Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the human rights of migrants; the Special Rapporteur on minority issues; the Special Rapporteur on the right to privacy and the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance

REFERENCE:
OL OTH 229/2021

21 October 2021

Excellencies,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association; Special Rapporteur on the human rights of migrants; Special Rapporteur on minority issues; Special Rapporteur on the right to privacy and Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, pursuant to Human Rights Council resolutions 40/16, 43/4, 41/12, 43/6, 43/8, 46/16 and 43/36.

In this connection, we would like raise our concerns regarding two pieces of pending European Union ("EU") legislation: the counter-terrorism agenda entitled "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond"[1] **[**hereinafter "Agenda"] and the Proposal for Amending Regulation (EU) 2016/794 [hereinafter "Proposal"].[2] The Agenda sets out a multilateral counter-terrorism strategy engaging EU entities, Member State entities, Europol, international governments and entities, citizens and more. The strategy adopts a four-pillar approach each with a concrete set of actions to be undertaken. The Pillars are named Anticipate, Prevent, Protect, and Respond respectively. The Agenda emanated from the European Commission and was sent to the Council and Parliament on 9 December 2020. The Proposal seeks to amend Regulation (EU) 2016/794 ("Regulation 2016/794") on the European Union Agency for Law Enforcement Cooperation (Europol). The declared aim of the Proposal is to "address those areas where stakeholders ask for reinforced support by Europol to help Member States keep citizens safe" by "strengthen[ing] the mandate of Europol." The Proposal also emanated from the European Commission on 9 December 2020 and is awaiting the First Reading from Parliament.

[1] COM(2020) 795 final.
[2] COM(2020) 796 final. Official title: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation.

Ms. Ursula von der Leyen, President of the European Commission
Ms. Ylva Johansson, Commissioner for Home Affairs of the European Commission
Mr. David Maria Sassoli, President of the European Parliament
Mr. Ilkka Salmi, EU Counter-Terrorism Coordinator

The Agenda and Proposal each elicit concerns about their potential adverse impact on human rights and fundamental freedoms. The Agenda contains concerning proposed actions under each of its pillared approaches and may unduly impact the freedom of association, freedom of expression and opinion, privacy rights, and impinge upon minorities by utilizing biased technology. In particular, concerns are raised about internet content monitoring, the use of artificial intelligence and the mass collection and sharing of data. The Proposal would also enable dramatically expanded data sharing between law enforcement, private entities and third countries. While Annex 5 of the Proposal does identify human rights and fundamental freedom concerns, all proposed measures are ultimately deemed necessary and lawful despite their potential impacts. The provisions of the Agenda and Proposal impact each of a range of rights and we address these concerns below.

Overview of Applicable International Human Rights Law

We remind the Commission and Parliament that security and human rights are not mutually exclusive endeavours. The UN General Assembly has affirmed and unanimously recognized that effectively combatting terrorism and ensuring respect for human rights are not competing but complementary and mutually reinforcing goals in the Global Counter-Terrorism Strategy. (A/HRC/60/288). Moreover, relevant provisions of Security Council resolutions 1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); as well as Human Rights Council resolution 35/34 and General Assembly resolutions 49/60, 51/210, 72/123 and 72/180 require that any measures taken to combat terrorism and violent extremism, including incitement of and support for terrorist acts, comply with States' obligations under international law, in particular international human rights law, refugee law and international humanitarian law. Counter-terrorism measures must conform to fundamental assumptions of legality, proportionality, necessity and non-discrimination. Wholesale adoption of security and counter-terrorism regulations without due regard for these principles can have exceptionally deleterious effects on the protection of fundamental rights, particularly for minorities, historically marginalized communities and civil society. We wish to reaffirm the importance of the full implementation of these obligations and standards in the context of EU counter-terrorism strategies and regulation.

The principle of non-discrimination is enshrined in articles 2, 4 and 26 of the International Covenant on Civil and Political Rights ("ICCPR"), article 7 of the Universal Declaration of Human Rights ("UDHR"), Title III of the Charter of Fundamental Rights of the EU, the International Convention on the Elimination of All Forms of Racial Discrimination and is widely considered to be jus cogens norms under international law from which no derogation is permitted. Discrimination is prohibited based on grounds of, inter alia, sex, race, colour, ethnic or social origin, religion or belief and political or any other opinion.

We respectfully refer to the EU's obligations under article 17 of the ICCPR, which protects against arbitrary or unlawful interference with a person's privacy, reputation and home. Article 17 permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s]

the tests of necessity and proportionality" (A/69/397, para. 30). Article 17 of the ICCPR also includes the right to protection of personal data, which, among other things, prevents States from requiring mass retention of personal data by companies and access to personal data outside of clearly defined circumstances and subject to safeguards. The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.[3] Privacy enables the full development of the person, while protecting against harms that stunt human development, innovation and creativity, such as violence, discrimination and the loss of the freedoms of expression, association and peaceful assembly. (A/HRC/43/52, para. 16).

In this vein, we highlight the following relevant international human rights standards under articles 19, 21, 22, 25 and 27 of the ICCPR which guarantee, respectively, the right to freedom of opinion and expression, the right to freedom of peaceful assembly, the right to freedom of association, the right to take part in the conduct of public affairs and the rights of persons belonging to minorities. We would like to emphasize that any restrictions on the right to freedom of expression must be compatible with article 19 of the ICCPR. The Human Rights Committee has highlighted that the protection afforded to article 19 is particularly strong with respect to expressions on political and human rights issues (see General Comment no. 34 paras. 2 and 3 and 20). Any restriction, to be compatible with the Covenant, must be provided by law, pursue one of the exhaustively enumerated aims in paragraph 3 of article 19, and be necessary and proportionate. We also refer your attention to the UDHR, to which all Member States are parties. Articles 19 and 20 of the UDHR also guarantee the right to freedom of opinion and expression and freedom of peaceful assembly.

