NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Reconvened concluding session

29 July – 9 August 2024

Submission of the Office of the United Nations High Commissioner for Human Rights

22 July 2024

I. Introduction

The Office of the United Nations High Commissioner for Human Rights (OHCHR) welcomes the opportunity to provide comments on the third revised version of a draft cybercrime convention, as published in May 2024[1].

Undeniably, cybercrime endangers the rights of people around the globe. A cybercrime convention under the auspices of the United Nations could reduce impunity by harmonising approaches to criminalisation, provide effective investigatory frameworks, and facilitate cross-border data exchange. For this to materialize it is vital to firmly ground the new treaty in international human rights law, in line with principles such as legality, necessity and proportionality, due process and the rule of law. Failing to do so would undercut efforts to address cybercrime, undermine trust and facilitate human rights violations and abuses. This would contribute to an environment that makes societies less safe, less vibrant and less just and fair.

Since the outset of the negotiations, OHCHR has offered comments and specific textual proposals on the draft Convention from a human rights perspective.[2] Many of these points have also been raised, in various forms, by many Member States, as well as civil society organizations and representatives of the private sector.

---

[1] A/AC.291/22/Rev.3.

[2] See https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/Presentations/Panel_1_OHCHR.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/AHC4_OHCHR_comments_10_January_2023.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/OHCHR_submission_5th_session_Ad_Hoc_Committee_Cybercrime.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/OHCHR1.pdf, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/OHCHR2.pdf.

The revised draft contains some welcome improvements. However, OHCHR remains concerned about significant shortcomings, with many provisions failing to meet international human rights standards. These shortcomings are particularly problematic against the backdrop of an already expansive use of existing cybercrime laws in some jurisdictions to unduly restrict freedom of expression, target dissenting voices and arbitrarily interfere with the privacy and anonymity of communications.

The following comments focus on **main areas** that appear particularly pertinent at the current stage of negotiations. They should not be understood as being exhaustive, given the large number of outstanding issues that need to be urgently addressed before adopting the treaty.

II. Respect for human rights

OHCHR welcomes the inclusion of references to human rights in **articles 6 and 24** underscoring respect for human rights as an overarching obligation and principle in the interpretation and implementation of the Convention. The imposition of criminal liability and the investigation and prosecution of criminal offences fall within a State's exercise of its legal authority vis-à-vis individuals, and is thus subject to the constraints set out under international human rights law. The inclusion of direct references to human rights reflects the Convention's recognition that establishing criminal offences and the investigation and prosecution of crime, including through international cooperation, raises complex issues with far-reaching human rights implications. It provides a basis for avoiding overly broad implementation of criminalization provisions and underscores the need to put in place robust safeguards to prevent arbitrary interference with individual rights, including full respect for due process of law and fair trial protections. This fundamental point could be further strengthened by including within article 6(1) of the current draft an **explicit reference to specific human rights instruments**, in particular the International Covenant on Civil and Political Rights.

OHCHR fully supports the addition of **article 6(2)** to the draft. This article expressly recognizes that the Convention would not permit human rights restrictions beyond those established in international human rights law. It also provides an important additional layer of protection against the worrying trend of using cybercrime laws and procedural measures to unduly restrict human rights.

III. Criminalization

Since the outset of the negotiation process, OHCHR has recommended that the **scope of criminalization under this instrument be narrow**, limited to cyber-dependent criminal offences. These are offences that are inherently linked to computer data and systems, such as crimes against the integrity, confidentiality and availability of data and systems, misuse of devices for the purpose of committing these crimes, and a limited number of specific computer-related offences, such as computer fraud. As previously noted, laws with overly broad definitions of cybercrime are frequently used to impose undue restrictions on the right to freedom of expression, for example by criminalizing conduct, related to online content, that is protected under international human rights law. Expanding beyond a narrow scope, in particular by including ambiguous or vague language and/or broad

formulation of offences, would greatly increase the risk of future human rights violations and abuses.

