EU contribution to the report of the Office of the UN High Commissioner for Human Rights for the thematic report on the relationship between human rights and technical standard-setting processes for new and emerging technologies- for HRC 53rd session

The European Union would like to thank the Office of the UN High Commissioner for Human Rights for the call for contributions for the upcoming report on the relationship between human rights and technical standard-setting processes for new and emerging technologies to be presented during the 53rd session of the Human Rights Council.

The contribution from the European Union has been drafted by the European External Action Service (EEAS) in consultation with the European Commission (DG CNECT and DG GROW).

The questionnaire was used as guidance to structure the input. Our contribution is structured as follows:

I) **Introduction**
II) **EU's global approach to Standardisation**
III) **Zooming in: EU's legislation on Artificial Intelligence**
IV) **Duties and responsibilities of standard setting organisations**

I) Introduction

In line with the EU Action plan for Human Rights and Democracy 2020-2024, the EU continues to take a strong stance in favour of regulating the digital sphere, in order to ensure that human rights are respected both online and offline.

In multilateral fora and in its bilateral relations, the EU promotes the right to privacy and data protection, and condemns internet shutdowns, online censorship, hate speech online, mass and arbitrary surveillance, online gender-based violence, information manipulation, disinformation and cybercrime. The EU continues to promote a human rights-based approach to the design, development, deployment, evaluation and use of Artificial Intelligence (AI).

The Council Conclusions on EU Digital Diplomacy adopted on 18 July 2022, underline that the EU digital diplomacy, built on universal human rights, fundamental freedoms, the rule of law and democratic principles, will be carried out in close collaboration with like-minded partners, and advance a human-centric and human rights-based approach to digital technologies in relevant multilateral fora and other platforms. EU's diplomatic efforts are in line with its strong efforts to regulate the digital space within the EU.

At the European Union level, we have put citizens at the heart of our digital discussions in order to develop digital policies that empower people and businesses to seize a human centred, sustainable and more prosperous digital future. This is the goal of the European Commission communication "**2030 Digital Compass: the European way for the Digital Decade**", which, among other policy objectives, seeks to ensure full respect for human rights in the digital space, including access to diverse, trustworthy and transparent

information, protection of personal data and privacy, and the protection of intellectual creation in the online space.

II) EU's global approach to Standardisation

The primary objective of standardisation in Europe is the definition of voluntary technical or quality specifications with which current or future products, production processes or services may comply.

European standardisation is organised by and for the stakeholders concerned based on national representation (the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC)) and direct participation (the European Telecommunications Standards Institute (ETSI)), and is founded on the principles recognised by the World Trade Organisation (WTO) in the field of standardisation, namely coherence, transparency, openness, consensus, voluntary application, independence from special interests and efficiency ('the founding principles'). In accordance with the founding principles, it is important that all relevant interested parties, including public authorities, civil society and small and medium-sized enterprises (SMEs), are appropriately involved in the national and European.

The EU supports an effective and coherent standardisation framework, which ensures that high quality standards are developed in a timely manner. The European Commission issues standardisation requests and supports financially the work of CEN, CENELEC, and ETSI. But it does not interfere with the standardisation setting conducted by industry or National Standardisation Bodies.

The EU's standardisation strategy adopted in 2022, leverages the European standardisation system to deliver on the twin green and digital transition and supports the resilience of the single market. Thus, it helps meeting the challenges of the digitisation of the economy by outlining the EU approach to standards. This aims at ensuring that technologies such as internet of things or artificial intelligence incorporate the respect for human rights, core democratic values and interests, data protection rules, and cybersecurity.

Standards are the silent foundation of the EU Single Market and global competitiveness. They help manufacturers ensure the interoperability of products and services, reduce costs, improve safety, and foster innovation. A product or a service complying with European standards supporting EU legislation and thus published in the EU Official Journal , guarantees that it is in line with EU law, thus it is fit for purpose, is safe and will not harm people or the environment.