Article 13 of the UDHR also guarantees freedom of movement. Everyone has the right to freedom of movement and residence within the borders of each state, and everyone has the right to leave any country, including his/her own, and to return to his/her country. This principle is affirmed by article 12 of the ICCPR and article 21 of the Treaty on the Functioning of the EU ("TFEU"), permitting movement between Member States of the EU. We further remind your Excellency about the rights to fair trial and due process guarantees ensuring the rights to a fair and public hearing by an independent and impartial tribunal (article 10, UDHR), with the guarantees necessary for his defence (article 11, UDHR), and principles of legal certainly, accessibility and foreseeability (article 7, ICCPR). We therefore reemphasize that the right to a fair trial must be strictly enforced and limitations must be proportionate, necessary and non-discriminatory. Article 14 of the ICCPR contains guarantees that State parties must respect, regardless of their legal traditions and their domestic law and these guarantees cannot be left to the sole discretion of domestic law to determine the essential content of [ICCPR] guarantees (CCPR/C/GC/32, para. 4). We respectfully remind the Commission and Parliament of the requirements under international human rights law for guarantees of procedural fairness and due process of law that comprise the right to equality before the courts and tribunals and the right to a fair trial in line with article 14 of the ICCPR. In order to fulfil this right, all forms of the administration of justice must guarantee that these rights cannot be deprived through procedural practices that interfere with the overall right to claim justice. (CCPR/C/GC/32, para. 2).

[3] See UN Human Rights Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Respect of Right to Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation, 8 April 1988, and A/HRC/39/29, paras. 26 – 41.

The Agenda and Proposal in brief

The Agenda conceptualizes a "Four pillar strategy to counterterrorism: Anticipate, Prevent, Protect, and Respond". Each pillar enumerates diverse action points to be undertaken by the European Commission, the European Parliament, the Council and Member States in an effort to combat terrorism at multiple phases of preparation, action and completion. For example, the *Anticipate Pillar* [hereinafter "Pillar I"] tasks the European Commission to develop risk assessment and peer review activities and employ increased technological capabilities. The *Prevent Pillar* [hereinafter "Pillar II"] seeks *inter alia* to restrict violent extremism online and urges the adoption of the "Regulation on preventing the dissemination of Terrorism Content Online" (This regulation was the subject of previous Special Procedures communications: OL OTH 71/2018 and OL OTH 73/2020), support for local actors through the Radicalisation Awareness Network ("RAN"), and strengthening prisons, rehabilitation, and reintegration. Under the *Protect Pillar* [hereinafter "Pillar III"], critical infrastructure enhancement is sought including improving the protection of public places and places of worship, and increasing border security. This will include the establishment of a dedicated watchlist under the European Travel Information and Authorisation System [hereinafter "ETIAS"] when it launches in 2022.[4] Under the *Respond Pillar* [hereinafter "Pillar IV"], the European Commission is requested to create a network of counter-terrorism financial investigators to improve cross-border financial investigations and to propose a mandate to negotiate a cooperation agreement between the EU and Interpol. Under Pillar IV, the Commission and the EU High Representative are encouraged to negotiate international agreements with third countries to exchange personal data with Europol. Further entrenchment between public and private sector information sharing is recommended and part of the strategy.

The Proposal seeks to strengthen the mandate of Europol and also emphasises public and private sector cooperation and information sharing. This will be done in several ways. First, the Proposal is to enable increased cooperation between Europol and private parties with the aim of countering the use of cross-border services, such as communication, banking or transport services, by criminals. The Proposal would also create new rules to enable Europol to process national data where a Member State or the European Public Prosecutor's Office ("EPPO") requests Europol's analytical support for a specific criminal investigation (if Europol supports that type of criminal investigation). Europol's cooperation with third countries would also be strengthened. The Proposal also claims that there will be increased Parliamentary oversight and accountability.

We acknowledge that the Agenda emphasizes that "[d]emocracy, rule of law, respect for fundamental rights in particular the right to privacy, freedom of expression, freedom of religion and the respect for diversity, are the foundation of our Union." The Agenda stresses that "[t]he inclusive and rights-based foundations of our Union are our strongest protection against the threat of terrorism". We acknowledge that the Agenda references "fundamental rights" several times underscoring the importance of protecting these rights. The Proposal also states the need to ensure that safeguards are present to ensure that fundamental rights, in particular data protection and privacy, are

[4] The information provided will be screened against the ETIAS watchlist as well as other databases, including the SIS, VIS, ECRIS, and proposed EES.

protected. The Agenda and the Proposal are extensive in their scope as well as on the specific areas to be covered. However, the Agenda and Proposal make only broad and generic references to human rights instruments and fundamental freedoms[5] and do not appear to provide any specific reference on how compliance with human rights will be ensured or the means that will be put in place to monitor and evaluate any negative impacts on these rights. Given the overarching function of our mandates to advance the protection and promotion of human rights and acknowledging that the Agenda and Proposal have significant human rights implications, we convey our views to support the work of relevant European Union organs in advancing full respect for human rights.

