22ND EU-NGO HUMAN RIGHTS FORUM

IMPACT OF NEW TECHNOLOGIES ON HUMAN RIGHTS

9-10 DECEMBER 2020

FINAL REPORT
DECEMBER 2020

MADALENA MOITA
GOPA.COM

Table of Contents

Acronyms

AI	Artificial intelligence
CCTV	Closed-circuit television
CSO	Civil society organisations
DG CNECT	Directorate-General for Communications Networks, Content and Technology (European Commission)
DG INTPA	Directorate-General for International Partnerships (European Commission)
EC	European Commission
EDRi	European Digital Rights
EEAS	European External Action Service
EU	European Union
FIDH	International Federation for Human Rights
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HRD	Human rights defender
HRDN	Human Rights and Democracy Network
LGBTI	Lesbian, gay, bisexual, transgender, and intersex
MENA	Middle East and North Africa
NGO	Non-governmental organisation
OECD	Organisation for Economic Cooperation and Development
ROAM	Rights, Openness, Accessibility, Multi-stakeholder participation
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
USA	United States of America

Executive Summary

01

The 22nd EU-NGO Human Rights Forum focused on the impact of new technologies on human rights. The Forum had a global reach, gathering participants from 107 countries, and was held virtually this time due to the COVID-19 pandemic. Most of the sessions were recorded, and together with background documents and content shared by the participants are available on the Forum's platform (https://eu-ngo-forum.b2match.io/).

The Forum acknowledged that digital technologies and the internet have changed the way people access and disseminate information. They have widened the stage for citizens to exercise their freedom of expression and participation, and have allowed for new forms of civic activism, for massive mobilisation, and the sharing of ideas and opinions. However, social media have also been the vehicle to fuel polarisation and spread inflammatory narratives with an insufficient and uncoordinated response to hate speech, disinformation, online abuse and even electoral manipulation.

Moreover, some states have been weaponising the online space, often with the pretext to fight hate speech or disinformation, including via internet shutdowns to silence the voice of opposition and human rights defenders.

There was consensus that a multi-stakeholder approach is essential as well as promoting digital rights in the multilateral fora, in particular in the UN context (Human Rights Council, General Assembly Third Committee, High Commissioner for Human Rights and UN Special Procedures).

Participants agreed that companies can and should do more to protect human rights in the digital sector, both online and offline. They should provide safeguards for users of their platforms, and explore more creatively and innovatively how to broaden the protection tools at their disposal to do so. A key element is to inform the users and to provide transparency on the algorithms used. For the digital transformation, self-regulation and voluntary commitments by companies are important but not sufficient. Voluntary action should be accompanied by regulation and

strong governance mechanism. EU representatives of several companies (Twitter, Facebook, Microsoft, Ericsson) presented the private sector's views and actions.

Many participants highlighted the normative power of the EU and its global influence on matters such as data privacy (GDPR legislation) or the upcoming Digital Service Act and legislation on artificial intelligence. NGOs and UN experts called on the EU to keep championing human rights in line with the new EU Action Plan for Human Rights and Democracy and the recently adopted EU Global Human Rights Sanctions Regime.

In response to the need to enhance digital skills of human rights defenders, training on digital security was organised in the margins of the Forum.

Some key takeaways include the following:

- Digital technologies have improved people's access to knowledge, information and public services, opening the space for citizen participation and increasing the capacity to collect data that can inform policies and foster governments' transparency and accountability. But they have also **generated severe power imbalances and human rights abuse worldwide**, from mass and targeted arbitrary surveillance against human rights defenders, to the proliferation of disinformation and hate speech polarising communities and disrupting democratic processes, to new forms of censorship and marginalisation of dissident voices.

- In addition, **the digital public space is not equally available or accessible for everyone**. A real digital gap exists, mirroring offline inequalities, especially for women, people living in poverty and/or in remote and rural areas, persons with disabilities and other minorities.

- Focusing on the human rights risks brought up by new technologies, the discussions during the Forum echoed the statement Michael O'Flaherty (Director of the European

Union Agency for Fundamental Rights) made on the first day of the Forum, that *human rights are as applicable online and offline*.

- In order to address the challenge of a rapidly changing digital environment, the participants were consensual in identifying the **imperative need for more regulation**. As the United Nations High Commissioner for Human Rights, Michelle Bachelet, pointed out, regulation processes can be complex, creating more abuse, consolidating discrimination, censorship and oppression; however, they are critical to ensure **a more human rights-centred approach to technologies**.

- Across the different sessions, participants emphasised that the **EU should then take the lead in the regulatory process**, using its convening power to open spaces for inclusive dialogue, ensuring that the private sector, academic experts and civil society have an active contribution in policy and legal frameworks design. Inclusive dialogue means also bringing to the table g**roups in vulnerable situations** that are being disproportionately affected by the new technologies' negative impact on human rights.

- The debate on accountability was clear: states bear the duty to ensure respect and protection for human rights, but the **private sector has the responsibility** to comply with international human rights norms and labour standards. This responsibility entails preventing and addressing adverse human rights impacts caused by their business activities, in particular by putting into place **due diligence** systems**,** conducting appropriate **risk assessments** and providing **access to remedy** for victims of abuse.

- Additionally, in order to ensure that digital companies are accountable, public and **independent scrutiny and oversight** are vital, and **multi-stakeholder monitoring mechanisms** should be in place.

- Participants called for a stronger role from the EU in **monitoring human rights violations** linked to digital technologies, and also in **responding** to these violations. This means the EU must be more active on the world stage in calling states to promote and protect human rights in the digital sphere and to avoid illegal practices such as mass surveillance, internet shutdowns or any forms of censorship. The EU should also increasingly liaise with private sector actors to require further transparency in these matters and impose restrictions on companies involved in bad practices.

- The EU should continue to act on the dual use: taking an international lead on control/prohibition of exports of surveillance software and equipment to repressive/authoritarian states.

- Human rights defenders participating in the Forum highlighted how civil society is having a vital role in monitoring and advocating on digital rights, but it needs to be supported by the international community, both in and outside the EU. Specific needs of support include funding and training on **digital protection and digital security skills**. Journalists need more support in fact checking.

- **Digital literacy** is key to ensuring transparency and needs to be reinforced: people need to be better informed and protected against disinformation, they need to know more about how algorithms work and how their data is being collected. Fostering **citizen engagement** is fundamental, including improving oversight and supporting litigation processes.

- The EU should also support communication channels and facilitate spaces for dialogue between **human rights defenders/civil society organisations and open-source experts, as well as representatives of the tech industry** to promote a common language and understanding of human rights and digital technologies.

- The **EU should also ensure internal/external coherence**, by mainstreaming human rights (online and offline) at the centre of all its policies, including on migration, security and trade, to make sure that the use of digital technologies complies with human rights standards.

- Addressing these risks and preventing and punishing human rights abuse is a responsibility of national states, but multilateral institutions, the private sector, tech experts, civil society organisations and human rights defenders, including the media, have an important role in monitoring, preparing information, forwarding critics, sharing thoughts, highlighting risks and developing solutions.

- The Forum evidenced a **collective drive for cooperation** and offered a glimpse of how the EU can expand its role in exploring community solutions, by shaping "a distinctly European and human rights-based approach to the digital world" (High Representative/Vice-President Josep Borrell[1]) that can reverberate worldwide.

---

[1] Keynote speech available at https://eeas.europa.eu/topics/sanctions-policy/90300/eu-ngo-forum-keynote-speech-high-representativevice-president-josep-borrell-opening-session_en

Introduction

This report aims to provide insight into the discussions and recommendations from the 22nd EU-NGO Forum on The Impact of New Technologies on Human Rights[2], held on 9-10 December 2020. The Forum was jointly organised by the European Commission, the European External Action Service (EEAS) and the Human Rights and Democracy Network (HRDN), reinforcing a long-term partnership in bringing together representatives of non-governmental organisations, human rights defenders from all over the world, international organisations, representatives of EU Member States and European institutions. It drew on these stakeholders' expertise to identify best practices and explore what role the EU can play to more effectively protect human rights in the new digital era.

