**Red en Defensa de los Derechos Digitales (R3D), Derechos Digitales (DD) and Electronic Frontier Foundation (EFF)' Oral Intervention on Criminal Procedural Measures**
**Delivered By Grecia Macias, R3D**
**Fourth Session - 9 January to 20 January 2023**

**11 January 2023**

Red en Defensa de Los Derechos Digitales, jointly with Derechos Digitales and the Electronic Frontier Foundation, welcomes the opportunity to address the Ad-Hoc committee on the Consolidated Draft of the proposed Cybercrime treaty.

We appreciate the opportunity to speak today on the safeguards needed to protect human rights, Articles 41 and 42.

We believe that human rights protections and safeguards should drive the scope of the Convention's provisions governing criminal procedure and law enforcement powers. How and under what circumstances police are allowed to access data during investigations can implicate people's rights and put them at risk.

We recommend that the treaty's scope is designed explicitly to prevent overreach and abuse. Therefore, we recommend that Article 41 limits the range of procedural measures to crimes established by the Convention.

Article 42, on condition and safeguards, is also fundamental as it aims to provide the safeguards applicable to the investigative powers contained in Articles 43 to 49. Hence it is necessary that additional safeguards are included, and existing ones are further clarified and strengthened to avoid the risk of human rights abuses in the applications of these functions.

At a minimum, we recommend the following:

- Article 42 should be more detailed and robust and should ensure that interferences with privacy are premised on a factual basis for accessing the data, in particular, a factual indication for suspecting that such person is planning, committing or having committed a criminal act;
- Article 42 should apply to all types of personal data, including non-content data such as metadata, traffic data, and subscriber information;
- Paragraph 2, Article 42 should be strengthened to require not only independent supervision but also prior independent or , strongly preferably, judicial authorization of surveillance measures;
- It should include a right to an effective remedy and user notification;
- Should add a provision to require that any investigative powers listed in this Convention should be conducted in ways that do not compromise the security of digital communications and services, and
- Explicitly prohibit any data processing and any interference with the right to privacy that is not lawful, necessary, legitimate, and proportionate.
- Finally, we recommend adding adequate grounds for the refusal of int'l cooperation.

**EFF, Derechos Digitales, Red en Defensa de los Derechos Digitales's Oral Intervention on Criminal Procedural Measures Delivered By Katitza Rodriguez**

Fourth Session - 9 January to 20 January 2023

Dear Madame Chair,

The Electronic Frontier Foundation, jointly with Derechos Digitales and Red en Defensa de los Derechos Digitales welcomes the opportunity to speak today.

To avoid duplication with other civil society participations, today we will focus on Articles 41, 43 & 46(4), 47 & 48.

Suggest narrowing the scope of Article 41 to core cybercrimes. Widening to **all crimes committed with the use of an ICT** significantly risks undermining human rights, including the right to privacy and the right to a fair trial.

Article 43 should be amended to require a strong factual basis for using expedited preservation orders. Such factual basis should verify the existence of whether there are factual indications for suspecting that such person is planning, committing or having committed criminal acts. We believe that all criminal procedural measures interfere with human rights and fundamental freedoms and require specific safeguards.

We have concerns with the obligations imposed on Art. 46(4), and suggest its amendments to clarify that it won't. compel persons with special knowledge to provide technical assistance. Such technical assistant could include compelling security experts to disclose vulnerabilities of specific software.

Let's imagine authorities are authorized to compel experts to exploit security flaws. In that scenario, authorities will more likely be incentivized to build an "arsenal" of security vulnerabilities to attack a target in the event of a criminal investigation.

This interest, in turn, will prevent authorities from notifying the affected provider, so the provider can fix the security vulnerability that has been discovered. If such a vulnerability is fixed, authorities will not longer able to exploit such vulnerability.

Patching vulnerabilities are critical to keeping billions of people safe from criminal attacks. It's an essential preventive measure against cybercrime. Hence, keeping billions of people safe far outweigh the possible facilitation of prosecution in individual cases.

Finally, Articles 47 and 48 should be deleted. At least, the scope of the text should be clarified to exclude state hacking powers. While the existing language, in our interpretation, does not authorize hacking powers, we have heard different interpretations in other global forums.

State hacking powers remain controversial and can cause collateral harm to the integrity and security of networks. There is no consensus as to when these powers can be appropriately invoked, and there is a risk that some State Parties will inappropriately implement Articles 47 and 48 to include this type of intrusive surveillance. Thank you.

**Access Now**
**<u>Item 6: Procedural measures and law enforcement</u>**
**Delivered by Raman Jit Singh Chima**

**11 January 2023**

We are glad to hear the recognition expressed by many states that the issue of procedural measures can have deep significance on a range of vital interests - including their intrusion on privacy and other protected human rights.

As we have noted before, we believe that ideally, procedural measures under this proposed treaty should apply primarily only for those matters included in the Criminalisation chapter, and which we believe should include only the "core" cyber-dependent crimes.