The principle of legality and lack of legal certainty regarding "terrorist content" and "European values"

We are concerned that the policies found in the Agenda and Proposal may not accord with the principle of legality for criminal offences enshrined in article 49 of the Charter of Fundamental Rights of the EU, Article 7 of the European Convention on Human Rights ("ECHR") and Article 15 of the ICCPR. Under the Charter of Fundamental Rights of the EU (Article 52.1), as well as the ECHR and the ICCPR, all of which are binding on EU Member States, any restrictions of these rights must be prescribed by law, which is clear and accessible, in pursuit of a legitimate purpose, and must be necessary and proportionate to achieve that purpose. The burden lies with the state to demonstrate that these conditions are met, including the necessity and proportionality of the restriction. It is thus particularly important that the EU does not put in place policy or legislation that would appear to signal a lessening of those requirements of proportionality and necessity at the national level. Restrictions must be consistent with all other human rights recognized in international law, may not impair the essence of the rights affected and may not be applied in a discriminatory or arbitrary manner.

The requirement that, where limitations on certain human rights are permissible, they must be "prescribed by law" reflects the well-established principle of legality, a principle that similarly applies to defining all criminal offences. Thus, laws must be clear and accessible and their application in practice must be sufficiently foreseeable. They must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. They must not confer unfettered discretion on authorities, but rather provide sufficient guidance to those charged with their application to enable them to ascertain the sort of conduct that falls within their scope. (A/73/361, para. 34). This principle has been affirmed by the European Court of Human Rights as an essential element of the rule of law and an important protection against arbitrariness.[6]

---

5 The Explanatory Memorandum to the Proposal stresses "the need to ensure full compliance with fundamental rights as enshrined in the Charter of Fundamental Rights (the "EU Charter"), and notably the rights to the protection of personal data and to respect for private life." The explanatory memorandum further recognizes that "[o]ther fundamental rights may also be affected, such as the fundamental right to non-discrimination in the context of research and innovation." The Proposal specifically refers to the EU, and the right to protection of personal data and right to privacy in recital 24 and recital 46. It also refers more generally to "fundamental rights and freedoms" in recital 24 and article 1, para. 12, para. 13, para. 32, and para. 41.

6 Del Rio Prada v. Spain, application no. 42750/09, Grand Chamber, 21 October 2013, para. 77.

The Agenda and Proposal refer to "terrorist content" without providing a definition of this term. Given that the Agenda and Proposal urge for the adoption of the related EU proposal for the "Regulation on preventing the dissemination of Terrorism Content Online" [hereinafter "Regulation"],[7] it is likely that the definition of "terrorist content" contained in that regulation will apply. As noted in a joint communication (OL OTH 73/2020) concerning this Regulation, there are significant gaps in precision, clarity and legal certainty in the Regulation. The experts regret that, to date, they have not received a response to this communication. The Special Rapporteurs warn that the overly broad definition of terrorist content in the Regulation may encompass legitimate expression protected under international human rights law and may limit freedom of expression more than is necessary and proportionate to protect national security, public order or safety. They are further concerned that the Regulation does not provide adequate guarantees of judicial oversight for restrictions to freedom of expression, which may lead to arbitrary implementation. The procedure for content removal orders in the Regulation may lead to undue limitations to the right to freedom of expression in the 27 Member States of the EU.

The Agenda proposes, amongst other measures, the adoption and implementation of the aforementioned Regulation which will allow Member States to ensure the swift removal of 'terrorist content' and require private companies to be more responsive. Similarly, under Pillar II, the Agenda proposes the adoption of the "Digital Services Act", under which online platforms will be obliged to assess risk "not only as regards illegal content and products" but also systemic risks to the protection of public interest, and of an EU Internet Forum/ EU Crisis Protocol aiming at the **"**moderation of publicly available content for extremist material online".

In pursuance of the same goal, the Proposal suggests the amendment of article 4(m) of Regulation 2016/794 to include providing support to Member States' actions of "taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions". The Proposal seeks to ensure that Europol will be able to exchange personal data with private parties, including hashes, IP addresses or URLs related to "terrorist content" deeming this exchange necessary in order to support Member States in preventing the dissemination of such content.

As outlined above, such measures, as with any imposed restriction or removal of publications, are likely to affect the right to freedom of expression. Whereas valid limitations to this right can exist in the context of terrorism (e.g., the prohibition on the incitement to terrorism), the above measures fail to define or circumscribe the extent of the suggested removals (*i.e.*, the terms "terrorist content" and "extremist material" are not defined). The Agenda also sets out to "extend the list of EU-level crimes to hate crime and hate speech based on race, ethnicity, religion, gender or sexuality" in the EU Code of Conduct on countering illegal hate speech online. Based on similar considerations as identified above, this measure is also likely to have a negative and disproportionate impact on the right to freedom of expression, especially if the

[7] COM (2018) 640 final (12.9.2018).

underlying legal prescription of this recommendation is not identified, and further details on what exactly is to constitute an "EU-level [crime]" are not provided.

Regarding broader criminalization (including of terrorist activities), the principle of legality requires that the law must classify and describe offences in precise and unambiguous language that narrowly defines the punishable behaviour. Multiple proposed offences in the Agenda and Proposal are inadequately precisely defined and proscribe conduct which would trigger criminal responsibility which is insufficiently foreseeable to satisfy the principle of legality. We encourage a thorough review of proposed criminal offences in the Agenda and Proposal with a view to amendment during ongoing consideration of the Agenda.

The collection, retention and use of Artificial Intelligence and biometric data and its impacts on human rights and fundamental freedoms

The Agenda and Proposal seek to expand the use of technology for the purposes of countering terrorism. Pillar I of the Agenda focuses on anticipating existing and emerging threats in Europe by, inter alia, exploring and promoting the use of Artificial Intelligence [hereinafter "AI"] (i) to allow for more efficient and accurate processing of large amounts of data; (ii) to develop new technologies, such as facial identification "capable of detecting terrorists on the move by comparing their facial image with a reference database"; (iii) to identify suspicious behaviour; and (iv) to identify and prevent the dissemination of terrorist content online.

