Resolution on the European strategies on artificial intelligence and data

Adopted at the ETUC Executive Committee of 2 July 2020

Key messages:

Robust European Artificial Intelligence (AI) and Data Strategies should:

• provide a legal and empowering European framework based on human rights, and therefore including labour and trade union rights and ethical rules.
• maintain and reinforce workers' protection, prevent disproportionate and undue surveillance at work, prohibit discriminatory treatments on the basis of biased algorithms, and prevent abuse of data protection and privacy, ensuring compliance and going beyond GDPR and maintaining their privacy when not at work.
• classify AI applications affecting workers' rights and working conditions as high-risk in principle and subject to appropriate regulation.
• address the specificity of the workplace, including the bargaining inequality between workers and employers. The principle of 'human remains in control' should apply to workers and managers.
• provide for AI and digital literacy schemes. Education and transparency of AI systems and of new technologies is important for workers to be able to understand, and be part of, the fair implementation
• provide for data governance at national, sectoral and company level, and strengthening workers' participation in the design, deployment, use and monitoring of AI technology and data strategy.
• provide for rules on business and developers' liability, including the reversal of the burden of proof in favour of workers, to balance the limited access to information to workers
• deliver a fit for purpose innovation, if AI technologies comply with the Treaty based precautionary principle
• provide for an EU data strategy with ambitious initiatives on cybersecurity transparency, portability, interoperability, fair taxation, regulating GAFAMs and other major platforms, operationalising the right to access, governance for access and sharing data, social benefits of data use/sharing.

Introduction and Context

Workers and labour relations have been facing disruptive transformation since the first industrial revolution. Technology and digital innovation have drastically transformed work and employment in unprecedented ways. Digitalisation in society dates back to the introduction of computers, so does artificial AI in attempting to reproduce or simulate the functioning of the human brain and physical processes. AI technologies are not new. However, they have gained new momentum in society, as they have rapidly evolved and covered a large part of the economy. Robotics and automation support often replace humans in dangerous, strenuous monotonous and repetitive tasks, as well as in tasks requiring great precision, even on a microscopic scale. AI is now also gradually supporting and possibly replacing analytical work.

AI refers to self-learning systems which can take over many human tasks (machine learning). AI is data driven: it is about data, linking data, putting information into a context, knowledge to be applied and reflected upon. Combined with robotics and access to big data, AI technologies form the backbone of the digital economy. They impact the daily life of citizens and have reached the workplaces. As such, the introduction and use of AI are key issues for work and society. They bring opportunities and challenges: on one side the undeniable major breakthrough technological

advances brought to medicine, space, mobility, communication to name but a few. On the other side risks of intrusive surveillance, breach of privacy and data protection and fundamental rights in general are exponentially growing.

The COVID-19 crisis has changed the societal context dramatically, impacting present and future generations in an unprecedented rapid way in the long term. Data and artificial intelligence are put in the forefront as solutions to tackle the pandemic, in medicine in the search for vaccines, drugs or treatments, as well as in the development of public tracing applications to identify potentially infected persons. The opportunities and challenges of such new technologies however should be carefully assessed. The Covid-19 crisis has also exacerbated the digital divide in all its aspects.

ETUC is convinced that labour protection and technological innovation can be compatible. Ensuring a just transition towards fair digitalisation and work are ETUC's guiding principle. While the EU must be at the forefront of technical innovation that benefits people, it should equally base its strategy on the European social model and its fundamental rights and values. The EU must be a driver in regulating innovation and in guaranteeing its compliance with workers' dignity, working conditions and well-being.

ETUC is of the opinion that an EU framework on AI should address the workplace dimension in an ambitious and proactive manner because workers are particularly concerned by AI technologies. The imbalance of power between employers and workers should lead the EC to consider a robust AI framework to create quality jobs, invest in worker's AI literacy, promote and increase the safeguarding of workers' rights, workers' protection and ensure that trade unions and workers' representatives participate actively in shaping AI at work. Such an AI framework should cover all workers and employers in the private and public sectors, for all business models including online platforms.

The EC has recently published two strategies which, steered in the right direction, can contribute to innovate and enhance EU technological leadership as well as to respond to new challenges, like the pandemic. These strategies are key determinants through which Europe is building its digital future[1]:- A White Paper on 'Artificial Intelligence: a European approach to excellence and trust'[2] and European Data Strategy[3]. It should be pointed out that the global AI market is currently led by countries that often do not comply with human rights in the development of this technology. Therefore, in its attempts to enhance the EU technological leadership, the EC should not compromise on issues such as human and workers' rights nor on the necessary involvement of workers' representatives and trade unions in shaping sustainable and ethical AI tools.

Artificial intelligence is undisputed for the sustainability of the economy, but Europe is lagging far behind the USA and Asian countries. Only a small percentage of companies use AI or plan to do so in the coming years. In this respect, the Commission's objective to mobilise l 20 billion annually in AI investments over the next ten years is an important step.

The EC rightly echoes the call raised by ETUC and the trade unions and different civil society organisations to reinforce the governance of data use in society and in the economy, in particular as data is the source of AI. This ETUC resolution addresses the main areas that the governance of data and AI should cover.