Digital technologies and human rights

Advances in new technologies have undeniably resulted in expanded access to knowledge, in faster and easier platforms for communication, and have offered civil society organisations (CSOs) and human rights defenders (HRDs) an open stage to mobilise communities, document human rights violations and share messages at a global scale.

But at the same time, new technologies do not come without risks and are also generating an adverse impact on the protection of human rights and on people's exercise of fundamental freedoms: governments around the world are using surveillance tools to monitor journalists, human rights defenders and political opponents; the right to privacy is being challenged by massive data collection and use; hate speech and disinformation are spreading; and, simultaneously, new forms of censorship are emerging. There is ongoing evidence as to how emerging technologies can exacerbate structural discrimination.

The COVID-19 pandemic also revealed the inequalities in access to reliable information and the importance of bridging the digital gap, which particularly impacts groups in vulnerable situations, including women, people living in poverty and/or in remote and rural areas, persons with disabilities and other minorities. The pandemic has been used as an excuse for imposing restrictions on human rights and fundamental freedoms; furthermore, it also highlighted the importance of fact checking and combatting fake news.

The EU and the digital space

Taking advantage of the benefits of the digital revolution and minimising its harms is one of the priorities of the European Commission for 2019-2024. Being determined to make this Europe's 'Digital Decade', the Commission is invested in making digital technologies work to improve people's lives.

The European Union has been taking steps to address the threats posed by digital technologies and to protect human rights, such as the European Digital Strategy[3], the Code of Practice on Disinformation[4], the Digital Services Act package[5] and the upcoming legislation on artificial intelligence (due in 2021). This concern is also well-reflected in the EU Action Plan on Human Rights and Democracy 2020-2024[6], which includes a proposal to engage with different stakeholders such as experts, multilateral institutions, businesses and civil society 'to share analysis and best practices [...] on how to enforce human rights frameworks and support democracy in the digital age'.

The EU-NGO Forum's topics were well aligned with this strategy, by focusing on the impact of new technologies on human rights.
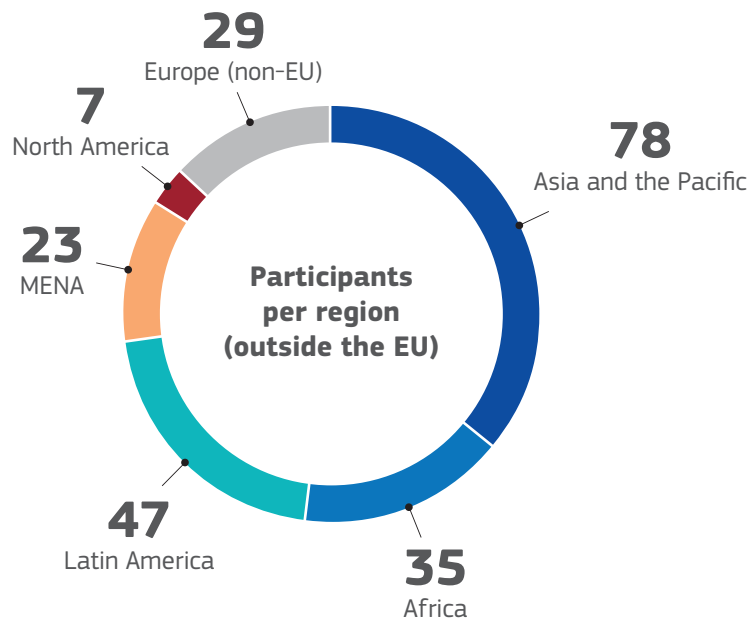
---

[2] This report was drafted by Madalena Moita, who benefitted from the support of a team of note takers that collected the main points and recommendations coming out of the discussions during the event.

[3] https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy
[4] https://ec.europa.eu/digital-single-market/en/code-practice-disinformation
[5] https://ec.europa.eu/digital-single-market/en/digital-services-act-package
[6] https://www.consilium.europa.eu/media/46838/st12848-en20.pdf

The 22nd EU-NGO Forum

Due to the COVID-19 pandemic, the Forum this year was held virtually. It offered the opportunity for people from all over the world to take part in the discussions: experts and human rights defenders from 107 countries attended.

29
Europe (non-EU)

7
North America

23
MENA

78
Asia and the Pacific

Participants per region (outside the EU)

47
Latin America

35
Africa

Participant partner countries per region

10
Europe (non-EU)

2
North America

21
Asia and the Pacific

13
MENA

17
Latin America

21
Africa
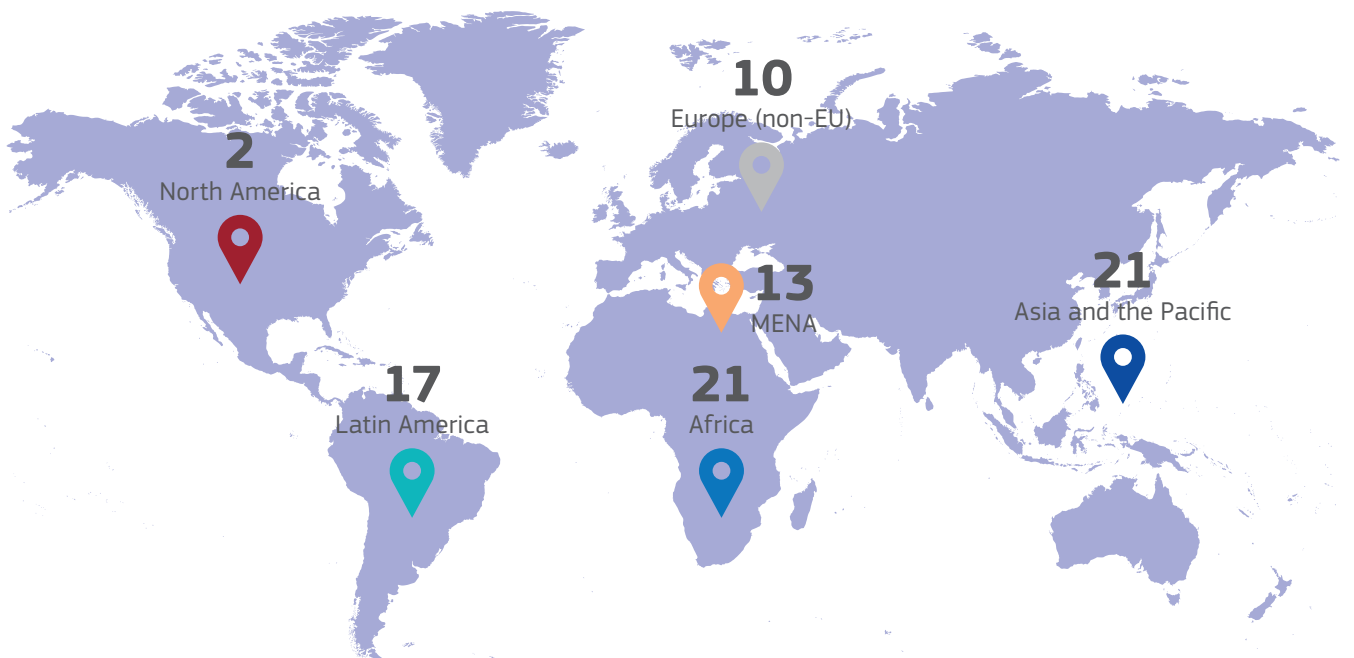
The Forum's discussions focused on four main themes:

I. Fundamental freedoms in the digital sphere:

- Opportunities for civil society and human rights defenders to increase online freedoms of both association and peaceful assembly.
- Identifying solutions to combat online threats such as cyber-harassment, hate speech and violent extremism.
- Roles of national states, public institutions and private companies in tackling disinformation while promoting media pluralism.
- Defending freedom of speech online.
- Stepping up action to combat internet shutdowns, and to overturn shutdowns and artificial limitations on the internet.

II. Technology, business and human rights – how to engage with the private sector

- Responsibility of businesses to prevent and address human rights abuse created or facilitated by new digital technologies.
- Dialogue with 'big tech' companies, including social media platforms on promoting and protecting human rights in the digital sphere.
- Use of new digital technologies by civil society and human rights defenders to enhance transparency, accountability, monitoring and reporting of business processes.