We welcome the effort made to provide a baseline, cross-cutting conditions and safeguard in the form of Article 42 in the Consolidated Negotiating Draft (CND). This is a good start, the beginnings of a foundation that must be further worked on. Specifically, we believe that Article 42 should avoid using the phrasing "adequate protection of human rights and liberties" - the word "adequate" should be dropped. We strongly support the current requirements at the end of 42(1), requiring the incorporation of principles of proportionality, necessity, and legality, and the protection of privacy and personal data; this language must remain.

The internationally accepted principles of necessity and proportionality provide us guidance on how Article 42 should be further improved. We shall submit to the AHC our previously published universal implementation guide for the Necessary and Proportionate principles, which provides detailed guidelines and a checklist on how legal mechanisms for access to protected information for investigatory purposes and communications surveillance should operate in a manner respecting international human rights law. Correspondingly, Article 42 should require that government applications involving measures under chapter III include the legal authority involved, the necessity of a search or other procedural mechanism being sought, and how the burden of proof has been satisfied. It should apply to all measures seeking the preservation, access to, search and seizure, or disclosure of protected information, and not be bound by legacy, outmoded legal approaches of different safeguards to metadata or content data.

We welcome recognition of the explicit reference to judicial or other independent supervision in Article 42(2). We recommend that 42(2) also require the conditions and safeguards to include reference to appeals and remedies, penalties for unlawful access, how emergency procedures would operate, as well as requirements around government transparency. Government transparency in the use of procedural measures and law enforcement mechanisms not only protects and furthers human rights; it provides useful information on what is and what is not working, and builds much needed trust and understanding.

We note that several states have called upon an expansion of the time period in Article 43 for which preservation of data can be requested. We admit our concern at the potential for abuse here, with preservation requests being transformed, for all purposes, into a general

data retention mandate instead. At minimum, we would stress that any expansion of the time period for preservation of requests should be subject to safeguards and oversight, including demonstrating necessity, proportionality, and legality for such requests of an additional 90 day preservation period before an independent judicial oversight mechanism.

We are concerned at the overbreadth of Article 46(3) with respect to empowering authorities to order persons knowledgeable with ICT systems to provide information to facilitate electronic search and seizure measures. Proposed powers for law enforcement or other measures on cybercrime cooperation should not necessitate the undermining of encrypted communications or the introduction of general vulnerabilities into software systems; such vulnerabilities facilitate greater insecurity and unauthorized access.

We echo the strong concerns expressed by many delegates here around the proposed Articles 47, 48, 49, and believe that these measures should not be included in the treaty at present.

Thank you Chair.

**Global Partners Digital**
**Oral statement on procedural measures and law enforcement**
**Delivered by Sheetal Kumar**

Thank you Chair, distinguished delegates, for the opportunity to provide our perspectives on the consolidated negotiating document or CND. Global Partners Digital works globally to support a digital environment underpinned by human rights. We have been following this process from its onset, and have provided contributions aimed at ensuring that the convention is aligned with international human rights law and standards.

Alongside our individual input available online, we have contributed to a joint letter and analysis, online as well, signed by 79 civil society organisations from more than 45 countries around the world. This letter is an expression of our joint concern about the risks posed to human rights.

Regarding the chapter on procedural measures and law enforcement, we echo those spoken before be - and - and endorse the statements made by [Red en Defensa de los Derechos Digitales (R3D)/ Derechos Digitales (DD)/ Electronic Frontier Foundation (EFF)/ Access Now/ Eticas Foundation]. We reaffirm that:

- **Under cluster 1**, the scope of procedures under Article 41 should be changed to apply only to core cyber-dependent cybercrimes.
- And that Article 42 should be adapted to integrate particular conditions and human rights safeguards. For example, we recommend:
    - Requiring prior independent, judicial authorization of surveillance measures and ex post independent monitoring.
    - Specifying that requests for authorization be made by an individual of a specified rank within a competent authority.
    - Providing an explicit guarantee of the right to an effective remedy.

    - Including a clear guarantee that investigative powers may not be used in ways that compromise the security of digital communications and services, as well as restricting government hacking of end devices.

- **Under cluster 2**, we support the recommendations of the delegations of Norway, Switzerland and Liechtenstein to strengthen the safeguards and to provide a higher threshold for the investigative powers contained in these articles, such as “just cause for suspicion”.
- We recommend that the language in Article 46(4) relating to the potential for obligations imposed on third parties either be amended to clearly provide protections against interferences with privacy-enhancing technologies, such as encryption or anonymity, or be removed.
- That Article 47 be modified to avoid the risk that it may be interpreted to justify blanket or indiscriminate data retention measures.
- And finally, that the scope of Articles 47 and 48 should be amended to exclude state hacking powers.

We would like to close by welcoming the efforts that have been made to ensure the inclusivity of the negotiations, and to call upon the Secretariat to continue in this vein to the fullest extent possible.

Thank you for your time and consideration.