GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Desafíos para las autoridades de justicia penal en materia de ciberdelincuencia en América Latina y el Caribe

Webinar 8 de mayo de 2020 - Preguntas

Miguel Monzón: Buenos días, ¿en qué medida está afectando la suplantación de identidad en el sector bancario o asegurador en la República Dominicana?

Claudio Peguero: No tengo cifras, pero sé que afecta bastante, en mi experiencia personal en el sector hace unos 5 años este era un componente importante del fraude.

Jose R. Gratereaux: Sabemos que se está trabajando para que todo se maneje de manera digital, sobre todo las denuncias, porque no tratan las denuncias como pasa en el 911, que las reciben vía teléfono, No lo contemplan Uds. recibirlas igual o vía un correo para trabajarla preliminarmente?

Claudio Peguero: Esto no depende de la Policía, sino de todo el sistema de administración de justicia en su conjunto, principalmente el Poder Judicial. Hemos venido trabajando en esto desde hace varios meses y se han logrado algunos avances. Hace unos días el Consejo Superior del Poder Judicial emitió la política POL-DTI-DTI-001 adoptando el uso de firmas digitales en sus procesos.

Jose R. Gratereaux: Veo que menciono el tema de las de únicas de los ciudadanos. Quisiera saber si Uds. han visto o manejado en RD fraudes o ataques a los programas de ayuda del gobierno?

Claudio Peguero: Sí, hemos visto varias campañas de phishing y smishing sobre los programas de ayuda del gobierno FASE y Quédate En Casa a través de la Tarjeta Solidaridad.

Vanessa Fusco: Estimado Profesor - Lo que piensa sobre la cadena de custodia en tema de prueba digital: están los actores de sistema de justicia capacitados para manejar y garantizar la integridad de esta prueba?

Marcos Salt: Gracias por la pregunta Vanessa. Sin duda a nivel regional, el tema de la capacitación de los operadores es una de las prioridades. Sin perjuicio de ello, es necesario realizar algunas precisiones. En muchos países ya están funcionando fiscalías especializadas, unidades policiales y cuerpos de investigadores judiciales que muestran un alto grado de capacitación y eficiencia en el trabajo con pruebas digitales.

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

El tema de que la evidencia digital adquiera cada vez más importancia en la investigación de cualquier delito nos obliga a pensar en programas de capacitación que alcance no solamente a las unidades especiales sino a todos los operadores del sistema penal.

En este sentido, mi idea es que hay que pensar en programas de capacitaciones básicos para todos los operadores del sistema y capacitaciones profundizadas para las unidades especializadas que tendrán que lidiar con los delitos informáticos y las cuestiones de prueba digital más complejas. Jueces, fiscales y abogados penales tendremos que capacitarnos en este tema y las facultades de derecho de la región deben incluir en sus programas de estudio todo lo relativo a los aspectos procesales de la prueba informática.

También resulta importante establecer protocolos básicos de cadena de custodia como guías.

Elizabeth Tenorio Reyes: para asumir este cambio de paradigma considera hacer cambios de forma inicial en la teoría del delito? y con ello sentar los cambios en los apartados procesales?

Marcos Salt: No creo que sea necesario adecuar los principios de la teoría del delito o cambios en las normas de la parte general de los CP. Sin perjuicio de ello, exigirá un trabajo importante de análisis dogmático de los tipos penales que prevén los delitos informáticos para hacer frente a su aplicación frente a realidades diferentes que plantean estos delitos.

La adecuación de las normas procesales entiendo que esta urgida por la necesidad de nuevos medios de prueba que no fueron regulados en los CPP que están pensados para el mundo físico.

Sergio Castillo Quesada: La utilización del concepto: identidad digital como elemento de tipicidad, en el tipo penal de suplantación de identidad digital establecido en el articulo 139 ter (Argentina), ha presentado algún tipo de discusión en cuanto al significado de identidad a nivel jurisprudencial?

Marcos Salt: El artículo al que haces referencia no ha sido sancionado. La Argentina no tiene aún tipificado del delito de mera suplantación de identidad en el CP. El proyecto de ley no fue tratado aún por el poder legislativo.

En el ámbito de la Ciudad de Buenos Aires se ha previsto la suplantación de identidad como contravención.

Hector Martinez: La prevención de delitos involucra la seguridad en los servidores y navegadores utilizados en internet. Siendo estos recursos que están fuera del control nacional, se dispone de recursos legales hacia las transnacionales que proveen esos productos para asegurar que se prevengan los ciberdelitos?

Marcos Salt: Claramente la prevención requiere de medidas de ciberseguridad y No es posible que un estado imponga a otros Estados medidas de ciberseguridad, más allá de los acuerdos internacionales.

En relación al sector privado, es posible pensar en requisitos y condiciones para empresas que operan en el territorio de cada país. Asimismo cada país fija su propia política de ciberseguridad en la que la prevención ocupa un lugar fundamental.

