GPD input to the Ad Hoc Committee on cybercrime

About GPD

Global Partners Digital is a social purpose company dedicated to fostering a digital environment.

INTRODUCTION

Global Partners Digital welcomes the opportunity to provide input to the Ad Hoc Committee's discussions ahead of the first reading of the "Preamble and General Provisions, Criminalisation and Procedural Measures and Law Enforcement" elements of the possible convention. In this response, we focus on recommendations to ensure that the convention respects, protects and promotes human rights.

Preamble and general provisions

The general provisions should set out the purpose, objective and scope of the convention. They should emphasise the protection of human rights as an explicit objective of the convention and provide that, for the avoidance of doubt, nothing in the convention should be understood or interpreted in a manner inconsistent with states' obligations under international human rights law. The general provisions should clearly state that efforts to combat cybercrime should protect and promote human rights and be consistent with states' human rights obligations as set forth in the the International Covenant on Civil and Political Rights (ICCPR) and other international human rights instruments and standards. The general provisions should also provide clear and specific definitions, for example of "ICT" and of cyber-enabled and cyber-dependent crime if they are used, which should be future-proof.

The scope of the convention should focus on efforts to combat cybercrime and exclude (if needs be, explicitly), cybersecurity, internet governance and other related but distinct topics.

Provisions on criminalisation

The scope of criminalisation should be narrowly focused on a small number of core cybercrimes where there is already international agreement, specifically:

- Gaining access to (or hacking) into computer systems without authorisation;
- Intercepting computer data and computer systems without authorisation;
- Interfering with computer data and systems without authorisation;

- Interfering with (or damaging) computer data and computer systems without authorisation; and
- The misuse of items intended to commit one of the other offences.

These criminal offences should be appropriately worded to ensure that they are not used (or misused) in ways which would undermine the exercise and enjoyment of human rights. This means that they should be clearly formulated and use precise definitions (set out in the convention) and avoid the use of vague or overly-broad terminology which may be interpreted in a subjective manner or result in over-criminalisation. Any criminal offences set out in the convention should include a requirement of intention to commit the offence and the availability of defences or discretion not to prosecute where the activity was carried out in the public interest. This will help ensure the protection of legitimate activities undertaken by journalists, academics, and security researchers.

The convention **should not** include further criminal offences. Specifically, the convention should not extend to content-related activity. Nor should the convention include criminal offences simply because they can be committed using ICTs, but focus on cyber-dependent criminal offences where ICTs are both the means and the target of the offence.

Provisions on procedural measures and law enforcement

We support the inclusion of appropriate procedural and investigative tools for the criminal offences provided for in the convention where there is existing international consensus on their utility and necessity, i.e. the expedited preservation of specified stored data; production orders relating to stored data and information; search and seizure of stored data on computers and other devices; real-time collection of traffic data; and the interception of content data. We do not support the inclusion of provisions mandating general data retention or preservation.

All of these procedural and investigative tools should be subject to strong safeguards designed to ensure that they are only used where necessary and proportionate, including that clearly articulated thresholds be satisfied before they can be used, and with appropriate authorisation and oversight by a judicial authority. The thresholds should always include the requirement for any action taken to be necessary and proportionate, and the use of any tools should always be subject to limitations on their scope and duration, and for the rights of individuals and third parties to be taken into account.

The most intrusive measures, such as the collection of traffic data, the interception of content data, and other forms of acquiring the content of communication should be limited to the investigation of the most serious crimes only due to the enhanced

risks they pose to the right to privacy. In terms of types of data, metadata and subscriber data can be as intrusive as content data, when gathered in aggregate. These types of data includes, but is not limited to contacts, "the who, what, when, and where of personal communications", and can include map searches, websites visited, location information, as well as information, including technical identifiers, about every device connected to every network. For this reason, access to these types of data should have the same protections as those that apply to content data: access to this data should be subject to the same conditions and protections as any other personal information, and judicial authorisation for use of such measures by law enforcement or other agencies should also be required.

All procedural and investigative tools should be subject to limitations in their scope and duration when authorised. Any convention should establish strict temporal limits for any access and storing of private communications, including personal data in criminal investigations, and put in place measures to ensure enforcement. Procedural and investigative tools should only be authorised where there is a reasonable suspicion that an individual has committed or is committing a criminal offence and should target only a specific, justified number of persons, such as suspects and third parties relevant to the investigation.

Procedural and investigative tools included in the convention should not directly or indirectly undermine or weaken privacy-enhancing technologies, such as encryption (including end-to-end encryption) or anonymity, as these are considered essential for cybersecurity and the enjoyment of freedom of expression online, particularly for vulnerable and marginalised groups, journalists and human rights defenders.

Mutual legal assistance mechanisms should include relevant safeguards and require approval of competent authorities in both states. A state party and third parties should always be free to refuse any request for mutual assistance where the receiving party considers that the provision of such assistance could pose a risk to an individual's human rights. Procedural tools should not undermine data protection standards in existing instruments that relate to cross-border data sharing, and include adequate safeguards. Public authorities and not industry or private parties should determine what, if any, data should be produced in response to a request for mutual legal assistance. Assessing the legality and validity of requests for data issued by foreign law enforcement authorities should be the task of public authorities. They should also be provided with sufficient capacity to scrutinise mutual legal assistance requests to sufficiently protect human rights in cross-border criminal investigations.