The EC has published a range of communications related to digitalisation simultaneously amongst the main ones, the communication on Shaping Europe's digital future[4], and a new industrial strategy for Europe dealing with digital transition[5]. In doing so, the EC clearly shows the strategic importance of digital technologies and of data. Most of the actions taken and foreseen in the digital fields intend to further deepen the internal market and in particular the Digital Single Market and will impact EU

---

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273

[2] https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[3] https://ec.europa.eu/info/files/communication-european-strategy-data_en

[4] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[5] https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf

industry, in particular the Digital Services Act package. ETUC welcomes the holistic approach to digitalisation and sees the willingness to provide coherence and consistency between the various initiatives to digitalise Europe, the economy and provide a better access to digital tools and infrastructure to business, workers and citizens. ETUC will however deal with digitalisation in a separate ETUC position on the new industrial strategy for Europe, due to its large scope.

Why is it important for ETUC to take a position on European AI and EU data strategies?

ETUC needs to remain active in the societal debate on AI to make it compatible with the objectives of social Europe, decent work and social progress. While the prospect of creating new employment opportunities, higher productivity and better earnings due to the rapid developments in AI have emerged, there are also fears that AI could also cause job losses and increase inequality. Investment in educating and up-skilling/re-skilling is therefore of utmost importance. Education policies aimed to better equip workers with the skills and competences needed to design and operate AI systems are crucial, however they will not be sufficient. Market dominance and market concentration of a handful of digital firms developing AI technologies and investing in AI ventures is a concern. Furthermore, tax policies should provide for a more balanced level playing field among companies, so as to allow AI technologies and their benefits to be shared more equally.

ETUC strongly believes that existing legislative tools like the GDPR do not adequately and sufficiently protect workers from the downsides of AI technologies, such as work-related stress and excessive pressure from intensive work schedules defined by AI. As developed further in this resolution, ETUC advocates for the strengthening of GDPR in the context of employment. ETUC further calls on national governments to ensure that institutions responsible for ensuring compliance with GDPR have adequate resources to do so.

Likewise, the ETUC is of the opinion that social dialogue structures, collective bargaining, information, consultation and participation of workers' representatives and trade unions are key to providing the necessary support for workers to better shape the introduction and monitoring of AI. Therefore ensuring that AI is respectful of workers' rights.

Employers' responsibility and accountability as industrial users of AI technologies, as well as ethical rules for developers and coders of algorithms, should create the appropriate legal certainty, predictability, and sound level playing field. Algorithms must comply with the rule of law and fundamental rights and be democratically designed and be understandable. They should be embedded in ethical rules. Free access to the source code must be ensured before the implementation of the AI system in the workplace. Risk assessments should demonstrate AI applications' effectiveness and compliance with verifiable transparency obligations for AI providers of an AI tool to be used at the workplace, as a prerequisite for placing it on the market.

ETUC recalls that an extensive and unregulated trust in technologies, can lead to costly failures. In extreme cases to fatalities. Self-driving vehicles have created accidents; workers have been made redundant on the basis of algorithmic decisions and platform workers have been fired for undertaking industrial action. The algorithm places at the heart of the problem the arbitrariness and decontextualisation of the decisions taken. Businesses have been hacked and workers' data have been seriously compromised. The protection of workers is therefore at stake. Proactive action should be undertaken to guarantee occupational safety, health, data protection, privacy, and human rights. Above all, it is of paramount importance that humans remain in command of the use and implications of any AI technology. Only a transparent regulatory framework can lead to predictability and secure the respect of fundamental rights of workers including privacy, and in which security and oversight are guaranteed.

Therefore, it is important for ETUC to raise workers' concerns and demands in the context of the EC white paper on AI, to ensure that AI and data driven technologies applied at the workplace are done in a safe, predictable and reliable legal framework. Such a framework must be without prejudice to national labour market models and the autonomy of national social partners and must encourage collective bargaining. ETUC stresses the importance of adopting a normative framework enabling

both workers and businesses to benefit from the opportunities of digitalisation, as well as establishing measures to prevent risks, work related abuses and violations of workers' rights. The introduction of AI technologies at the workplace should involve workers' representatives before introducing those technologies so as to organise upskilling and reskilling schemes. It should not lead to redundancies. ETUC stresses the importance of adapting the current legislative framework to enable both workers and businesses to benefit from the opportunities of digitalisation, as well as establishing measures to prevent risks, work related abuses and violations of workers' rights.

ETUC wants to make sure that real opportunities of deployment of AI and data are available to workers, and their representatives, and that opportunities are available for social partners in the context of social dialogue at European, national, sectorial and company level. AI can be useful to help in arduous tasks, improve security, improve performance and redistribution of gains among the workers.

What are the current international and national legal protection?

International and European legal instruments reaffirm the need to protect and involve workers when it comes to introducing new technologies at work. They build the fundamental basis on which any policy on AI and data should be elaborated.

International Standards

The first fundamental principle in the 'Declaration of Philadelphia' of the International Labour Organization (ILO), is that "labour is not a commodity". Workers' rights and working conditions stem from this principle. When it comes to AI and data strategies, workers' data and workers' privacy are not a commodity either, such data should not be extracted and processed for business profit or for any other commercial purposes.

