



III Reunión de Consultas por el Convenio de Budapest sobre Ciberdelincuencia y la eventual adhesión del Uruguay (Montevideo, 11 agosto 2022)

# Uruguay y el Convenio de Budapest sobre la Ciberdelincuencia

Cristina Schulman  
Presidente  
Comité de la Convención sobre la Ciberdelincuencia, Consejo de Europa

Alexander Seger  
Secretario Ejecutivo  
Comité de la Convención sobre la Ciberdelincuencia, Consejo de Europa



[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

1



## El problema del cibercrimen ...

**Cybercrime To Cost The World \$10.5 Trillion Annually By 2025**  
Every U.S. business is under cyberattack

**Online child abuse racket: CBI raids 77 spots,**  
40% Increase in Ransomware Attacks in Q3 2020

**40% increase in Ransomware Attacks in Q3 2020**

**Artificial intelligence could be used to hack connected cars, drones warn security experts**  
Cyberattacks on vulnerabilities in connected vehicles could have very real physical consequences if security isn't managed properly.

**Warning: Domestic cyber terrorism on the rise in 2021**

**Child protection**  
**DNA Exclusive: Women soft target of cyberbullying online violence on social media**  
In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of cyber violence. The DNA analysis will look into the different aspects of cyber violence against women relate to nearly 400 million women around the world.

**Fifteen times more child sexual abuse material found online than 10 years ago**  
Experts from Internet Watch Foundation demand UK uses online safety bill to protect children

**Covid-19 lockdowns drive spike in online child abuse**  
Post Covid, corporates see huge increase in cyber crimes

**Sarah Marsh**  
Sat 13 Nov 2021 07:00 GMT

2

# ... y las pruebas electrónicas en relación con CUALQUIER delito

**Pruebas en un sistema informático**

- Delitos relacionados con COVID-19
- Crimen de guerra
- Violencia sexual en línea contra los niños
- Violencia contra las mujeres
- Injerencia electoral
- Terrorismo
- Blanqueo de capitales
- Tráfico de drogas
- Corrupción
- Fraude
- Homicidio
- Secuestro
- Delitos de odio
- Delitos médicos
- CUALQUIER DELITO

3

# Ciberdelitos y pruebas electrónicas: el problema de la territorialidad y la jurisdicción

¿Dónde está el crimen?  
 ¿Dónde están los datos, dónde están las pruebas?  
 ¿Quién tiene las pruebas?  
 ¿Dónde está el límite de los poderes de las agencias de aplicación de la ley?

- ▶ Carácter transnacional del ciberdelito y las pruebas electrónicas
- ▶ Delito y jurisdicción en el ciberespacio
- ▶ Necesidad de cooperación público/privada e internacional

4

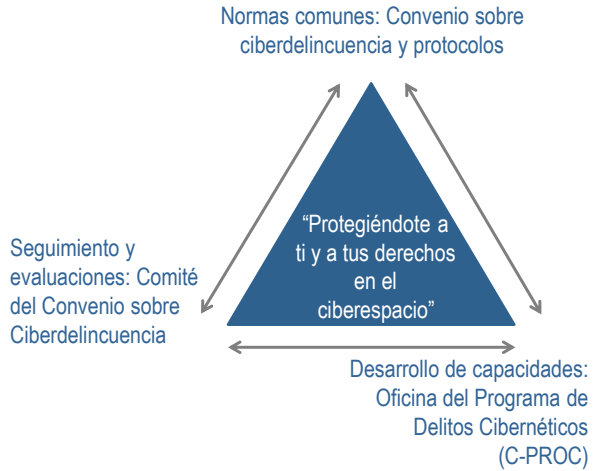


## Convenio sobre la Ciberdelincuencia

Las Partes del Convenio (2001), en su legislación penal, deben adoptar:

- Delitos específicos contra y por medio de sistemas informáticos
  - Poderes procesales con salvaguardias para investigar la ciberdelincuencia y obtener pruebas electrónicas en relación con cualquier delito
  - Cooperación internacional en materia de ciberdelincuencia y pruebas electrónicas
1. Protocolo adicional sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (2003)
  2. Protocolo relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas (2022)

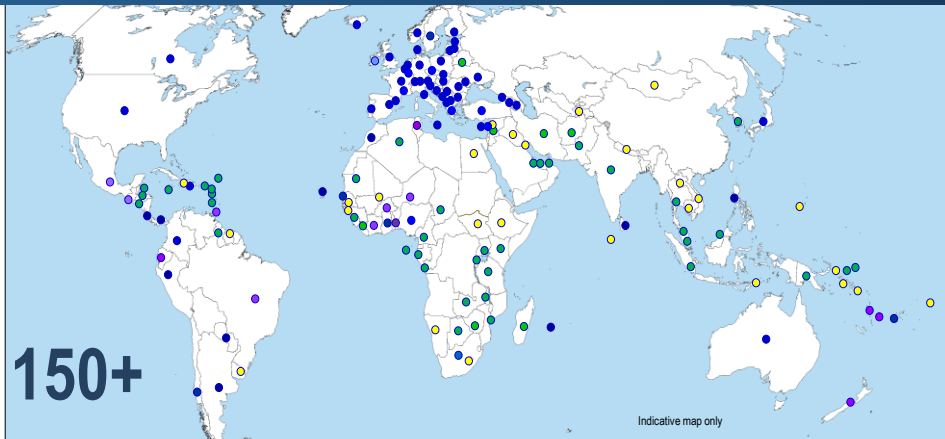
### El mecanismo del Convenio



5




## Alcance de la Convención sobre ciberdelincuencia



Parties:	67		
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	45+
Invited to accede:	13	Further States drawing on Budapest Convention for legislation:	30+
	= 82		= 75+

6



## Adhesión al Convenio

### Artículo 37 – Adhesión al Convenio

[e] Consejo de Europa ... podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración.

#### Fase 1:

- Un país con legislación en vigor o en etapa avanzada
- Carta del Gobierno al Consejo de Europa expresando su interés en la adhesión
- Consultas (CdE/Partes) sobre la decisión de invitar
- Invitación a adherir (válida por 5 años)

#### Fase 2:

- Procedimiento nacional (por ejemplo, decisión del parlamento nacional, promulgación de legislación interna)
- Depósito del instrumento de adhesión

7



## Beneficios del Convenio



### Beneficios

- ✓ Legislación más fuerte y consistente
- ✓ Cooperación internacional más eficiente entre las Partes
- ✓ Más investigación, enjuiciamiento, adjudicación de casos de delitos cibernéticos y pruebas electrónicas
- ✓ Asociaciones de confianza y cooperación público/privada Catalizador para el desarrollo de capacidades
- ✓ Mejor desempeño en ciberseguridad
- ✓ Participación en el Comité de Convención de Cibercrimen (T-CY)
- ✓ Participación en el establecimiento de normas futuras (Notas de orientación, Protocolos y otras adiciones al Convenio de Budapest)
- ✓ Contribución a los derechos humanos/estado de derecho en el ciberespacio

**“Costo”:** Compromiso de cooperar

**¿Desventajas?**

8



## Las disposiciones del Convenio sobre Ciberdelincuencia

1. Derecho penal sustantivo
2. Derecho procesal
3. Cooperación internacional

9



## Las disposiciones del Convenio / Derecho penal sustantivo

Art. 1	Definiciones
Art. 2	Acceso ilícito
Art. 3	Interceptación ilícita
Art. 4	Ataques a la integridad de los datos
Art. 5	Ataques a la integridad del sistema
Art. 6	Abuso de los dispositivos
Art. 7	Falsificación informática
Art. 8	Fraude informático
Art. 9	Delitos relacionados con la pornografía infantil
Art. 10	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
Art. 11	Tentativa y complicidad
Art. 12	Responsabilidad de las personas jurídicas
Art. 13	Sanciones y medidas

10



## Las disposiciones del Convenio / Derecho procesal

- Art. 14      Ámbito de aplicación de las disposiciones de procedimiento
- Art. 15      Condiciones y salvaguardias
- Art. 16      Conservación rápida de datos informáticos almacenados
- Art. 17      Conservación y revelación parcial rápidas de los datos sobre el tráfico
- Art. 18      Orden de presentación
- Art. 19      Registro y confiscación de datos informáticos almacenados
- Art. 20      Obtención en tiempo real de datos sobre el tráfico
- Art. 21      Interceptación de datos sobre el contenido
- Art. 22      Jurisdicción

11



## Las disposiciones del Convenio / Cooperación internacional

- Art. 23      Principios generales relativos a la cooperación internacional
- Art. 24      Extradición
- Art. 25      Principios generales relativos a la asistencia mutua
- Art. 26      Información espontánea
- Art. 27      Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables
- Art. 28      Confidencialidad y restricción de la utilización
- Art. 29      Conservación rápida de datos informáticos almacenados
- Art. 30      Revelación rápida de datos conservados sobre el tráfico
- Art. 31      Asistencia mutua en relación con el acceso a datos informáticos almacenados
- Art. 32      Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público
- Art. 33      Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico
- Art. 34      Asistencia mutua relativa a la interceptación de datos sobre el contenido
- Art. 35      Red 24/7

12

## Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba

### First Protocol:

Opened for signature  
2003

By August 2022:

- 33 Parties
- 12 Signatories

Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (ETS 189)

- Artículo 1 – Finalidad
- Artículo 2 – Definición “*material racista y xenófobo*”
- Artículo 3 – Difusión de material racista y xenófobo mediante sistemas informáticos
- Artículo 4 – Amenazas con motivación racista y xenófoba
- Artículo 5 – Insultos con motivación racista y xenófoba
- Artículo 6 – Negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad
- Artículo 7 – Cooperación y complicidad

13

## 2º Protocolo Adicional relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas (12 Mayo 2022)

La ciberdelincuencia: una amenaza para

- ▶ Los derechos humanos
- ▶ La democracia
- ▶ El Estado de Derecho

Obligaciones positivas:

- ▶ Asegurar los medios para proteger los derechos de las personas, incluso contra la delincuencia

Problema:

- Proliferación de la ciberdelincuencia
- Hoy en día, todos los delitos implican pruebas electrónicas
- Las pruebas están en algún lugar en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas
- No se dispone de medios eficaces para obtener la divulgación de pruebas electrónicas
- Menos del 0,1% de los casos de ciberdelincuencia acaban en juicios y condenas
- ▶ ¿Se hace justicia a las víctimas?

2º Protocolo Adicional ayuda a afrontar estos desafíos

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

14

## 2º Protocolo Adicional al Convenio sobre la Ciberdelincuencia: contenido

### Preámbulo

#### Capítulo I: Disposiciones comunes

- Artículo 1 Finalidad
- Artículo 2 Ámbito de aplicación
- Artículo 3 Definiciones
- Artículo 4 Idioma

#### Capítulo II: Medidas de cooperación reforzada

- Artículo 5 Principios generales aplicables al Capítulo II
- Artículo 6 Solicitud de información sobre el registro de nombres de dominio
- Artículo 7 Divulgación de la información de los abonados
- Artículo 8 Dar efecto a las ordenes de otra parte para la producción acelerada de información sobre los abonados y datos de tráfico
- Artículo 9 Divulgación acelerada de datos informáticos almacenados en caso de emergencia
- Artículo 10 Asistencia mutua en caso de emergencia
- Artículo 11 Videoconferencia
- Artículo 12 Equipos conjuntos de investigación e investigaciones conjuntas

#### Capítulo III – Condiciones y salvaguardias

- Artículo 13 Condiciones y salvaguardias
- Artículo 14 Protección de datos personales

#### Capítulo IV: Disposiciones finales

- Artículo 15 Efectos del presente Protocolo
- Artículo 16 Firma y entrada en vigor
- Artículo 17 Cláusula federal
- Artículo 18 Aplicación territorial
- Artículo 19 Reservas y declaraciones
- Artículo 20 Situación y retirada de las reservas
- Artículo 21 Enmiendas
- Artículo 22 Solución de controversias
- Artículo 23 Consultas de las Partes y evaluación de la aplicación
- Artículo 24 Denuncia
- Artículo 25 Notificación

15

## 2º Protocolo Adicional al Convenio de Budapest: instrumentos eficaces + salvaguardias fuertes

### Medidas para una respuesta más eficaz de la justicia penal:

- Cooperación directa con los proveedores de servicios de otras jurisdicciones para obtener información sobre los abonados
- Solicitudes directas a los registradores de información sobre los registros de nombres de dominio
- Medidas más eficaces para adquirir datos de abonados y de tráfico mediante la cooperación intergubernamental
- Cooperación acelerada en situaciones de emergencia
- Investigaciones conjuntas y videoconferencias

### Sujeto a un sistema de salvaguardias especialmente fuerte:

- El artículo 2 – ámbito de aplicación del Protocolo: investigaciones o procedimientos penales relativos a la ciberdelincuencia y a las pruebas electrónicas
- El artículo 13 incorpora el artículo 15 del Convenio para garantizar una protección adecuada de los derechos humanos y de las libertades, satisfaciendo así el principio de proporcionalidad
- El artículo 14 incluye salvaguardias detalladas sobre la protección de los datos personales, únicas en un tratado de justicia penal
- Los artículos mencionan los tipos de datos a divulgar
- Los artículos mencionan la información a incluir para permitir la aplicación de las salvaguardias nacionales
- Reservas y declaraciones para permitir salvaguardias nacionales y limitar la información divulgada

16