Against this background, OHCHR has previously raised concerns about proposals to widen the scope of criminalization to include broadly-defined provisions on issues such as hate speech, extremism and terrorism and welcomes that they have not been included in the current draft. However, plans to negotiate an **optional protocol**, focusing on additional crimes, raises concerns as it is likely that such overbroad provisions could be included in a new protocol, contravening international human rights standards of legality, necessity and proportionality.

In this context OHCHR also notes with concern the new **suggested title of the Convention** "United Nations Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System)". This could be interpreted as defining any criminal act done via an ICT system as cybercrime. Such an approach would be particularly problematic against the background of article 1, which defines the purposes of the Convention as combatting and preventing "cybercrime". Read together with the title, this could lead to an expansive interpretation of the purposes that would contradict the attempts at limiting the scope of criminalization under the Convention to clearly and narrowly defined offences.

OHCHR remains concerned about the open-ended nature of **article 4** (formerly article 17). Article 4, now in a very prominent place in the draft Convention, requires States to adopt measures to broaden the Convention's coverage to offences under other international instruments when committed through the use of a computer system. The actual scope of this provision is not clear, due to the lack of an exhaustive list of relevant offences, making it currently impossible to assess its future impacts. It risks expanding problems experienced in the application of other treaties, such as those with overly broad definitions of terrorism. The provision could also lead to establishing disproportionate liability regimes for service providers, which in turn would threaten the right to freedom of expression. Thus, **OHCHR recommends the deletion of article 4 to ensure a narrow scope and clear application of the Convention.**

Criminal offences must be formulated with sufficient precision, as required by the principle of legality, to permit affected individuals reasonably to foresee exposure to liability with respect to certain conduct, ensure consistency in the enforcement of the law and avoid unfettered discretion for authorities enforcing the norm. Criminal law should target only such behaviour that requires criminal sanctions as a response and ensure that other acts are not at risk of being criminalized. In this regard, OHCHR refers to its previously submitted comments to the Ad Hoc Committee.[3]

Regarding **articles 7 through 12**, **OHCHR recommends explicitly including the existence of a qualified form of intent** such as "dishonest" or "criminal intent" as a prerequisite of criminalization of the conduct covered by the instrument. This would prevent the application of the Convention to broader acts of uncertain sweep. The formulation "intentionally" currently used in the Convention remains vague and could permit the criminalization of actions that are not harmful, but in fact beneficial for the

[3] https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multistakeholders/OHCHR1.pdf, particularly pp 3-6.

public interest and society at large. For example, cyber-security experts and researchers, seeking to identify system weaknesses for purposes of strengthening them and/or to prevent cybercrime, could readily be captured by article 7 on "illegal access" to computer systems, which criminalizes the intentional access to the whole or part of a computer system without a right. The article currently sets out a standard of qualified intent only as a discretionary option for States in article 6(2) rather than a default requirement in article 6(1).

If agreeing on changes to the articles themselves proves to be difficult, in particular given difficulties in finding appropriate language to describe the elevated intent required, an interpretative note could be an alternative, albeit less preferable way to provide additional clarity.

OHCHR further notes that the article related to **online child sexual abuse or sexual exploitation material** (article 14) fails to adequately prevent the criminalization of children for self-generated content. **Article 14(4)** of the current draft provides that States "may take steps to exclude the criminalization of children for self-generated material" and of material produced as part of a consensual sexual relationship. The element of 'taking steps' as well as the optional character of the provision weakens this exclusion and does not offer sufficient protection of the rights of the child as required by international law. OHCHR believes that this discretionary commitment does not provide adequate protection for the rights of the child as guaranteed under international law.[4] OHCHR therefore recommends replacing the word "may" with "shall" to explicitly preclude criminalization of self-generated material by children, when it is incompatible with international human rights law.

Article 14 raises further complex questions regarding the type and scope of content considered to be "child sexual abuse or child sexual exploitation material" and the conduct sought to be criminalized. In particular, the criminalization of content that "represents" a child (**article 14(2)**) could encompass, for instance, legitimate expressions of art and literature depicting fictitious individuals, as well as news reporting or historic research about instances of child sexual abuse. Without enhancing the precision of the provision or establishing adequate exceptions, this article risks enabling improper censorship of journalistic, scientific and artistic material.

OHCHR notes that **article 16** (non-consensual sharing of intimate images) applies only to individuals above 18 years of age (article 16(2)). While the reasoning behind this limitation appears to be that children cannot consent to sharing of intimate images, OHCHR is concerned that the current formulation may leave a protection gap for individuals below the age of 18 whose images are shared without consent. By merely making it optional for States to extend article 16 to children under the age of 18 "if they

[4] The Committee on the Rights of the Child in its General Comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25) states, in relation to criminalization of children for self-generated material: "Self-generated sexual material by children that they possess and/or share with their consent and solely for their own private use should not be criminalized. Child-friendly channels should be created to allow children to safely seek advice and assistance where it relates to self-generated sexually explicit content." (para 118); and "Children may be alleged to have, accused of or recognized as having infringed, cybercrime laws. States parties should ensure that policymakers consider the effects of such laws on children, focus on prevention and make every effort to create and use alternatives to a criminal justice response" (para 117).

are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation", children in jurisdictions that make no use of this option would lack protection against non-consensual sharing of intimate images that do not constitute child sexual abuse or exploitation. Replacing the word "may" with the word "shall" would help closing this gap.

OHCHR would like to express concern about the current version of **article 18**. It would require from States Parties to establish liability of legal person "for participation in the offences in accordance with this Convention". Unlike article 19 the wording of article 18 does not require any intentionality whatsoever. This omission risks extending liability to service providers for acts of their users, including for content they upload or share. This would compel service providers to implement stringent measures to avoid liability, including the scanning and filtering of all communications and data on their platforms and services. This approach would lead to undue interferences with the right to privacy on a mass scale and incentivize the removal and blocking of vast arrays of content protected by human rights. **To prevent these significant risks, OHCHR recommends amending article 18(1) to include an explicit intentionally requirement.** Article 18(1) would then read as follows:

> "*Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention,* ***if the legal person had at a minimum actual knowledge of the specific offence committed***."

IV. Procedural measures & conditions and safeguards

Several of the procedural measures relevant to the investigation of cybercrime, such as those relating to surveillance and data collection, are particularly intrusive in nature, interfering with the right to privacy and other rights, and call correspondingly for a robust framework of conditions and safeguards to prevent misuse or abuse. The draft Convention has significant shortcomings in this regard.

The **wide scope of Chapter IV** (Procedural Measures and Law Enforcement), which effectively covers any crime that may leave a digital trail (see article 23(2)(b)(c)) gives reason for concern. OHCHR recommends that the scope of procedural measures be limited to the investigation of the criminal offences established in Chapter II. If it is nevertheless decided that the scope of procedural measures should be broader than the criminal offences established in the Convention, OHCHR recommends limiting the scope of procedural measures to 'serious crimes', defined as a crime carrying a punishment of a maximum deprivation of liberty of at least four years applies in both the requesting and the requested State, and with an additional qualitative element of 'harmfulness' applied to the offence, such as death or bodily harm, clearly defined financial crimes or infliction of coercive acts.

Moreover, **article 23** of the draft Convention provides that all procedural measures, except for interception of content data, could be available to investigate any sort of crime, irrespective of the nature and gravity of the criminal offence in question. For example, provisions of search and seizure of computers and data under the Convention might be activated for 'lèse majesté' crimes or for artistic expressions that might be considered 'propaganda against the State', when they are in fact legitimate expressions under human

rights law. This is difficult to reconcile, in practice, with the obligation to respect human rights and the principles of necessity and proportionality applicable to law enforcement measures generally.

OHCHR is further concerned at the lack of explicit language in **articles 23 and 24** to ensure that procedural measures are applied only when (i) there are reasonable grounds to believe that a criminal offence has been or will be committed; (ii) relevant information concerning the offence will likely be obtained through the measure. This risks enabling rights-restrictive measures without any justification under international human rights law. The phrase "grounds justifying application" might be able to be interpreted in a way to cover these requirements but lacks clarity and specificity.

In general, article 24 **fails to establish a robust binding regime of human rights-based guardrails** by merely listing a range of possible conditions and safeguards but leaving it to the discretion of States Parties when and how to apply those. References to the principles of legality and necessity, prior judicial or other independent authorization of the exercise of those powers, adequate notification and other transparency measures for affected individuals and entities; and respect for the confidentiality of privileged communications, including attorney-client communications[5] are entirely missing.

A provision that would address the concerns raised in the preceding paragraphs, while covering both domestic procedural measures and international cooperation, could read as follows:

> *1. The obligation to establish, implement and apply any of the powers and procedures under this Convention applies only insofar as it is necessary for the investigation of specific criminal offences established by this Convention.*
> *2. States Parties shall ensure that such powers and procedures are carried out only if a factual basis gives reason to believe that a criminal offence established by the Convention has been or will be committed and that relevant information concerning the offence will be obtained through the measure.*
> *3. Those powers and procedures shall be subject to effective conditions and safeguards, in accordance with the State Party's obligations under international human rights law. Such conditions and safeguards shall, inter alia, incorporate the principles of legality, necessity and proportionality, require prior judicial or other independent authorization and review of the exercise of those powers, establish limitations of the scope and the duration of such powers or procedures, provide for adequate notification and other transparency measures for affected individuals and entities, provide for access to effective remedies for any individual suffering damage as a result of the exercise of such powers or procedures, and respect confidentiality of attorney-client and other privileged communications.*
> *4. Confidentiality of powers and procedures under this Convention, including when imposed on service providers, shall be limited to the time period and extent necessary to enable the effective investigation of the specific crime at issue. All persons affected by the powers and measures at issue shall be notified as soon as*

[5] See Basic Principles on the Role of Lawyers, adopted on 7 September by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, principle 22, according to which "Governments shall recognize and respect that all communications and consultations between lawyers and their clients within their professional relationship are confidential.". For further discussion of protection of confidentiality in the attorney-client relationship see the Report of the Special Rapporteur on the independence of judges and lawyers, A/71/348, paras 45-49.

such notification may not interfere with the effective investigation of the specific crime.

With regard to specific measures, OHCHR recommends the **deletion of article 29** (real-time collection of traffic data) and **article 30** (interception of content data). Due to their highly intrusive nature and broad potential scope, such measures would likely be disproportionate to combating most criminal offences. Imposing an obligation under the Convention to conduct such measures for a broad range of criminal offences, even extending to nonserious ones, and without a clear requirement of prior judicial authorization that can assess their lawfulness, necessity and proportionality, would pose major risks of misuse and abuse through arbitrary interference with the right to privacy, including through for massive data collection. This concern is exacerbated by the current realities that many States' domestic legal frameworks and institutional capacities may be unprepared to prevent and mitigate such risks.

OHCHR also recommends the deletion of **article 28 (4)** (search and seizure of stored data), which carries particular risks for the effective protection of human rights. For example, the provision could allow States to compel third parties to disclose vulnerabilities of certain software, in other words assist the State to find ways to enter a computer system. Similarly, it could allow the State to compel decryption, the disclosure of encryption keys or the provision of active assistance in decryption. Orders could not only target the operators of the ICT system at issue, but any person, including the operator's employees, which may not even be located in the same jurisdiction as the operator itself. The measures required could even enable the alteration of the content of communications.

Article 28(4) could thus enable surveillance of various kinds of communications, including in multi-jurisdictional cases, leading to disproportionate interference with the confidentiality and security of communications. Moreover, if authorities were permitted to compel third parties as proposed in article 28(4), such access could be readily applied for a range of broader, unrelated purposes, such as surveillance, without a requirement of judicial authorization. Moreover, identifying software vulnerabilities without closing possible security gaps could compromise existing security standards in communications and may as a result facilitate the commission of cybercrime.