The ILO Centenary Declaration for the future of work adopted by the International Labour Conference at its 108th session, in Geneva, on 21 June 2019, refers in its section III that 'The Conference calls upon all Members, taking into account national circumstances, to work individually and collectively, on the basis of tripartism and social dialogue, and with the support of the ILO, to further develop its human-centred approach to the future of work by (…) promoting sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all through policies and measures that ensure appropriate privacy and personal data protection, and respond to challenges and opportunities in the world of work relating to the digital transformation of work, including platform work'[6].

Also, at the international level, the OECD has published 'Principles on AI', it specifically calls for workers to be supported for a fair transition[7].

Council of Europe

Surveillance, monitoring, and tracking practices are not only intrusive but raise specific concerns about data protection. Related risks including the misuse of these technologies are extremely high, given the economic and financial importance of, and weight given to, data nowadays: data is the new gold. ETUC recalls the safeguards for the right to privacy and the right to data protection, laid down by the Council of Europe in the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' the so-called 'Convention 108+'[8]. In April 2020, the Council of Europe's Committee of Ministers adopted Recommendation CM/Rec(2020) on the human rights impacts of algorithmic systems, this provides a set of guidelines calling on Member State governments to ensure that they do not breach human rights through their own use, development or

---

[6] https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_711674.pdf

[7] https://www.oecd.org/going-digital/ai/principles/

[8] For the moment the 'old Convention 108' is still in force. The Convention 108+ will only enter into force when ratified by all Parties to Treaty ETS 108, or on 11 October 2023 if there are 38 Parties to the Protocol at this date. Today (June 2020) the latter is ratified by Bulgaria, Croatia, Lithuania, Poland and Serbia.

procurement of algorithmic systems as well as to ensure that governments, as regulators, should establish effective and predictable legislative, regulatory and supervisory frameworks that prevent, detect, prohibit and remedy human rights violations, whether stemming from public or private actors. Furthermore, reference can also be made to the 'Declaration of the Council of Europe on 'Digital tracking and other Surveillance technologies'[9]. As well as to the Recommendation on Artificial Intelligence and Human Rights "Unboxing artificial intelligence: 10 steps to protect human rights" of the Council of Europe Commissioner for Human Rights of May 2019.

On 11 September 2019, the Committee of Ministers of the Council of Europe set up an Ad hoc Committee on Artificial Intelligence (CAHAI), the main objective of which is 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[10]. Finally, it was decided to set up within the Steering Committee of Human Rights (CDDH), the overarching monitoring body to all Council of Europe conventions and instruments, a dedicated subgroup, a 'Drafting Group', on human rights and artificial intelligence (CDDH-INTEL). The main task of this Drafting Group outlined as follows: 'on the basis of developments in the member States, within the Council of Europe and in other fora, prepare, if appropriate, a Handbook on Human Rights and Artificial Intelligence and contribute to possible standard-setting work which would be undertaken within the Organisation'.

The Council of Europe also reflected [11] on the impact of AI during the Covid-19 pandemic, providing a detailed list of states implementing Covid-19 apps for tracing. These reflections show that AI is on the one hand being used as a tool echoing the high hopes that data science and AI can be used to confront the virus. On the other hand, AI seems to lead to a new era of personal control, revealing new capacities for state surveillance of individuals, in particular when it becomes binding and compulsory by making it part of ordinary law. More substantially, it may also create new cases of discrimination and stigmatisation, via contact tracing or proximity tracing. The trustworthiness and usefulness of these AI algorithms are therefore key and should be addressed to prevent inequalities. The extensive use of AI technologies may also lead to the acceptance of such applications, even when the pandemic crisis is over, to maintain public order or control employees. Therefore, the question of the limitation and control of AI technologies impacting freedom and rights should be addressed.

In the same vein, the European Convention on Human Rights foresees that the 'right to respect for private and family life', whereby, 'Everyone has the right to respect for his private and family life, his home and his correspondence'[12]. It should also be recalled that Article 11 of the European Social Charter (ESC) enshrines the right to protection of health. In a 'statement of interpretation on the right to protection of health in times of pandemic' of April 2020, the European Committee of Social Rights (ECSR), the main supervisory body of the ESC, acknowledged that Member States must take all necessary emergency measures in a pandemic and that this might include, amongst others, testing and tracing. However, all such measures must be designed and implemented having regard to the current state of scientific knowledge and in accordance with relevant human rights standards.

European Union

The Treaty of the European Union foresees that 'everyone has the right to the protection of their personal data. The European Parliament and the Council (…), shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities that fall within

---

[9] https://rm.coe.int/09000016805916c9

[10] For a more dedicated information on the work of the Council of Europe and AI, see also: https://www.coe.int/en/web/artificial-intelligence/home

[11] https://www.coe.int/en/web/artificial-intelligence/ai-covid19

[12] Art. 8 ECHR https://www.echr.coe.int/Documents/Convention_ENG.pdf. It is further specified that 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 society 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 or morals, or for the protection of the rights and freedoms of others.

the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[13]

The Charter of fundamental rights of the EU foresees that 'Everyone has the right to the protection of personal data concerning him or her. 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. Compliance with these rules shall be subject to control by an independent authority'[14].

