"Nuevos Desafíos de la evidencia digital. El Acceso trasfronterizo de datos en los países de America Latina[1]"

Marcos Salt[2]

1. Objetivo del informe

El presente informe está orientado a analizar los conflictos que genera tanto a nivel normativo como práctico, el acceso transfronterizo de datos en los países de América Latina. O sea, aquellas investigaciones penales en las que resulta necesario el acceso a datos informáticos alojados en servidores ubicados físicamente en jurisdicciones diferentes a la de las autoridades que tienen a su cargo la investigación o sea en lugares en los que no cuentan con poderes jurisdiccionales (Ya sea que la información esté alojada en servidores en países extranjeros o, en el caso de países federales como Argentina o México, en servidores alojados en provincias en las que la autoridad que lleva adelante la investigación no tiene poder jurisdiccional). Los avances tecnológicos han hecho que el tema que es objeto de análisis, de por sí difícil, se torne más complejo aún convirtiéndose en uno de los factores principales que atentan contra el éxito de las investigaciones en entornos digitales. La tendencia a alojar información en la nube (cloud computing) y la posibilidad de que no se pueda determinar en qué país está alojado el servidor que contiene la información o evidencia digital necesaria para una investigación

[1] El presente trabajo es una versión corregida de la presentación realizada en Octopus 2012, Estrasburgo, Francia, "Transborder Access to Stored Computer Data in Latin American Countries".

[2] Profesor de Derecho Penal y Procesal Penal de la Universidad de Buenos Aires.

penal (data flows)[3] es hoy un obstáculo de difícil solución para los organismos de persecución penal estatal y fruto de enormes divergencias tanto a nivel académico como de política internacional a la hora de buscar soluciones normativas tanto en las legislaciones de los diferentes países como en los convenios de cooperación internacional. Sin embargo, como veremos, la cuestión no ha recibido aún un tratamiento profundo en el ámbito regional (ni a nivel legislativo ni en la casuística jurisprudencial).

El escollo principal surge de la propia estructura de los sistemas informáticos e internet (un mundo virtual sin fronteras físicas) y su difícil tratamiento por ordenamientos normativos atados a la idea de la territorialidad y la soberanía de los estados.

A fin de describir el estado de la discusión, se realizara una somera descripción de los principios que rigen la aplicación territorial de la ley penal sustantiva en los Códigos penales latinoamericanos y, especialmente, de las normas que rigen la aplicación de la ley procesal penal en el espacio tanto en los derechos internos como en las normas de cooperación internacional que posibilitan la realización de medidas de prueba en extrañas jurisdicciones. En este punto se hará especial hincapié en los principios generales que inspiran las normas de los tratados regionales sobre cooperación en materia penal.

Este último aspecto resulta clave para definir la situación actual del problema y para analizar posibles mejoras que, si bien requieren cambios en los sistemas penales internos, demandan de manera fundamental acuerdos a

[3] El acceso a los datos puede ser necesario en una investigación penal para la realización de cualquiera de las medidas de prueba típicas de investigaciones en entornos digitales. Ya sea para preservar los datos, para proceder a un registro y eventual secuestro de datos como para la intercepción en tiempo real de datos de tráfico o datos de contenido. Como modelo de medidas procesales de investigación cf. Convención de Budapest (COC, artículos 14 a 21).

nivel internacional que se plasmen en modificaciones en los sistemas de cooperación en materia penal.

Asimismo, a los fines de facilitar el análisis de la problemática, intento describir qué está sucediendo en "la práctica" de las investigaciones que llevan adelante hoy los órganos de persecución penal con el marco normativo vigente. Esto es, los problemas que se plantean ya no sólo desde un punto de vista dogmático normativo sino en la "vida real" de las investigaciones.

En el desarrollo del trabajo tomo como modelo de comparación y ejemplo de normativa internacional la Convención Europea sobre Delitos Informáticos (Convención de Budapest –CoC)- que trata el tema y adquiere fundamental importancia por su influencia en la legislación interna de numerosos países (no sólo de aquellos países miembros de la convención).

Finalmente, intentaré aportar algunas conclusiones personales y posibles soluciones.

2. Planteo general del problema.

La obtención de evidencia digital tanto para la persecución de los denominados delitos informáticos como para la investigación de cualquier delito cuando la evidencia se encuentra almacenada en entornos digitales ha generado la necesidad de introducir importantes cambios en los sistemas procesales penales cuyas normas de evidencia fueron diseñadas pensando en la evidencia física[4]. En efecto, los cambios vertiginosos en la informática y las telecomunicaciones han generado un cambio sustancial en la forma de

[4] Cf. Marcos Salt, "Tecnología Informática: ¿un nuevo desafío para el proceso penal", XXV Congreso Nacional de Derecho Procesal, Rubinzal editores, Buenos Aires, Argentina, pag. 856. Y, en el ámbito del Derecho anglosajón, Orin Kerr, "Digital Evidence And The New Criminal Procedure", Columbia Law Review, vol 105:279; en el ámbito del derecho continental europeo un interesantes estudio de derecho comparado, Fredesvinda Insa, "La Admisibilidad de las Pruebas Electrónicas ante los Tribunales. Luchando contra los Delitos Tecnológicos", AEC 2006.

afrontar la investigación no sólo de los delitos informáticos sino también de los delitos tradicionales cuando ellos se cometen por medios informáticos o cuando es necesario para su persecución la obtención de evidencia digital contenida en sistemas informáticos o en dispositivos de comunicaciones[5].