Hector Martinez: Los delitos requieren legalidad anticipada para poder aplicarles esa legalidad. Que tanto anticipo a formas delincuenciales en formato cibernético se puede aplicar a las actualizaciones legales por hacerse?

Marcos Salt: Una buena legislación penal debería prever tipos penales con la suficiente neutralidad tecnológica para no requerir adecuaciones permanentes.

La convención es un buen ejemplo en este aspecto. Los tipos penales previstos todavía tienen vigencia hoy aún cuando cambiado de manera significativa muchas de las formas de comisión por ejemplo de los fraudes informáticos o de los daños a sistemas informáticos.

Vanessa Fusco: Cómo vieron los delitos contra niños en la pandemia? Hubo un aumento de las denuncias de crímenes de distribución de material con abuso sexual infantil?

Fredy Bautista: Sí, se ha evidenciado un incremento en el número de casos de distribución de casos de abuso sexual infantil en Internet y las tendencias también cambian y ahora se enfocan en el material autogenerado por menores de edad, niños niñas y adolescentes, desde sus propios teléfonos celulares, en ocasiones a cambio de dinero en criptoactivos o monedas virtuales muchas de ellas también vinculadas a plataformas de juegos en línea.

Algunas fotografías tienen como destino pares o amigos (conocidos) de las victimas por prácticas vinculadas al Sexting, sin embargo ese material, puede llegar a foros en línea de distribución.

Antonio Piña Alonso: La legislación europea en materia de investigación de delitos cibernéticos ha ido incorporando nuevos derechos, como el derecho del entorno virtual, reforzando la protección del ciudadano frente a la injerencia policial. ¿Cómo valora la actual situación en el ámbito de la región?

Marcos Salt: A nivel jurisprudencial Hay importantes resoluciones de los tribunales de casación y las cortes supremas de los diferentes países. Entiendo que sería importante un mayor desarrollo por parte de la CIDH y la CIDH.

A nivel constitucional hay países que han incorporado algunos derechos (por ej. Habeas data, autodeterminación informativa). También en materia legislativa se ha avanzado en la regulación de la protección de datos personales. Sin embargo, creo que uno de los temas en los que existe un cierto atraso. Fundamentalmente es necesario regular las garantías frente a las nuevas herramientas probatorias que permite la tecnología informática. Esto torna más urgente la reforma procesal a la que hice referencia en la charla.

Emilio Porras: En la cooperación asimétrica Estado-empresa proveedora de servicios de internet, que validez probatoria tiene la información obtenida en la medida en que implica prescindir de los canales formales cuyo valor radicaba en la fiabilidad que otorgaba a la evidencia gestionada entre autoridades públicas?

Camila Bosch Cartagena: El valor probatorio de la información obtenida de manera directa de los proveedores de servicios que se encuentran en otros países, dependerá de las leyes procesales internas de cada país. En Chile, no hemos tenido problema de admisibilidad de este tipo de pruebas ya que la única información que obtenemos de proveedores de servicios extranjeros es información de abonado (ver definición de este concepto en el artículo 18.3 Convenio de Budapest) la cual no infringe garantías fundamentales. Tampoco se ha objetado por falta de fiabilidad ya que se incluye toda la información respecto a cómo se solicitó la prueba y cómo se obtuvo.

Claudio Peguero: Esta cooperación asimétrica que describe está respaldada en órdenes judiciales del Estado requirente atendiendo a la presencia (física o virtual) de ese proveedor en su territorio, por lo tanto tiene las mismas formalidades de un caso domestico.

Marcos Salt: En la jurisprudencia se ha admitido esta prueba, generalmente como "noticia del delito" en los casos de informes que dan inicio a las causas o como indicio o fuente de nuevas pruebas. No solamente hay un problema de validez sino también de fiabilidad a la hora de la valoración en un juicio. De allí la importancia de no utilizar esta prueba como prueba única sino validarla con otros elementos. Por estos motivos es fundamental el avance del protocolo adicional que va a dar más certezas.

Emilio Porras: En la medida en que la tecnología es transversal a todos los delitos y que la investigación penal es multidisplinaria, considera como mejor opción crear equipos técnicos de asesoramientos a los fiscales abogados antes que fiscalías especializadas?

Camila Bosch Cartagena: En mi opinión, efectivamente todo fiscal o abogado que trabaje en el sistema penal debe tener conocimientos sobre evidencia digital y cibercriminalidad, ya que cómo se señaló en la presentación, para cualquier investigación podremos usar evidencia en formato electrónico para acreditar hechos relevantes.

Sin embargo, las fiscalías especializadas también son relevantes dado que pueden tener un rol en causas de alta complejidad y que puedan resolver de manera más efectiva dada sus conocimientos y experiencia en la materia.

Claudio Peguero: Los procesos de formación que estamos llevando a cabo en República Dominicana para Fiscales y Jueces en la Escuela Nacional del Ministerio Publico y la Escuela Nacional de la Judicatura respectivamente están orientados a dotar a todos los Fiscales y todos los Jueces de las herramientas básicas necesarias sobre evidencia digital ya que ciertamente está presente en casi todos los delitos. No obstante, el **delito informático** *per se* requiere de un nivel mucho mayor de especialización en muchos temas que hacen necesario, de momento, la existencia de unidades especializadas de fiscalía y de policía.