The Fundamental Rights Agency FRA dedicated a large range of its activities to data protection[15]. However, little to no attention is given to workers' data protection and AI applications at work.

EU directives and regulations framing minimum labour standards fall short on providing worker protection when it comes to the impact of AI technologies at work. The European Framework Directive on Safety and Health[16] has not been adapted and revised taking into account emerging and new risks pertaining to AI. It is however worth mentioning the general principle provided by the Framework Directive of setting the responsibility on risk prevention on the employer. The General Data Protection Regulation[17] has only one provision referring to processing worker's data at the workplace. ETUC and trade unions have repeatedly requested that these instruments should be adapted according to the reality of the workplaces of today.

In 2019, the EC issued guidelines on ethics for trustworthy AI[18], this was elaborated by the High-Level Expert Group on AI, according to which AI should be lawful (i.e. respecting all applicable laws and regulations), ethical (i.e. in line with ethical principles and values, and robust (both from a technical perspective while taking into account its social environment). Furthermore, AI technologies should meet 7 requirements: 1. human dimension and oversight, 2. technical robustness and safety, 3. privacy and data governance, 4. transparency, 5. diversity non-discrimination and fairness, 6. environmental and societal well-being and 7. accountability. The 2020 European Social Partners Framework Agreement on digitalisation includes a section on Artificial Intelligence recalling the need for the human-in-control principle, in which there is a commitment to respect and comply with safety and security controls.

Within the European Commission strategy "Shaping Europe's digital future", ETUC provided input to the public consultation on the White Paper on Artificial Intelligence and that on the European Strategy for data, stressing the human rights dimension which applies to the digital revolution and with a focus on labour and trade union rights.

This human rights approach has been the ETUC's stance when contributing to recent initiatives of the European Parliament on Artificial Intelligence, namely the "Digital Services Act: adapting commercial and civil law rules for commercial entities operating online" [JURI/9/02298 2020/2019(INL)], the "Framework of ethical aspects of artificial intelligence, robotics and related technologies" [JURI/9/02261 2020/2012(INL)], and the "Civil liability regime for artificial intelligence" [JURI/9/02298 2020/2019(INL)].

ETUC will follow up any further action on AI and data to be undertaken by the European governing bodies, such as the Digital Services Act aiming to establish clear rules for all businesses to access the Single Market, to strengthen the responsibility of online platforms and to protect fundamental rights, which the Commission will present later this year. It will also propose a review of the eIDAS

[13] Art. 16 TEU https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT

[14] Art. 8 CFREU https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

[15] https://fra.europa.eu/en/themes/data-protection

[16] https://osha.europa.eu/en/safety-and-health-legislation/european-directives

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[18] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

regulation[19], allowing for a secure electronic identity that puts people in control of the data they share online. This resolution will provide the basis for ETUC's contribution to the development of these initiatives. The White Paper on Artificial Intelligence, setting out options for a legislative framework for trustworthy AI, was adopted on February 2020, and a follow-up on safety, liability, fundamental rights and data is scheduled for the fourth trimester of 2020. The European Data Strategy aimed at making Europe a global leader in the data-agile economy was adopted in February 2020 and a legislative framework for data governance is announced for the fourth trimester of 2020. A possible Data Act may be put forward in 2021. New and revised rules to deepen the Internal Market for Digital Services, by increasing and harmonising the responsibilities of online platforms and information service providers and reinforcing the oversight over platforms' content policies in the EU, may be scheduled for the end of 2020, as part of the Digital Services Act package.

At the beginning of 2019, the CEN (European Committee on Standardization) and CENELEC (European Committee for Electrotechnical Standardization) Technical Boards created the Focus Group on AI aimed at mirroring the activities at international level. In this manner they could identify potential specific European requirements, and act as an interface with the European Commission. This Focus Group is not meant to develop standards on AI but acts more as a forum to discuss European policy and how it can translate in terms of standardisation. It also explores the potential application of existing standardisation tools for AI. In the framework of ETUC's work on standards, a trade union task force has been created that follows the work of this Focus Group.

The Conclusions of the Council of the European Union on "Enhancing Well-being at Work", invites Member States to "enforce the existing Union Framework, keeping in mind the Member States' possibility to go beyond the minimum requirements laid down therein, proceed with the implementation of the Work-Life Balance Directive and follow the Council Recommendation on access to social protection for workers and the self-employed".

ETUC demands

ETUC's demands on an EU framework for AI and an EU data related strategy address the need: for inclusive governance and clear rules; adequate regulation and policy infrastructure securing good protection of workers and necessary investment; to secure that the precautionary principle should apply to AI technologies; to guarantee AI technologies, by which humans remain in control, and which is compliant with labour rights and a sound use of data; to strengthen the application of GDPR to the reality of the workplace, and to involve social partners and strengthen industrial democracy.

1. Ensure governance of data, AI and markets

The EU Commission intends to promote cross-sectoral measures for data access and use for a data-agile economy, involving both private and public players and points to the prioritisation of standardisation activities over legislation to foster data interoperability.