The Proposal appears to advance implementation of these goals. Article 4 of the Regulation (EU) 2016/794 will be amended to add the following to the list of tasks to be performed by Europol: "proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and validation of algorithms for the development of tools". Article 18(2)(e) is also amended to add the following to the list of purposes for which Europol may process personal data: "research and innovation regarding matters covered by this Regulation for the development, training, testing and validation of algorithms for the development of tools". Article 30 adds biometric data to the special categories of personal data that may be processed by Europol.

There is no agreed-upon international definition of AI. That AI is so broad and vaguely defined, including in the Agenda and Proposal, leaves tremendous discretion to Governments (and private entities) to develop AI-related technologies that would not fall within the scope of current legal frameworks that provide only skeletal regulation in the field of AI. While AI technology (such as facial identification), as well as the collection and processing of biometric data, offers advantages from a security perspective, the technology simultaneously raises several highly problematic human rights issues including, inter alia, the right to equal protection of the law without discrimination, the right to privacy, freedom of expression and opinion, and the right to freedom of movement.

The use of AI in the Agenda and Proposal may violate the principle of non-discrimination

Pillar I of the Agenda promotes the use of AI in order (i) to allow for more efficient and accurate processing of large amounts of data; and (ii) to develop new technologies, such as facial identification "capable of detecting terrorists on the move by comparing their facial image with a reference database". Generally, AI enables the processing and analysis of an enormous amount of data in real time and is already in use globally. Facial recognition technology, however, is still imperfect and the use of facial recognition software within law enforcement raises the risk of unlawful arrest due to error and overreach. Given the error rates of current facial recognition technology, these inaccuracies could lead to increased wrongful arrests due to misidentification, as well as raising profound challenges of discrimination and profiling in practice.

The Commissioner for Human Rights of the Council of Europe notes that machines function on the basis of what humans tell them.[8] Therefore, if a system is created with human biases (conscious or unconscious), the result will inevitably be biased. These bias-induced errors can lead to false positives or false negatives, including in the counter-terrorism context. The use of facial recognition can lead to expansive violations of the rights to equality and non-discrimination. In the 2020 report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, a cited 2019 review of 189 facial recognition algorithms from 99 developers around the world found that "many of these algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics." (A/HRC/44/57, para.12). The Report added that there can therefore no longer be "any doubt that emerging digital technologies have a striking capacity to reproduce, reinforce and even to exacerbate racial inequality within and across societies." (A/HRC/44/57, para.12). The data collected from flawed systems can potentially lead to discrimination against or exclusion of certain populations, notably minorities along identities of race, ethnicity, religion and gender." (A/HRC/44/57, para. 7). Articles 26 and 27 of the ICCPR ensure equal protection before the law and enshrine the prohibition of discrimination of characteristics such as race, colour, or minority status. In addition, article 5 of the International Convention on the Elimination of Racial Discrimination States the obligation of States parties to guarantee the right of everyone, without distinction as to race, colour, or national or ethnic origin, to equality before the law. Article 3 of the ICCPR and the International Covenant on Economic, Social and Cultural Rights ("ICESCR") guarantees the right of equality between genders. The use of AI systems that may propagate implicit biases undermines these principles. In this regard, the Committee on the Elimination of Racial Discrimination, in its General Recommendation N° 36 (CERD/C/GC/36) non preventing and combating racial profiling by law enforcement official, has asserted that particular risks emerge when algorithmic profiling is used for determining the likelihood of criminal activity either in certain localities, or by certain groups or even individuals (para 33). The Committee

[8] 'Safeguarding human rights in the era of artificial intelligence', Council of Europe Commissioner for Human Rights Human Rights Comment, July 3, 2018, available at https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence (last consulted September 14, 2021).

has recommended that before procuring or deploying algorithmic profiling systems, States should adopt appropriate legislative, administrative and other measures to determine the purpose of their use and to regulate as accurately as possible the parameters and guarantees that prevent breaches of human rights (para 58). It also recommends States to carefully assess the potential human rights impact prior to employing facial recognition technology, which can lead to misidentification owing to a lack of representation in data collection (para 59).

We note that the Agenda states that "[o]ne key aspect to developing trustworthy AI applications is ensuring that the data used to train algorithms is relevant, verifiable, of good quality and available in high variety to minimise bias for instance towards gender or race". The Agenda also acknowledges that "AI applications should be developed and used with proper safeguards for right[s] and freedoms". The Proposal recommends that Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights. In the absence of further detail as to how these safeguards will be guaranteed in practice, however, such rhetoric is not sufficient to alleviate concerns regarding the implications that the proposed use of facial recognition for counter-terrorism and law enforcement purposes offers adequate protection from discrimination.

The use of AI proposed in the Agenda and Proposal to target "terrorist content" may violate freedom of expression and opinion, and freedom of association and assembly

Pillar I of the Agenda also proposes to use AI "(iv) to identify and prevent the dissemination of terrorist content online." The Agenda notes that law enforcement bodies are already developing innovative solutions to respond to terrorist threats based on AI technology, including "to identify terrorist content online and stop its dissemination, to prevent the creation of new terrorist accounts on social media and detect symbols. The Proposal supplements this portion of the Agenda by enabling Europol to cooperate and to exchange personal data with private parties for the purpose of identifying which Member States have jurisdiction in respect of particular terrorist content online. The Proposal suggests that "Europol should be able to exchange personal data with private parties, including hashes, IP addresses or URLs" related to content "depicting harm to life or physical integrity, or calling for imminent [such] harm […] in particular where this content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers." Processing personal data for the development of AI to identify "terrorist content" is deeply concerning. Neither the Agenda nor the Proposal list any specific criteria by which personal data will be collected or how it will enable the AI technology. Given this lack of clarity, such data retention does not appear to comply with States' human rights obligations described above.

