**Follow up to the European Parliament non-legislative resolution on artificial intelligence: questions of interpretation and application of international law
in so far as the EU is affected in the areas of civil and military uses and
of state authority outside the scope of criminal justice**

1. **Rapporteur:** Gilles LEBRETON (ID / FR)
2. **Reference numbers:** 2020/2013 (INI) / A9-0001/2021 / P9\_TA-PROV(2021)0009
3. **Date of adoption of the resolution:** 20 January 2021
4. **Competent Parliamentary Committee:** Committee on Legal Affairs (JURI) and Committee on Foreign Affairs (AFET)
5. **Brief analysis/ assessment of the resolution and requests made in it:**

The resolution covers civil and military use of artificial intelligence (AI) and calls for an EU legal framework for ethical aspects, liability, transparency and accountability for AI. The resolution highlights that a harmonised approach to AI should be based on a common definition of AI and calls for steps to ensure that the fundamental values of the European Union, the principles of the Charter of Fundamental Rights and international human rights legislation are upheld.

Concerning the uses of AI in defence, the resolution [reiterates the European Parliament’s call](https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html) for an EU strategy to prohibit lethal autonomous weapon systems (LAWS) as well as a ban on the so-called ‘killer robots’. The European Parliament underlines that human dignity and human rights must be respected in all EU defence-related activities and calls on the Commission to support the research, development, deployment and use of AI for preserving peace and preventing conflict (paragraph 42). On the civil use of AI, the resolution specifically focuses on the use of AI systems in connection with the exercise of state authority and in public services, including health, justice and transport. The resolution stresses that strict control criteria, among others regarding AI’s security, transparency, accountability, non-discrimination, social and environmental responsibility, are necessary to ensure that the use of AI systems in the decision-making process of public authorities does not negatively affect citizens. The resolution also calls on the EU to take a leading role in creating and promoting a global framework governing the use of AI, in military and civil domains, alongside the United Nations (UN) and the international community. To enhance EU competitiveness in AI research, the report advocates a stronger dialogue between Member States, researchers, academics, civil society and companies, which the Commission should promote.

1. **Response to the requests and overview of the action taken, or intended to be taken, by the Commission:**

Overall, the Commission welcomes the Parliament’s resolution on “*artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice.*” It emphasises the importance of artificial intelligence and highlights the benefits and complex challenges in civil and military areas, as well as the need for a comprehensive EU legal framework for AI.

***Definition of AI***

The Commission takes note of Parliament's call to adopt a common **European legal framework with harmonised definitions** and common ethical principles (paragraph 1). In this context, the Commission notes the Parliament-proposed definitions of an ‘AI system’ and for the concept of ‘autonomous AI’. As set out in its White Paper on Artificial Intelligence[[1]](#footnote-1), the Commission considers that AI definition needs to be future proof. As a follow up to the White Paper, a legislative proposal for a regulatory framework for AI is scheduled for the first half of 2021. The Commission considers that in any new legal instrument, the definition of the technologies concerned will need to be precise enough to provide the necessary legal certainty, while leaving some flexibility to accommodate technical progress. The results from the public consultation that the Commission carried out in the first half of 2020 have also highlighted the need for a clear definition of the scope of the future regulation. The Commission is therefore very carefully examining the definition and possible scope of application of potential regulation and it agrees with the European Parliament that a European legal framework with a harmonised definition and common principles is necessary.

The White Paper on AI does not address the development and use of AI for military purposes.

However, the Commission and the Member States have started preliminary consultations in 2020 to discuss challenges associated with the control of trade in dual-use items that use AI and could have military or other security applications. It is also planned to set up an expert group in 2021 to pursue discussions on controls of trade of emerging technologies, including those using artificial intelligence. Moreover, in view of the adoption of the new Dual-Use export control Regulation in 2021, the Commission is considering possible options for the control of exports of certain AI-powered cyber surveillance technologies, including facial recognition and biometrics, with a view to prevent their possible misuse for human rights violations.

***AI and the defence industry***

The resolution calls for increased **investments in European AI for defence** and in the critical infrastructure that sustains it (paragraph 55), and for increased **defence cooperation** among Member States and the development of new European defence capabilities in AI (paragraph 85). AI as a key enabling technology for all defence capability areas will increasingly be addressed in the European Defence Fund’s (EDF) annual work programmes.