Muchos países modificaron su legislación procesal para prever las medidas especiales necesarias para la investigación en entornos digitales y para adecuar los mecanismos de obtención de pruebas tradicionales cuando, por sus características especiales, la evidencia digital requería de recaudos diferentes a los previstos para la evidencia física[6].

Otros países, en cambio, siguieron el camino de aplicar analógicamente las normas existentes para la evidencia física "forzando" su interpretación para los supuestos de obtención de evidencia digital. Según entiendo, este camino es limitado o insuficiente y genera importantes lagunas que afectan tanto la eficiencia de las investigaciones como a una adecuada protección de las garantías individuales, especialmente el derecho a la intimidad.

La Convención de Budapest (CoC[7]) advirtió este problema y la necesidad de introducir un conjunto de herramientas procesales especiales tendientes a la obtención de evidencia digital para la investigación no sólo de los

[5] Estos cambios, según entiendo, pueden significar desde el punto de vista del análisis científico del derecho procesal penal y también de las normas de cooperación internacional regidas por los principios del derecho internacional público, un "cambio de paradigma" cuyas consecuencias no han sido aún advertidas en todos sus alcances. Cf. Marcos Salt, ob cit. Y "International legal cooperation in cybercrime matters: Challenges for countries of Latin America", presentación en Octopus conference, Estrasburgo, Francia, 2009. disponible en www.coe.int.

[6] Así, a modo de ejemplo, la necesidad de prever poderes procesales para "asegurar los datos de tráfico de comunicaciones", la elaboración de estándares normativos diferentes para el registro y secuestro de datos en entornos digitales en comparación con el registro y secuestro de documentos en soporte papel, una interpretación diferente del alcance de la doctrina de *plain view* en el registro y secuestro de evidencia en entorno digitales, mecanismos diferentes para asegurar la cadena de custodia, etc.

[7] Council of Europe Convention on Cybercrime (ETS n.185)

denominados delitos informáticos incorporados en la Convención – CoC, arts. 2 a 11- sino también a los demás delitos cometidos por medios informáticos y la recolección de evidencia digital en la investigación de cualquier delito que así lo requiera. Esta decisión de introducir normas procesales especiales para la obtención de evidencia digital constituye, según entiendo, uno de los aciertos más importantes[8] de la Convención de Budapest que hasta el presente es el principal acuerdo internacional sobre la materia que ha expandido su influencia en la legislación interna de países en todos los continentes.

Sin embargo, el creciente uso de internet, la convergencia de las comunicaciones y la tendencia creciente a la utilización de la computación en la nube (*cloud computing*) generan nuevos desafíos y ponen nuevamente en tensión a los principios tradicionales del sistema penal[9]. En el tema que es objeto de este trabajo, uno de los pilares básicos del sistema penal, nada menos que la idea de *soberanía nacional* como base de la fijación de los poderes procesales de las autoridades de cada país y límite infranqueable de fronteras físicas para la actuación de la justicia de un país en otro, entra en crisis[10]. Este principio tradicional del Derecho Penal pero fundamentalmente del Derecho internacional Público, es la base de la cooperación tradicional en materia penal mediante las "rogatorias" o "exhortos" entre estados tal como

[8] Cf. CoC, Artículo 14. En el mismo sentido, las reglas de cooperación internacional de la convención, artículo 23 están construidas como espejo de las medidas procesales previendo su necesidad de obtención mediante cooperación internacional. Cf. . Marcos Salt, "International legal Cooperation in Cybercrime Matters: Challenges for countries of Latin America", trabajo presentado en "**Octopus Conference"**, Estrasburgo, Francia, 2009. disponible en www.coe.int.

[9] Cf. Jan Sponele, "Cloud Computing and Cybercrime Investigations: Territoriality vs the power of disposal?", Discussion paper, www.coe.int/cybercrime .

[10] En un sentido contrario, sosteniendo que los registros y secuestros de datos no implican una violación al principio de territorialidad, cf. Jack Goldsmith, "The internet and the Letitimacy of Remote Cross Border Searches", publicado en Public Law And Legal Theory Working Paper nro. 16, The Law School, University of Chicago, 2001.

fue concebida y construida en tratados internacionales, regionales y bilaterales.

Lo cierto es que tal como veremos en los puntos siguientes, en la base del planteo de este trabajo está la posibilidad de que la "eficiencia" en determinadas investigaciones pueda poner a las autoridades de un país ante la disyuntiva que puede generar la necesidad de acceder a información contenida en servidores en el extranjero sin contar con las herramientas procesales necesarias o con los canales de cooperación internacional y de cooperación o regulación del sector privado (generalmente la información está alojada en servidores de empresas privadas) necesarios para hacerlo de manera **legítima y con la rapidez que la investigación requiere**.

Así como fue objeto de preocupación los problemas que podía generar para una eficiente persecución de los delitos informáticos la posibilidad de su fácil comisión a distancia y de allí la necesidad de armonizar las legislaciones para evitar la imposibilidad de persecución en países que no contaran con legislación penal adecuada –los denominados paraísos informáticos seguros-, también resulta necesaria la adecuación de las legislaciones procesales para permitir medidas de investigación y hacer posible su efectiva persecución penal. De allí que el desafío de adecuar las legislaciones procesales homogenizando determinadas herramientas resulta ineludible y un paso fundamental para lograr eficiencia en cooperación penal internacional en esta materia. En realidad, según creo, la cooperación entre países requiere previamente de la adecuación procesal de los derechos internos.