ETUC is convinced of the need for clear legal provisions on the responsible use of data, interoperability of the systems and conditions for data access. Such rules would not only provide more predictability and legal certainty for business, they would make the market fairer for businesses, workers, consumers and citizens. In managing better big data, interoperability rules would enable other European service providers to enter the market and prevent concentration and quasi-monopoly or an excessive share in the market. The COVID-19 crisis has shown how video-conference services have been dominated by non-European players which have led to scandals on data protection policies as GDPR does not apply to non-European players. Increased diversification would ensure a more transparent and democratic environment.

Security of data storage and access is key, therefore the EU and the Member States need to remain in control. It should be technically feasible and secure to ask an organisation to transfer the individual's personal data to another organisation, or to receive the data in an interoperable format.

---

[19] *EC Regulation No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, eIDAS.*

By doing this, individuals should get control over their data and organisations should demonstrate their compliance with EU data protection and privacy rules. Appropriate and effective sanctions should deter from any violations of data protection rules. Currently, tracing applications barely provide for the necessary security, in particular in terms of anonymisation and pseudonimisation of the data collected and stored and access to it. The consent of workers is not properly informed, as information is often hidden or difficult to access, or actualisation of apps set tracing application as default option. Workers must receive clear and transparent information of the purpose and the use of the collection of their data. Collection of workers' data must be done in consultation with and participation of the trade union representatives. The Data Protection Officers should be informed. Workers must be able to make a free and voluntary decision.

The additional challenge is to ensure that public services have the capacity – particularly in terms of resources, staff and training – to be able to control the introduction of AI and make the necessary investment in independent AI technology. Public service policies on AI should be driven by the public interest and users' real needs. It is also crucial that public authorities continue to explore the potential to develop independent and autonomous digital public services and infrastructure.

Additionally, ETUC calls for an inclusive framework that protects and promotes open-source, no-profit, social economy initiatives as relevant actors. A framework that gives these sectors the possibility to exist as AI and data driven technologies, which are mostly dominated by the corporate sector. An AI and data governance framework will help to achieve a common approach to operate in the European Digital Single Market, and a fair ground for the labour market where worker's rights are guaranteed.

Data access, storage and processing compliance with GDPR is key. The EC's strategy calls for the establishment of mechanisms to make it easier for individuals to allow the use of the data they generate for the public good, a concept that the strategy refers to as "data altruism". ETUC questions the altruism objectives that may be pursued for commercial purposes and it expresses concern about violation of privacy and surveillance, mostly in vulnerable situations like the employment relationship.

The EC's standpoint, when claiming that individuals allow the use of the data they generate on the basis of explicit and unambiguous consent, is controversial. Situations such that data collection (not least in the light of the coronavirus spread) where consent is based on opting out of a system, or practically inexistent or "forced", have proven the contrary. In addition, risks brought by biased and malicious management of data cover potential issues of discrimination, unfair practices and "lock-in effects" and cybersecurity threats. It should be reminded that non-discrimination is a fundamental right to be complied with.

2. Develop regulation for all platforms in the EU market

The situation of platform workers is not covered in this resolution, as it will be addressed by the ETUC in its upcoming position for the protection of non-standard and platform workers' rights.

Cybersecurity is a key element of data protection, even at an individual level and requires substantial investment and specific training plans: education and trainings allows the creation of the necessary culture to recognise and limit cyber risks from the very beginning.

To help Europe achieve the Sustainable Development Goals set out by the United Nations, a strong data governance framework should be in place. Such a framework should include the regulation of the GAFAMs[20] and similar platforms in the market, which are increasingly integrating different business activities, distorting fair competition in the market. Competition rules on anti-trust should be adapted to more effectively address the specificities of digital markets characterised by platforms with significant network effects, including risks of monopsony effects. Such regulation should be clear, dissuasive and prevent structural competition problems resulting in unfair competition, incontestable market concentrations and exacerbation of existing (social) inequalities. The rules

---

[20] *https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai*

must be designed to defend public interests, beyond mere competition or economic considerations, also taking into account effects on the labour market, working conditions and workers' rights.

Digital companies should contribute in a fair and progressive manner in terms of the tax on revenues generated within the EU. According to estimates, the EU has lost €5 billion in tax from Google and Facebook over the last three years[21]. Public authorities must be able to put in place fair taxation on added value and capital, and on companies benefitting the most from the transition, like in the digital sector, and to benefit from a fair share of this massive wealth, to pay for the vital services and infrastructure these companies depend on. This would echo demands and actions of member states like France to adopt digital taxation, in the expectation of the finalisation of long awaited global digital tax negotiations.

Equally, GAFAMs and other platforms should be subject to, and must comply with, the GDPR and privacy rules in Europe. Workers' rights should be fully respected, and workers' representation should be fully guaranteed.

3. Europe needs adequate regulation and policy infrastructure

The EC strategy on AI and data calls for the implementation of the different pieces of applicable legislation to the actions of the strategy through "self- and co-regulatory mechanisms and technological means to increase trust".