- Respective responsibilities of states and companies to identify, mitigate and address human rights impacts from new digital technologies, with a focus on mandatory human rights due diligence and access to remedy.

III. Privacy and surveillance

- How mass and targeted arbitrary surveillance threatens human rights defenders and civil society.
- Current methods of arbitrary surveillance: facial recognition and other biometric surveillance.
- Current uses and impact of mass surveillance: border management, social credit system.

IV. Artificial intelligence development – opportunities and risks

- Current international efforts to regulate AI in the area of human rights.
- Opportunities, risks and technological reliability issues in the use of AI applications in the fields of justice and access to education. How AI can be used to promote and protect human rights.
- AI leading to discrimination or impeding the realisation of human rights (digital divide, bias, discriminations in law enforcement of access to work and social services). Impact on individuals in vulnerable situations: migrants, ethnic and religious minorities, children.

Different formats of sessions were organised for each of the thematic areas:

Main thematic panel	Public interactive expert session	Closed interactive expert session
• Key experts intervening for a broader audience, live-streamed	• Shorter interventions from speakers followed by open discussions with the participants	• For an exclusive audience of human rights defenders, conceived to generate safe and transparent discussions

Opening the discussions and setting the scene

The Opening session mapped the complexity of the issues at stake and the main concerns to be debated.

The 22nd edition of the EU-NGO Forum occurred in what was *a difficult year for human rights worldwide*, as stated by the High Representative of the European Union for Foreign Affairs and Security Policy and Vice-President of the Commission, **Josep**

Borrell, in his welcome remarks, particularly due to the context generated by the COVID-19 pandemic. The High Representative praised how the theme of the Forum was timely, with repressive laws spreading and a crackdown on the online and offline civic space, rendering the work of human rights defenders more crucial than ever.

Jutta Urpilainen, the EU Commissioner for International Partnerships, reinforced how the European Commission is committed to working with partners to ensure that the digital transition and new technologies continue to promote universal human rights, particularly under the framework of the new EU Action Plan on Human Rights and Democracy 2020-2024.

Michelle Bachelet, the United Nations High Commissioner for Human Rights, pointed out that one of the main challenges was that the digital public space is not equally available for everyone, mirroring offline inequalities, especially for women, people living in poverty, those in rural areas and minorities, and that it can become hostile in polarised debates marked by hate speech, harassment and dissident voices being marginalised. She also affirmed that state regulation is critical, but it can be complex, creating more abuse, consolidating discrimination, censorship and oppression. The High Commissioner underlined that the legislators' goal should be first and foremost to "make the digital space work for everyone".

The President of the International Federation for Human Rights (FIDH), **Alice Mogwe**, raised concerns about the response of states in protecting human rights running behind the pace of technological advances of private companies and the danger of leaving the regulation to the market. The UN Guiding Principles on Business and Human Rights are critical and its recommendations should be put to effective use.

Finally, **Eamon Gilmore**, the EU Special Representative for Human Rights, emphasised the need for multilateral solutions, and emphasised that the EU is now better equipped to tackle attacks on civil society with the newly approved EU Sanctions Regime[7] and the new Action Plan on Human rights and Democracy. The Special Representative reaffirmed the EU's commitment to taking the lead on norm-setting worldwide, as it did with the relevant steps of the GDPR, the Code of Practice on Disinformation, and as it is taking now with the current work on the upcoming legislation on artificial intelligence (due in 2021) with a rights-based approach.

The opening high-level panel was followed by the setting-the-scene session that gathered representatives from EU institutions – the European Parliament represented by Vice-President **Heidi Hautala**, and the Chair of the Subcommittee on Human Rights, **Marie Arena**; the European Commission, represented by **Giuseppe Abbamonte**, Director for Media Policy, at the Directorate-General for Communications Networks, Content and Technology (DG CNECT); and the independent European Union Agency for Fundamental Rights, represented by the Agency's Director, **Michael O'Flaherty** – and experts and human rights defenders from two renowned organisations

working on human rights: **Sharon Hom**, Executive Director at Human Rights in China, and **Eliška Pírková**, Europe Policy Analyst at Access Now.

These issues were debated in more detail in the thematic sessions, including the interactive ones where human rights defenders had the opportunity to share experiences and challenges. The main topics addressed in those thematic sessions are presented in the next chapters.

The key elements extracted from this discussion were:

- **The EU is urged to lead on these complex issues:** it has both the obligation and the opportunity to continue to defend human rights and to put them at the centre of policies.

- **Human rights are applicable online as well as offline.**

- There is a need for a **mandatory Human Rights and Environment Due Diligence Law** (mHREDD) to ensure digital platforms are acting in a respectful way.

- The **quality of dialogue between the states and businesses** should be improved and supported by a common vocabulary to ensure mutual trust.

- Policy needs to be **fact-based**.

- There is a need to **invest in support to civil society, both in and outside the EU**.

- The EU must restrict the **export of digital technologies on surveillance to non-democratic states**.

- **Truth, transparency and initiative** need to be incorporated into the governance of new technologies to ensure citizens can trust them.

- **Social media's algorithmic-induced addiction** is being used on people in a way that threatens democracy (like China's social credit system).

- **Open source and independent tech developers** need to work closely with civil society and human rights defenders.

---

7 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2419

Fundamental freedoms

‘

The European Union stands by Joshua Wong, and by all who are facing charges because they are defending fundamental freedoms.

Josep Borrell, High Representative for Foreign Affairs and Security Policy and Vice-President of the EU Commission, Opening Statement

Digital technologies and the internet have empowered citizens to exercise their freedom of expression and participation, and reinforced civic activism, facilitating massive mobilisation and the sharing of ideas and opinions. At the same time, as the EU Human Rights and Democracy Action Plan 2020-2024 emphasised, digital technologies 'can also have a negative impact, such as spreading disinformation and hate speech, enabling new forms of violence [...], limiting freedom of expression and reducing civil society space, reinforcing discrimination and structural inequalities'.

This dilemma puts social media platforms at the centre of the debate. Social media has fuelled polarisation and inflammatory narratives. Without international standards and common definitions on hate speech and disinformation, the platforms, in the face of fake news, online abuse and even electoral manipulation, are left to self-regulation based on what is defined as illegal content and on community guidelines, which have not been enough.

Some states, with the pretext to fight hate speech or disinformation, have reinforced repression, with the aim of silencing the voice of opposition and human rights defenders, including via internet shutdowns. One of the main topics addressed during the fundamental freedom sessions was precisely this increase in threats and online harassment to journalists and human rights defenders.

In his opening speech, the High Representative, Josep Borrell, made reference to these episodes, mentioning the case of Hong Kong activist Joshua Wong. Invited to participate in the Forum, Joshua Wong ended up being arrested before the event.

Journalists and human rights defenders have been subject to defamation and criminalisation all over the world, with no support from the digital platforms. This raised the question about who is accountable when citizens are harmed in the digital sphere by hate speech, and panellists agreed that accountability should be shared between states and companies. Governments and

platforms should work together to regulate and mitigate online and offline effects.

It was also mentioned how human rights have to be privileged against the commercial interest of the platforms that benefit from the spreading of disinformation and sensationalist content when users' engagement is monetised.

Digital technologies have generated new forms of activism, enabling fluid, decentralised and leaderless movements, which has facilitated the resistance to repression. Human rights defenders have been relying increasingly on the online space: it helps connect movements from different countries, facilitates the collection and dissemination of testimonials, and the reporting on disappearances. It has also been helpful to mobilise internally and broadcast internationally, and to protect activism.

However, the same tools are being used as a weapon by states for propaganda, surveillance and repression. States have been leading defamation and criminalisation campaigns targeting journalists and human rights defenders, they have been restricting online content, conducting internet shutdowns, passing cyber laws and disinformation laws, and attacking infrastructures. Some countries are also building state-run parallel internet systems, putting at risk a transparent and accessible internet for all.

