Misión Permanente de Costa Rica ante las Naciones Unidas
211 E. 43rd Street, Room 1002, New York, NY 10017. Tel: (212) 986-6373

Insumos para el tercer período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos.

Coordinación Comisión Ciberseguridad y Ciberdelincuencia Poder Judicial

Courtesy Non-Official English version available in the final part of the document

Nueva York, Julio 5 2022

Preámbulo

Consciente del rol y del profundo impacto que las tecnologías de la información y las comunicaciones ejercen en la convivencia de las sociedades actuales, el Estado costarricense se congratula y califica como valioso, pertinente e ineludible, el esfuerzo conducido por la comunidad internacional y que tiene como objetivo final la aprobación de una *Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos* (en adelante, la Convención).

Costa Rica cree firmemente que el Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) constituyó una paso decisivo y de trascendental importancia en esta materia. De tal suerte, su estructura y contenido deberán erigirse en un marco de referencia para la nueva regulación. Puesto en otros términos, los esfuerzos de los Estados miembros, bajo la honorable coordinación del Comité, deberán situar siempre su mirada en las estipulaciones allí estatuidas.

Es imperativo tomar en consideración que el Convenio de Budapest data del año 2001 y, naturalmente, las discusiones que condujeron a su aprobación final son aún más antiguas. Consecuentemente, han sido muchas y profundas las

modificaciones operadas desde entonces en el campo de la informática y las tecnologías de la información.

Son múltiples y variadas las nuevas hipótesis delictivas que inciden -muchas veces con total impunidad- en la esfera de los derechos humanos de las personas. Piénsese (sin ser exhaustivos en esta enunciación) en los retos que supone la inteligencia artificial en relación con la intimidad, el derecho a la imagen o la autodeterminación informativa. Lo mismo se puede predicar de la capacidad de programar armas letales autónomas. Igualmente alarmante es la capacidad de las nuevas tecnologías (así, por ejemplo, los cripto activos) para burlar las regulaciones de los organismos financieros locales e internacionales y, por esa vía, facilitar la legitimación de capitales, o bien, la comisión de otros delitos comunes de enorme gravedad. Es también contundente el efecto que las redes sociales ostentan en las relaciones interpersonales de nuestras sociedades. Colateralmente, todo un abanico de situaciones ignominiosas se ha presentado: difusión masiva de discursos del odio, manipulación del electorado en los procesos democráticos de elección popular, entre otros.

Así las cosas, y sin perder de vista la ruta iniciada por Budapest, corresponde en esta ocasión sintonizar un derecho convencional que responda a las nuevas realidades delictivas. Se entiende que esa sintonía nunca podrá ser absoluta e incluso se reconoce que padece una antinomia o contradicción fundacional, toda vez que está condenada a nacer con algún grado de desface. La realidad de nuestras sociedades digitales y de la información caminará a un paso siempre más veloz que el Derecho. Sin embargo, lejos de desmotivar, aquella aserción debe impulsar a trazar una Convención ágil y que permita a los Estados miembros ejercer un poder de modulación o -puesto en los términos del Tribunal Europeo de Derechos Humanos- un margen de apreciación a partir del cual exista una adecuación a los ordenamientos internos.

Indudablemente, y dado el carácter trasfronterizo de la criminalidad ligada a las nuevas tecnologías, la cooperación y asistencia entre Estados debe ser piedra angular de los esfuerzos desplegados por los Estados bajo la dirección del Comité.

En segundo término, crear un elenco de categorías delictivas ajustado a los tiempos actuales y a partir del cual los Estados desarrollen una ulterior codificación, es igualmente ineludible. También las medidas procesales y preventivas deberán tener asegurado su espacio. Finalmente, y dada la especialidad de la materia, un apartado inicial con un glosario o listado de definiciones será necesario.

A continuación se presente al honorable Comité un sucinto listado de los temas cuyo tratamiento es ineluctable en la Convención.

I. Cooperación internacional

La cooperación y la asistencia internacional deben ser piedras angulares de la Convención. Los siguientes son algunos de los puntos que deberían resultar abarcados.

Aspectos Generales

El deber de las partes de cooperar entre sí, para los fines de las investigaciones o los procedimientos propuestos en la Convención ha de erigirse en un principio general de acatamiento obligatorio. Indudablemente, las reglas de los ordenamientos internos deben ser observadas, pero la consagración convencional de un derecho de cooperación -con las consiguientes obligaciones internacionales que ello supone- es más que necesario si se pretende contar con un tratado dotado de fuerza normativa.