There is however little applicable AI legislation, in general and even less when it comes to the workplace. In addition, delegating the responsibility to regulate AI to private actors with vested interests is questionable. This will inevitably lead to wide differentiation in terms of protection, with a clear bias for putting on the market AI technologies on the basis of productivity and competitiveness. ETUC calls on the Commission to fill this regulatory gap and to enact new EU law to be implemented through national legislation or, where relevant, through collective agreements. As workers interact with digital and fast changing working environment, there needs to be a framework that protects them. ETUC is of the opinion that a European AI regulatory framework should be adopted and implemented. 'Ethics Guidelines for Trustworthy Artificial Intelligence' should be included in such regulatory framework. It would equally serve businesses and the workforce, providing legal predictability and certainty and a sound level playing field for all, whereas ethical guidelines deliver little to no practical added value and lead to a fragmented approach. The same goes for issues related to liability.

In the same vein, the Commission seems to favour self-regulation, codes of conduct, and standardisation processes regarding the creation of a cloud data services marketplace that should comply with European requirements on data protection and security. Again, it is questionable whether private norms can and should provide the necessary safeguards in term of security and reliability of AI technologies. They can only be complementary to legally binding rules that guarantee a common playing field, which is much needed when it comes to regulating data servers operating in the EU. Cloud services in particular should be secure and reliable.

Since cloud data services process a vast amount of data of individuals, ETUC calls on the EU Commission to assess the risks related to cloud services and to provide clear rules to regulate them. In times of technological and societal changes, the EC should foster a governance framework to enhance data protection while keeping control of it. Such governance should include trade unions and workers representations, who are aware of the situations and needs of workers and businesses alike. Furthermore, it will serve to guarantee the risk assessment of the development and use of AI systems at the workplace.

Such a framework should not prejudice the national labour market models and the autonomy of national social partners and must encourage collective bargaining.

---

[21] *GUARASCIO, Francesco. (2017, September 13) EU lost up to 5.4 billion euros in tax revenues from Google, Facebook: report. Reuters. Retrieved from: https://www.reuters.com/article/us-eu-tax-digital/eu-lost-up-to-5-4-billion-euros-in-tax-revenues-from-google-facebook-report-idUSKCN1BO226*

4. The precautionary principle should apply to AI technologies

ETUC is of the opinion that innovation and precaution go hand in hand and there is no evidence that precaution hinders innovation. The often-invoked concept of "innovation principle", with no legal value, is used to detract the precautionary principle, which is enshrined in the Treaty of the Functioning of the European Union[22]. The precautionary principle can sustain technological developments and give direction to innovation. More specifically, ETUC believes that it is key in the decision-making process, where uncertainty prevails about the unintended consequences and the potential adverse effects that a technology might bring.

The Committee of Ministers of the Council of Europe has recently issued recommendations[23] related to the impact of algorithmic systems on human rights. It called on its 47 Member States to take a precautionary approach to the development and use of algorithmic systems and adopt legislation, policies and practices that fully respect human rights. This rationale becomes even more relevant at the workplace where workers are in an imbalanced power-relation derived from their employment contract, which is even more disadvantageous for atypical and precarious workers. The recommendations of the Council of Europe are aimed at employers. Where automated decision making at the workplace can negatively impact workers, the precautionary principle should apply. The ETUC is of the opinion that such technologies are inappropriate to resolve issues relating to both individual and collective labour relations.

5. Prioritise AI applications embedding labour rights and a sound use of data.

The deployment of AI technologies at the workplace can have many applications, where benefits can be real. For example, these technologies can be deployed to improve safety and security, improve working conditions through assistance systems, or to help master challenging tasks. These applications, and how they are used, need to be transparent to the workforce, so that workers can understand the purposes and outcomes of such applications as well as the use of the collected data.

However, the risks associated with AI technologies are equally important and may vary depending on the sector, the context in which the technology is applied, and the national regulatory framework. Risks should be properly identified and addressed to be avoided and mitigated. Specific attention should be paid to the prevention of occupational health and safety risk, including psychosocial risks. ETUC demands that risk assessment be carried out to counteract the possible adverse outcomes. This also requires the involvement of trade unions. A prerequisite for risk assessment in the workplace would set out the duty of AI developers and designers towards transparency and information about the functionality, opportunities and possible adverse effects that the AI technology and, in particular, the algorithms could bring. This is key to clarifying the responsibilities of the various actors involved. ETUC challenges current business models that abusively collect and use workers' data.

Algorithms are well-known to be a possible source of different kinds of discrimination, as they are often built on stereotypes and limited diversity in data sets and design team; ETUC identified high risks of gender-based discrimination[24]. Equal emphasis should be put on risks related to the use of biased algorithms when it comes to violation of workers' rights. A significant example is Deliveroo's practice to disconnect workers from the platform because of their industrial action. The same applies, when algorithms are circumventing hiring and firing procedures, where decisions are left to AI applications, for example Amazon algorithms dismiss workers without the intervention of a human

---

[22] *See Art.191 TFEU*

[23] *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies). Available at:* *https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154*

[24] *ETUC (2020) Artificial Intelligence will it make bias against women worse? https://www.etuc.org/en/publication/artificial-intelligence-will-it-make-bias-against-women-worse*

decision on the basis of programmed benchmarks[25]. Such practices should be normatively addressed, discouraged and sanctioned. ETUC opposes business models unduly collecting and using workers' data. ETUC asks the governments' institutions to support research to develop measurement studies and bias prevention methodologies to prevent the spread of biased discriminatory algorithms. Algorithms should be audited in relation to their purpose. The use of traceability helps to guarantee the social and environmental conditions of the manufacturing of AI products and services.