Access Now representatives in the Forum made reference to their recent study, which stated that in 2019 alone, 33 countries ordered internet shutdowns or intentional disruptions of

03

the network[8]. In 2020, the situation deteriorated, with these new forms of censorship blocking access to information on the COVID-19 pandemic and during moments of political unrest.

Activists face threats online that also have offline effects. They are often confronted with a dilemma between their safety and avoiding self-censorship. This is more visible in authoritarian regimes and increases the security risks of human rights defenders, but the risk is in fact more widespread, affecting also democratic regimes. Participants agreed that the EU has to put more pressure on governments and platforms to protect freedom of expression, and particularly on social media companies not to take part in the restrictions of online content and civic space. Governments, CSOs, and multilateral institutions should also be more vocal against internet shutdowns.

Litigation was also mentioned as a possible solution, particularly in the fight against internet shutdowns. Legal action has been undertaken and advocated for by CSOs, and positive decisions from the courts have set relevant precedents, but since these processes are lengthy and costly, human rights defenders need to be supported.

From the side of civil society, the organisations present also voiced their right to monitor tech platforms to ensure they are accountable.

The representatives of social media platforms in the Forum acknowledged their responsibilities, and indicated their openness to dialogue with different stakeholders. They asked for more regulation, since it would provide them with clear guidance. They also stressed the importance of education and awareness raising to enable individuals to make more informed choices and decisions when engaging on social media.
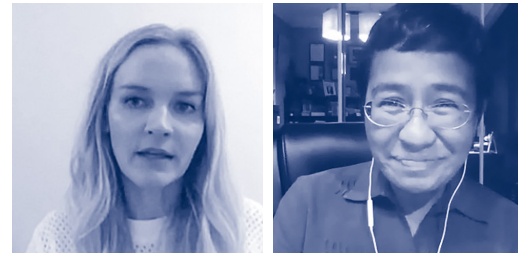
Aura Salla

Maria Ressa

Patrick Penninckx

Participants agreed that a rights-based approach is needed to regulate the digital space, even if it was recognised that a one-size-fits-all solution would be hard to define. The countries in which sites like Facebook operate are very diverse, rendering the regulation processes more complex. The EU's Digital Services Act[9] and the Digital Market Act[10] are welcomed, including by opening up the opportunity for replication.

This concern was also shared by the audience that posed the question of how states and social platforms can address fake news, hate speech and disinformation in a way that still respects and protects freedom of expression and opinion.

👤 Anonymous
For all speakers: can we leave to big companies to decide what can be published online? How to reinforce role of institutions and civil society?

👤 Anonymous
We've seen young activists leg Sri Lanka's Cyber Guardians) take on leading roles in promoting a healthy online space. How can the EU & MS better support them?

👤 Anonymous
How can we fight against the dominance that social media have on information?

---

8 https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

9 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

10 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

The issue had already been brought up in the session on setting the scene, with Giuseppe Abbamonte, Director for Media Policy at DG CNECT accentuating the uniqueness of the EU's Code of Practice on Disinformation[11], even if it still called for increased transparency.

An internationally agreed framework for the internet was indeed recognised as critical by all participants. UNESCO has recently created the ROAM framework – Rights, Openness, Accessibility, Multi-stakeholder participation – that was introduced by Guy Berger, Director for Freedom of Expression and Media Development. The ROAM framework is currently being piloted in 12 countries during the 2019-2020 period. Although mainly a normative framework, it could be used as a benchmark for laws on the internet that CSOs can use to keep states accountable as it was agreed amongst UNESCO member states.

Another proposal coming from the discussions was to include the right to unrestricted access to the internet in other internationally agreed-upon standards, such as a criterion for democratic elections. This could be adopted by the EU in the handbook for electoral monitoring as an area of focus for electoral observers.

The EU can have a paramount role in advocating for a free, open and secure internet for all, setting the standard for other countries and supporting them in adapting legal frameworks accordingly.

Recommendations from these thematic sessions:

- Self-regulation on social media platforms is not enough to protect people's rights. There is a need for multi-stakeholder dialogue and regulatory frameworks.

- Improve the EU monitoring system on the use of cybersecurity technology to ensure it is not used by states against human rights defenders.

- The EU should be more critical and put pressure on authoritarian regimes that criminalise all kinds of expression, as well as be stricter towards EU companies, restricting them from working with non-democratic states that curtail freedoms of expression.

- Connect decision-makers and private sector actors fighting hate speech with civil society actors in the field.

- Provide more support to journalists and those checking facts.

- Technology users should be supported to become better equipped to identify fake news or disinformation.

- The EU's election monitoring could integrate unrestricted internet access as a criterion for democratic elections.

---

[11] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Technology, business and human rights

04

Upholding human rights, although first and foremost a duty of national states, is a responsibility of all actors in society, including businesses. The UN Guiding Principles on Business and Human Rights provide the global framework for states and companies to ensure respect for human rights in business activities, including a clear responsibility for businesses to prevent and address negative effects on human rights caused by their operations or supply chains.

New digital technologies have an important impact on the way business activities are carried out. Technologies such as social networks, automation, artificial intelligence and the Internet of Things may create social, cultural and economic value. However, the same technologies can also lead to new or aggravated human rights abuses. By transforming the ways in which businesses operate, including those businesses that host new ways of social interaction, digital technologies call into question the role and responsibility of companies in protecting human rights.

The sessions on technology, business and human rights focused on the responsibility of businesses to prevent and address human rights violations generated or facilitated by digital technologies, and the respective roles of states as duty bearers and of civil society as rights-holders. The sessions gathered representatives from large digital companies like Microsoft, Twitter and Ericsson; from multilateral organisations and Member States (EU, UN B-Tech Project, OECD, the Danish Tech Ambassador), and civil society organisations working on business and human rights, particularly digital rights (Centre for Democracy and Technology, Mass Communications Foundation, World Benchmarking Alliance, Business and Human Rights Resource Centre, Clean Clothes Campaign, Vietnam Committee on Human Rights, Videre, Paradigm Initiative, Global Network Initiative).

The discussions showed that the responsibility to respect human rights in business activities must be shared between companies, states and civil society. Whereas businesses are making efforts to improve their policies, the debate underlined that the private sector can and should do more to protect human rights

Anne Marie Engtoft Larsen   Tyler Gillard – OECD   Guus Houttuin
EEAS Brussels

and democracy and that further regulation by national states is key. Businesses welcomed the UN Guiding Principles but would appreciate further state guidance.

In some cases, companies have been complicit with governments in human rights abuse. The example of Vietnam was presented, in which Facebook slowed access and removed online content to comply with repressive laws. Particularly when working in authoritarian contexts and when the civic space is shrinking, the private sector cannot be complicit with surveillance tactics, internet shutdowns or any forms of censorship, but must ensure transparency.

Participants identified key priorities to improve the private sector's role, from ensuring safeguards for people using their services, to ensuring an open and neutral internet, and enhanced accountability. It was also suggested that diverse tools to manage content could be considered, instead of simply removing it (labels, contextualisation, etc.).

With regards to due diligence, it was mentioned that it needs to be complemented by other aspects, such as access to remedy. Traditional due diligence approaches are not always easily applied to emerging issues in network communications; they are also failing to address negative human rights impacts in the digital sector. Impact assessments are also key, including informing the public debate.
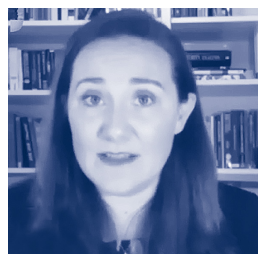
22ND EU-NGO HUMAN RIGHTS FORUM
9-10 DECEMBER 2020

👤 Anonymous
How should and how can large corporations stand up to human rights violations coming from the side of governments?

👤 Anonymous
Should the EU consider AI challenges when drafting its 2021 legislation on Human Rights Due Diligence or we need only a more specific AI legislation?

👤 Anonymous
How can civil society partner with companies to hold governments accountable?

In addition to stronger state regulations, civil society and users can play an important role in enhancing the private sector's respect for human rights. For example, after major social media leaks, a proportional exodus from platforms was not verified. Businesses need to see the effects of eroding trust by users.