The European Commission supports the participation of societal stakeholders (consumers, environment, SMEs, trade unions) in the European standardisation activities. Overall, stakeholders can participate in the work of the national standardisation bodies that are then involved in the CEN and CENELEC activities, or directly in ETSI if they are member of it. The ESOs provide annual reports on the participation of societal stakeholders in their activities.

III) Zooming in: EU's legislation on Artificial Intelligence

Artificial Intelligence (AI) is a fast evolving family of technologies. AI systems can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies, especially in high-impact sectors, such as climate change, environment and health, the public sector, finance, mobility, manufacturing, agriculture or home affairs. However, the same elements and techniques that power the socio-economic benefits of AI can also bring about significant risks to human rights, democracy, and the rule of law.

Human rights and fundamental freedoms affected by AI development and use

The increasing use of new technologies such as **AI** systems can possibly affect the enjoyment of a wide range of **human rights** and fundamental freedoms guaranteed by international **human rights** instruments, including civil and political rights, as well as economic, social, and cultural rights.

Patterns and prescriptions identified by AI systems, involving highly complex data, algorithms and models, are often difficult or impossible to explain ("black boxes") and may contain hidden biases.

AI systems frequently rely on large data sets, often including personal data. This incentivizes collection, storage and processing of large amounts of personal data, which can pose risks to the right to privacy, unless appropriate safeguards, such as privacy preserving techniques, are being applied. AI tools are for example widely used to seek insights into patterns of human behaviour in order to *i.a*. make inferences and predictions. Such applications combined with those that are used for instance for prioritization of contents in search engines, ads micro-targeting, content moderation, highly personalised products and services, or systems interacting with human bodies, including brains may undermine the ability of people to make conscious choices and exercise agency. This raises questions with regard to personal autonomy and the right to freedom of opinion, and expression, and provides tools for manipulation.

AI can be instrumental to set up wide-scale surveillance systems. Remote biometric identification[1] is considered to carry a high risk to the right to privacy as a large part of the population can be extensively monitored and tracked in all places where such systems are operated. AI-based facial recognition surveillance in public places expands the abilities of State authorities to survey protests and may enable reprisals against those exercising their right to freedom of peaceful assembly, and to freedom of association, leading to the general shrinking of civic space. Due to a degree of errors in AI systems, or when they rely on low-

[1] Remote biometric identification (RBI) relies on biometric information (e.g. facial images, iris scans, gait analysis) and can give governments the ability "to ascertain the identity (1) of multiple people, (2) at a distance, (3) in public space, (4) absent notice and consent, and (5) in a continuous and on-going manner." Laura K. Donohue, "Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age." Georgetown Law, 2012. https://scholarship.law.georgetown.edu/facpub/1036/

quality data sets (unrepresentative, faulty and incomplete data, poor research/data collection design, limited volume and lack of diversity, historical biases) or algorithms, they may produce discriminatory or otherwise incorrect results. AI systems may also perpetuate and even further exacerbate racial, ethnic, religious, gender-related or other biases historically embedded in societies.

AI systems providing social scoring of natural persons for general purpose may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the inherent human dignity, the principle of non-discrimination and the values of equality and justice. The European Commission´s new proposal for an Artificial Intelligence Act bans certain social scoring AI systems.

Efforts to address human rights aspects of AI

Over the recent years, discussions have emerged at national, regional and international levels on ways of promoting cutting-edge, but also human centric and trustworthy AI, with appropriately and proportionally managed risks.

