncertainty of invisible technologies, and to find new ways of effectively integrating tacit knowledge into the workflow and work process.

Labour in the age of AI

7 dimensions that future regulation should address

Superpowers, states and companies around the world are all pushing hard to win the AI race. Artificial intelligence (AI) is of strategic importance for the EU, with the European Commission recently stating that 'artificial intelligence with a purpose can make Europe a world leader'.

Europe can only become a global digital leader if it remains faithful to its fundamental rights, social dialogue and tripartite participation, which is why workers, through trade unions, have to be at the table of negotiations and contribute to the co-creation of both national and a European AI strategy. Seven dimensions in particular should be discussed when such negotiations take place.



#AI4workers

V. Conclusions

'In the gaps between obligations and prohibited practices, there is a vast hinterland of possibility. Good regulation steers innovation away from potentially harmful innovation and into areas of this hinterland where society can benefit.' Giovanni Buttarelli, keynote speech on privacy, data protection and cyber security in the era of AI, 24 April 2018.

Regulating by values is how Europe can become a genuine global player in AI while remaining faithful to its democratic identity and refusing to abandon the many workers who risk losing their job or whose lives will be affected by AI.

Given the disruptive nature of AI and its ability to permeate all aspects of life, at work and beyond, it is imperative to establish a relevant, comprehensive and protective AI governance framework. Regulating by values is how Europe can become a genuine global player in AI while remaining faithful to its democratic identity and refusing to abandon the many workers who risk losing their job or whose lives will be affected by AI. The governance framework we need must be based on legislation; EU lawmakers should steer away from ethical guidelines or non-binding codes of conduct in order to determine what is legitimate or not.

European lawmakers need to look across the whole ecosystem in which AI systems will exist. They should ensure that existing legislation remains relevant by updating it and trying to anticipate the future evolution of rapidly evolving technologies. This process needs to be open and involve consulting all stakeholders. AI is going to change the nature of the relationship between companies and workers who, through their trade unions, must have the ability to shape and contribute to the creation of a European AI regulatory strategy, with a focus on the seven dimensions presented in this Foresight Brief.

AI is going to change the nature of the relationship between companies and workers who, through their trade unions, must have the ability to shape and contribute to the creation of a European AI regulatory strategy.

As Stephen Hawking pointed out in a column he wrote for the Guardian in 2016, 'The automation of factories has already decimated jobs in traditional manufacturing, and the rise of artificial intelligence is likely to extend this job destruction deep into the middle classes, with only the most caring, creative or supervisory roles remaining.' This is the very real kind of risk we need to protect workers from. Relevant legislation can help, as can social dialogue, which must be promoted as another key component of AI governance. Social partners have a role to play and collective agreements can complement European and national legislation, help to take into consideration specific sector or company realities and, finally, protect society and workers from the risk of AI totalitarianism.

References

AccessNow (2018) Human rights in the age of artificial intelligence. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Algorithm Watch (2019) AI Ethics Guidelines Global Inventory. https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/

Arntz M., Gregory T. and Zierahn U. (2016) The risk of automation for jobs in OECD countries: a comparative analysis, Paris, OECD.

Auplat C. (2012) Nanotechnology and sustainable development, New York, Routledge.

Biason K. (2018) Is a "code of conduct" legally binding? https://legalvision.com.au/is-a-code-of-conduct-legally-binding/

Cihon P. (2019) Standards for AI governance: international standards to enable global coordination in AI research & development. Technical report, Oxford, Future of Humanity Institute, University of Oxford. https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf

Computers, Privacy & Data Protection (2020) Regulating facial recognition technology. https://www.cpdpconferences.org/cpdp-panels/regulating-facial-recognition-technology

Corporate Europe Observatory (2018) The 'innovation principle' trap. Industries behind risky products push for backdoor to bypass EU safety rules. https://corporateeurope.org/en/environment/2018/12/innovation-principle-trap

Corporate Europe Observatory (2013) The innovation principle: « Stimulating economic recovery », Letter from 12 CEOs, 24 October 2013. https://corporateeurope.org/sites/default/files/corporation_letter_on_innovation_principle.pdf

Council of Europe (2019) Unboxing artificial intelligence: 10 steps to protect human rights. https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Dheu O. (2020) EU report on AI, new technologies and liability : key take-aways and limitations. https://www.law.kuleuven.be/citip/blog/eu-report-on-ai-new-technologies-and-liability-key-take-aways-and-limitations/

EESC (2019) Building trust in human-centric artificial intelligence (Communication). https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/building-trust-human-centric-artificial-intelligence-communication

ETUC (2016) ETUC resolution on digitalisation: «Towards fair digital work». https://www.etuc.org/en/document/etuc-resolution-digitalisation-towards-fair-digital-work

ETUC (2020) AI-Humans must be in command.https://www.etuc.org/en/document/ai-humans-must-be-command

European Commission (2019a) First results of the EU Code of Practice against disinformation. https://ec.europa.eu/digital-single-market/en/news/first-results-eu-code-practice-against-disinformation