In addition, benchmarking can contribute by turning human rights due diligence into a competitive advantage for business. Civil society organisations are already involved in developing benchmarks on companies' performance regarding respect and protection of human rights and digital inclusion. Research demonstrated that, although the ICT sector is making progress in these areas, the majority of ICT companies are still lagging behind when compared to other sectors. Further progress is needed, particularly considering how fast the sector is growing.

EU and the USA, to ensure they can be informed and participate in policy design. Considering how the global south is strongly impacted by the activities of the business sector, these civic actors should be supported to ensure they can have a say on policy-making processes.

Finally, it was emphasised that governments must advance national and international efforts to close the digital 'governance gap', particularly by reinforcing bilateral and multilateral partnerships. They need to harmonise responses to digital challenges in order to foster a level playing field, and state regulation needs to be well aligned with international human rights standards. The EU has taken critical steps to regulate its internal market and can now take the lead in globalising standards.

"

We have to make the case for human rights to be good for businesses.

Civil society organisation representative during closed session.

It is also critical for people to be aware of how the technological processes work, including, for example, content moderation and sharing data with third parties. People and civil society have to be given tools to ensure they can keep exercising their fundamental freedoms and conducting their work. In order to ensure businesses can be held accountable, public and independent scrutiny and oversight are vital; multi-stakeholder monitoring mechanisms should be put in place. For example, community-based monitoring would be more effective and respectful of human rights.

The communication flow should be improved both ways. On the one hand, companies could be more transparent in their reporting processes. On the other, businesses would also benefit from clearer standards when developing rights-centred tech solutions, and from the support of states and CSOs to tailor the language on conceptual terms to the business sector.

Civil society and human rights defenders need additional support, particularly activists and organisations based outside the

Recommendations from these thematic sessions:

- Governments should lead internal efforts to protect human rights in the digital sector, both online and offline, and provide more governance tools, including binding standards.

- The EU should play a leading role in globalising standards.

- Leading companies must adopt a principled approach to human rights.

- Benchmarking and the regulation of competition can contribute towards creating a race to the top by turning human rights due diligence into a business competitive advantage.

- Develop a 'business case' for companies to uphold human rights.

- Due diligence needs to be supplemented by other aspects, such as access to remedy.

- More support should be provided to civil society based outside the EU (and the USA) to ensure meaningful participation in the policy setting.

- Support more efficient communication towards tech companies to make them align with human rights obligations, including by breaking up silos between business and civil society.

Privacy and surveillance

05

The surveillance of individuals is not a new subject, particularly those targets with an active critical and opposition role against national states. The means available to carry out surveillance have seen drastic changes pushed by new technologies. These emerging tools, such as CCTV, drones, spyware, facial recognition and other biometric systems, completely alter the level of scrutiny for those holding these technologies, posing new threats to political activists, journalists and human rights defenders. Surveillance has been expanded, based not only on more sophisticated tools but also on inexpensive and accessible-to-all alternatives, enabling mass surveillance of entire communities, yet is becoming harder to detect[12].

The impact of these new surveillance technologies on human rights and on the exercise of fundamental freedoms was at the centre of the debate during the sessions on privacy and surveillance, as well as possible solutions to respond to these problems. These sessions brought together experts like the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, and David Kaye, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, EU officials, and civil society representatives from Amnesty International-Amnesty Tech (Danna Ingleton), Article 19 (Barbora Bukovská and Paulina Gutiérrez), among others.

One of the key elements of the discussion was how surveillance systems are becoming an increasing threat to human rights defenders, journalists, opposition critics and civil society in general. Mass surveillance and targeted arbitrary surveillance of human rights defenders and civil society organisations because of their work are both illegal under international human rights law.

In some cases, as Sharon Hom mentioned in the session on setting the scene, massive surveillance tools are trying to *incen-*

David Kaye   Danna Ingleton   Fionnuala Ní Aoláin

tivize desired behaviour. Attacks are increasing, becoming more pervasive and harder to detect. The pandemic has also exacerbated the situation since people are more willing to abdicate their privacy to fight the spreading of the virus.

Many of these technologies were developed and increasingly used in the wake of the 9/11 terrorist attacks with the fight against terrorism justifying the proliferation of surveillance tools and the collection and sharing of biometric data. National security legal frameworks and even the United Nations Security Council Resolutions have enabled this proliferation. In particular, UN Special Rapporteur Fionnuala Ní Aoláin made reference to how the Security Council Resolution 2396 (2017)[13] incited all states to collect biometric data for border management and counter-terrorism. This has been happening in a context where states have different definitions of terrorism and different rules in terms of data protection.

This permissive environment has allowed for security policies and tools to be taking over and undermining fundamental rights. Human rights discussions need to be occurring within the security sphere. A better regulation is needed in order to ensure compliance with international human rights standards, which must include legal restrictions on such surveillance technologies when they violate international human rights frameworks[14].

---

12 Human Rights Council, Surveillance and Human Rights, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, https://www.undocs.org/A/HRC/41/35

13 https://undocs.org/en/S/RES/2396(2017)

14 EDRi (2020). 'Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and Member States'. https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Both authoritarian governments and democratic countries deploy these technologies. State institutions and governments lack transparency on the procurement and use of these new technologies. Data is being collected from people's smartphones and computers in an invisible way, collected in bulk and then sold with no export controls.

If states have the responsibility to respect and protect human rights, the private sector too has a responsibility to comply with international norms. The UN Guiding Principles on Business and Human Rights make for an important regulation, but they are non-binding. Due diligence responsibility should apply to all stages, including the sale and transfer of surveillance products.

There is an opportunity to engage with companies, when limited instruments are accessible to engage with and influence states, apart from 'naming and shaming' those using mass surveillance technologies. It is key to work with the private sector, encouraging it to set up internal accountability mechanisms. It is also critical to work with companies from the design stage to ensure fundamental rights are considered. In addition, risk assessments should be conducted at all phases, including design, but also development, transfer, storage and destruction.

The need to safeguard encryption as a protection mechanism was also highlighted, reinforcing the relevance of privacy and individual security.

and audience alike shared their litigation experiences and lessons learnt from cases in Mexico, Serbia, Poland and Brazil, among others. The main idea was that investigating mass surveillance can benefit from the support of different actors, particularly for evidence gathering: from citizens and communities that can gather data and document mass surveillance hardware, to targeted journalists, human rights defenders and activists for identifying the presence of software, to the media, including informing citizens and raising awareness, to technology experts who can identify practices and tools often hard to detect.

The available legal instruments for strategic litigation vary from country to country, and also depend on whether they incorporate regional or international laws. In some cases, the launch of a Freedom of Information Request has been helpful to disclose information, even if in some other cases it has proven unsuccessful because authorities claim that the information is classified for national security reasons.

The lack of cooperation from governments, particularly in providing evidence, is indeed one of the main challenges for strategic litigation, and is often supported by citizens due to concerns for public safety when justified by the fight against terrorism and crime. This is just one more reason that emphasises the importance of keeping people informed and building community around the issue and at all stages of the strategic litigation process. Organisations fighting surveillance can also face retaliations

Anonymous
How should and how can large corporations stand up to human rights violations coming from the side of governments?

Anonymous
Should the EU consider AI challenges when drafting its 2021 legislation on Human Rights Due Diligence or we need only a more specific Ai legislation?

Anonymous
How can civil society partner with companies to hold governments accountable?

Apart from laws and regulation, and articulation with the business sector, other avenues to deal with the threats generated by mass surveillance were linked to the tech literacy of both citizens and civil society organisations, of which the latter also requires additional funding for training on digital protection and digital security.

There was also a specific session on how strategic litigation can be paramount in the defence against surveillance. Practitioners

and reprisals, which make it advisable for them to continuously conduct risk assessments and design and adapt security plans accordingly. Wider coalitions with different stakeholders, including UN Special Rapporteurs, are an advantage to reinforce the advocacy strategy.