Marcos Salt: Creo que ambas opciones son válidas y hay experiencias positivas de ambas formas de fiscalías en la región. Depende de las necesidades y formas de organización de cada país y provincia.

Sin duda es necesario que todos los fiscales adquieran conocimientos sobre la materia y que cuenten con equipos de apoyo técnico.

En el futuro creo que las especializadas estarán destinadas a delitos informáticos específicos y de mayor complejidad.

Fidel Jeldes: Puede crearse una fuerza internacional para cybercrime?

Claudio Peguero: En cierto modo ese es el rol de INTERPOL y de las distintas redes 24/7. Existe una cooperación internacional que va en crecimiento sobre el tema de los ciberdelitos, aunque por supuesto aun nos falta bastante por desarrollar y mejorar.

Fredy Bautista: Existen iniciativas globales como los JCAT Join CyberCrimeTask Force que buscan combinar esfuerzos de muchas unidades policiales especializadas en investigar cibercrimen, bajo el liderazgo o iniciativa de Europol e Interpol. Estos esfuerzos deben considerarse acompañados de Fiscales y ministerio público.

Mario Mafud Ledesma Harón: ¿Es muy pretencioso pensar que desde un organismo internacional (como la comunidad europea por ejemplo) pueda crear un área que pueda acceder, mediante un convenio con la empresas de servicios de Internet (ej. Facebook) para dar respuestas más ágiles y adecuados al sistema judicial?

Camila Bosch Cartagena: El problema principal para la entrega de información por parte de los proveedores de servicio radica en las leyes de datos personales, así como también en los contratos de prestación de servicio que dichos proveedores tienen con sus suscriptores. Esas son las dos principales limitaciones que los ISP pueden tener para poder entregar información, sobre todo si se trata de autoridades extranjeras (es decir, autoridades de países distintos a aquellos donde el ISP se encuentra situado). Estos problemas tendrían que ser abarcados por el convenio propuesto.

El Segundo Protocolo de Budapest (sobre obtención de evidencia digital en la nube), que se encuentra en redacción dentro del Consejo de Europa, intenta hacer frente a este tipo de problemas pero no pensando en un convenio con los proveedores de servicio sino que, buscando maneras de permitir la cooperación directa entre las autoridades extranjeras y los proveedores de servicio, como también agilizando los métodos existentes de cooperación internacional.

Claudio Peguero: Se ha discutido bastante con los proveedores de servicios "globales" y varios Estados la idea de crear un portal único para este tema. Es una idea aun en desarrollo.

Marcos Salt: Creo que los organismos internacionales deben trabajar en generar instrumentos para que la justicia de cada país pueda obtener respuestas adecuadas. Este es el objetivo del Protocolo adicional.

Daniel Ríos: Teniendo en cuenta el aumento en el número de denuncias de ciberdelitos y contrastado con el bajo margen de sentencias penales condenatorias como respuesta jurisdiccional a dichas denuncias: ¿Cómo mejorar los índices de aplicación de la justicia en entornos digitales?

Camila Bosch Cartagena: No existe una única solución para mejorar la persecución penal de los delitos informáticos o de los delitos cometidos a través de medios informáticos, pero creo que hay dos factores que son claves: la primera es crear capacidades nacionales a través de aprendizaje tanto técnico como jurídico respecto a cómo perseguir el cibercrimen dadas sus características. En este sentido, es necesario que quienes sean los llamados a investigar estos delitos se especialicen en conocer el fenómeno y estén constantemente capacitándose al respecto dado la rapidez con la que avanza la tecnología. Cómo segundo factor clave es importante que exista una inversión para dotarse de herramientas que permitan investigar y realizar análisis forense de la evidencia digital.

Marcos Salt: Reforma de los ordenamientos procesales; Capacitación de los operadores del sistema penal; Mejoramiento de los canales de cooperación internacional; Reformas institucionales en los diferentes países.

PANEL

Claudio PEGUERO, General de Brigada, Asesor en Asuntos Cibernéticos del Director General de la Policía Nacional, Miembro en el Comité Directivo (T-CY) de la Convención de Budapest, Coordinador Nacional del Proyecto GLACY+, República Dominicana

Marcos SALT, Profesor de Derecho Penal y Derecho Procesal Penal, Universidad de Buenos Aires, Miembro en el Comité Directivo (T-CY) de la Convención de Budapest, Argentina

Camila BOSCH CARTAGENA, Abogada Asesora, Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado, Fiscalía Nacional, Chile

Fredy BAUTISTA, Coronel (Reserva Policial), Policía Nacional de Colombia, fundador y primer director del Centro Cibernético, experto en Ciberseguridad, Investigación de Cibercrimen y Perito en Informática Forense, Colombia