The objective of the EDF is to foster competitiveness, efficiency and the innovation capacity of the European technological and industrial base throughout the Union. It does so by supporting collaborative research and development (R&D) projects that are consistent with defence capability priorities commonly agreed by the Member States. The EDF aims at contributing to greater efficiency of defence spending within the Union, achieve greater economies of scale, reduce the risk of unnecessary duplication and reduce fragmentation of defence products and technologies. There is a clear trend of digitisation of military operations and missions, and Europe’s armed forces cannot afford to lag behind in these new developments. AI can bring many benefits for the armed forces by providing faster and better information and decision-making, by ensuring collaborative warfare and providing for greater protection of soldiers from risky tasks or for systems that take care of routine tasks. The EDF precursor programmes, the Preparatory Action for Defence Research (PADR) and the European Defence Industrial Development Programme (EDIDP), already provided funding to three AI-related defence projects.

The resolution also recalls the **dual-use potential of AI-enabled solutions** (paragraph 86). In the implementation of the EDF, the Commission will aim at exploiting synergies between civil and military research and will explore necessary mechanisms to ensure the complementarity of funded R&D actions in the civil and defence domain, avoid double-funding and foster uptake or spill-over of the results between the two domains. The Action Plan on synergies between civil, defence and space technologies[[2]](#footnote-2) establishes a methodology and a list of concrete actions to this aim.

Furthermore, the resolution calls for AI-enabled systems in security and defence to ensure that humans are in charge to exert meaningful control (paragraph 26) and recalls its position that the use, the development or **the production of lethal autonomous weapon systems** without meaningful human control is not eligible for EDF funding (paragraph 41). In response to these calls, it should be highlighted that the EDF Regulation requires that R&D projects supported by the Fund should comply with relevant international, Union and national law, as well as with the ethical principles reflected in them. The EDF Regulation specifically prohibits the funding of actions related to the development of LAWS without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes against humans. It allows the possibility of providing funding for actions for the development of early warning systems and countermeasures for defensive purposes.

The Commission will also attach great importance to ensure that the R&D projects selected for funding are ethically sound. The EDF Regulation foresees an ethical screening and assessment procedure set out in Article 7 that provides for ethical screening of all fundable R&D projects, including for R&D projects involving emerging technologies such as AI. Actions that are not ethically acceptable are rejected. This addresses the resolution’s call for high **ethical standards** for the use of AI in various areas of the defence sector (paragraph 81). The Commission is preparing a guidance on ethics for applicants and independent experts assisting the Commission in the ethical screening and assessment of EDF projects. The guidance will be published in summer at the launch of the first EDF call. The Commission will also monitor the compliance with ethical aspects of EDF funded projects during their entire lifecycle.

Concerning the **dialogue with stakeholders** (paragraph 26), the Commission shall, for the implementation of the EDF, be assisted by a Committee within the meaning of Regulation (EU) 182/2011 (EDF Programme Committee) and as such provides for the dialogue with Member States. The Commission will also engage in discussions with relevant stakeholders, including researchers, academics, civil society and the private sector to ensure the success of the Fund.

***AI and cybersecurity***

The resolution shares the view of the Parliament on the importance of **cybersecurity** (paragraph 57). Cybersecurity and cyber defence are important features for both civil security and defence.

The Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, recognised the need to establish synergies between cyber defence actions within the scope of the EDF and Union activities in the field of cybersecurity. The EDIDP, being one of the precursor programmes for the EDF, selected for funding projects related to the development of a cyber-situational awareness platform, a tactical and military encrypted network, and a state of the art European command and control solution for the conduct of military operations (paragraphs 4, 11 and 57). Investments in collaborative capability development projects in cyber defence are likely to continue under the EDF.

Moreover, on 16 December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy adopted the EU Cybersecurity Strategy for the Digital Decade[[3]](#footnote-3) that sets out how the EU will enhance the protection of its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open Internet. The Cybersecurity strategy forms a key component of the Commission’s approach set out in its Communication on ‘Shaping Europe’s digital future’[[4]](#footnote-4), the Recovery Plan for Europe, the EU Security Union Strategy[[5]](#footnote-5), the Global Strategy for the EU’s Foreign and Security Policy, and the European Council Strategic Agenda 2019-2024. Furthermore, to address specific AI-related cybersecurity risks, the EU Agency for Cybersecurity (ENISA) established a multidisciplinary Ad Hoc Expert Group on cybersecurity topics related to AI.