The EU is a key actor in supporting lawyers working on strategic litigation. The EU can raise issues of concern with the partner countries' authorities, and has been collaborating closely with

the UN Special Procedures, including the UN Special Rapporteur on the situation of human rights defenders (HRDs). The EU also has a large toolbox to protect and assist HRDs, including special flexible funds that can be mobilised quickly for those at risk (among others, the Protectdefenders.eu protection programme[15]) and for providing legal support.

During the closed session on how privacy and surveillance has impacted the work of human rights defenders, HRDs shared their experiences and good practices. The main threats identified included online censorship, online smear campaigns, cyber espionage, facial recognition, tracking, hacking of accounts, infiltration in virtual groups, frozen bank accounts and targeted internet shutdowns. In addition, concern was raised that offline and online tools are being used in an articulated manner, leading to increased pressure and threats against human rights defenders. It was highlighted that HRDs in the EU also face threats, although not the same as those outside the EU.

Although, in general, HRDs lack the knowledge on how to protect themselves from these technological threats, some tools can be helpful. End-to-end encrypted messaging and mailing systems such as Signal and ProtonMail can be useful for safer communications. And cooperation with digital platforms can be beneficial to share civil society reports and documentation on abuse that help to build a counter-narrative.

Additional recommendations were made to the EU (see box below), including on how to improve the EU's role in supporting the monitoring of rights violations generated by surveillance tools, or on the investment in capacity building within EU institutions.

---

[15] https://www.protectdefenders.eu/en/supporting-defenders.html#emergency-support

Recommendations from these thematic sessions:

- The EU should take the lead in improving legislation and oversight, including providing civil society with a framework to act and advocate.

- The EU should consistently monitor human rights violations linked to the abusive use of advanced surveillance technologies for surveillance The EU should raise concerns for these acts of abuse in its bilateral diplomacy and in the multilateral fora.

- The EU should continue to act on the dual use, taking an international lead on control/prohibition of exports of surveillance software and equipment to repressive/authoritarian states.

- Certain standards in terms of data governance, non-discrimination, accuracy and robustness must be built in at the conception phase of new technologies.

- A community approach is needed to bring various strands of thought together in strategic litigation (civil society can collect data to support litigation, tech experts contribute in identifying tools often hard to detect, etc.).

- Provide adequate funding to ensure that CSOs have the capacity to act and engage at national, regional and international levels.

- Training on digital protection is essential, particularly for vulnerable human rights defenders. Supporting capacity strengthening of monitoring, advocacy and strategic litigation could help journalists and human rights defenders under surveillance.

- Facilitate exchange between HRDs from within and outside the EU, and foster and facilitate dialogue between big tech companies and HRDs on digital issues including surveillance

- A web platform could be created where civil society can document violations of human rights in the digital sphere, including informing political dialogue between the EU and the authorities concerned.

- Consider increasing the level of protection for HRDs within the European Union.

- Invest in capacity and training within EU institutions, because digital threats and surveillance are also applicable to the EU itself. Mutual learning between EU institutions should be encouraged.

Artificial intelligence

06

Artificial intelligence (AI) is currently at the centre of the EU agenda. The current context of the COVID-19 pandemic has created incentives for the use of AI, not only in terms of health but also to replace humans and their respective processes with automated processes. Recognising the opportunities offered by AI, but also the potential risks it entails, including in terms of human rights and fundamental freedoms, the EU is working towards a new legal framework to regulate AI. Along these lines, the European Commission recently presented the *White Paper on Artificial Intelligence – A European approach to excellence and trust*[16].

Artificial intelligence can help improve healthcare, contribute to more efficient farming and productive systems, and to climate change mitigation and adaptation, among many other uses. But the EU's White Paper also highlights that AI 'entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes'.

These risks were at the core of the Forum's sessions on artificial intelligence. The sessions gathered experts from a variety of backgrounds, including specialists that are helping the EU and other development partners navigating the dilemmas of AI. Also present were key civil society organisations in the field, such as EDRi (European Digital Rights), Article 19, the World Web Foundation and the Alliance for Inclusive Algorithms.

Participants debated how AI is being used for border management[17], law enforcement and workers' surveillance; how it is generating conditionality in the delivery of public services and affecting democratic processes. They also highlighted how these risks are deepening discriminations and broader societal inequalities, and have an impact on the exercise of fundamental
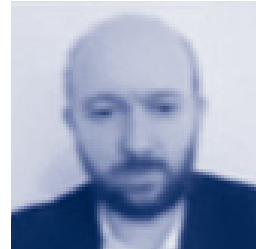

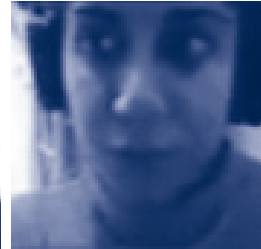Dafna Feinholz
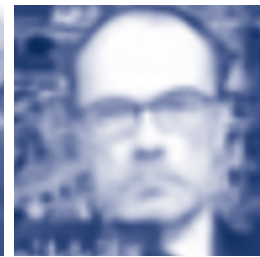
Juha Heikkila

Vidushi Marda

Ben Wagner

Andrea Renda

Sarah Chander

freedoms, including on rights that are not necessarily easy to spot. Andrea Renda, a member of the European Commission's High-Level Expert Group on Artificial Intelligence, observed in his intervention how there is growing evidence that the use of AI systems can lead to important impacts on virtually all fundamental rights, only a few of which are explicitly mentioned and protected in EU legislation. New challenges are emerging that have not been regulated yet, like protecting the integrity of the brain.

Artificial intelligence is undeniably developing fast and regulation processes are lagging behind. Panellists addressed the current efforts to regulate AI internationally, as well as the current non-binding guidelines drafted by several international bodies. There was a consensus on the importance of the EU to take the lead on regulation initiatives, as well as the potential impact of other parts of the world following.

And as was repeated in one of the Forum sessions during the consultation on the White Paper on AI, 90 % of the contributions

---

16 White Paper on Artificial Intelligence, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

17 EDRi (2020). 'Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up'. Available at: https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf

mentioned that their main concern is the conformity with fundamental rights that should be at the heart of regulatory efforts.

The EU wants to be at the forefront of innovation and AI development, but also to ensure that AI is beneficial and safe for everyone. Considering the many risks that are generated by well intended artificial intelligence, it is critical, on the one hand, to conduct risk assessments but, on the other, to embed accountability measures in AI systems. It was also mentioned how important purpose orientation is when working in AI, as well as foresight.

Juha Heikkilä, Head of Unit Robotics and Artificial Intelligence at DG CNECT, mentioned how appropriate regulation can open the opportunity for more innovation. Andrea Renda seconded this perspective and reinforced the fact that regulation can guide innovation, showing the way for the innovation that is needed and which can contribute to sustainable development.

On the challenges of navigating these blurred issues, speakers also defended the fact that algorithms should be more transparent. As Sharon Hom pointed out in her intervention during the session on setting the scene, people do not yet have a full understanding of how the algorithms are controlling their lives, and "even the developers do not know the extent of control and how machines are learning". In this context, risk assessments are critical at different stages, particularly since as risks are often not easily identifiable, they may vary from context to context, and there might be both individual and collective risks.

Civil society representatives and human rights defenders drew attention to the need to move beyond ethical principles and technical solutions, and instead called for comprehensive legislative governance responses, including the setting of regulatory limits on the uses of artificial intelligence that fundamentally contravene human rights. Sarah Chander of European Digital Rights pointed out that such uses may include the use of biometrics to facilitate mass surveillance, predictive policing systems resulting in the over-policing of marginalised communities, and the extraction of data in situations of major power imbalance, such as in migration management and at the border[18].
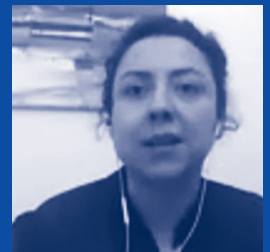
Processes like the GDPR are considered major advancements, but are not enough, particularly since the risks of artificial intelligence go beyond the individual dimension. It was stressed that collective and broader societal harms have to be addressed, in addition to individual rights. In this regard, CSOs have the capacity and the resources to collect evidence on the harms caused by AI, particularly on shrinking the space for civil society and abusing fundamental freedoms. The monitoring role of CSOs is critical, but it needs to be a shared burden.

Panellists also voiced concern over the imperative to observe how the "benefits" of AI are being distributed. AI systems often play a role in reinforcing and amplifying existing societal problems, a fact that has also been the case during the COVID-19 pandemic.

There was a consensus that those who develop AI need to be closer to those who are subject to its impacts, including groups in vulnerable situations. There is also an opportunity for a regulation to address these impacts, and the power imbalance between those who extract data and those whose data is being extracted and used – ethnic minorities, LGBTI persons, persons from the global south. This calls for more inclusive policy-making processes and a people-centred and rights-based artificial intelligence regulation.

> **We need a positive agenda. We need "GDPR" moment for economic, gender and race equality for AI.**
>
> Renata Avila

Civil society representatives also called on the EU's influence to ensure coherent respect and protection of human rights and fundamental freedoms throughout its different policies, providing the examples of the EU Migration Pact and the potential expansion of biometric surveillance on migrants that raise grave concerns. The Forum was also reminded that profiling has occurred in EU countries. Participants also linked this problem with the challenge for the EU of having 27 Member States with differing views and legal frameworks on artificial intelligence.

Finally, it was mentioned that people need to know more on how the regulation is being prepared, and on AI in general: *they need to be able to distinguish if they are talking to a human being or to a computer*, evidencing the relevance of increased digital literacy.

---

18 European Digital Rights (2020). 'Recommendations for a Fundamental Rights-based Artificial Intelligence Regulation'. Available at: https://edri.org/wp-content/uploads/2020/06/AI_EDRiRecommendations.pdf

22ND EU-NGO HUMAN RIGHTS FORUM
9-10 DECEMBER 2020

👤 Anonymous

Given the complexity & reach of AI. how can NGOs that are not AI specialists participate meaningfully in devyloping standards & auditing use?

👤 Anonymous

Human rights need to be at the core of the regulation of AI. Why isn't the EU doing more in this area?

👤 Anonymous

Is the EU have any plan to enforce regulation/guidelines to ensure that AI is not used to shrink freedom spaces? Its not only about Ethics but about Rights.

👤 Anonymous

Is it possible to agree on a global ethical charter for the use of artificial intelligence?

👤 Anonymous

Can we move on from a discussion on 'ethics' and focus on human-rights compliance of AI? And assess the impact on human rights first. then the risk level next?

Recommendations from these thematic sessions:

- Human rights must be prioritised in regulatory efforts on AI, including the drawing up of regulatory 'red lines' for uses of AI that are incompatible with human rights.

- EU should take the lead to incentivise UN member states and the private sector to ensure a rights-based approach to AI development.

- All actors (national states, civil society, private sector including social media platforms) need to contribute to a new vision for AI.

- Support citizen engagement and promote more inclusive processes; not enough women are involved in developing and regulating AI. A more diverse policymaking table is needed, including with a focus on groups in more vulnerable situations.

- Reinforce the accountability of all actors, including national states and business sector/social media platforms.

- Contribute to making it explicit how states are using AI systems for public decisions and what the work of the authorities is whose job it is to supervise AI systems.

- Ensure coherence in all EU policies: commitments on human rights and AI need to be discussed not only at human rights fora, but also when discussing trade and security policy, migration, etc.

- Further public awareness and digital literacy are needed.

Conclusions

The 22nd EU-NGO Human Rights Forum was held in a year that was particularly challenging for human rights and human rights defenders worldwide. Digital technologies are being weaponised by states to shrink civic space and by companies to monetise people's privacy and data. The fast progress of these technologies has challenged the capacity of policy-makers and legislators to catch up, often leaving the private sector with the role of self-regulating and self-monitoring the respect and protection necessary for human rights.

In this turbulent context, the discussions during the Forum were clear in acknowledging **both the potential and the risks of new digital technologies**, and that these risks have an impact on human rights and fundamental freedoms, not only at an individual level but also in a societal dimension. In this context, governance mechanisms and a regulatory framework are critical.

There was a consensus in all thematic sessions that **the EU can have a pivotal role in leading this much-needed regulatory process**. Businesses have a responsibility to comply with human rights standards, but national states are the essential duty bearers. States are the actors with the duty to protect and respect human rights.

The legislators' goal should be first and foremost to *make the digital space work for everyone*: putting the dignity of people at the centre and safeguarding all human rights, from the right to privacy, to non-discrimination, to taking part in decision-making processes. This requires building extended coalitions where a plurality of actors should have a say.

Tech companies have a disproportionate power due to their capacity to collect and use data compared to the citizens using their technology. The Forum's audience was firm in declaring that the private sector must **ensure safeguards to prevent and mitigate adverse impacts on human rights**. If due diligence is a vital tool, it is not enough and the private sector needs more robust guidance and clearer obligations. **Transparency and accountability** need to be reinforced.

The EU should use its power to apply pressure to national states violating human rights through internet shutdowns, mass surveillance tools, etc. **But it also needs to urge digital companies that are being complicit** with states to respect international law standards.

This also calls for a **stronger role for civil society and human rights defenders**. Civil society is already playing a major part in identifying solutions and in monitoring big tech companies and governments' use of data and their respect for fundamental freedoms, but CSOs and HRDs need to be supported and trained to deal with the new emerging challenges, including in terms of digital **security and digital literacy**. Civil society organisations and HRDs also need to have a seat at the table in decision-making processes.

As Sharon Hom highlighted, CSOs do not come to the table with the same space for intervening. It is necessary to ensure that CSOs and human rights defenders have this space, including those representing **women and groups in more vulnerable situations**, such as migrants, LGBTI, ethnic and religious minorities, persons in precarious socio-economical situations. Moreover, it was also mentioned that there is the need to foster meeting **points between the tech world and civil society**, particularly via the open-source world and with the possibility of building more sustainable platforms. **Civil society needs to be involved from the beginning** to ensure that the private sector is considering human rights from the design stage.

07

The reflections led to an imperative for broader and more inclusive dialogue spaces. In all these efforts, the EU is in an advantageous position to **facilitate the dialogue** between all stakeholders. The EU can be a **standard-setter** and push **for human rights to be at the centre of these conversations and of the regulatory processes**.

A strong **will to cooperate** was evident from the diverse stakeholders present at the Forum, from the EU and multilateral agencies' representatives, to civil society organisations and human rights defenders and the private sector. The closing session, on the second day of the Forum, coinciding with the anniversary of the signature of the Universal Declaration of Human Rights, ended with an optimistic shared sense that there is the opportunity to work better together to ensure that the human rights of all people are realised in digital technologies.
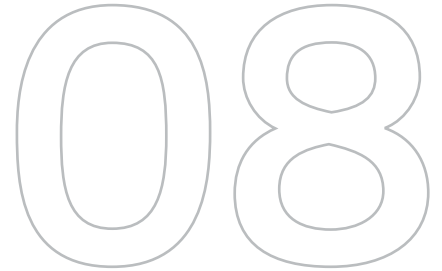
This Forum was not a 'one-off' event; it is the beginning of a process. The EU will work now on analysing all the recommendations from the different sessions, most of them available at the Forum's platform (https://eu-ngo-forum.b2match.io/). The EU will continue to actively engage with civil society, human rights defenders, the private sector and UN member states to protect and promote human rights in the digital sphere.

22ᴺᴰ EU–NGO HUMAN RIGHTS FORUM
9-10 DECEMBER 2020

What is the most important that the EU can do to enhance freedom of expression online?

Attention to minorities

Work w/ private sector

Pressure on social media

Regulation (EU members!!)

Support independent media

Law enforcement

eungoforum2020

Regulation

Education

Support media literacy

Legislate & control

Fake checking

Create awareness

Support grassroots orgs

Monitorbigmediacompanies

Enforcement Standards

Annex: Full agenda

08

Wednesday, 9 December 2020

10.00–12.00   **Public thematic panel: Artificial intelligence – State of play of international efforts to regulate AI**
Moderator: Ben Wagner – Assistant Professor, Faculty of Technology, Policy and Management, TU Delft
Speakers:
- Andrea Renda – Senior Research Fellow at CEPs, member of the European Commission High-level Expert Group on Artificial Intelligence
- Dafna Feinholz – Chief of Bioethics and Ethics of Science and Technology, UNESCO
- Sarah Chander – Senior Policy Adviser, European Digital Rights
- Vidushi Marda – Senior Programme Officer, Article 19
- Juha Heikkilä – Head of Unit Robotics and Artificial Intelligence, Directorate-General for Communications Networks, Content and Technology, European Commission

12.00–13.30   **Interactive expert session: Artificial intelligence (I) – Addressing artificial intelligence harms: Individual, collective, societal**
Moderator: Sarah Chander – Senior Policy Adviser, European Digital Rights
Speakers:
- Paul Nemitz – Adviser, Directorate-General for Justice and Consumers, European Commission
- Griff Ferris – Legal and Policy Officer, Fair Trials
- Chenai Chair – Digital Policy Officer, World Wide Web Foundation

12.00–13.30   **Interactive expert session: Private sector (I) – Enabling engagement of civil society with business and its processes**
Moderator: Javier Martín Cerracín – Policy Officer – Human Rights, European External Action Service
Speakers:
- Christen Dobson – Senior Project Lead, Business and Human Rights Resource Centre
- Paul Roeland – Transparency Lead, Clean Clothes Campaign
- Jacqueline Geis – Chief Executive Officer, Videre
- Gbenga Sesan – Executive Director, Paradigm Initiative
- Jason Pielemeier – Policy Director, Global Network Initiative

14.00–16.20   **Plenary opening session**
Video Message:
- Josep Borrell – High Representative of the EU for Foreign Affairs and Security Policy / Vice-President of the European Commission
- Jutta Urpilainen – Commissioner for International Partnerships, European Commission

High-level panel:
- Michelle Bachelet – United Nations High Commissioner for Human Rights
- Eamon Gilmore – EU Special Representative for Human Rights
- Alice Mogwe – President of the International Federation for Human Rights

Setting the scene
Moderator: Jennifer Baker
Speakers:

- Heidi Hautala – Vice-President of the European Parliament
- Giuseppe Abbamonte – Director for Media Policy, Directorate-General for Communications Networks, Content and Technology, European Commission
- Michael O'Flaherty – Director of the European Union Agency for Fundamental Rights
- Marie Arena – Member of the European Parliament, Chair of the Subcommittee on Human Rights
- Sharon Hom – Executive Director at Human Rights in China
- Eliska Pirkova – Europe Policy Analyst, Access Now

16.30-18.00 **Interactive expert session: Fundamental rights and freedoms (I) – Fighting internet shutdowns, censorship and cybercrime laws**
Moderator: Adrian Shahbaz – Director for Technology and Democracy, Freedom House
Speakers:

- Felicia Anthonio – #Campaigner and #KeepItOn Lead at Access Now
- Bahar Saba – MENA Programme Officer, Article 19
- Olivier Luyckx – Head of Unit Security, Nuclear Safety, Directorate-General for International Cooperation and Development, European Commission
- Guy Berger – Director for Freedom of Expression and Media Development, UNESCO

16.30-18.00 **Interactive expert session: Privacy and surveillance (I) – Exchange between human rights defenders: How have surveillance technologies impacted their work**
Speakers:

- Raphael Warolin – Policy Officer, European External Action Service
- Christine Mardirossian – Project Manager, Directorate-General for International Cooperation and Development, European Commission

Thursday, 10 December 2020

9.00-10.30 **Interactive expert session: Fundamental rights and freedoms (II) – Online activism: Strategies for empowerment and mobilisation**
Moderator: Elizabeta Kitanović – Conference of European Churches
Opening remarks: Nathan Law – Pro-Democracy Activist
Speakers:

- Roman Pratasevich – Journalist, Democracy activist
- Mohamad Najem – Executive Director, SMEX
- Alain Amrah Horutanga – Blogger, co-founder of YAGA

9.00-10.30 **Interactive expert session: Privacy and surveillance (II) – How to challenge surveillance through litigation?**
Moderator: Ilia Siatitsa – Legal Officer, Privacy International
Speakers:

- Paulina Guttiérez – Law and Policy Programme, Article 19
- Đorđe Krivokapić – Assistant Professor, Faculty of Organisational Sciences, University of Belgrade
- Dominika Bychawska-Siniarska – Human rights lawyer

10.30-12.30 **Public thematic panel: Technology, business and human rights – Human rights challenges and responses from IT companies: Where we are and where we can go**
Moderator: Guus Houttuin – Senior Adviser on Trade Issues, European External Action Service
Speakers:

- Mark Hodge – Senior Adviser, B-Tech Project, United Nations
- Anna Herold – Head of Unit for Audiovisual and Media Services Policy, Directorate-General for Communications Networks, Content and Technology, European Commission
- Iverna McGowan – Director of Europe Office, Center for Democracy and Technology
- Stephen Turner – Director EU Public Policy, Twitter
- Cornelia Kutterer – Senior Director for EU Rule of Law & Responsible Tech, Microsoft
- Alexey Kozliuk – Program Director, Mass Communications Foundation

12.30-14.30   **Public thematic panel: Fundamental rights and freedoms in the digital sphere – Enhancing freedom of expression online whilst fighting disinformation and hate speech**
Moderator: Lutz Güllner – Head of the Division on Strategic Communications, European External Action Service
Speakers:
- Patrick Penninckx – Head of Information Society Department, Council of Europe
- Maria Ressa – CEO and President, Rappler
- Aura Salla – Public Policy Director, Head of EU Affairs, Facebook
- Ritwajit Das – International Dalit Solidarity Network

14.30-16.30   **Public thematic panel: Privacy and surveillance – Arbitrary mass and targeted surveillance: Are we facing an irreversible process?**
Moderator: Barbora Bukovská – Senior Director for Law and Policy, Article 19
Speakers:
- Danna Ingleton – (Acting) Co-Director, Amnesty Tech
- David Kaye – Law Professor, University of California, Former United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
- Fionnuala Ní Aoláin – UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism
- Irina Orssich – Team Leader, Technologies and Systems for Digitising Industry, Directorate-General for Communications Networks, Content and Technology, European Commission

16.30-18.00   **Interactive expert session: Artificial intelligence (II) – Fostering artificial intelligence governance: Ensuring human rights compliance, ensuring justice**
Moderator: Amba Kak – Director of Global Policy & Programs
Speakers:
- Oliver Unger – Legal Officer, German Federal Ministry of Justice and Consumer Protection
- Philip Dawson – Fellow on Technology and Human Rights, The Carr Center for Human Rights
- Renata Avila – Alliance for Inclusive Algorithms

16.30-18.00   **Interactive expert session: Private sector (II) – Obligations for states and companies in a digital age: Reflection on their respective role and responsibilities**
Moderator: Guus Houttuin – Senior Adviser on Trade Issues, European External Action Service
Speakers:
- Anne Marie Engtoft Larsen – Denmark Tech Ambassador
- Tyler Gillard – Head of Sector Projects, Responsible Business Conduct Unit, OECD
- Camille Le Pors – Lead, Corporate Human Rights Benchmark, World Benchmarking Alliance
- Théo Jaekel – Corporate Responsibility Expert, Ericsson
- Penelope Faulkner – Vice-President, Vietnam Committee on Human Rights (VCHR)

18.00-19.00   **Closing session**
Moderator: Jennifer Baker, Journalist
- Barbora Bukovská – Senior Director for Law and Policy, Article 19
- Sarah Chander – Senior Policy Adviser, European Digital Rights
- Iverna McGowan – Director, Europe Office, Center for Democracy and Technology
- Adrian Shahbaz – Director for Technology and Democracy, Freedom House

Closing speeches
- Luisa Ragher – Head of Human Rights Division, European External Action Service
- Chiara Adamo – Head of Unit Gender Equality, Human Rights and Democratic Governance, Directorate-General for International Cooperation and Development, European Commission
- Sylvain Mossou – Advocacy and Training Officer, EuroMed Rights