European Commission (2019b) Ensuring EU legislation supports innovation. What the Innovation Principle is, how it was developed, links to Innovation Deals as well as the better regulation research and innovation tool. https://ec.europa.eu/info/research-and-innovation/law-and-regulations/innovation-friendly-legislation_en

European Commission (2018a) Code of practice against disinformation. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission (2018b) Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, SWD(2018) 137 final. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

European Commission (2018c) Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Accompanying the document : Report from the Commission on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products, COM(2018) 246 final, 7 May 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=SWD:2018:157:FIN&from=EN

European Commission (2008) European Commission adopts Code of Conduct for Responsible Nanosciences and Nanotechnologies Research. https://ec.europa.eu/commission/presscorner/detail/en/IP_08_193

European Parliament (2015) The precautionary principle: Definitions, applications and governance. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2015)573876

Expert Group on Liability and New Technologies – New Technologies Formation (2019) Liability for artificial intelligence and other emerging digital technologies, Luxembourg, Publications Office of the European Union.
Frey C.B. and Osborne M.A. (2017) The future of employment: How susceptible are jobs to computerisation?, Technological forecasting and social change, 114, 254-280.
Garnett K. J. (2019) Is the innovation principle compatible with a European Green Deal? https://b-lin-g.com/2019/11/29/is-the-innovation-principle-compatible-with-a-european-green-deal/
Garnett K., Van Calster G. and Reins L. (2018) Towards an innovation principle: an industry trump or shortening the odds on environmental protection?, Law, Innovation and Technology, 10(1), 1-14.
Hawking S. (2016) This is the most dangerous time for our planet, The Guardian, 1 December 2016. https://www.theguardian.com/commentisfree/2016/dec/01/stephen-hawking-dangerous-time-planet-inequality
Holder C., Iglesias M., Triaille J.-P. and Van Gysegnem J.-M. (eds.) (2019) Legal and regulatory implications of Artificial Intelligence. The case of autonomous vehicles, m-health and data mining, Luxembourg, Publication Office of the European Union.
IG METALL (2019) Transformationsatlas wesentliche Ergebnisse. https://www.igmetall.de/download/20190605_20190605_Transformationsatlas_Pressekonferenz_f2c85bcec886a59301dbebab85f136f36061cced.pdf
Jenkins R. (2001) Corporate codes of conduct. Self-regulation in a global economy, Technology, Business and Society Programme Paper 2, Geneva, United Nations Research Institute for Social Development.
Jobin A., Ienca M. and Vayena E. (2019) The global landscape of AI ethics guidelines, Nature Machine Intelligence, 1, 389–399. https://doi.org/10.1038/s42256-019-0088-2
King A. A. and Lenox M. J. (2017) Industry self-regulation without sanctions: The chemical industry's responsible care program, Academy of Management Journal, 43(4), 698-716.
Lecher C. (2019) How Amazon automatically tracks and fires warehouse workers for 'productivity'. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations
Metzinger T. (2019) EU guidelines: Ethics washing made in Europe, Der Tagesspiegel, 8 April 2019. https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html
Mijatović D. (2019) We need to act now and put human rights at the centre of artificial intelligence designs, Speech at the High level conference "Governing the Game Changer - Impacts of artificial intelligence development on human rights, democracy and the rule of law", in Helsinki, Finland. https://www.coe.int/en/web/commissioner/-/-we-need-to-act-now-and-put-human-rights-at-the-centre-of-artificial-intelligence-designs?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fcommissioner%2Fspeeches%2Ftags%2Fdunja+mijatovic
Ponce Del Castillo A. (2018) Artificial intelligence: a game changer for the world of work, Foresight Brief 05, Brussels, ETUI. https://www.etui.org/Publications2/Foresight-briefs/Artificial-intelligence-a-game-changer-for-the-world-of-work
Ponce Del Castillo A. (2017) A law on robotics and artificial intelligence in the EU?, Foresight Brief 02, Brussels, ETUI. https://www.etui.org/Publications2/Foresight-briefs/A-law-on-robotics-and-artificial-intelligence-in-the-EU
Revak H. (2012) Corporate codes of conduct: binding contract or ideal publicity?, Hastings Law Journal, 63 (6), 1645-1670.
Tricart J.-P. (2019) Legislative implementation of European social partner agreements: challenges and debates, Working Paper 2019.09, Brussels, ETUI. https://www.etui.org/Publications2/Working-Papers/Legislative-implementation-of-European-social-partner-agreements-challenges-and-debates
TUAC (2017) Shaping the introduction of AI for the benefit of All. TUAC Briefing on the OECD Conference on Artificial Intelligence, Paris, 26-27 October 2017. https://tuac.org/news/shaping-introduction-ai-benefit/
UNI EUROPA ICTS (2019) Position on Artificial Intelligence. http://www.uni-europa.org/wp-content/uploads/2019/12/AIUniEuropaWeb_en.pdf
Winfield A. (2019) Ethical standards in robotics and AI, Nature Electronics, 2, 46-48.
World Economic Forum (2020) The global risks report 2020, Geneva, WEF. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
All links were checked on 17.02.2020.

The ETUI is financially supported by the European Union. The European Union is not responsible for any use made of the information contained in this publication.