The Artificial Intelligence Act, the European Commission proposal for a legislative framework for artificial intelligence, was published in 2021 and has since been discussed by the co-legislators, i.e. the European Parliament and the Council of the European Union. The AI Act, once adopted, will promote trustworthy, human-centric AI and the development of AI-related standardisation initiatives and international cooperation frameworks. The proposed framework will be applied directly in the same way across all Member States, and it applies equally to all providers, regardless of where they are based, which wish to place AI systems and products on the EU market. The AI Act is a flexible and proportionate legal framework based on a future-proof definition of AI and a risk-based approach, intervening where it is necessary owing to the unacceptable or high risk to the safety or to the fundamental rights of persons. The AI Act proposes to ban a small number of uses of AI that are not compatible with our values and violate fundamental rights, whereas so-called high-risk uses of AI will be subject to a number of requirements concerning, for example, training data, transparency, human oversight and risk management. Before putting a high-risk AI system on the market or into service in the EU, the provider of the system must perform an *ex ante* conformity assessment. This assessment is aimed at demonstrating that the system complies with the mandatory requirements for trustworthy AI. The AI Act will be implemented by means of harmonised standards that are to be developed based on a standardisation request by the European Commission.

IV) Role, duties and responsibilities of standard setting organisations

As mentioned, the EU promotes a human rights-based approach to the whole life cycle of telecommunication/ICT technologies – including design, development, deployment, use and disposal - as part of a human-centric vision of the digital transformation, including in international standard-setting processes.

In this light, the EU believes that international partners should work together to achieve a digital transformation based on openness, inclusion, equality, sustainability, resilience and security. The **International Telecommunication Union (ITU**), as a member of the UN family, has a particularly instrumental role in this endeavour and should lead by example. The EU encourages the ITU, to work with ISO/IEC and other global Standard Development Organisations (SDOs) to develop international telecommunications/ICTs standards that are consistent with existing international frameworks on human rights and fundamental freedoms.

The ITU must guarantee that all its outputs are in **full compliance with international human rights law**. In particular, it should avoid any discussion or decision on AI standards posing potential risks to human rights and fundamental freedoms of individuals, including right to privacy and to non-discrimination, and freedoms of expression, association and assembly.

Over the past year, certain ITU members are pushing for standards incompatible with universal values of human rights, which could – if adopted – negatively impact individuals and users worldwide.

This year, we welcome the close cooperation and consultation between the ITU leadership and the Office of the High Commissioner for Human Rights, which reflects the tight, intrinsic link between technical standard setting activities and international human rights principles. We encourage other SDOs to also engage with the OHCHR on this issue.

Inclusive consultation processes

It is equally important that the ITU, which builds upon the expertise of various stakeholders, including industry, SMEs, civil society and academia, redoubles its efforts to make its procedures more transparent and accessible, by including organizations and individuals active on human rights aspects of telecommunications/ICTs and representing affected and marginalized communities. Forging consensus and making sure that all stakeholders are heard forms a critical part of the ITU´s work and contributes to the high credibility of its outcomes.

Some of the common obstacles faced by stakeholders in accessing consultation processes and achieving meaningful participation are: access rights and fees, lack of resources, ability to travel to the consultations, language of the consultations or Intellectual Property Rights.

Some **key actions that should be carried out by the ITU** and other SDOs are:

- Making documentation, including during the drafting process, easily accessible to the public – without prohibitive fees.
- Establishing or strengthening public consultation processes.
- Including a greater diversity of voices, especially women, young people and those from the Global South, and other members of civil society in vulnerable situations. This would require actively reaching out to and inviting such communities to take part in the SDOs' work.
- Foster mutual understanding between the tech community and human rights actors.

Although there is not a “one size fits all”, the EU wants to recall the relevance of **WTO principles on standardisation** - transparency, openness, impartiality, consensus, efficiency, relevance and consistency-, which remain key elements for the development of standards, no matter if on a national or international level.

An open and inclusive process of standard-development will result in more credible and safer products, reflecting the needs of users.

The EU will continue to engage actively within ITU. As the largest donor to the ITU development activities, the EU also closely cooperates with the ITU and the African Union on various projects in Africa, including the “Policy and Regulation Initiative for Digital Africa” (PRIDA). We also launched in December 2020 a “Digital for Development” (D4D) Hub: a multi-stakeholder coordination mechanism for sharing digital expertise with four regions. The projects will contribute to the achievement of meaningful connectivity, which will empower individuals with the use of safe, open, and secure connection, matched with the necessary digital skills.