The human rights implications of the broad and vague phrase "terrorist content" intersects with the concerns associated with AI, all discussed above. Freedom of expression is protected by article 19 of the UDHR, article 19 of the ICCPR, as well as article 11 of the Charter of Fundamental Rights of the EU. Similarly, article 20 of the UDHR, article 22 of the ICCPR and article 12 of the EU Charter guarantee the freedom

of association. These rights are central to a free and democratic society and may only be curtailed where prescribed by law, in the pursuit of a legitimate purpose, while meeting the strict tests of necessity and proportionality. We emphasize that the right to freedom of expression extends 'not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Moreover, as the right to access to information extends to all types of information, States "bear the burden of justifying any withholding of information as an exception to that right". (A/70/361, para. 8)

We also would like to recall that the Special Rapporteur on the rights to freedom of peaceful assembly and of association noted in a report that although States have an interest in protecting national security and public safety, which are legitimate grounds for restricting such freedoms, these laws should not be drafted in ways that give opportunities for abuse through broad and subjective concepts in the definition of terrorism. The vagueness of the concept of "terrorist content", as well as of the surveillance law, not only makes it extremely difficult to determine with reasonable certainty what kind of conduct online would be considered "terrorism", but also often fail to target specific individuals on the basis of a reasonable suspicion. The Special Rapporteur further noted that surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision.

United Nations human rights mechanisms have stressed that freedom of expression is a prerequisite for the effective promotion and protection of a broad range of human rights, including freedom of opinion. Therefore, as a matter of principle, limitations on freedom of expression must remain the exception and should be applied strictly so as to "not put in jeopardy the right itself". (CCPR/C/GC/34 para. 21) The use of AI to identify and prevent the dissemination of "terrorist content" may curb legitimate expressions of free speech and expression. Neither the Agenda nor the Proposal (which refers broadly to Europol's mandate to "develop, train, test and validat[e] algorithms for the development of tools") specify how these tools will be developed and implemented to avoid infringing on the freedom of expression.

The conscious or unconscious biases that affect AI produced facial recognition like those discussed above can become part of algorithms that target, identify and prevent the dissemination of "terrorist content". Given that any algorithm is imperfect, its application can stifle online freedoms creating censorship of practices and expression and can be further used to restrict freedom of association under articles 21 and 22 of the ICCPR, notably by removing groups, pages and content that facilitate organization of in-person gatherings and collaboration. This is particularly concerning considering the important role that social media plays in organizing peaceful protest movements both nationally and globally. The use of AI-enabled algorithms, for instance to remove statements, symbols, or online groups that do not align with the "European way of life" or "European values" alluded to (but not defined) in the Agenda, could have a serious chilling effect on freedom of expression.

The use of AI proposed in the Agenda and Proposal may violate freedom of movement

We note particular concern that the use of AI tools can impede the individual's right to freedom of movement as protected by international human rights treaty law, such as article 13 of the UDHR, article 12 of the ICCPR and article 21 of the Treaty on the Functioning of the EU ("TFEU"), permitting movement between Member States of the EU. She notes that in systems that combine data from satellite imagery, facial recognition-powered cameras and cell phone location information, among other things, AI can provide a detailed picture of individuals' movements, to the point of being able to predict individuals' future location. Such a tool could therefore easily be used by governments to facilitate more precise restriction of the freedom of movement, whether that be at the individual or group level.[9]

The use and retention of biometric data in the Agenda and Proposal may violate the right to privacy and non-discrimination

Article 30 of the Proposal amends the Regulation by adding biometric data under the special categories of data. In paragraph 2, the first sentence is replaced by the following:

"2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data and biometric data for the purpose of uniquely identifying a natural person or data concerning a person's health or sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol.";

The right to privacy is guaranteed under article 12 of the UDHR, article 17 of ICCPR, as well as articles 7 and 8 of the Charter of Fundamental Rights of the EU. This right protects the unlawful or arbitrary interference with a person's privacy, which includes identifying information about an individual, such as their biometric data, as well as information concerning their private life.10 Programs allowing for the collection and retention of personal information, whether or not that information is subsequently used, constitutes an interference with individual privacy rights (A/HRC/27/37 para. 20). Any interference with a person's privacy rights must, in turn, be prescribed by law, specifying the precise circumstances in which such interference is permitted, and must not be discriminatory. (A/HRC/27/37). The General Assembly has highlighted that "the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance,

[9] Human Rights in the Age of Artificial Intelligence, Access Now, November 2018, available at https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf (last consulted on March 25, 2021), p. 21.

[10] Office of the United Nations High Commissioner for Human Rights, Human Rights, Terrorism and Counter Terrorism, Fact Sheet No. 32 (the 'Fact Sheet'), p. 45.

interception and data collection, which may violate or abuse human rights, in particular the right to privacy." (A/RES/68/167; A/RES/69/166; A/RES/71/199).

