LA TECNOLOGÍA EN EL DESARROLLO DEL PROCESO PENAL

Centro de Formación de la Cooperación Española
Cartagena de Indias, Colombia
3 al 5 de diciembre de 2018

GOBIERNO DE ESPAÑA
MINISTERIO DE JUSTICIA
MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
aecid
Cooperación Española

INTRODUCCIÓN

"Nuestros datos personales son disponibles. Lo que se aloja en las redes, queda en las redes":

La irrupción del ámbito digital en el mundo cambió ostensiblemente las dinámicas de nuestra vida en sociedad. Desde nuestras relaciones interpersonales, hasta el sentido unidireccional que tenía la comunicación, arrebatándole a la prensa tradicional el monopolio de la información y por ende, estimulando su democratización. Su advenimiento es parte fundamental del fenómeno globalizador que borró fronteras y plantó bandera en ese intangible y hoy lóbrego universo del ciberespacio.

Las nuevas tecnologías crearon ciudades invisibles que forman unas maneras distintas de comunicación e interacción, pero que no hacen parte del Estado-Nación, simplemente son una especie de realidad paralela con sus propias tensiones, conflictos y complejidades. Esto supone unos retos superlativos que los países han tardado en estudiar para poder adaptarse a estas nuevas 'realidades' virtuales, que por supuesto, ya no son un tema menor. "La prueba digital ya no es una novedad, pues casi todos dependemos de los teléfonos celulares y smartphones".

LO DIGITAL LLEGÓ AL ESCENARIO JUDICIAL

El uso de pruebas digitales en los procesos judiciales crece todos los días. En la actualidad, la gran mayoría de los casos de derecho civil, penal, familiar o laboral incluyen pruebas virtuales que van desde conversaciones en WhatsApp hasta el registro de la huella en el celular, pasando por correos electrónicos, videos y 'escuchas grabadas'. Todo lo que se escriba o grabe en una plataforma digital, red social o aplicación ya cuenta como prueba en el proceso.

El uso excesivo de dispositivos digitales nos hace más vulnerables al rastreo y pone en riesgo la seguridad de nuestros datos e información personal, de allí el esfuerzo global en procura de una normativa precisa para su protección, ya que como los datos son el petróleo del siglo XXI.

Otra de las preocupaciones recurrentes que inquieta a los operadores judiciales locales, es que hay países que dentro de su ordenamiento jurídico tienen unos protocolos que deben cumplir al momento de la obtención, valoración e incorporación de la prueba, estos son: procurar su integralidad, es decir, no alterar e intervenir el material recabado ni afectar derechos fundamentales como la privacidad. Y si la información no es pública, es menester pedir al juez una orden judicial para que la plataforma digital proporcione la información requerida.

En ese sentido, se alerta sobre una normativa de información de acceso público que está volcada en interpretaciones erróneas, pues, por ejemplo, en algunos países la Policía usa Twitter para publicar datos del imputado violando así la presunción de inocencia.

DERECHOS FUNDAMENTALES Y PRUEBA DIGITAL

"Pasamos de robar gallinas a hacer estafas en internet"

En la actualidad, la aportación de la prueba digital es cada vez más regular en las jurisdicciones, es común y recurrente el uso de las tecnologías en el ámbito de la administración de justicia. Este crisol de fuentes probatorias debe incorporarse al proceso judicial a través de procedimientos y protocolos legalmente previstos.

En la obtención de la prueba digital, se debe garantizar la autenticidad e integralidad de la misma; es decir, en el primer concepto debe existir la certeza sobre la persona que lo ha elaborado o de quien se atribuya el documento; y la segunda, consiste en garantizar que no haya sufrido ninguna alteración o intervención. Las pruebas obtenidas con violación del debido proceso son nulas de pleno derecho y si se rompe un protocolo de custodia es muy difícil salvar la prueba.

Desde esta perspectiva, se establecen la diferencias entre prueba digital (PD) y el documento electrónico; la PD es 'toda información con valor probatorio que es almacenada o transmitida de forma digital o binaria'; mientras que el documento electrónico es 'un escrito, comunicación, imagen, dibujo, programa o información de cualquier tipo, ya sea que se encuentre almacenado o se mantenga en papel, en medios electrónicos, de audio, visuales, o cualquier otro', son dinámicos y pueden ser alterados y modificados en cualquier momento.

La evidencia electrónica es la recabada mediante el uso de medios análogos, es decir, la grabación de una conversación telefónica. La PD yace en formatos lógicos y se aplican procedimientos y requerimientos diferentes. Todas estas pruebas se reciben pero deben estar sometidas a valoración, contraste y peritaje.

Existen tres fases de la identificación y uso de la prueba digital: la obtención de la información donde las partes en conflicto deben acceder a aquella de forma lícita y sin violar los derechos fundamentales; en la incorporación de los datos al proceso, se deben cumplir los requisitos de pertinencia, necesidad, licitud y admisibilidad procesal. Previo cumplimiento de los pasos anteriores sobre obtención e incorporación, la prueba digital será objeto de valoración por parte del juez o tribunal. Es importante acudir al control horizontal, esto quiere decir, que la parte contraria conozca la prueba. La evidencia o prueba digital debe someterse a un riguroso análisis pericial.