The EC White Paper proposes a risk-based approach to help ensure that the regulatory intervention is proportionate. Basically, the Commission suggests normatively regulating only those AI applications that, on the basis of criteria yet to be defined, are considered 'high risk'[26]. All other AI applications would thus be only subject to voluntary self-regulation.

The ETUC welcomes the fact that 'in light of its significance for individuals and of the EU acquis' the EC has identified 'the use of AI applications for recruitment processes as well as in situations impacting workers' rights be always considered as "high-risk"' in principle, and has proposed corresponding regulations to guarantee a higher protection for workers. ETUC explicitly demands that AI applications introduced at the workplace and impacting workers' rights and working conditions should be classified as high-risk in principle and subject to appropriate regulation. ETUC also demands that the high-risk classification for applications affecting workers be extended to all employed persons and include the working conditions and career prospects of employees. For consistency and coherence, such rules should be binding and enforceable, via legislation and/or collective agreement, as voluntary guidelines have reduced and fragmented impacts, and their effectiveness is very limited. ETUC believes that the liability regime of AI applications at work deserve proper attention, whereby the burden of proof should lie on employers, to balance the limited access to information to workers. Liability should rest on developers, coders, AI designers and business, and not with AI systems.

ETUC calls for algorithmic transparency and accountability. All algorithm-based decisions should be explainable, interpretable, understandable, accessible, concise, consistent, transparent, in line with GDPR principles and provisions. To comply with this requirement, all algorithm-based decisions that have an impact on workers must be audited by an independent body. The approach to data processing needs to be dynamic because its use is part of a process, from the extracting process to the correlations and causations between them.

ETUC calls for greater diversity in the designing of algorithms which takes into consideration gender perspective and the heterogeneity of society. Consequently, diversity standards must be established in the teams that program these computer solutions, favouring the presence of women and minority groups in them, in order to transpose the existing gender balance in our society. For all these reasons, we propose to articulate measures to promote gender equality and diversity among those responsible for programming and auditing algorithms.

6. Strengthen GDPR rules at work

The EU white paper on AI and the EU strategy for data barely take into account workers' interests. It is unfortunate that no reference is made to Art.88 GDPR, on processing data in the context of employment which could be used as leverage for enhanced data protection for workers. Such data could specifically relate to recruitment, performance, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and dismissals. Furthermore, trade union representatives should be involved in monitoring the compliance with the GDPR of a given AI system at the workplace. The aim is to lay down measures to safeguard the human dignity,

---

[25] *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

[26] *As example the White Paper suggests that 'In light of its significance for individuals and of the EU acquis addressing employment equality, the use of AI applications for recruitment processes and in situations impacting workers' rights would always be considered "high-risk". (…)The use of AI applications for the purposes of remote biometric identification and other intrusive surveillance technologies, would always be considered "high-risk" and therefore the below requirements would at all times apply.'*

legitimate interests and fundamental rights, with particular regard to the transparency of processing data, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity, and monitoring systems at the workplace.

ETUC calls on the Commission to enhance the Union framework on privacy, data protection and security, to better regulate the internet-connected objects and networks that connect and process data. Therefore, ETUC is of the opinion that employers should inform workers and workers' representatives about which data is collected, where this data is stored, who or which institution or organisation is processing this data, the purpose of this data processing and to whom or to which other institutions or organisations this data is transmitted. ETUC calls on the Commission to enhance the EU framework on privacy, data protection and security, to better regulate the internet-connected objects and networks that connect and process data.

ETUC is of the opinion that any EU framework on AI should therefore address specifically workplace related situations and tackle possible abuses. It should promote the recourse to social dialogue and collective agreements to shape a sustainable design, introduction and monitoring of AI technology at work. Additionally, trade unions should be able to contact national data protection authorities and provide them with information about specific situations of workers.

As a prerequisite, trade union representatives should be equipped with the necessary skills and knowledge to cope with this request and be involved in the process. Such support rests on information and consultation rights enshrined in EU and national legislation and collective agreements. They should therefore be observed as mandatory rules for the governance of data appertaining to labour. However, the proposed framework fails to address the specific needs for workers in the imbalance of bargaining power existing in an employment relationship to secure their rights.

Whenever workers' data is collected and processed at the workplace or in the frame of the enterprise operations, workers' freely given, specific, informed and unambiguous consent is key as well as prior information and consultation of their representatives. However, and as ruled by the GDPR, for the majority of data processed at work, the legal basis cannot and should not be the consent of the employees due to the unbalanced nature of the employer and employee relationship. Processing may be necessary on other grounds, e.g. for the performance of a contract or it may be imposed by law. When consent is used as a legal basis for data processing, consent should therefore in principle only be valid if supported by a collective agreement and it is renewed throughout the process of data processing. The same logic needs to apply when the employer processes workers' data for further/other uses that were not foreseen before. Likewise, sectorial and cross-sectorial collective agreements are key instruments, when it comes to reaching agreements on workers' data going beyond the company level.

ETUC calls for a democratisation of AI and data governance. Trade unions must play a significant role in the new governance of data and AI and the EC must ensure that GDPR rights are fully guaranteed in the employment context. This is particularly true when it comes to the exercise of unambiguous and informed consent but also the right to access information on AI applications, the right to rectification, the right to erasure (thus extending "the right to be forgotten" to the work environment), the right to restrict processing, the right to data portability (as transferring the personal data of a worker can be of particular interest in certain contexts, as ratings), the right to object (request ceasing of processing of the personal data of a worker) and the right not to be subject to a decision based solely on automated processing.

7. Guarantee workers' protection via social dialogue and collective bargaining

A robust AI and data governance should enable workers to: (a) not be negatively affected by algorithmic decision making and effectively get knowledge of the logic involved in any automatic processing of data concerning him/her; (b) not surrender their privacy rights; (c) adequately exercise their data protection rights at work, including the assistance of trade unions to achieve so and (d) enable workers' representatives to play a key role in deciding how workers' data is used, stored or shared within the context of employment.

Public rules leading to even more intrusive surveillance based on AI technology are adopted in relation to extraordinary events like a terrorist attack or a pandemic. Such rules should be subject to prior democratic debate, limited to a specific duration of time, and followed by democratic decisions. However, in many occurrences, due to the emergency, rules are passed, restricting or infringing fundamental rights, which are increasingly fighting back against these systems[27]. Tracking and surveillance technologies are increasingly present in society, which puts workplace privacy and data protection at risk. Workplace surveillance can involve direct, indirect and remote technologies and analytics. They often unduly impact workers and threaten their rights, such as the freedom of association, of expression, non-discrimination and digital freedoms. They also amplify existing inequalities. Surveillance is not, by default, legitimate, necessary or proportionate at the workplace. AI and digital strategies must ensure that labour inspectorates and trade unions are effectively empowered to control the extent and the lawfulness of AI related surveillance technologies. Workplace surveillance can involve direct, indirect and remote technologies and analytics. They often unduly impact workers and threaten their rights, such as the freedom of association, of expression, non-discrimination and digital freedoms. An example of this would be Facebook attempting to blacklist the word "unionize" from its application "Facebook Workplace".

In accordance to Art 9 GDPR on the processing of special categories of personal data, ETUC calls on the EC to respond to this threat and ban intrusive surveillance technologies, including biometric and facial recognition, data driven analytics incorporating algorithmic predictions and chip implants. The related risks and potential for abuse largely outweigh the benefits. At work, such AI technology may lead to significant violations of workers' privacy. In exceptional situations, biometric processing technologies, such as facial recognition, should remain extremely exceptional and be limited to specific and clear circumstances established by law or, where relevant, a collective agreement. This could lead to a system designed on data protection (a privacy-by-design), allowing the use of "intrusive" technologies only with a robust protection of users and their data.

The DNA of the European Social Model lies in the tripartite organisation of social policies. In the same vein, European trade union organisations and employers' associations should be associated with the co-creation of the European AI and Data strategy to engage in AI technologies that serve quality employment, enhanced qualifications and upskilling, outsourcing of tasks, promoting working conditions and an environment that is respectful of workers, health and safety, workers' privacy and data protection. and effective access to social protection.

ETUC welcomes the call for investment in skills and general data literacy with a dedicated funded program under "Digital Europe", included in the EU strategy for data. ETUC also welcomes the call from the Council of the European Union stressing that "adequate education, training, life-long learning and skills are a prerequisite for an innovative and competitive workforce". ETUC calls for concrete support in early identification of skill needs and planning of employment and of future skills needs. Thus building 'Data literacy' through on-the-job training schemes to make AI more accessible to workers and workers' representatives. Equally the EC should develop and support 'AI literacy', so that workers are able to understand the role of data and AI in their workplace, its impact on the organisation of their work, be critically aware about the role and impact of working with AI systems, and level up their AI literacy for any job in their working life and achieve a stronger role in the socio-economic transition. This would definitely raise the ability to engage with AI and data management by trade unions in the working environment.

Likewise, if AI systems use personal data, that data should be used in a way that is legal and comprehensible to anyone concerned. Workers and their representatives on all levels must be appropriately informed about AI methods, and AI systems should be designed and documented in a way that allows the decisions to be traced and understood. The demands concerning documentation, transparency, and traceability may differ depending on each system's function, application scope and risks".

---

[27] EDRi (2020) Surveillance: Document Pool. https://edri.org/facial-recognition-document-pool/

ETUC is of the opinion that an independent public authority could be dedicated to the monitoring of AI technologies and should address the specificities of the workplace. Such authority could be equipped with regulatory powers and trade unions should be significantly represented in its decision-making bodies. The idea of an EU Agency on AI would be innovative. However, ETUC would prefer to opt for the existing EU bodies and complement their mandate with AI related dimension, in coordination with dedicated national authorities. ETUC could consider calling on the European governing bodies to give a mandate to the Fundamental Rights Agency (FRA) to deal with AI, with a focus on labour related aspects.