We express concern about the expansion of the Proposal to include biometric data to be collected and processed by Europol. Biometric data are highly sensitive and unique to individuals. Given how new and imperfect many of these technologies are, they are vulnerable to hacking or cyberattacks, exposing the persons identified to physical or financial risks. Additionally, there is continual emphasis placed throughout the Agenda and Proposal on the need to share data between public and private entities, including data collected through Europol. If subsequently private companies are entrusted with collecting biometric data, there may be very few legal limits on how they can share and use the information gathered. Even with personal data being collected by government agencies, there is a risk of a purpose misuse. The United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter Terrorism stressed that in developing systems to collect biometric data, it is important to put in place safeguards with respect to data protection and human rights standards.[11]

While the stated purpose of collecting the biometric data is to prevent or combat crime, there has also been research demonstrating that biometrics data can reveal information such as age, gender, ethnicity and even critical health issues such as diabetes, Alzheimer's disease and such confidential and sensitive information may function as a basis for direct or indirect unlawful discrimination between people crossing borders. While having established data protection frameworks, the EU does not attach sufficient safeguards and protection to biometric information in this context, at times as a consequence of the gap between technological advances and regulation. As outlined above, biometric data is linked to an individual's characteristics that make this person unique and identifiable and consequently must be characterized and protected as such in EU law, if the Union is to adequately address the risks attached to its collection and use.

Countering terrorist financing and human rights

Pillar II of the Agenda concerns measures to prevent terrorist attacks from occurring by "addressing and better countering radicalization and extremist ideologies before they take root" and preserving the "European way of life". To achieve this, Pillar II focuses, *inter alia* on (i) countering extremist ideologies online and (ii) screening investments. The Proposal likewise provides measures for removing terrorist content online and screening investments. This will again require greater sharing of data and information between Europol, Members States and private entities. Unlike the Pillar I, Pillar II does not refer to the importance of ensuring and protecting fundamental rights in the context of preventing terrorist attacks (with the exception of the rights of the children of foreign terrorist fighters). This renders Pillar II seriously deficient in terms of addressing and centring human rights implications of proposed prevention measures, particularly with regards to the right to privacy.

[11] United Nations Compendium of Recommended Practices for the Responsible Use & Sharing of Biometrics in Counter Terrorism, p. 31.)

Pillar II of the Agenda provides that the EU and Member States "must ensure that projects which are incompatible with European values do not receive support from government or European funds." In a similar fashion, the Proposal sets out restrictive measures relating to foreign direct investment on the grounds of security or public order, establishing a framework for the "screening" of such investments into the EU. We note our concern that this type of measure could conflict with the freedom to conduct a business, established under article 16 of the Charter of Fundamental Rights of the EU. This is especially so, considering the lack of specificity regarding the meaning of "European values" and the "grounds of security or public order". Based on the same consideration, the principle of non-discrimination, mentioned above, could also be engaged.

Though focused on the response to terrorism, Pillar VI also addresses financing and terrorism. The EU has communicated its intent to negotiate a cooperation agreement with Interpol to expand the EU-US Terrorist Finance Tracking Program and to advance negotiations for an EU-US agreement on cross-border access to electronic evidence. All of these proposed measures involve the analysis and/or transfer of EU citizens' personal data to non-EU entities, *i.e.,* international organizations and so-called "*key*" third-party States, which do not share and are not bound by the EU's Human Rights standards, especially with regards to data protection. As such, these proposed future measures pose a special risk to the rights of privacy, data protection, and therefore require specific human rights attention from EU authorities.

While a number of Security Council's resolutions require all States to criminalize terrorist acts, including the financing of terrorism, freezing the funds of persons and prosecuting those who finance, plan, support or commit terrorist acts or provide safe havens, these actions should be undertaken in complete compliance with existing human rights principles.

The indiscriminate collection and retention of data and impacts on human rights

We note our concern that the EU's current and future strategy to expand the collection, transfer, access and retention of personal data in order to better respond to terrorist attacks directly affects individuals' rights to privacy in general and their right to the protection of personal data in particular. Specifically, articles 18(a), 24, 26(a) and 27(a) of the Proposal for a Regulation (2020/0349) aim to reinforce and/or extend the ability to process, analyse, transmit and store personal information with EU institutions, Europol as well as private parties in times of crisis. Found throughout the Agenda and the Proposal are numerous mentions of various methods, means and justifications for the large scale and indiscriminate collection and retention of data. Consequently, it is essential for the EU to make sure that its proposed measures strictly comply with international human rights standards as well as all applicable laws, particularly the General Data Protection Regulation 2016/679 [hereinafter "GDPR"]. Strict compliance should be enforced at all stages (data collection, access, analysis, transfer and retention) and for all partners, whether they are private or public bodies.

The Proposal amends article 30.2 of Regulation 2016/794 to enable the processing of personal data, by automated or other means, "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership"

and of genetic and biometric data for uniquely identifying a natural person, or data concerning "a person's health or sex life or sexual orientation." This is stated to be allowed "only where strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol." Relatedly, article 37.3 of the Regulation 2016/794 states that Europol "shall restrict rather than erase" personal data after the data subject exercises its right to rectification, erasure or restriction, if there are reasons to believe that "erasure could affect the legitimate interests of the data subject". The Agenda and the Proposal recommend increased collection, retention and sharing of data between Europol, Members States and private entities.

These proposed measures entail substantial risk of breaches of the rights to privacy and data protection, safeguarded under article 17 of the ICCPR. The measures involve collection of information about persons and, therefore, limit the privacy and privacy dependent rights of such persons, as well as raise profound questions about how the data is to be protected. Furthermore, the fact that article 37.3 prescribes the data's restriction rather than erasure in certain cases raises concerns relating to arbitrary future access to or abuse of that data. The specific measures may also have an impact on the principle of non-discrimination. The collection of broad categories of data such as "racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership" appears prima facie to constitute disproportionate interference with human rights of specific groups of people and raise the question of the profiling's conformity with the principle of non-discrimination (A/HRC/4/26, paras. 32-62). Moreover, by virtue of the profiling including parameters relating to "political opinion, religious or philosophical beliefs" and "trade union membership" and depending on what procedures are meant to follow from that profiling, the particular measures may affect the rights to freedom of opinion and expression, freedom of thought, conscience and religion, and freedom of association. The Agenda and Proposal have regrettably not set specific safeguards to ensure that any limitations to the particular rights are construed narrowly and that they are not used to curb the rights of political opposition parties, trade unions or human rights defenders.