***AI and civil protection***

Regarding the resolution’s call on the Commission to facilitate research into and discussion on the opportunities for using **AI in disaster relief, crisis prevention and peacekeeping** (paragraph 18), the Commission would like to point to the EU civil security research programme. Since 2007, this programme funded more than 700 projects with over EUR 3 billion. It includes exploring the use of AI in disaster relief and crisis prevention. In particular, projects from the Disaster Resilient Societies (DRS) part of the programme are exploring the use of AI in disaster relief and crisis prevention, noting, however, that AI is an enabler and not an objective per se. Moreover, there are many technological developments supported by the EU security research programme that may also make use of AI: from interoperable communications to robotics to detection of (or using) Unmanned Aerial Vehicles, to wearable equipment just to name a few. Examples of the supported projects include:

- TOXI-TRIAGE (Integrated And Adaptive Responses To Toxic Emergencies For Rapid Triage: Engineering The Roadmap From Casualty To Patient To Survivor [http://toxi-triage.eu](http://toxi-triage.eu/)), which researched detection of chemical substances through unmanned vehicles and helping triage of victims (e.g. in the aftermath of an explosion).

-ANYWHERE (EnhANcing emergencY management and response to extreme WeatHER and climate Events [http://anywhere-h2020.eu](http://anywhere-h2020.eu/)), which developed an impact-forecasting system for hydrometeorological extreme events with direct communication to civil protection units, helping rapid decision-making for examples for evacuations of areas of flashfloods risks.

While the EU civil security research programme is mainly focused on internal civil security and addresses peacekeeping only occasionally, it includes examples of research on technology and knowledge to support peacebuilding and/or civilian humanitarian missions (such as in the GAP project (Gaming for Peace, <https://cordis.europa.eu/project/id/700670>), and in the iTRACK project (Integrated system for real-time TRACKing and collective intelligence in civilian humanitarian missions [https://www.itrack-project.eu](https://www.itrack-project.eu/)). The Commission will continue supporting research on opportunities – as well as challenges – of AI for disaster relief and crisis prevention and preparedness throughout the civil security research programme of Horizon Europe. More examples of projects and details can be found on the Commission’s Community Research and Development Information Service (CORDIS) (<https://cordis.europa.eu/en>).

***Other societal uses of AI***

The Parliament notes that the use of **AI systems in the decision-making process** **of public authorities** can result in biased decisions that negatively affect citizens, and therefore stresses that use of AI systems should be subject to strict control criteria regarding their security, transparency, accountability, non-discrimination, social and environmental responsibly, among others (paragraph 52). This position is broadly in line with the White Paper proposed requirements for high-risk AI applications that should comply with certain mandatory requirements (e.g. as regards training data, documentation and record keeping, transparency, human oversight, accuracy and robustness). The Commission is currently analysing the content of these possible requirements and the possible corresponding obligations for providers and users of high-risk artificial intelligence systems. The Commission will carefully examine the various requirements proposed by the Parliament.

The Commission agrees that use of facial recognition systems need to be carefully assessed (paragraph 56). As regards the gathering and use of biometric data for remote identification purposes in public areas, such as facial recognition, the Commission, is currently assessing the issue, taking account of the identified specific risks and of fundamental rights, notably the data protection rules, and of the views expressed in the resolution.

**Skills for AI-driven solutions**

The Commission shares Parliament’s insistence on the importance of investing in human skills, including **digital skills**, in order to adapt to scientific progress involving AI-driven solutions (paragraph 24). The White Paper on AI underlined that the European approach to AI will need to be underpinned by a strong focus on skills to fill competence shortages. The results of 2020 European enterprise survey on the use of technologies based on AI suggest that one of the key barriers European companies face when adopting AI technologies is the availability of employees with adequate AI skills.

In September 2020, the Commission adopted a new Digital Education Action Plan for the period 2021-2027[[6]](#footnote-6). This action plan includes specific actions for the improvement of AI skills into the larger context of promoting digital skills. In detail, a specific action will promote the understanding of emerging technologies and develop ethical guidelines of AI and Data usage in education and training. Additionally, the Action Plan foresees the update of the digital competences framework, in order to include emerging technologies, such as AI, data management, just to name a few. The Commission has also supported EU Code Week, a volunteer-led movement that brings computational thinking, coding, robotics, tinkering with hardware, computer science, AI and digital skills to as many people as possible.At the end of 2020, in order to support Member States in their effort to increase the specialised education offer in AI, the Commission awarded grants to four networks of universities, small and medium sized enterprises (SMEs) and AI excellence centres to deliver excellent master’s programmes in AI, for a total of EUR 6.5 million. The selected networks should jointly design and deliver high-quality and hands-on master’s programmes in different Member States, with a specific focus on human-centric AI, AI application for the public administration and AI for healthcare. All the programmes should also include AI ethics courses and part of the content should be made available online through the Digital Skills and Jobs Platform translated into all EU languages.

Furthermore, in its Communication on ‘2030 Digital Compass: the European way for the Digital Decade’ (COM(2021) 118 final), the Commission identified a digitally skilled population and highly skilled digital professionals as one of the four ‘cardinal points’ for mapping the EU’s trajectory, as part of a ‘Digital Compass’ to translate the EUʼs digital ambitions for 2030 into concrete targets and to ensure that these objectives are met. The Communication recalls that the European Pillar of Social Rights Action Plan includes the objective to increase the share of adults with basic digital skills to 80% by 2030[[7]](#footnote-7), and includes the target to increase the number of employed ICT specialists to 20 million by the same year, with convergence between women and men.

Regarding the Parliament’s call to duly take this into account as part of the implementation of Directive 2005/36/EC (paragraph 24),the Commission notes that Directive 2005/36/EC does not define the skills or other training requirements for professions except for certain ones, mostly in the health area with a view to facilitating mobility. The Commission recalls that Directive 2018/958 (Proportionality Test Directive) aims at preventing unjustified or disproportionate regulatory requirements for regulated professions from being put in place. Rigorous application of the framework for ex-ante proportionality assessments will help Member States in preventing unjustified hindrance of AI developments and at the same time in ensuring the protection of justified public interest objectives.

**AI and data protection**

As regards data protection issues related to AI (paragraph 62), the Commission recalls that pursuant to the General Data Protection Regulation (GDPR), the European Data Protection Board (EDPB) has the task to ensure the consistent application of this regulation. The EDPB may issue guidelines to this end as regards processing activities falling within the scope of the GDPR and the Law Enforcement Directive. The EDPB has already issued guidelines on automated decisions, including profiling. It has announced in its Work Programme to issue guidelines on AI.

**AI and judicial matters**

Regarding paragraph 73 of the resolution, it is worth recalling that legal tech companies may develop creative software applications. It is up to the judicial administrations to decide if they need these applications to increase the quality and efficiency of courts (e.g. for the analysis and summary of written submissions, case-law research, translation, anonymisation,) by automating routine and repetitive tasks, provided of course that the applicable rules of EU and national law are respected. When it comes to the substance of a case, an algorithm cannot replace the human judge. Software can be used to gather information or automate processes and procedures based on patterns or rules, where those procedures do not allow for discretion. However, judicial decisions involving abstract and conceptual thinking are highly unlikely to be subject to automation given the limits of AI technology, and, in any event, must not be fully automated.

**AI and transport**

The resolution calls to continue promoting AI research and the exchange of good practices in transport (paragraph 77) and to carry out an evaluation of the use of AI and similar technologies in the transport sector (paragraph 84). In December 2020, the Commission adopted its Sustainable and Smart Mobility Strategy, which provides (among other things) for the development of an AI roadmap for mobility. The Commission also announced a European mobility data space in its European Data Strategy[[8]](#footnote-8) published in February 2020. AI technologies affect all modes of transport and the EU has already developed initiatives to benefit from its potential, including in road, aviation, rail and waterway sectors. For example, in the road transport sector, the Commission underlines the work of the Cooperative, Connected and Automated Mobility (CCAM) Platform and of the upcoming CCAM Partnership under Horizon Europe, which will include a cluster on procedures, methods and tools for the validation of high-level automation. Moreover, in the automotive sector, new rules on automated vehicles, cybersecurity and software updates of vehicles will become applicable as part of the vehicle type approval and market surveillance legislation as from 7 July 2022.

1. COM(2020) 65 final [↑](#footnote-ref-1)
2. COM(2021) 70 final [↑](#footnote-ref-2)
3. JOIN(2020) 18 final [↑](#footnote-ref-3)
4. COM(2020) 67 final [↑](#footnote-ref-4)
5. COM(2020) 605 final [↑](#footnote-ref-5)
6. COM(2020) 624 final [↑](#footnote-ref-6)
7. COM (2021) 102 [↑](#footnote-ref-7)
8. COM(2020) 66 final [↑](#footnote-ref-8)