En este contexto, hoy resulta necesario atender también la problemática que podría generar que países o empresas se conviertan en "paraísos de evidencia digital" (safe heavens of evidence) que dificulten la investigación no sólo de los delitos informáticos sino de todo tipo de delitos. Por ejemplo, el

alojamiento de la información relevante de bandas de criminalidad organizada en servidores ubicados en países que no cuenten con herramientas procesales adecuadas o que no admitan ningún mecanismo de cooperación internacional y garanticen **la inaccesibilidad de la información sin ningún tipo de excepción**. Llevando estos casos a un extremo, es posible imaginar un futuro en el que el registro y secuestro de computadoras y otros soportes de almacenamiento electrónico no arroje nunca resultados positivos ya que los usuarios alojaran la información servidores de alojamiento externos que generalmente no estarán ubicados en el domicilio allanado.

Este nuevo desafío requiere especial atención y nuevas soluciones que tengan en cuenta el balance necesario entre la "*eficiencia en la investigación de los delitos*" y la necesidad de "*protección de las garantías procesales en el mundo digital*". Especial atención deberá darse a la hora de buscar soluciones al derecho a la intimidad de los ciudadanos (estándares de protección de datos personales) y el derecho a la libertad de expresión, pilares básicos de la sociedad democrática, que pueden verse afectados seriamente por normas sin un adecuado balance de los principios en juego.

Asimismo, la problemática pone en crisis el sistema de cooperación regional e internacional en materia penal requiriendo nuevas formas de cooperación o de aceptación de la intervención judicial de un Estado en otro y generando la necesidad de nuevos principios de derecho internacional público que permitan respetar adecuadamente la soberanía nacional de los países y principios de igualdad en la relación de forma tal de que no se convierta en una excusa para avalar el intervencionismo de algunos estados sobre otros.

El problema, de extrema complejidad tanto jurídica como política, se relaciona también de manera ineludible con la regulación de la cooperación entre sector público y sector privado ya que en un alto porcentaje de los casos

problemáticos la información está en manos del sector privado titular de los servidores donde la información que es objeto de investigación está alojada. De esta manera, no es solo un tema de cooperación internacional entre países sino también de relación entre el sector público y privado. Ambos temas confluyen y se interrelacionan de manera ineludible tornando la solución más compleja aún.

Algunos de los casos a los que se enfrentan diariamente hoy las autoridades de persecución penal ayudan a ejemplificar las aristas de los problemas que requieren soluciones jurisprudenciales con la ley vigente y efectuar los cambios normativos necesarios no sólo a nivel de los derechos internos, sino fundamentalmente en el plano de la cooperación internacional[11].

Supuesto 1: Casos de Acceso directo por parte de las autoridades de un Estado a datos alojados en extraña jurisdicción

[11] No será objeto de tratamiento en el presente trabajo los casos de acceso directo a datos alojados en servidores en extrañas jurisdicciones pero de **"libre acceso general" (open source)**, o sea disponibles al público sin la necesidad de utilizar claves o romper barreras especiales de seguridad. Supongamos que en un caso es necesario como evidencia una nota periodística publicada por un diario de un país extranjero que no sólo se edita en papel sino que tiene una versión digital alojada en un servidor fuera del territorio en el cual las autoridades a cargo de la investigación cuentan con poderes jurisdiccionales suficientes. La obtención de ese documento como evidencia es sencilla y puede ser realizada por cualquier persona a través de los buscadores normales. A modo de ejemplo, pensemos en un caso por calumnias a través de la prensa. Conseguir el artículo en cuestión es posible sin necesidad de requerirlo por rogatoria internacional. Hay datos más complejos aún que están disponibles en internet sin ningún tipo de barrera. Pensemos en el supuesto de las bases de datos públicos sobre titularidad de propiedades, tributarios, etc. Si bien el tema generó controversias en el ámbito académico y jurisprudencial, hoy es aceptado mayoritariamente como válido utilizando diversos argumentos. Cf. Especialmente, Nicolai Seitz, "Transborder Search: A new Perspective in Law Enforcement"?, Yale Journal of Law and Technology, Volume 7, año 2005. El tema ha sido resuelto también en sentido positive por la Convención Europea en el artículo 32 a. Mayores problemas puede presentar según entiendo las investigaciones realizadas de manera preventiva como por ejemplo el "rastrillaje" de internet que realizan fuerzas de seguridad de numerosos países en búsqueda de contenidos ilegales, aún en los casos en los que las búsquedas se realizan en sistemas abiertos y las potentes herramientas de entrecruzamiento de datos en redes abiertas con fines de investigación penal.

Un juez dicta una orden de allanamiento para registrar y secuestrar en las oficinas de un banco toda la información disponible sobre un sospechoso x (por ejemplo, los movimientos de la cuenta bancaria correspondientes a un determinado período de tiempo). El juez ordena que la medida sea cumplimentada con colaboración de un perito informático o de expertos de una unidad especial de delitos tecnológicos pertenecientes a una fuerza de seguridad. Los peritos encuentran la información buscada pero advierten al juez que, si bien pueden acceder desde las terminales informáticas de la sede del banco para la cual cuentan con orden de allanamiento legítimamente otorgada, la información está alojada en un servidor que está en un país extranjero o en una provincia diferente (en el caso de un país de organización política federal). Surgen un sinnúmero interrogantes de difícil solución utilizando la normativa vigente:

- ¿Puede procederse al registro y secuestro de la información sin recurrir a los mecanismos de cooperación internacional que vinculan a ambos países? ¿Supongamos que no existe clave o de acceso que deba ser "destrabada" por los investigadores ya que la información es accesible desde la terminal ubicada en el domicilio para el cual el juez libró la orden de allanamiento sin necesidad de nuevos procedimientos informáticos?
- ¿Puede obtenerse la clave mediante técnicas de "ingeniería social" o colocando programas espías especiales introducidos en la computadora del imputado para grabar las contraseñas que luego voy a utilizar para la investigación?
- ¿Si no es posible el secuestro de la información porque entendemos que ello significaría una violación al principio de territorialidad, resulta

por lo menos válido proceder al copiado de la información sin removerlo ni alterarlo ni asegurarlo de manera alguna?

Supuesto 2: Acceso a datos a través de la cooperación del sector privado.

En estos supuestos, los organos de persecución penal no acceden a la información de manera directa sino a través de empresas del sector privado como por ejemplo, Microsoft, Google, entidades bancarias, etc.

Supongamos, por ejemplo, que en una investigación es necesario acceder a la información contenida en una cuenta *webmail* (Gmail, Hotmail, Yahoo, etc.) o a los documentos contenidos en un servicio de alojamiento de datos cuyos proveedores de servicios tienen los servidores en un extranjero (por ejemplo, "dropbox"):

- ¿Es necesario que el pedido sea realizado a través de los mecanismos de cooperación internacional (exhorto internacional) o resulta válido requerir la información a la oficina comercial de la empresa que tiene sede en el país en el que se lleva a delante la investigación.
- ¿Resulta válido obtener la evidencia a través de pedidos directos vía mail a la sede de la empresa donde se encuentra el servidor sin dar ningún tipo de información al país donde esta empresa tiene su sede?
- ¿Supongamos que por razones técnicas ni siquiera es posible conocer en un momento determinado en qué país está alojada la información que cambia de servidor constantemente?

Como el lector podrá apreciar, todos estos interrogantes son de difícil solución con el marco normativo vigente (tanto en lo que se refiere a las normas procesales sobre evidencia como a los principios de la cooperación internacional) que no previó los cambios vertiginosos que se produjeron en la tecnología informática y de las telecomunicaciones.

3. Los principios generales sobre aplicación territorial de la ley penal sustantivita y procesal y su ineficacia para solucionar los problemas que plantea el acceso transfronterizo de datos y la obtención de prueba en "la nube" (*cloud computing*).

Resulta evidente que los principios generales tradicionales vigentes en la región tanto para determinar la ley penal aplicable en materia penal como para determinar el poder jurisdiccional para la aplicación de medidas de coerción o la obtención de evidencia en diferentes países, no han sido adaptadas a los desafíos que presenta en ambas áreas la era digital. Ello resulta más evidente a partir de la revolución generada por internet y, más complejo aún, a partir del crecimiento de la tendencia a alojar la información (potencial evidencia en un proceso penal) en servidores ubicados en extrañas jurisdicciones o incluso en varios servidores ubicados en países indeterminados.

Tanto las legislaciones internas de los diferentes países como los tratados regionales de cooperación en materia penal vigentes en la región, siguen atadas, con pequeñas variaciones pensadas a partir de la necesidad de hacer frente de manera eficiente a la persecución de los modernos fenómenos de la criminalidad organizada trasnacional, a principios pergeñados con una fuerte impronta del principio de territorialidad y la vigencia y protección del principio de la soberanía nacional de los diferentes países. O sea, las fronteras físicas como "barreras inexpugnables" para la actuación del sistema judicial de un país en el otro. Salvo recurriendo a la cooperación de las autoridades judiciales del país requerido por medio de sistemas de cooperación de diferentes niveles de eficiencia y rapidez, las fronteras físicas actúan como límite de la competencia y de la intervención de la autoridad judicial de un país en otro territorio distinto al que le otorgo poderes jurisdiccional.

El mismo principio rige también dentro del derecho interno de los países de la región de organización política federal (tal el caso de México y Argentina), en los que los sistemas judiciales de las diferentes provincias o estados federados deben recurrir a la cooperación interprovincial para poder actuar fuera de su territorio.

I. Aplicación territorial de la Ley penal sustantiva

En términos generales, con escasas excepciones, los países de América Latina establecen como principio general para la determinación de la ley penal sustantiva aplicable a un hecho, el principio de territorialidad con excepciones limitadas. El principio de personalidad o nacionalidad es extraño a las legislaciones latinoamericanas salvo escasas excepciones.

a) <u>Principio de territorialidad</u>:

De acuerdo a este principio general adoptado por los países de América Latina, la ley penal de cada país se aplica exclusivamente a los *hechos "cometidos" dentro del territorio del Estado que la sanciona.*

Dentro de esos límites, la ley penal se aplica al autor del hecho con prescindencia de su condición de nacional o de extranjero y prescindiendo también de las pretensiones punitivas de otros Estados. En los delitos a distancia, o sea cuando el lugar de la acción no coincide con el lugar en el que se produce el resultado, puede generarse alguna duda sobre la ley penal aplicable ya que el término "cometidos" abarca acción y resultado. Así, a modo de ejemplo, en los casos de daños informáticos en los que la acción es realizada en un país y el resultado alteración o supresión de datos se produce en otro el lugar de la acción se produce en un país y el resultado en otro, siendo, por lo tanto, ambos países "lugares de comisión del delito".

b) <u>Principio de real o defensa</u>

Este principio presente en los códigos de la región, significa en términos prácticos, una posibilidad de excepción al principio de territorialidad, ya que determina la aplicación de la ley penal y la competencia de un Estado para el ejercicio de su poder penal en aquellos casos en los que con independencia del lugar de comisión de la acción, el interés vulnerado o el perjuicio al bien jurídico generado por el delito se traduzca en una afectación al país; por ejemplo, la falsificación de moneda que si bien se realiza en un territorio extranjero puede generar alteraciones en la economía del estado que aplica el principio de defensa para aplicar la ley penal. La consecuencia de este principio es la posible aplicación del derecho penal de un Estado a delitos cometidos fuera de su territorio, pues la principal finalidad de ese derecho es la defensa o protección de los intereses nacionales.

c) Principio de personalidad de la ley penal, o principio de nacionalidad, según el cual la ley del Estado sigue al nacional donde quiera que vaya, de modo que la competencia se determina por la nacionalidad del autor del delito, denominado principio de personalidad activo (el código italiano, o francés, por ejemplo) o de la víctima en cuyo caso se denomina, principio de personalidad pasivo (el código italiano). Este principio no es común en las legislaciones de América Latina.

d) Principio universal, según el cual la ley penal tiene validez universal, de modo que la acción penal puede ser promovida por todo Estado, cualquiera que sea el lugar de comisión del delito o la nacionalidad del autor. El fundamento de este principio es la aplicación de la ley penal a acciones de extraordinaria gravedad y afectación del derecho internacional como los delitos de lesa humanidad y crímenes de guerra que afectan por igual a todas las naciones.

En la legislación penal de la región rige, por regla, el principio de territorialidad, y sólo en forma excepcional se utiliza el principio real o de defensa como correctivo. El principio de personalidad o nacionalidad, activa o pasiva, y el de universalidad tradicionalmente han sido extraños a los países de la región, aunque algunas legislaciones los han ido incorporando expresamente en sus Códigos Penales (sólo a modo ejemplo el CP de Colombia y el de Costa Rica[12]). Asimismo, internacionalmente se ha aceptado para determinados tipos de delitos el principio universal a través de convenciones internacionales, sólo a modo de ejemplo, el Estatuto de Roma, al cual han adherido países latinoamericanos con fuerte tradiciones en el principio de territorialidad (como por ejemplo, México, Chile y Argentina).

[12] Para un análisis del sistema del Código penal de Costa Rica, Cf. arts. 4 y ss. De manera especial sobre la posibilidad de iniciar proceso en Costa Rica por hechos punibles cometidos en el extranjero, ver art. 6:

Podrá incoarse proceso por hechos punibles cometidos en el extranjero y en ese caso aplicarse la ley costarricense, cuando:

1) Produzcan o puedan producir sus resultados en todo o en parte, en el territorio nacional;

2) Hayan sido cometidos por personas al servicio de Costa Rica y no hubieren sido juzgadas en el lugar de comisión del hecho, en virtud de inmunidad diplomática o funcional; y

3) Se perpetraren contra algún costarricense o sus derechos.

4) Hayan sido cometidos por algún costarricense. (Así adicionado el inciso anterior por el artículo 1°, punto 2., aparte a) de la Ley de Fortalecimiento de la Legislación contra el Terrorismo, N° 8719 de 4 de marzo de 2009). Para la aplicación del principio universal Cf. Art. 7: *"Independientemente de las disposiciones vigentes en el lugar de la comisión del hecho punible y la nacionalidad del autor, se penará, conforme a la ley costarricense, a quienes cometan actos de piratería, terrorismo o su financiamiento, o actos de genocidio; falsifiquen monedas, títulos de crédito, billetes de banco y otros efectos al portador; trafiquen, ilícitamente, armas, municiones, explosivos o materiales relacionados; tomen parte en la trata de esclavos, mujeres o niños; se ocupen del tráfico de estupefacientes o de publicaciones obscenas; asimismo, se penará a quienes cometan otros hechos punibles contra los derechos humanos y el Derecho internacional humanitario, previstos en los tratados suscritos por Costa Rica o en este Código."* (Así reformado por el artículo 1°, punto 1., aparte a) de la Ley de Fortalecimiento de la Legislación contra el Terrorismo, N° 8719 de 4 de marzo de 2009).

Como Ejemplos de extraterritorialidad en Código penal colombiano, Cf. Art. 15.

De manera tal, que la impronta del principio de territorialidad sigue siendo la regla en la región.

En el caso del Código Penal Argentino, el artículo 1º establece que la ley argentina se aplica a los delitos cometidos en el territorio argentino y a aquéllos cuyos efectos deban producirse en el territorio. En el mismo sentido, a modo de ejemplo, lo establecen el Código Penal Chileno (arts. 5 y 6) y el Código Mexicano (art. 1°).

La ley penal, en general, es de aplicación territorial, y esto significa que tiene valor sólo en los límites del territorio que la sancionó, principio que domina la aplicación de la ley penal en el espacio, de manera que el lugar de comisión del hecho (*forum delicti commissi*), sin perjuicio de las ambigüedades a que conduce la expresión "comisión", determina, de ordinario, la ley penal aplicable y soluciona los conflictos de leyes que pudiera existir, por vía de principio.

II. La aplicación de la ley procesal de un país en otros países para medidas de investigación que se deben realizar extraterritorialmente.

En el caso de la ley procesal penal no rige ni se aplica el principio de "territorialidad" de la misma manera que con la ley penal sustantiva. Si bien la situación varía de acuerdo al convenio de cooperación que rige la relación entre los países, lo normal es que exista aplicación extraterritorial de la ley procesal para la realización de las medidas de cooperación solicitadas a extrañas jurisdicciones cuando van a ser realizadas por las autoridades del país requirente. Por ejemplo, un juez argentino, a quien se le permite tomar un testimonio en el extranjero, aplica, ordinariamente, la ley procesal penal argentina y no la ley del país extranjero donde debe realizar la medida aun cuando concurra al país extranjero personalmente a realizar la medida.

El verdadero principio que rige la aplicación de la ley procesal, para el caso de decidir la aplicación de una de varias leyes de vigencia simultánea, es el de ***lex fori.*** Este principio expresa que el tribunal competente para instruir el procedimiento aplica la ley procesal sancionada por el poder soberano que creó el tribunal, que lo invistió con el poder jurisdiccional que ejerce. Un juez aplica, ordinariamente, la ley correspondiente al poder soberano que lo invistió, cualquiera que sea el territorio donde cumple el acto, salvo la existencia de una excepción, especialmente reglada[13].

En el ámbito de los convenios regionales más importantes que prevén asistencia jurídica mutua en materia penal, si bien se procura establecer sistemas más ágiles de cooperación internacional, empero respetan del mismo modo la soberanía de cada Estado y el principio de *lex fori*. Así, a modo de ejemplo, la *Convención Interamericana sobre Asistencia Mutua en Material Pena*l, la *Convención de las Naciones Unidas contra la Corrupción* y el *Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales del Mercosur*. Los criterios generales de estos tres instrumentos internacionales son:

* La desformalización y mayor agilidad en las solicitudes de asistencia jurídica recíproca en investigaciones penales.

* No se faculta a un Estado parte ejercer funciones jurisdiccionales en el territorio de otro Estado.

* Las solicitudes se ejecutan de acuerdo a la ley del Estado requerido. Se permite que el Estado requerido, en tanto no sean legislaciones incompatibles,

[13] Pueden existir excepciones al principio *lex fori*. Así, por ejemplo, La ley argentina n° 22.172 que establece el *Convenio de comunicación entre tribunales de la República*, en el art. 2°, permite que el juez exhortado aplique, a pedido del exhortante, la ley procesal de este último, esto es, aquella por la cual tramita el juicio, en lugar de la ley propia del juez que lleva a cabo el acto, quien, ese caso, aplica una ley extraña, que no procede del poder soberano que lo invistió como tal.

aplique formas y procedimientos especiales solicitados por el Estado requirente.

* En las medidas cautelares (allanamientos, secuestros, embargos, etc.) se aplica la ley procesal del Estado requerido.

* El Estado requerido puede denegar la asistencia en determinados tipos de delitos o situaciones, por ejemplo, en casos de delitos políticos; tributarios (salvo en la Convención contra la Corrupción); en donde se afecte el orden, seguridad e intereses públicos fundamentales; etc.

En conclusión, es posible afirmar que, de acuerdo al principio general de "soberanía nacional" que determina los principios que rigen la aplicación de la ley penal en el espacio (tanto la ley penal sustantiva como la procesal), los poderes procesales y las herramientas procesales de cada país para la investigación en entornos digitales sólo pueden ser utilizados por sus autoridades solamente en el marco de su territorio. Conforme a las normas vigentes en la región Latinoamericana, en los casos en que las autoridades advierten que las evidencias deben ser obtenidas en un país extranjero deberán requerirlas mediante los mecanismos de cooperación internacional que rijan la relación entre ambos países. Resta aún la discusión a fin de determinar si, en los supuestos antes planteados, se trata de evidencia que debe ser obtenida en el extranjero o si es posible interpretar que al no requerir la presencia física de las autoridades de un país en otro sino sólo de su actuación a través de medios digitales, constituyen casos de producción de prueba en extrañas jurisdicciones.

4. Experiencias prácticas ¿El sentido común supera las normas?

Con la finalidad de incluir en este trabajo información de las soluciones que se están adoptando de hecho en algunos de los supuestos planteados

anteriormente, realice consultas con autoridades de diferentes países y expertos del sector privado.

De acuerdo a la información recabada, no existe en los países de la región normas expresas y claras que regulen la cuestión. Así, en casos similares a los planteados en el supuesto 1 (acceso directo), comúnmente si no es necesario destrabar claves se continuará con la medida copiándose los datos que la orden de allanamiento prevé. De hecho, es común que la circunstancia de que para obtener la información se haya ingresado a un servidor en el extranjero o en la nube, ni siquiera será informada al juez ni se dejará constancia en el acta del allanamiento. Prevalece la idea de que al haberse ingresado a través de una terminal ubicada en el lugar físico alcanzado por la orden de allanamiento, la circunstancia de que la información esté alojada en un servidor en otro lugar es irrelevante. O sea, no se consideran casos en los que se viole el principio de territorialidad.

Un perito informático especializado en la obtención de evidencia digital consultado sobre el tema me planteó el tema en los términos del título de este punto 4. Concretamente me dijo que el problema de la ciencia jurídica es que se había alejado del sentido común: *"quieren aplicar principios y conceptos de un mundo con fronteras físicas al fenómeno de la información en internet que no tiene fronteras"*. Evidentemente, no es que los juristas no tengamos sentido común sino que nos atenemos a normas jurídicas que pueden haber quedado desactualizadas.

Lo cierto es que, de acuerdo a la práctica de los peritos y especialistas de fuerzas de seguridad consultados, en su labor diaria si la orden de allanamiento los habilita al ingreso a un espacio físico y al acceso a las terminales de computadoras que allí encuentren para buscar determinada información, acceden a ella sin perjuicio del lugar en el que la información

esté alojada ya sea que conozcan que el servidor en el que la información está alojada se encuentre en un país extranjero o no. O sea que en la práctica utilizan el criterio de "*ubicación de la terminal desde la que acceden a la información*". Si la terminal está en el espacio físico cubierto por la orden de allanamiento no prestan atención al lugar de la ubicación física del servidor al que están accediendo. La única excepción parece ser que el acceso a la información a la que acceden desde la terminal requiera la realización de operaciones informáticas especiales como "romper claves de acceso".

En el caso de la cooperación del sector público con el sector privado tampoco existen reglas claras, mucho menos normas emanadas de leyes o convenciones internacionales (salvo la referencia de las empresas más importantes del sector a la vigencia de las leyes de EEUU en las que se encuentran radicadas sus casas centrales[14], muchas veces utilizada como justificación para no brindar la información requerida por países de la región[15]). Antes bien, la situación es solucionada en la práctica diaria de las

[14] Así, por ejemplo, Microsoft, Google, Facebook , AOL, etc. En los últimos tiempos se ha verficado un reconocimiento por parte del sector privado de la necesidad de brindar información transnacional con independencia de la ubicación de los servidores. Así a modo de ejemplo la guía de Facebook denominada "Facebook Law Enforcement Guidlines", establece *Solicitudes internacionales: Debido al crecimiento de la población en Facebook en el ámbito internacional reconocemos la necesidad del organismo de aplicación de la ley internacional. Favor enviar solicitudes según nuestras guías a subpoenafacebook.com;* En el mismo sentido, Cf, AOL LLC, Public Safety & Criminal Investigations. Law Enforcement Manual.
En el caso de Microsoft es posible pedir la preservación de datos por un plazo de 180 días. Es posible también obtener de manera directa los datos registrales y los logs de conexión en una comunicación Estado – empresa que incluso en algunos países puede hacerse a través de la oficina local e, incluso en algunos supuestos a través de estudios jurídicos designados por la compañía. Asimismo se puede obtener la información de contenido cuando se encuentren involucrados menores de edad (pedofilia) o cuando peligre la integridad física de una persona de forma inminente.

[15] La cuestión no es solo motivo de controversia en los países de América Latina, cf. Francesco Cajani, "Technologies and Business vs. Law –Cloud Computing, Transborder

investigaciones mediante acuerdos formales o informales con las diferentes empresas y no son los mismos acuerdos ni se aplican de manera similar en todos los países de la región. En muchos casos no se trata de “acuerdos” sino de guías elaboradas “unilateralmente” que el sector privado entrega a las autoridades de los diferentes países sobre la información que puede ser obtenida, bajo qué condiciones y los mecanismos para obtenerla. O sea que tanto el tipo de evidencia, los supuestos en los que es posible obtenerla y el mecanismo “procesal” son definidos por las empresas del sector privado.

Esta situación de “anomia” es peculiar ya que, en los hechos, el sector privado se ha constituido en una suerte de legislador que regula de qué manera y en qué supuestos coopera con las autoridades de los diferentes países. Ello supone un riesgo no sólo para la eficiencia en investigaciones sino también para la protección de los datos personales que quedan sujetos a normas poco claras y cambiantes desconocidas en muchas ocasiones por los usuarios.

Cabe destacar que en estos casos, a los que refiere el supuesto de dos de los casos de ejemplo planteados al principio del trabajo, el acceso transfronterizo de datos se da sin participación alguna de las autoridades del Estado donde se encuentra el servidor en el que los datos están alojados y sin rogatoria internacional alguna en un diálogo directo entre estado requirente – empresa privada.

Según entiendo, la falta de discusión jurídica profunda de estos problemas en los países de la región tanto a nivel jurisprudencial como académico ha favorecido estas prácticas que permitieron solucionar las cuestiones planteadas sin que exista una línea jurisprudencial que advierta sobre la posible violación a principios de la soberanía procesal de otros países o la posible nulidad de la

---

Access and data retention: a legal perspective from the State wich is conducting an investigation”, trabajo presentado en Octopus 2012, Estrasburgo, Francia, 2012.

evidencia así obtenida. Es obvio que esta solución, basada más en un desconocimiento del problema por parte de los operadores del sistema judicial, no será definitiva y requerirá soluciones normativas más claras y, hasta que ello ocurra, un análisis jurisprudencial más profundo.

5. La solución de la Convención del Consejo de Europa

Quienes tuvieron a su cargo la redacción de la COC vislumbraron el problema aunque sólo lograron acuerdo para regular dos situaciones que hoy, con el avance de la tendencia al alojamiento de la información "en las nubes", pueden resultar limitadas[16]. Asi el artículo 32 de la Convención establece[17]:

[16] Las explicaciones de los redactores expresadas en los puntos 293 y 294 del reporte explicativo son indicativas de las dudas que el tema generaba y aún genera: "293. La cuestión de si una Parte puede acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua fue una cuestión que examinaron detenidamente quienes redactaron el Convenio. Hubo un examen detallado de los casos en los cuales puede ser aceptable que los Estados actúen de manera unilateral y aquellos en los que puede no serlo. En última instancia, quienes redactaron el Convenio determinaron que no era posible todavía elaborar un régimen completo y vinculante desde el punto de vista legal que regule este campo. En parte, esto se debió a la falta de experiencias concretas respecto de este tipo de situaciones hasta la fecha, y, en parte, esto se debió a que se consideró que la solución adecuada a menudo es resultado de las circunstancias concretas de cada caso, lo que hace difícil formular normas generales. En última instancia, los redactores decidieron sólo enunciados en el artículo 32 de la Convención de las situaciones en las que todos coincidimos en que la acción unilateral es admisible. Acordaron no regulan otras situaciones hasta el momento en que la experiencia ha ido obteniendo más y más debates pueden celebrarse a la luz de la misma. En este sentido, el Artículo 39, párrafo 3 establece que no se autorizan ni se excluyen otras situaciones.
294. El Artículo 32 (Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público) aborda dos situaciones: primero, cuando los datos a los que se ha de acceder sean accesibles al público y segundo, cuando una Parte ha accedido a datos o recibido datos ubicados fuera de su territorio a través de un sistema informático de su territorio y ha obtenido el consentimiento legal y voluntario de la persona que tiene autoridad legal para revelar los datos a la Parte a través de ese sistema. La cuestión de quién está "legítimamente autorizado" a revelar datos puede variar dependiendo de las circunstancias, la naturaleza de la persona y la ley aplicable de que se trate. Por ejemplo, el correo electrónico de una persona puede estar almacenado en otro país por un proveedor de servicios, o una persona puede deliberadamente almacenar datos en otro país. Estas personas pueden recuperar los datos y, siempre que tengan la autoridad legal, pueden

Artículo 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Como se puede apreciar, la norma prevé la posibilidad de acceso transfronterizo de datos en dos supuestos:

- Cuando estos sean de acceso público.
- Cuando se obtiene consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos.

Este último supuesto genera muchas dudas de interpretación que requieren sobre quién es la persona autorizada y sobre la posible afectación del principio de territorialidad y soberanía al "saltearse" toda intervención del Estado nacional en el que se encuentra el servidor que aloja la información que es requerida por las autoridades de otro Estado.

---

voluntariamente revelar los datos a los agentes del orden o permitir a esos funcionarios acceder a los datos, según lo dispuesto en el artículo".

[17] En su redacción en idioma original: **Article 32 –Trans-border access to stored computer data with consent or where publicly available**
A Party may, without the authorization of another Party:
a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Es posible también advertir posibles conflictos para el derecho de las personas cuyos datos son revelados por una empresa del sector privado sin poder ejercer defensa conforme a las leyes del Estado del lugar donde el servidor está alojado ni acceder a la justicia de este Estado defender los datos.

6. Algunas conclusiones

- La eficiencia en las investigaciones en entornos digitales requiere atender a la problemática que podría generar que países o empresas se conviertan en "paraísos de evidencia digital" (*safe heavens of evidence*) que dificulten la investigación aprovechando el enorme desarrollo de la computación en las nubes y la posibilidad de alojamiento de información en extrañas jurisdicciones.
- En términos generales, tanto en las legislaciones de los países de la región como en los convenios regionales de cooperación en materia penal regionales, tiene fuerte impronta el principio de "soberanía nacional" que determina los poderes procesales y las herramientas procesales de cada país para la investigación en entornos digitales sólo pueden ser utilizados por sus autoridades en el marco de su territorio (*lex fori*). De manera tal que, conforme a las normas vigentes en la región, en los casos en que las autoridades advierten que las evidencias deben ser obtenidas en un país extranjero deberían requerirlas mediante los mecanismos de cooperación internacional que rijan la relación entre ambos países. Queda a salvo la posibilidad de que se

prevean medidas de intervención directa en los casos de urgencia que deberían preverse normativamente.

- Los nuevos mecanismos tanto procesales como de cooperación internacional deben asegurar que la eficiencia en la investigación no se convierta en una amenaza para la vigencia de los derechos humanos, especialmente el derecho a la intimidad ni formas de intervencionismo de algunos estados sobre otros ni de intervención desmedida en la actividad de las empresas proveedoras de servicios.
- Según entiendo, el artículo 32 de la CoC no da satisfacción a los problemas prácticos que hoy genera el acceso transfronterizo de datos y requiere una reinterpretación o reelaboración teniendo en cuenta tanto la tendencia al crecimiento del alojamiento de información relevante para las investigaciones en la nube y la experiencia práctica de los últimos años.
- En este sentido, guías o recomendaciones que colaboren con la aplicación jurisprudencial de las reglas o, incluso alguna modificación o protocolo adicional sobre evidencia digital en general en el que este tema sea atendido de manera especial, resulta aconsejable.

- Es necesario identificar y dar un trato diferente a la situación de los datos que, si bien están alojados en otro territorio, se encuentran claramente bajo el control de una persona física o jurídica del territorio en el que se lleva adelante la investigación
- Una nueva interpretación sobre los términos *lawful authority to disclosure data* es necesaria y atendiendo a que claramente

significará siempre una disminución del poder de soberanía de los estados, esta posibilidad debe ser prevista con carácter excepcional y prever algún tipo notificación de la manera más rápida posible al estado en el que la información está alojada.

- Es necesario regular normativamente los procedimientos para la realización de las medidas que signifiquen acceso transfronterizo. O sea no sólo los supuestos excepcionales en los que se admita la medida sino también de que manera y bajo qué garantías se concreta la medida.