The qualification set out in article 30.2 of the Proposal referring to necessity and proportionality is welcome but inadequate; the circumstances in which interference is permitted are not specified in sufficient detail, nor are "Europol's objectives" in this realm sufficiently defined (Regulation (EU) 2016/794, article 3).

Internal/external borders and freedom of movement, right to privacy, and principle of non-discrimination

Pillar III of the Agenda deals with strengthening the counter-terrorism response with a focus on "reducing vulnerabilities that could be exploited by terrorists". The Agenda asserts that protection will be achieved by greater securitization of borders and denying terrorists the means to carry out attacks. According to both the Agenda and Proposal, more action is needed to protect and modernize external border management for the EU and encourage Member States to rapidly meet the objective of "systematic checks of all travellers against relevant databases" at external borders, with limited use of derogations.

To achieve this requires a "new and upgraded large-scale EU information systems [to] improve security and make external border controls more effective and efficient" and a number of mechanisms will be deployed. The Entry/Exit System ("EES"),[12] an automated system for registering travellers from third countries, is deemed to be of crucial importance. Another related system is the European Travel Information and Authorization System ("ETIAS"),[13] a pre-travel authorization system for visa-exempt travellers, with a watch list, which will enable the use of information on those suspected of or linked to terrorism. It is indicated that in the future, checks will also be possible against the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN)[14] system, a centralized system of Member States, holding conviction information on third-country nationals and stateless persons.

These systems have human rights implications, including structural implications for *inter alia* freedom of movement and freedom from discrimination on religious, ethnic, racial or other grounds. Structural protections ought to be developed to address the ways in which discrimination is produced and reproduced through digital technologies, and these protections ought to be in place prior to the deployment of such technologies. This means the EU must not only address "explicit racism and intolerance in the use and design of emerging digital technologies, but also, and just as seriously, indirect and structural forms of racial [and other] discrimination that result from the design and use of such technologies". (A/HRC/44/57, para. 48). The use of watch-lists is an area of ongoing concern for the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Placement of individuals or groups on a terrorism watch list should be necessary and proportionate and should therefore only be conducted in response to an actual, distinct and measurable terrorism act or demonstrated threat of an act of terrorism. As noted above, ill-defined and overly broad construal of the crime of terrorism necessarily implies a failure to meet the requirements of necessity and proportionality. Only through an adequately construed definition of terrorist acts can the necessity and proportionality elements for listing be met to ensure that the Government's listing is in response to an actual, distinct and measurable threat as defined by law.

The Agenda notes that in December 2018, the Schengen Information System (SIS) Regulations entered into force introducing new measures to improve information exchange. The Agenda then urges Member States to implement all SIS functionalities and roll out the fingerprint search functionality, particularly at extended borders. Under article 4(1)(r) of the Proposal, Member States should also enter alerts in the SIS system, about third-country nationals subject to a return decision and on refusals of entry and stay which would make for example prohibitions of entry and stay visible to all relevant authorities. These new rules appear to be in accordance with the specific objective set forth in the Proposal which aims at "providing frontline officers with the result of Europol's analysis of data received from third countries on suspects and criminals when and where this is necessary. The stated goal is to enable frontline officers to take informed decisions when they check a person at the external border or within the area without controls at internal borders."

[12] Regulation (EU) 2017/2226, 9.12.2017, OJ L 327.
[13] Regulation (EU) 2018/1240, 19.9.2018, OJ L 236/1.
[14] Regulation (EU) 2019/816, 22.5.2019, OJ L 135/1.

We note our unease at the creation of a digital border that functions to reinforce parallel border regimes (A/75/590, para. 8). The effect of this parallel functionality affects mobility and can arbitrarily restrict a person's ability to migrate or seek protection in another State. The move to 'smart technologies' to control the border also has a disproportionate impact on certain national origin, ethnic and racial groups. We refer to the report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance on "Racial discrimination and emerging digital technologies: a human rights analysis". In the report, the Special Rapporteur highlighted that emerging digital technologies are developed and deployed in ways that are uniquely experimental, dangerous and discriminatory in the border and immigration enforcement context. By so doing, they are subjecting refugees, migrants, stateless persons and others to human rights violations, and extracting large quantities of data from them on exploitative terms that strip these groups of fundamental human agency and dignity (A/75/590, para.3).

The Proposal further provides for the use of Advance Passenger Information ("API") and Passenger Name Record ("PNR") and the data collected will potentially be used for countering serious crime. The Proposal further encourages the use of PNR data which enables identification of previously unknown threats and provides intelligence leads, urging Member States to collect PNR data for intra-EU flights as well. The increasing collection and use of API and PNR data by States globally raises serious concerns over potential infringements of privacy and related rights. Strict oversight of API and PNR data collection is needed, and we encourage the EU to develop robust and rule of law compliant independent oversight of collection, storage, use and transfer of API and PNR data.

Though the EU has robust data protection frameworks, relevant protections and safeguards may not apply or apply in a modified format to information collected by law enforcement and, even more so, if data collection and processing happens in a national security context. The GDPR does not apply to data processed by law enforcement and criminal justice authorities. Such processing is governed by the Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes (the "Police Directive").[15] Furthermore, neither the GDPR nor the Police Directive regulate data collection, retention, processing and sharing to the extent this happens for purposes of national security.[16] This leaves an obvious human rights lacunae which appears inconsistent with States' international human rights obligations.

