A Roadmap for Human Rights in Digital Diplomacy

Presentation to the Council Working Party on Human Rights in Foreign Policy (COHOM)

6 December, 2023

In July 2022, the European Union (EU) unveiled its new strategy on 'Digital Diplomacy', spelling out the block's approach to digital foreign policy. The strategy was timely and necessary because authoritarian States such as China have been investing in shaping global tech law and policy for years. The EU is an impressive normative power with international reach. For instance, the General Data Protection Regulation (GDPR), the EU's landmark privacy legislation has been copied by many other countries the world-over. Now that the EU has further expanded its repertoire with the Digital Services Act (on content moderation), and a number of other significant digital regulations, how can the EU capitalise on the so-called '*Brussels effect*', and realise its stated goal to …'actively promote universal human rights and fundamental freedoms, the rule of law and democratic principles in the digital space'? CDT Europe argues that the EU will need to invest more time, resources and energy to ensure that its foreign digital policy packs a full punch, and of course does not unwittingly undermine its existing human rights foreign policy. The *Brussels effect* should be understood in a more complex manner than simply copy and pasting legislation which can bring its own perils, rather a deeper review of how, with a refreshed and clarified digital foreign policy tool kit, the EU can ramp up its work for human rights and democracy.

We note with appreciation the EU Annual Human Rights Report for 2022, which outlines how the External Action Services, and member states have advocated for and supported a human rights-based approach to digital technologies.

We support an approach that uses a range of modes of engagement, which is appropriate given the emerging nature of some issues in question. With this document, we provide a top-level overview of important entry points and opportunities for the EU's further work in this area.

I wish to address a number of areas today;

(1) Capacity and strategy - How to Ramp up Work on Digital Diplomacy
(2) Digital Censorship & Online Expression
(3) Human rights in the Age of Surveillance

(4) Artificial Intelligence
(5) Workers and Technology

1. Capacity & Strategy - How to Ramp Up Work on Digital Diplomacy?

Technology and human rights is a technical subject matter. This is why any increase in work in this area must necessarily involve capacity building and dedicated resources.

To give one example, anyone who has worked in business and human rights over the years will understand that much of the debates have centered around increasing accountability and liability as necessary for corporate involvement in human rights violations. It is therefore puzzling why when it comes to content moderation, human rights experts speak of the need for liability protections for corporations. This is because if platforms are made liable for users' speech, they will err on the side of caution and over-remove lawful speech. This would be a problem everywhere, but is a more acute problem in jurisdictions where governments are involved in curbing all dissent or cracking down on human rights defenders. The EU Digital Services Act has codified this rights protection, but has also made clear when companies are liable in line with the concept of due diligence in the UN guidelines on business and human rights companies would not be liable for user-generated content, only human rights harms that result from their own products and services, use of personal data in microtargeting could be an example of this. This nuance is not an obvious one, and one that has to be explicitly explained and embedded into EU foreign policy and practice.

The need for technical expertise should also be a strong incentive to work with **civil society as real partners** in this area. There are a number of existing global coalitions and partnerships in which the EU should certainly have a dedicated engagement strategy. Examples include the Freedom Online Coalition; the Global Encryption Coalition, the DSA Alliance. There are also many NGOs with representatives here in Brussels that also have chapters or offices across the world, such as Access Now, Amnesty International, etc. At CDT Europe we have successfully played a facilitation role, with the support of the French, the Czech and Spanish EU presidencies, between EU Council Working Groups and civil society. We organised a civil society roundtable series and have already had sessions covering the Digital Services Act, the Child Sexual Abuse Regulation and the EU AI Act. Indeed we are currently working on an event for next year which will look at the implementation of the EU Digital Services Act, and we would love to work with you all to ensure that there is dedicated time to consider the foreign policy elements of this new landmark law.

Indeed, given the profound impact that many of these new EU laws regulating our online world will have, it is a moment where there is an urgent need to pay attention to **internal-external coherence** on EU policy and practice. To give a concrete example, protecting the digital security of human rights defenders has been a fundamental part of EU human rights foreign policy for some time. Yet, recent EU regulatory proposals have proposed undermining end-to-end encryption. Such a proposal is particularly jarring to the hundreds of journalists and

human rights defenders currently in detention all around the world. Their "crime"? Defending the rights of others and standing up for democracy. In Turkey, to cite one example, many have gone to prison simply for using encrypted messaging services — an act in itself deemed criminal by the authorities. The UN High Commissioner for Human Rights, the European Commissioner for Human Rights, and countless other human rights experts have been clear that the right to communicate securely via end-to-end encryption has to be protected.

It is crucial that policy and laws that could have such a profound impact on foreign policy be *actively debated before* any final conclusions are drawn. As a practical matter this might involve more joint sessions of different working parties, say perhaps a joint session of COHOM with the the Working Party on Telecommunications and Information Society (TELCO) or the Horizontal Working Party on Cyber Issues (Cyber) or Law Enforcement Working Party (LEWP). Civil society can also help bridge these gaps by highlighting the contradictions and potential policy clashes as they arise.

2 Digital Censorship & the Regulation of Online Expression and Civic Space

"Digital censorship" can involve direct or indirect state action that seeks to prevent or suppress online communication, or to punish online expression, through laws, policies, or practices that are inconsistent with states' international human rights obligations. While some forms of digital censorship are direct and overt (such as internet shutdowns or laws prohibiting certain content), the suppression of expression and information can take other forms, such as government pressure on content moderation processes through methods contrary to the rule of law, and mandates to locate data and personnel in-country to increase the government's leverage over private companies.

Mis- and disinformation continue to present challenges to democratic societies, threatening trust in and the integrity of elections and jeopardsing public health. But some efforts to combat mis- and disinformation can pose significant threats to freedom of expression and privacy online, and it is crucial for governments to combat disinformation through approaches that are transparent, accountable, and that promote human rights. Unfortunately, many governments, including governments in the region, have used "fake news" laws and other efforts to combat disinformation as a pretext to crack down on independent journalists and other dissenting speech.

Thankfully, the conclusion of the EU Digital Services Act (DSA) means that there is now **a common EU policy** on platform regulation. This strengthens the hand of the EU's foreign policy arm. Although not perfect, the DSA includes a number of essential rights-preserving provisions and principles that the EU should now extrapolate into its foreign policy. The DSA is aligned with international human rights standards such as the UN Guiding Principles on business and human rights. This approach could be used to inspire EU advocacy in the development of similar policies in other jurisdictions. The building of rights-protection into

content moderation policies on intermediary liability combined with industry due diligence sets a precedent that the EU could promote and try to make the global standards in this area.

The DSA will bring unprecedented transparency to such systems, and importantly also allow researchers to independently examine such data. In its broader foreign and development policy, this would mean that the EU must formally proactively discourage government takedowns without safeguards, and emphasize the link between privacy protections at national level and the proliferation of disinformation.

Efforts to address these priorities could include:

- Clearer acknowledgement that disinformation campaigns are driven more by improper exploitation of personal data, as well as often opaque operation of algorithms.
- A formal policy and strategy whereby the EU discourages government takedowns without safeguards, and emphasizes the link between privacy protections at national level and the proliferation of disinformation.
- Commitments for governments not to engage in digital censorship activities and to affirmatively respect and protect human rights online, using, for example, criteria articulated by the Freedom Online Coalition.
- Commitments by partner nations to petition to join the Freedom Online Coalition (or at a minimum to engage in diplomatic coordination with Freedom Online Coalition members at key intergovernmental organizations, including the UN and the ITU, around issues of Internet governance).
- Commitments from governments to engage in multistakeholder consultation around issues of online content regulation and to support civil society participation in policymaking processes.
- Commitments to make use of existing subject-specific multistakeholder initiatives, such as the Christchurch Call to Action, as fora for discussion, shared learning, and addressing global challenges within a framework that champions human rights and an open Internet.
- Commitments to create senior-level government positions focused on the impact of technology on human rights.
- Commitments to provide sustained funding for human rights-protecting technology. Examples could include:
    - funding for the Open Technology Fund and similar initiatives;
    - funding to support civil society and oversight bodies to increase government accountability with respect to digital rights and the rule of law.
- Information Sharing about regulatory approaches to promote:
    - frameworks for government accountability related to technology
    - user rights when content is removed from social media platforms
    - transparency in content moderation
    - researcher access to technology platform data as a way to support platform accountability
    - countering mis/disinformation (see specific topic on this below).

- Cooperation mechanisms to identify shared threats to election integrity resulting from coordinated campaigns by foreign actors.
- Information sharing about methods to address threats to election integrity, for example:
    - mechanisms that allow social media platforms, election officials and civil society watchdogs to monitor threats and pursue responses in real time
    - strategies for public officials to counter mis- and disinformation, for example by ensuring they use official web domains (.gov, not .com) and preemptively focus on sharing authoritative information.

- Commitment to provide/increase funding for election integrity or health information integrity research, and to provide/increase funding for civil society organisations that can increase public accountability for how social media companies and news outlets disseminate information.
- Information sharing about methods to increase the opportunity for independent research on data held by social media companies, while protecting individual privacy, to better understand the effects of mis- and disinformation in various countries, cultures, and languages.

3. Surveillance Technology

The growing availability of surveillance technologies for government and private use creates significant concerns for human rights and democracy. In addition to the concerns presented by the use of facial recognition technology and other surveillance tools by law enforcement and government actors, the surveillance-for-hire industry presents a substantial threat through which private actors can use invasive software tools and other data collection strategies to target individuals. The Pegasus Project revealed the scale of this problem, identifying at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware from 2016-2021. A coalition of over 150 civil society organizations and independent experts have called on governments to regulate the export, sale and use of surveillance technology, with concrete recommendations that we urge you to review. The extent of the Predator scandal has been more recently revealed.

The EU, as you know, already has the Dual Use Regulation, however as both scandals showed its implementation has not been robust enough, its provisions not clear enough on human rights, and frankly that we will need more tools beyond this regulation to fully prevent exports of Spyware. The UN High Commissioner for Human Rights has called for a moratorium on the trade of such surveillance technology until robust regulation is in place to protect human rights. The EU and its member states could become leaders in articulating the elements of regulation of spyware use that are necessary to protect human rights. Given that the Dual Use Regulation has been in force in the EU, examining its strengths and weaknesses could put the EU in a strong position with a clear evidence-base behind it to advocate for what effective regulation of

trade in spyware might look like. The lack of provisions in the EU AI on export control for cyber surveillance technology could also be a missed opportunity.

The proposed Cybercrime Treaty at the UN General Assembly, currently in final stage negotiations, has raised alarms across global civil society and industry for its overbroad scope of what constitutes "cyber" crime, high potential to violate human rights in cross jurisdictional data storage and sharing lacking oversight, and inclusion of mechanisms for investigating and prosecuting crimes.

Some relevant steps could include:

- Call for a moratorium on the export, sale and transfer from the EU of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards.
- The EU should put NSO on its global sanction list and take all appropriate action to prohibit the sale, transfer, export, import and use of NSO Group technologies, as well as the provision of services that support NSO Group's products, until adequate human rights safeguards are in place.
- The EU [and its Member states] should take the lead in establishing adequate human rights safeguards governing use of spyware.
- EU member states should collectively reject the proposed Cybercrime Treaty at the UN General Assembly and work with aligned, democratic countries to do the same.

4. Artificial Intelligence / Data-Driven Decision Making

There is a growing awareness that AI technology can bring not only new opportunities, but also risks – including the risk that AI or data-driven decisionmaking in fields such as employment, lending, housing, or access to public benefits can reinforce existing biases in society, or make decisions in a way that evades public scrutiny and accountability.

The EU AI Act will be a landmark law and the first of its kind to attempt to regulate the way in which AI works.

In terms of foreign policy the EU could encourage:

- Commitments for countries to adhere to the OECD AI Principles. Given the principles' high level nature, these should be seen as a baseline to improve upon with more specific commitments and frameworks for cooperation/information sharing.

- Principles that recognize the potential for AI, while clearly warning about the risks in various use cases. Set clear red lines on the most dangerous use cases of AI such as social scoring and facial recognition technology.
- Information sharing about risks that arise in different use cases and countries' own experience deploying and specific ways to address those risks, such as:
    - how to conduct or require meaningful audits and impact assessments
    - approaches to public notice / explanation / transparency regarding how AI systems are used
    - processes to improve procurement and public accountability around government use of AI in the administration of public benefits
    - ways to evaluate the appropriateness of using AI (such as facial recognition technology) for law enforcement purposes
- Commitments to develop domestic programs/frameworks to better ensure responsible and accountable use of AI in the administration of government programs, or the use of AI by law enforcement.
- Commitment to provide/increase funding for research on responsible AI.

5. Workers & Technology

New surveillance technologies and data-driven assessment tools are making it easier for companies to monitor workers in the workplace, and make inferences about employees and applicants for employment based on a wide variety of data points. Examples include the use of AI in hiring or promotion decisions; "bossware" that closely monitors workers' activities to assess performance and efficiency in both factories and office environments; and software that analyzes workers' social media activities. These tools present clear risks for workers' privacy, autonomy, ability to organise, right to equal treatment, and physical and mental safety. The EU. should raise awareness about these threats and demonstrate its commitment to protecting workers' interests. Some potential strategies include:

- Shared Principles that recognise the risks of work-related surveillance tools for workers' privacy, autonomy, ability to organize, right to equal treatment, and physical and mental safety. These could articulate clear red lines on certain topics, like the extension of surveillance technology outside the workplace, or the use of surveillance technology to impede worker organizing.
- Developing a cooperative mechanism or information sharing between the labour departments of participating nations about the types of technologies being deployed to monitor and evaluate workers, their prevalence and impacts, and approaches to regulation and/or oversight. These efforts would overcome the significant information asymmetry that makes it hard for workers, advocates and governments to engage in oversight of such tools.