En materia de extradición

- Se debe autorizar la extradición de personas por los delitos establecidos en la Convención, siempre y cuando se respete el principio de doble incriminación.

- Debe incluirse el compromiso de las partes a autorizar la extradición por los delitos que se establezcan en la Convención. Del mismo modo, deben incluirse dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que celebren entre sí.

• En los supuestos de que una parte reciba una solicitud de extradición de otra parte con la cual no haya celebrado ningún tratado de extradición, la Convención deberá servir como fundamento jurídico de la extradición en relación con los delitos ahí contenidos.

• La extradición estará sujeta a las condiciones establecidas en el derecho interno de la parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los cuales se puede denegarse el requerimiento.

• La Convención deberá consagrar el principio "*aut dedere aut judicare*" de forma que, si una parte deniega la extradición de un sujeto requerido como sospechoso de haber perpetrado uno de los delitos convencionalmente definidos, debe entonces proceder a activar su propia jurisdicción con el fin de conducir la persecución y el juzgamiento.

Asistencia mutua

• El compromiso de cada parte de brindar asistencia mutua para la investigación, obtención de prueba y el juzgamiento de los delitos relacionados con la ciberdelincuencia es indispensable. En el mismo sentido, también es plausible introducir previsiones que permitan regular la asistencia interestatal en casos de ciber ataques que se estén desarrollando *in situ*.

• En caso de emergencia, cada parte debe estar en capacidad de transmitir solicitudes de asistencia o comunicación en condiciones de seguridad y autenticación. La parte requerida debe aceptar la solicitud y dar respuesta en forma expedita por cualquiera de los medios a su alcance.

• Deben existir las condiciones para que la partes puedan compartir los datos relativos a antecedentes penales. No obstante, es importante que se trate de registros oficiales y que se respeten los plazos de caducidad de tales inscripciones (ello en resguardo del derecho al olvido).

• Se contemple en el Convenio la facultad de la parte requerida de fijar condiciones en su derecho interno para la tramitación de las solicitudes de asistencia mutua, incluidos los motivos por los que puede denegar la cooperación.

- Las partes deberán estar facultadas para que, dentro de los límites de su derecho interno, y sin petición previa, puedan comunicar a otra parte información obtenida en el marco de sus propias investigaciones, cuando consideren que la revelación de dicha información podrá ayudar a la parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en la Convención, o bien, cuando se estime que existe mérito para formular una petición de cooperación.

- Es fundamental regular el deber de la parte requerida de informar sin demora del resultado de la ejecución de una solicitud de asistencia, con el consiguiente deber de motivar cualquier denegación o aplazamiento de la asistencia solicitada, o bien, informar de cualquier causa o circunstancia que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

- Debido a la información sensible que usualmente media en esta materia, debe establecerse la posibilidad de que la parte requirente solicite a la parte requerida que preserve la confidencialidad de la solicitud. En caso de que la parte requerida no pueda cumplir esta petición de confidencialidad, lo deberá comunicar inmediatamente a la parte requirente, para que esta determine entonces si pese a ello desea ejecutar la solicitud.

II. Medidas preventivas

El Estado costarricense estima oportuna la inclusión dentro del Convenio de medidas preventivas tendientes a desarrollar y promover prácticas y políticas a lo interno de los Estados parte para prevenir este tipo de delincuencia, medidas que incluyan la cooperación internacional y asistencia mutua para reforzar los mecanismos de defensa frente a posibles ciberataques. Asimismo, se estima valiosa y deseable la capacitación y asesoría para la elaboración de protocolos y procedimientos para salvaguardar la integridad informática de las instituciones públicas y privadas frente a la ciberdelincuencia, así como fortalecer aquellas entidades cuyo mandato apunta a la vigilancia y supervisión para hacer frente a

posibles intromisiones por parte de la ciberdelincuencia en los sistemas gubernamentales y privados.

Es esencial que se incorpore en la Convención como parte de esas medidas preventivas la necesidad de que cada Estado parte adopte mecanismos de evaluación y actualización periódica de las prácticas y procedimientos para adaptarse al vertiginoso fenómeno de la ciberdelincuencia.

De la misma manera, resulta necesario incorporar medidas tendientes a que los Estados parte adopten acciones para informar y sensibilizar a la población acerca de los peligros asociados al fenómeno de la ciberdelincuencia. En línea con lo anterior, se sugiere desarrollar campañas de información a través de los medios de comunicación colectiva, así como propiciar la participación ciudadana a fin de construir instrumentos para prevenir y combatir este tipo de delincuencia.

Se estima pertinente la inclusión del deber de colaboración entre los Estados parte a fin de promover las medidas preventivas e impulsar la participación en proyectos internacionales para la prevención de la ciberdelincuencia.

III. Mecanismos de implementación

Al igual que se establece en otros instrumentos internacionales de similar naturaleza (como lo es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio de Budapest), es importante que se estipule que cada Estado parte al suscribir la Convención deberá adoptar las medidas legislativas y administrativas que estime oportunas para su implementación, así como incluir dentro de su ordenamiento jurídico interno aquellos delitos tipificados en el mismo, pudiendo adoptar medidas más severas o estrictas que las estipuladas en la Convención para combatir el fenómeno de la ciberdelincuencia de acuerdo al contexto normativo y constitucional de cada Estado miembro.

IV. Disposiciones finales

En cuanto a la firma, se considera importante que la Convención quede abierto a la firma de los Estados que hubiesen participado en el proceso de negociación que condujo a la preparación del texto final. Al margen de lo anterior, y siendo el tema de relevancia mundial, el instrumento deberá quedar abierto para su adopción también por todos aquellos Estados u organizaciones internacionales o regionales que desarrollen políticas de seguridad informática y que hubiesen estado ausentes en el proceso de creación normativa precedente. Bajo los mismos términos deberá estipularse la posible adhesión futura de más suscriptores.

Previa consulta a los Estados Parte, se considera adecuado que se contemple que se podrá hacer invitación a otros Estados que no sean parte ni hayan intervenido en la elaboración, para adherirse a la Convención, sobre todo atendiendo a la necesidad de abordar el fenómeno de la ciberdelincuencia mediante una efectiva y eficiente cooperación y asistencia internacional que se haga extensiva a otros Estados pese a no haber suscrito inicialmente la Convención.

Además, se considera oportuno que disponga que la Convención que se adopte requerirá la ratificación o aprobación respectiva, según lo disponga la normativa interna de cada Estado parte.

En cuanto a la solución de posibles controversias entre los Estados parte en la interpretación del Convenio, tal y como se estila en otros instrumentos internacionales de naturaleza similar, resulta conveniente que se resuelvan mediante la negociación, o bien, que se sometan a un procedimiento de arbitraje una vez que se hayan agotado los mecanismos de negociación entre los Estados.

En lo concerniente a las reservas, se estima necesario delimitar expresamente en la Convención las normas que podrán ser objeto de reserva. No obstante, debe tenerse especial consideración a fin de que las mismas no sean incompatibles con los objetivos y fines que persigue la Convención, particularmente, en lo atinente a la persecución penal de determinadas figuras delictivas,

instrumentos de investigación, así como mecanismos y procedimientos de cooperación y asistencia internacional, que son los ejes sobre los cuales se asienta este instrumento para combatir la ciberdelincuencia.

En materia de enmiendas, al igual que se estila en distintos instrumentos internacionales vigentes, debe contemplarse la posibilidad de que los Estados parte las propongan. La materia objeto de estudio es esencialmente dinámica y la capacidad de la Convención para adaptarse frente a los nuevos fenómenos y modalidades delictivas, es vital.

Finalmente, se estima oportuno contemplar la posibilidad de complementar el contenido del Convenio mediante la implementación de protocolos específicos, los cuales serán interpretados a la luz de las disposiciones convencionales originales, pero servirán para regular algunos procedimientos específicos.

Courtesy Non Official Translation

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

Coordination Commission Cybersecurity and Cybercrime Judiciary

Preamble

Aware of the role and profound impact that information and communication technologies have on the coexistence of today's societies, the Costa Rican State welcomes and finds valuable, pertinent and unavoidable, the effort led by the international community that has, as its final objective, the adoption of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (hereinafter, the Convention).

We firmly believe that the European Convention on Cybercrime (Budapest, 2001) constituted a decisive step of transcendental importance in this matter. In this way, its structure and content should become a reference framework for the new regulation. Put in other terms, the efforts of the member states, under the honorable coordination of the Committee, should always focus their attention on the stipulations established therein.

Apart from the above, it is imperative to take into consideration that the Budapest Convention dates back to 2001 and, naturally, the discussions that led to its final approval are even older. Consequently, there have been many and profound changes since then in the field of computing and information technology.

Entering the third decade of the 21st century, there are multiple and varied new criminal hypotheses that affect -often with total impunity- in the sphere of people's human rights. Think (without being exhaustive in this statement) of the challenges posed by artificial intelligence in relation to privacy, the right to image or informational self-determination. The same can be said of the ability to program lethal autonomous weapons. Equally alarming is the ability of new technologies (such as, for example, crypto assets) to circumvent the regulations of local and international financial organizations and, in this way, facilitate money laundering, or the commission of other extremely serious common crimes. The effect that social networks have on interpersonal relationships in our societies is also overwhelming. Collaterally, a whole range of ignominious situations has arisen: massive dissemination of hate speech, manipulation of the electorate in democratic processes of popular election, among others.

This being the case, and without losing sight of the route initiated by Budapest, it is appropriate on this occasion to tune in to conventional law that responds to the new criminal realities. We understand that this harmony can never be absolute and we even recognize that it suffers from a foundational antinomy or contradiction, since it is condemned to be born with some degree of discrepancy. The reality of our digital and information societies will always move faster than the law. However, far from discouraging us, that assertion should encourage us to draw up an agile convention that allows the Member States to exercise a power of modulation or - put in the terms of the European Court of Human Rights - a margin of appreciation based on which there exists an adaptation to internal regulations.

Undoubtedly, and given the cross-border nature of crime linked to new technologies, cooperation and assistance between States must be the cornerstone of the efforts deployed by the States under the direction of the Committee. Secondly, creating a list of criminal categories adjusted to current times and from which the States develop a subsequent codification, is equally inescapable. Procedural and preventive measures must also ensure their space. Finally, and given the specialty of the subject, an initial section with a glossary or list of definitions will be necessary.

Below we present to the honorable Committee a brief list of the issues whose treatment is unavoidable in the Convention.

I. International cooperation

As was mentioned earlier, international cooperation and assistance must be the cornerstones of the Convention. The following are some of the points that should be covered.

<u>General features</u>

The duty of the parties to cooperate with each other, for the purposes of the investigations or procedures proposed in the Convention, must become a general principle of mandatory compliance. Undoubtedly, the rules of internal legal systems must be observed, but the conventional consecration of a right of cooperation -with the consequent international obligations that this entails- is more than necessary if the aim is to have a treaty endowed with normative force.

Regarding extradition

• The extradition of persons for the crimes established in the Convention must be authorized, as long as the principle of double criminality is respected.

• The commitment of the parties to authorize extradition for the crimes established in the Convention must be included. In the same way, said crimes must be included among those that may give rise to extradition in any extradition treaty that they conclude with each other.

• In the event that a State receives an extradition request from another State with which it has not concluded an extradition treaty, the Convention must serve as the legal basis for extradition in relation to the crimes contained therein.

• Extradition will be subject to the conditions established in the domestic law of the requested State or in the applicable extradition treaties, including the reasons on which the request may be denied.

• The Convention must enshrine the principle "aut dedere aut judicare" so that, if a State denies the extradition of a subject required as suspected of having perpetrated one of the conventionally defined crimes, it must then proceed to activate its own jurisdiction in order to conduct the prosecution and trial.

Mutual Assistance:

• The commitment of each State to provide mutual assistance for the investigation, collection of evidence and prosecution of crimes related to cybercrime is essential. In the same sense, it is also plausible to introduce provisions that allow interstate assistance to be regulated in cases of cyber attacks that are taking place in situ.

• In the event of an emergency, each State must be able to transmit requests for assistance or communication under conditions of security and authentication. The requested State must accept the request and respond promptly by any of the means at its disposal.

• The conditions must exist so that the State can share data related to criminal records. However, it is important that they are official records and that the expiration dates of such registrations are respected (this in order to protect the right to be forgotten).

• The Convention contemplates the power of the requested State to set conditions in its domestic law for the processing of mutual assistance requests, including the reasons for denying cooperation.

- The States must be empowered so that, within the limits of their internal law, and without prior request, they may communicate to another State information obtained in the framework of their

own investigations, when they consider that the disclosure of said information may help the State recipient to initiate or carry out investigations or procedures in relation to crimes provided for in the Convention, or when it is considered that there is merit to formulate a request for cooperation.

• It is essential to regulate the duty of the requested State to inform without delay of the result of the execution of a request for assistance, with the consequent duty to justify any denial or postponement of the requested assistance, or report any cause or circumstance that make the execution of the request impossible or that may significantly delay it.

• Due to the sensitive information that usually mediates in this matter, the possibility for the requesting State to request the requested State to preserve the confidentiality of the request must be established. In the event that the requested State cannot comply with this confidentiality request, it must immediately notify the requesting State, so that the requesting State can then determine whether, despite this, it wishes to execute the request.

II. Preventive measures

The Costa Rican State deems important the inclusion within the Convention of preventive measures tending to develop and promote practices and policies within the State parties to prevent this type of crime, measures that include international cooperation and mutual assistance to strengthen defense mechanisms against possible cyber attacks. Likewise, training and advice for the development of protocols and procedures to safeguard the computer integrity of public and private institutions against cybercrime is considered valuable and desirable, as well as strengthening those entities whose mandate demands to surveillance and supervision to deal with a possible interference by cybercrime in government and private systems.

It is essential that the Convention incorporates as part of these preventive measures the need for each State State to adopt mechanisms for evaluating and regularly updating practices and procedures to adapt to the dizzying phenomenon of cybercrime.

In the same way, it is necessary to incorporate measures so that the States Parties adopt actions to inform and sensitize the population about the dangers associated with the phenomenon of cybercrime. In line with the above, it is suggested to develop information campaigns through mass media, as well as promote citizen participation in order to build instruments to prevent and combat this type of crime.

The inclusion of the duty of collaboration between the States Parties in order to promote preventive measures and encourage participation in international projects for the prevention of cybercrime is deemed pertinent.

III. Implementation Mechanisms

As established in other international instruments of a similar nature (such as the United Nations Convention against Transnational Organized Crime and the Budapest Convention), it is important to stipulate that each State Party, when signing the Convention, must adopt the legislative and administrative measures that it deems appropriate for its implementation, as well as including within its internal legal system those crimes typified in it, being able to adopt more severe or strict

measures than those stipulated in the Convention to combat the phenomenon of cybercrime according to the legal and constitutional context of each Member State.

IV. Final provisions

Regarding signature, it is considered important that the Convention be open for signature by the States that participated in the negotiation process that led to the preparation of the final text. Apart from the foregoing, and being the topic of global relevance, the instrument should also be open for adoption by all those States or international or regional organizations that develop computer security policies and that had been absent in the process of creating preceding regulations. Under the same terms, the possible future adhesion of more subscribers must be stipulated.

After consulting the States parties, it is considered appropriate to contemplate the possibility of inviting other States that are not parties and have not participated in the preparation, to adhere to the Convention, especially in view of the need to address the phenomenon of cybercrime. through effective and efficient international cooperation and assistance that is extended to other States despite not having initially signed the Convention.

In addition, it is considered opportune to provide that the Convention that is adopted will require the respective ratification or approval, as provided by the internal regulations of each State Party.

Regarding the solution of possible controversies between the States parties in the interpretation of the Convention, as is the case in other international instruments of a similar nature, it is convenient that they be resolved through negotiation, or that they be submitted to a procedure of arbitration once the negotiation mechanisms between the States have been exhausted.

With regard to reservations, it is considered necessary to expressly define in the Convention the rules that may be subject to reservation. However, special consideration must be taken so that they are not incompatible with the objectives and purposes pursued by the Convention, particularly with regard to the criminal prosecution of certain criminal figures, investigation instruments, as well as mechanisms and procedures of international cooperation and assistance, which are the axes on which this instrument is based to combat cybercrime.

In terms of amendments, as is customary in various international instruments in force, the possibility that the States Parties propose them should be considered. The subject matter of study is essentially dynamic and the ability of the Convention to adapt to new phenomena and criminal modalities is vital.

Finally, it is considered important to contemplate the possibility of complementing the content of the Convention through the implementation of specific protocols, which will be interpreted in light of the original conventional provisions, but will serve to regulate some specific procedures.