The Agenda and Proposal may impact the right to fair trial

Pillar IV of the Agenda outlines the response actions for the aftermath of a terrorist attack and the "urgent action [that] is needed to minimise its impact and allow for the swift investigation and prosecution of the perpetrators." The proposed measures seek, *inter alia*, "to strengthen the Europol mandate" by "enable[ing] Europol to cooperate effectively with private parties"; to foster the exchange of personal data, including financial information, to prevent, investigate and prosecute terrorist and other

[15] Directive EU 2016/ 680

[16] The EU lacks competence to directly legislate in this area as the Treaty on European Union provides that "national security remains the sole responsibility of each Member State." *See* Consolidated Version of the Treaty on European Union (TEU), article 4(2).

criminal offense; and to address the conduct of terrorism investigations and prosecutions. These proposed measures to respond to terrorist attacks are likely to continue to infringe upon the following fundamental rights: the rights to privacy and to the protection of personal data and the right to a fair trial in general. The potential infringement on privacy rights permeates every layer of the EU counter-terrorism Agenda.

The right to a fair trial, in general, typically includes the following rights: presumption of innocence; right to a hearing; right to due process; right to be informed of the measures taken against him/her and to know the case against him/her; right to be heard within a reasonable time by the relevant decision-making body; right to effective judicial review by a competent and independent review mechanism; right to an effective remedy. The broad right to a fair trial is protected, *inter alia*, by articles 14 and 15 of the ICCPR, articles 47-50 of the EU Charter and article 6 of the ECHR. All of these aspects of the general right to a fair trial may potentially be negatively affected by Pillar IV of the Agenda. We underscore that it is of paramount importance that the evidence extracted from personal data be obtained in a lawful manner.

The EU's counter-terrorism strategy can potentially negatively affect defendants' entitlement to the disclosure of evidence since such evidence may be obtained via classified intelligence processes. It is therefore necessary for courts to ensure and defend the right to a fair trial while advancing the security obligations of States. The EU's various schemes for personal data collection and analysis – both currently in place and proposed ones – give EU Member states and EU institutions an even more substantial advantage over the defendant in terms of finding and processing data-based evidence during investigations and criminal trials. As such, the EU's agenda may put defendants at a serious disadvantage in front of the prosecution, in breach of the adversarial principle and the principle of equality of arms between the prosecution and the defence guaranteed by the ICCPR.

Additionally, Pillar IV briefly addresses the issue of battlefield evidence,[17] highlighting that it is "paramount for prosecution" and committing to support Member States to use the information to identify, detect and prosecute returning foreign terrorist fighters, through best practices, exchange of information and project financing. We are highly concerned about State use of battlefield evidence, particularly its significant potential adverse impact on fair trial. Additionally, the European External Action Service will continue to support and strengthen cooperation with third countries specifically naming the US, including exchange of information. Indeed, the Communication from the Commission to the Parliament also advises that it is working closely with Member States and key partner countries "to ensure that battlefield evidence is shared and used effectively for identification, detection at EU's borders and prosecution." There is no more detail provided as to the appropriate safeguards of processing and sharing such data and particularly mentioning third countries such as the US, where protection standards may not be equivalent, again contravenes safeguards in place to ensure privacy rights.

[17] The Communication defines it as "information uncovered and collected by military forces during battlefield operations or by private parties in a conflict zone".

Conclusion

Given the potential for adverse effects on fundamental freedoms and human rights, particularly the freedom from discrimination, the right to privacy, freedom of expression and opinion, freedom of assembly and association, freedom of movement, and the right to a fair trial, we express our concern about both the Agenda and the Proposal. The provisions of the Agenda and Proposal may potentially infringe on all of these guarantees across multiple provisions, affecting several of these freedoms and rights pervasively throughout the legislation. We recommend a thorough re-examination of both Agenda and Proposal and a re-evaluation of the principles of necessity and proportionality to ensure compliance with the EU's international human rights obligations.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all cases brought to our attention, we would be grateful if you could provide any additional information and/or comment(s) you may have on the above-mentioned issues.

1. Please provide information in details of how the counterterrorism efforts of the European Union comply with the United Nations Security Council resolutions 1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2242 (2015), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); as well as Human Rights Council solution 35/34 and General Assembly resolutions 49/60, 51/210, 72/123 and 72/180, in particular with international human rights law requirements of same.

2. Please provide additional information about how the proposed expansion of "AI" is consistent with the standards of necessity and proportionality, and how the Commission and Parliament consider that it respects the principles of precision and legal certainty set out in the ICCPR.

3. Please provide information for the terms "European values", "terrorist content", and how the Commission and Parliament explain their operational consistency with human rights norms of legal precision.

4. Please provide information on how the proposed process of implementing the mass data collection and retention systems in this Agenda is compatible with the principles of necessity, legality, proportionality, and non-discrimination and safeguards the rights to privacy, association, liberty and freedom of movement.

5. Please provide information on how the enhanced third-party and non-EU data sharing programme complies with international standards safeguarding the right to privacy.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from the European Commission and Parliament will be made public via the communications reporting website within 48

hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept the assurances of our highest consideration.

Fionnuala Ní Aoláin
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Irene Khan
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Clement Nyaletsossi Voule
Special Rapporteur on the rights to freedom of peaceful assembly and of association

Felipe González Morales
Special Rapporteur on the human rights of migrants

Fernand de Varennes
Special Rapporteur on minority issues

Ana Brian Nougrères
Special Rapporteur on the right to privacy

E. Tendayi Achiume
Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance