Poderes procesales en la convención de Budapest: “viejos y nuevos problemas de investigación en entornos digitales”

Santo Domingo

Febrero 2024

msalt@derecho.uba.ar

@saltmarcos

Tics y un cambio de paradigma del proceso penal: la importancia de los poderes procesales de la COC

- Entorno digital como generador de cambio de paradigma del proceso
- Prueba digital vs prueba física. Regulación expresa vs. libertad probatoria
- Los medios de prueba en la COC
- El “going dark” de las investigaciones/nuevas herramientas de investigación/necesidad de limites
- Los problemas para el sistema de cooperación internacional en materia penal

Prueba digital y los interrogantes para el proceso penal

- Guía de Prueba Electrónica del Consejo de Europa: : “La prueba electrónica es **aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial**”
- Eoghan Casey: “Cualquier dato almacenado o transmitido utilizando computadoras que sustenta o rechaza una teoría sobre cómo ha sucedido un delito o que acredita elementos fundamentales del delito tales como la intención o posibles coartadas”

Libertad probatoria vs. “Nulla coactio sine lege”. La diferencia entre medios de prueba e investigación.

Art. 30 CADH: **Las restricciones permitidas**, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, **no pueden ser aplicadas sino conforme a leyes** que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas.

Ámbito de aplicación de las disposiciones procesales (COC, art. 14)

1 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para **establecer los poderes y procedimientos** previstos en la presente Sección a **los efectos de investigación o de procedimientos penales específicos.**

2 Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

- a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
- b otros delitos cometidos por medio de un sistema informático; y
- c la obtención de pruebas electrónicas de cualquier delito.

Condiciones y salvaguardas (COE art. 15)

- 1 Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y **salvaguardias previstas en su derecho interno**, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades fundamentales, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u **otros instrumentos internacionales aplicables en materia de derechos humanos, y que debe integrar el principio de proporcionalidad.**

Condiciones y salvaguardas

2 Cuando proceda, **teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate**, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3 Siempre que sea conforme con el interés público, y en particular la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Medidas procesales Básicas: Convención de Budapest

- Aseguramiento de datos: Art 16: diferenciación
  con la retención de datos.
- Orden de presentación: Art. 18
- Registro y Confiscación de datos almacenados: Art. 19
- Obtención en tiempo real de datos de tráfico: Art. 20
- Obtención en tiempo real de datos de Contenido: Art. 21

Datos generados alrededor de una comunicación electrónica

Dato de abonado

Datos necesarios para identificar a un usuario de un servicio

Ej: nombre, alias, documento, forma de pago y domicilio de facturación, lugar de prestación, etc.

Dato de tráfico

Cualquier dato relacionado a la cadena de una comunicación a través de una red de comunicaciones

Indican el origen, destino, ruta, hora, fecha, tamaño, duración, o el tipo de servicio subyacente. COC , art. 1, d.

Dato de contenido

El contenido mismo de una comunicación

Ej: en un mail es lo que lee el receptor, el contenido de una imagen, etc.

Problemas

- Quién puede pedir cada tipo de datos.
- Datos de abonado, datos de tráfico, contenido como categorías todavía válidas
- Datos de conexión
- IP fija vs IP dinámica. CASE OF BENEDIK v. SLOVENIA (Application no. 62357/14)
- Datos de geolocalizción (caso Carpenter)
- Corte Constitucional Alemania 1BvR 1873/13 (27 /5/2020)

Aseguramiento de Datos

Law Enforcement Online Requests

vs

Retención general de Datos

Aseguramiento de datos como medida procesal

- El aseguramiento de datos actúa como una especie de "cautelar probatoria".
- Facultad otorgada a las autoridades en una **causa penal concreta** para que ordenen a los titulares o administradores de sistemas informáticos que aseguren (impidan su alteración) de datos alojados en su sistema que pueden ser de utilidad para una investigación.

Art. 16 de Convención de Budapest

- 1. "…permitir a sus autoridades competentes ordenar o imponer de otro modo la **conservación rápida de datos electrónicos específicos**, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.
- 2. "…obligar a dicha persona a conservar y a proteger la **integridad** de los datos durante el tiempo necesario, hasta un máximo de **noventa días**, con el fin de que las autoridades competentes puedan **obtener su revelación**. las partes podrán prever la renovación de dicha orden.
- "…obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación **a mantener en secreto…"**

Orden de presentación

- "Facultad otorgada a autoridades de persecución penal de ordenar, en el marco de una **investigación penal concreta**, que una persona entregue o comunique datos informáticos determinados o datos relativos a los abonados que **obren en su poder o estén bajo su control**, almacenados en un sistema informático o en un dispositivo de almacenamiento de datos".
  - **Siempre datos del pasado y no futuros**

ART. 18 COC

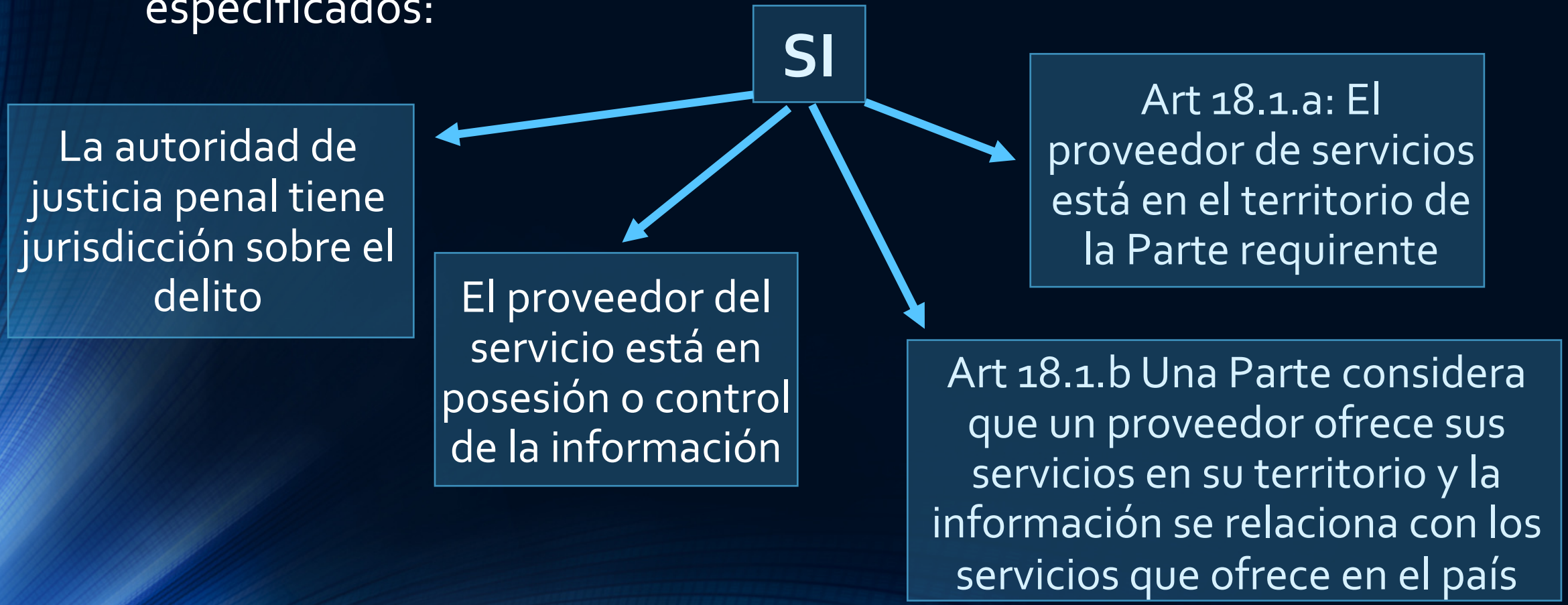
Orden de presentación. "1. …ordenar:

a) A una persona ***que se encuentre en su territorio*** *que comunique determinados datos informáticos que posea o que se encuentren* ***bajo su control****, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos;*

b) a un proveedor de servicios que ofrezca ***prestaciones en el territorio*** *de esa Parte que comunique los datos que* ***posea o que se encuentren bajo su control relativos a los abonados*** *en conexión con dichos servicios.*

Interpretación art. 18 relación a datos de abonado

- La orden de presentación de información de abonado en virtud del art 18 del Convenio de Budapest podría ordenarse en una investigación penal concreta y con respecto a abonados especificados:



Registro y Secuestro de datos (coe, 19)

• *Art. 19. Registro y confiscación de datos. Facultar a sus autoridades a* ***registrar o a tener acceso****:*

- *a. a todo* ***sistema informático*** *o a parte del mismo,* ***así como a los datos informáticos en él almacenados****; y*
- *b. a todo* ***dispositivo de almacenamiento*** *informático que* ***permita almacenar datos informáticos*** *en su* ***territorio****.*
- *Prevé una posibilidad de extensión del registro dentro del territorio*

Registro y secuestro. continuación

- *Confiscar u obtener los datos:*

- *a. **confiscar** u obtener de un modo similar un **sistema** informático o una parte del mismo, o un **dispositivo** de almacenamiento informático;*
- *b. realizar y conservar una **copia** de esos **datos** informáticos;*
- *c. **preservar la integridad** de los datos informáticos almacenados pertinentes; y*
- *d. hacer **inaccesibles** **o** **suprimir** dichos datos informáticos del sistema informático consultado.*
- *ordenar a toda persona que conozca el funcionamiento de un sistema o las medidas aplicadas para proteger los datos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir art. 19*

Registro y secuestro de datos y los interrogantes actuales

- ¿Cuándo se produce el registro y secuestro de dato? Diferencia entre dispositivo físico y digital.
- ¿La extracción o copia forense forman parte del registro? Es diferente en el caso de la extracción y copia de datos de teléfonos
- ¿Cuándo entran en juego las garantías vinculadas al derecho de defensa y con qué alcance? ¿Al secuestrar los dispositivos, acceder a los datos, hacer la copia forense/extracción, durante el análisis?**¿QUÉ NORMA APLICO?**
- **Operaciones tecnicas en el lugar Datos en memoria ram/triage**
- **Plain view en entornos digitales**
- **¿Extensión de registro y secuestro de datos?**
- **¿Cooperación del sector privado en la ejecución de la medida?**
- **¿Cuándo se devuelven los dispositivos y los datos?**

Interceptación de datos de tráfico: Artículo 20 (Convención de Budapest)

- "Cada parte adoptará las medidas legislativas para facultar a sus autoridades competentes :

a) A obtener o grabar con medios técnicos existentes en su territorio, o a obligar a los proveedores de servicios, obtener o **grabar en tiempo real los datos relativos al tráfico**

b) A fin de garantizar que el proveedor de servicio no informe a los infractores sobre la investigación, obliga a los estados a **adoptar legislaciones que garanticen que los proveedores de servicios mantengan la confidencialidad de la investigación**, teniendo la ventaja que queda eximido de la obligación de informar a los usuarios

Límites y condiciones (art. 20)

- El poder debe ejercerse en relación con **comunicaciones específicas**
- No está permitido el ejercicio de este poder para la vigilancia y obtención generalizada o indiscriminada de grandes volúmenes de datos relativos al tráfico
- Las Partes pueden adoptar medidas en relación con las comunicaciones **dentro de su territorio**
- Una comunicación se considera dentro de un territorio si una de las partes que se comunican (seres humanos o equipos) se encuentra en el territorio o si el equipo informático a través del cual pasa la comunicación se encuentra en el territorio

Interceptación de datos de contenido (art. 21)

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de **delitos graves** que deberá definirse en su derecho interno a:
   a. a obtener o grabar con medios técnicos existentes en su territorio, y
   b. a obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:
      i. obtener o grabar con medios técnicos existentes en su territorio, o
      ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

   en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

- Los datos de contenido son altamente intrusivos de la privacidad por lo que este poder solo puede ejercerse en relación con delitos graves a determinar por las legislaciones nacionales

Art. 21 continuación

La autoridad competente tiene poder para:

- obtener o grabar directamente los datos relativos al contenido
- obligar a un proveedor de servicios obtener o grabar datos relativos al contenido
- obligar a un proveedor de servicios a prestar su colaboración y su asistencia a la autoridad competente

Nuevos desafíos procesales/ probatorios (“going dark”)

- Anonimato en la navegación
- Encriptación de archivos
- Comunicación por IP/ “par a par”
- Monedas digitales
- técnicas de suplantación de identidad
- Alojamiento en nube y pérdida de localización

Nuevos medios de investigación/prueba: controversias procesales y desafíos para la cooperación internacional:

Rastrillajes/ Uso de datos obtenidos en fuentes abiertas

Agente encubierto y entregas vigiladas

Datos geolocalización/"geofence warrant"

Escuchas directas en lugares cerrados

Uso de inteligencia artificial

Técnicas de "remote forensic"

Acceso transfronterizo de datos y validez de la prueba

Muchas gracias

@SALTMARCOS
MSALT@DERECHO.UBA.AR