V. International cooperation

The current broad scope of international cooperation also raises a series of human rights concerns. The draft under discussion would facilitate, and perhaps even require, international collaboration on a potential range of acts of exceptional breadth qualified by some States as crimes, even if the criminalization of such acts runs counter to international human rights standards. To avoid such outcomes, OHCHR recommends a **narrow scope** for the purposes of international cooperation: in other words, that the provisions on international cooperation relate only to criminal offences established by the Convention itself.

If it is decided that the scope of international cooperation extends beyond that, OHCHR would recommend that international cooperation is, at a minimum, limited to "**serious criminal offences**", defined with a requirement that the maximum deprivation of liberty of at least four years applies in **both the requesting and the requested State**, and with

an **additional qualitative element of harmfulness** applied to the offence, such as death or bodily harm, clearly defined financial crimes or infliction of coercive acts. Such limitations would ensure a clearer framework for international cooperation, ensuring that States can cooperate meaningfully and without overwhelming the capacities of requested States, while mitigating the risk of potential misuse. In this context, it should also be noted that in article 35(1)(c), the phrase starting with "including serious crimes established" seems superfluous and should be deleted:

> *(c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime~~, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention~~.*

Moreover, it is of paramount importance that the Convention adopts an **adequate range of conditions and safeguards** for cooperation and mutual legal assistance. A lack of clearly defined conditions and safeguards would conflict with States' human rights obligations and would likely lead to protection gaps and facilitate governmental overreach. It is essential that the final Convention provides for conditions and safeguards with respect to international cooperation which are at least at the level provided in the chapter on law enforcement and procedural measures. Against this background, OHCHR welcomes the inclusion of **article 23(4)** that extends the application of article 24 to cooperation scenarios. However, the framework established this way still lack clarity and specificity. OHCHR's proposal for a **general safeguards clause**, as provided above in the section on Chapter IV would ensure a stronger human rights protection framework.

To ensure that the treaty will be an effective basis for cooperation in combatting crime and not facilitate human rights-violating overreach by States, in particular for political purposes, it is vital that it provides for **strong mandatory grounds for refusal** of cooperation. The Convention should include Convention should include at least the following three bases to refuse international cooperation and mutual legal assistance:

- Where there is an absence of dual criminality – in other words, where not all cooperating states have criminalized the act subject to international cooperation and mutual legal assistance
- Where the request for international cooperation and legal assistance relates to political offences
- Where there is a reasonable belief that assistance could contribute to violations and abuses of human rights, including but not limited to discrimination prohibited under international human rights law.

Against this background, OHCHR welcomes the inclusion of **article 40(22)**, which would cover prosecutions and punishments on the basis of prohibited grounds for discrimination. The ground for refusal should be expanded to cover human rights violations more broadly and be made mandatory as an expression of the duties to respect and to protect under international human rights law. To this end, OHCHR proposes the following language, introducing a **new paragraph 21bis and amending paragraph 22**:

> *21bis. Mutual legal assistance shall be refused (a) if there are reasonable grounds to believe that the criminal offence will be treated as a political offence by the requesting State; (b) if there are reasonable grounds to believe that the*

cooperation or assistance will result in a violation of human rights; (c) if the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or other proceedings under their own jurisdiction.

22. ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ Mutual legal assistance shall be refused if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.

VI. Conclusion

The concluding session is a pivotal moment for human rights in the digital age. Tackling cybercrime and enabling international cooperation in criminal investigations must go hand in hand with upholding and advancing human rights. OHCHR urges all negotiating parties to make all efforts to ensure that the new treaty comprehensively integrates human rights throughout the entire text, strictly adhering to international law, standards and principles. Failure to achieve such integration could jeopardize the protection of human rights of people world-wide, undermine the functionality of the internet infrastructure, create new security risks and undercut business opportunities and economic well-being.

OHCHR takes this opportunity to reaffirm its commitment to supporting Member States, and in particular delegations participating in the Ad Hoc Committee's session, in the drafting and—if adopted—implementation of a new Cybercrime Convention that can deliver comprehensively on its promise to address cybercrime in line with international human rights standards.

Summary of textual proposals

Title

United Nation Convention against Cybercrime ~~(Crimes Committed through the Use of an Information and Communications Technology System)~~

Article 2

"Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty ***in both the requesting and requested State and involving death or bodily harm, financial crimes or coercive acts****;*

Article 4

Deletion of the article.

General provision on conditions and safeguards

1. The obligation to establish, implement and apply any of the powers and procedures under this Convention applies only insofar as it is necessary for the investigation of specific criminal offences established by this Convention.
2. States Parties shall ensure that such powers and procedures are carried out only if a factual basis gives reason to believe that a criminal offence established by the Convention has been or will be committed and that relevant information concerning the offence will be obtained through the measure.
3. Those powers and procedures shall be subject to effective conditions and safeguards, in accordance with the State Party's obligations under international human rights law. Such conditions and safeguards shall, inter alia, incorporate the principles of legality, necessity and proportionality, require prior judicial or other independent authorization and review of the exercise of those powers, establish limitations of the scope and the duration of such powers or procedures, provide for adequate notification and other transparency measures for affected individuals and entities, provide for access to effective remedies for any individual suffering damage as a result of the exercise of such powers or procedures, and respect confidentiality of attorney-client and other privileged communications.
4. Confidentiality of powers and procedures under this Convention, including when imposed on service providers, shall be limited to the time period and extent necessary to enable the effective investigation of the specific crime at issue. All persons affected by the powers and measures at issue shall be notified as soon as such notification may not interfere with the effective investigation of the specific crime.

Articles 7

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed ~~intentionally~~ ***with dishonest or criminal intent****, the access to the whole or any part of an information and communications technology system without right.*

2. A State Party may require that the offence be committed by infringing security measures, ~~with the intent of obtaining electronic data or other dishonest or criminal intent~~ or in relation to an information and communications technology system that is connected to another information and communications technology system.

Similar changes should be made to articles 8-10 and 12.

New paragraph following article 14(2)

Material of manifestly artistic, educational, or scientific character and without the involvement of persons under the age of 18 years shall be exempted from art 13(1).

Article 14(4)

*4. States Parties ~~may take steps to~~ **shall** exclude the criminalization of States Parties shall exclude the criminalization of:*

(a) Conduct by children for self-generated material depicting them as described in paragraph 2 of this article; or

(b) Conduct set forth in paragraph 1 of this article, relating to material described in paragraph 2 (a) to (c) of this article, where such material is produced as part of a consensual sexual relationship, as determined by domestic law and consistent with applicable international obligations, and is maintained exclusively for the private and consensual use of the persons involved.

Article 16(3)

*3. A State Party ~~may~~ **shall** extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.*

Article 18(1)

*Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention, **if the legal person had at a minimum actual knowledge of the specific offence committed**.*

Article 23(2)

2. Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to.

(a) The criminal offences established in accordance with this Convention;

*(b) Other criminal offences **considered serious criminal offences** committed by means of an information and communications technology system; and,*

*(c) The collection of evidence in electronic form of any ~~criminal~~ offence **established in accordance with this Convention or of serious criminal offences**.*

Article 28(4)

Deletion of the paragraph.

Articles 29 and 30

Deletion of both articles.

Article 35(1)(c)

(c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime~~, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention~~.

Article 40(21bis) & 22

21bis. Mutual legal assistance shall be refused (a) if there are reasonable grounds to believe that the criminal offence will be treated as a political offence by the requesting State; (b) if there are reasonable grounds to believe that the cooperation or assistance will result in a violation of human rights; (c) if the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or other proceedings under their own jurisdiction.

*22. ~~Nothing in this Convention shall be interpreted as imposing an obligation to afford~~ Mutual legal assistance **shall be refused** if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.*