CONCEPTO, LICITUD Y OBTENCIÓN DE LA PRUEBA DIGITAL

"Creamos Internet para ser libres pero al final terminamos poniéndonos los grilletes":

El delito informático o 'ciberdelito' aumenta vertiginosamente en tanto el espectro de internet se amplía, a pesar de que los niveles de riesgo se reducen. Estos delitos requieren un esfuerzo probatorio adecuado. Los más populares: El phishing, método que un hacker usa para obtener información sensible o personal de un nativo digital; las estafas de robo de identidad, donde el 'ciberdelincuente' tiene acceso a las cuentas bancarias; el acoso en redes, cyberbullying o cyberacoso, frecuente sobre todo en las redes sociales; el sexting, que es el envío de mensajes pornográficos a través de teléfonos celulares; y el grooming, que es el acoso sexual a menores de edad en la red.

La naturaleza virtual de este tipo de prueba, demanda que su documentación se haga a través de la captura de los archivos informáticos que contienen los metadatos que acreditan su existencia. Es necesario entonces una evidencia electrónica, una suerte de soporte susceptible de almacenar información digital con la finalidad de acreditar hechos ante los Tribunales. No obstante, para que una evidencia electrónica sea admitida ante el operador judicial, se deben cumplir los siguientes requisitos, no sin antes recordar, que la prueba se debe obtener de manera lícita para que sea valorada en juicio.

1. Licitud: en el proceso de obtención de la evidencia digital, no se puede vulnerar el derecho a la intimidad del afectado ni el secreto de las comunicaciones.

2. Integridad: el soporte no puede tener ningún tipo de alteración o intervención.

3. Autenticidad: garantizar que la evidencia aportada es idéntica a la muestra original, preservada a través de la cadena de custodia, lo cual garantiza que no ha sido manipulada en el proceso de acceso, obtención, transferencia y almacenamiento de los datos.

4. Claridad: imprescindible la figura de los peritos informáticos en el ejercicio de la prueba pericial. Existe en la mayoría de países latinoamericanos un déficit de dicha figura, haciendo así más complejo el proceso de valoración e incorporación de la

evidencia en el proceso penal por su naturaleza digital.

La incorporación de la prueba digital en un proceso nacional, cuyo origen ha sido otro país distinto, requiere de las autoridades un esfuerzo importante en orden a no presentar como absoluto un principio de no indagación del origen de esa prueba, pero tampoco de una incorporación de manera absoluta sin tener en cuenta los principios básicos de respeto a los derechos fundamentales. Es necesaria una cierta armonización legislativa y de estándares de incorporación de prueba transnacional en materia digital.

INCORPORACIÓN AL PROCESO DE LA PRUEBA DIGITAL

"Se intervienen las comunicaciones solo cuando hay indicios delictivos":

Las tecnologías de la información y las comunicaciones –TIC- han reconfigurado las dinámicas sociales, desde lo laboral hasta lo afectivo. Esas relaciones digitales a través de mensajes vía WhatsApp, correo electrónico, chat de Facebook e Instagram, Inbox en Twitter, dejan vestigios digitales; en consecuencia, la prueba que se aporta en juicio proviene de un soporte digital.

Esta nueva realidad probatoria plantea varios dilemas por resolver: la evolución constante de medios tecnológicos, la insuficiencia normativa, la incorporación al procedimiento, la falta de medios para su verificación y análisis, y la falta de conocimiento por parte de los actores que intervienen en la administración de justicia.

Ahora bien, como se destacó arriba, en el ámbito judicial cada vez es más frecuente la aportación de pruebas de origen digital en juicio, se hace entonces necesario definir el protocolo adecuado para aportarlos y que adquieran pleno valor probatorio en el proceso judicial. La prueba digital puede incorporarse al proceso conforme a los diferentes medios de prueba, ya sea través de su impresión en formato papel, mediante la aportación de los propios documentos electrónicos (públicos, oficiales y privados), la grabación de la prueba testifical o interrogatorio del investigado; el reconocimiento judicial o inspección ocular, destacando a este respecto la pericial informática.

Las principales modalidades de las fuentes de prueba digital son: El correo electrónico y los datos asociados, WhatsApp y otros sistemas de mensajería instantánea, mensajes SMS, los mensajes a través de las redes sociales como Facebook, Twitter, Google+, Tuenti, Instagram, Snapchat, Badoo y páginas web.

Cuando el proceso judicial está en soporte papel, lo habitual es convertir toda la prueba a documento escrito en papel para su incorporación al procedimiento, sin perjuicio de los soportes digitales que se puedan adjuntar como piezas de convicción. No obstante, ya existen sistemas procesales que se documentan en soporte digital, así está sucediendo en muchos de los órganos judiciales de España; en este caso puede incorporarse la prueba digital en su propio formato electrónico para su valoración en el procedimiento, audios, videos o documentos informáticos, hasta el punto que los atestados policiales, (Documento oficial redactado por la Policía en el que se explica cómo se ha producido un delito), se remiten a través de una red segura de comunicación (Lexnet); del mismo modo, las declaraciones practicadas en instrucción y los juicios se graban, quedando incorporadas al proceso mediante la firma electrónica del Letrado de la Administración de Justicia.

En el proceso penal español, resulta trascendental la LO 13/2015 al introducir una novedosa regulación sobre las medidas de investigación tecnológica y que requieren autorización judicial al limitar derechos fundamentales, a este respecto cabe destacar: la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos de seguimiento y localización, así como el registro de dispositivos masivos de información y registros remotos de equipos informáticos.

Es necesario hacer énfasis en el registro de dispositivos masivos de información, es decir, en la incorporación al proceso judicial de la información contenida en ordenadores, cedés, deveudés, memorias digitales, pendrives, discos duros externos, teléfonos móviles, tablets, servidores, routes, GPS, así como en la información contenida en la nube (icloud, Dropbox, drive), y especialmen-

te la necesidad de autorización judicial para el acceso y registro de estos dispositivos. Sobre este particular, se deben adoptar las cautelas necesarias para asegurar la integridad de los datos, especialmente en el volcado de la información contenida en estos dispositivos y en la cadena de custodia.

Por último, se subraya la importancia de los métodos más modernos de investigación tecnológica como el registro remoto de dispositivos informáticos, que consiste en la instalación de un software para el examen a distancia del dispositivo y sin conocimiento del titular, lo que supone una medida muy invasiva en los derechos fundamentales del investigado y, por tanto, de uso restringido a determinadas investigaciones.

CIBERDELINCUENCIA, RETOS DE LA INVESTIGACIÓN CRIMINAL

"La tecnología ofrece anonimato y el anonimato envalentona al delincuente, a quien le toca crear espacios de impunidad para protegerse del Estado":

Las redes sociales, más que ecosistemas digitales de interacción e información, debate y controversia, se pensaron con un fin de lucro, de ahí el advenimiento del comercio electrónico que ha puesto nuestros datos personales en riesgo ante la ciberdelincuencia. Todo lo estamos haciendo on line, compras, operaciones bancarias, pagos electrónicos, etcétera. En esta era de las transacciones digitales, la piratería, la falsificación o clonación de datos y la publicación de contenidos ilegales, son algunas de las actividades delictivas más frecuentes.

Casos recurrentes de ciberdelincuencia informática, entre otras mencionadas, son la suplantación de identidad, el robo de información personal como claves bancarias, y la distribución de virus informáticos. Lo preocupante es que el número de 'ciberdelitos' aumenta y las actividades delictivas se están sofisticando e internacionalizando cada vez más, para lo cual se requiere cooperación entre los países para desarticular estos delitos informáticos. Urge entonces la armonización de la legislación para una adecuada cooperación internacional. Por corregir está que la mayoría de países no cuentan con las herramientas técnicas ni tecnológicas para enfrentar el 'cibercrimen', la creación de unidades especializadas de los órganos de Investigación penal y de una agencia de protección de datos. Y lo más importante: corregir la ausencia de normas sobre la obtención de pruebas digitales.

LOS DELITOS DE LA VIOLENCIA DE GÉNERO COMETIDOS A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS

"La libertad de expresión no legitima la injuria, calumnia e incitación al odio y a la violencia".

A lo largo de este curso se ha destacado cómo las nuevas tecnologías han trastocado las relaciones interpersonales, introduciendo nuevas herramientas para el contacto humano que acarrean riegos jamás pensados. Internet genera espacios donde se expone la vida personal, lo cual supone otras formas de relaciones afectivas que pueden traer consigo violencia contra las mujeres. La violencia de género tiene nuevas formas de manifestarse, de tal forma que los delitos tradicionales como las amenazas e injurias se pueden cometer a través de Whatsapp o las redes sociales, lo que provoca nuevas formas de cometer los mismos delitos, pero con novedosos medios probatorios.

También surgen nuevas figuras criminales, que no solamente afectan a las mujeres sino también a la comunidad LGTBI, como puede ser el sexting (transmitir imágenes íntimas de la víctima que se obtuvieron con su consentimiento), stalking (acoso u hostigamiento que altera el desarrollo de la vida cotidiana de la víctima) y la usurpación de identidad en la red (utilizar los datos de un tercero en su perjuicio para hacerse pasar por él en la red).

El discurso de odio y estigmatización en las redes sociales

El anonimato envalentona. Las redes sociales permiten incrementar la comunicación personal pero también sacar lo peor de nosotros; los algoritmos crean una peligrosa burbuja ideológica que solo nos muestra lo que queremos leer y ver de acuerdo a nuestra ideología, gustos e intereses. Se usa como arma política para dividir porque ataca a la emocionalidad del 'ciberusuario' que comparte fakenews indiscriminadamente sin

verificar su contenido solo porque refuerza sus prejuicios y emociones.

Miles detrás de una pantalla, bajo el anonimato, destilan veneno contra sus contradictores, fabulando intrigas, imputando falsos delitos y dañando el buen nombre de terceros. Por eso se dice que ya no existe el derecho a libre expresión sino al de la injuria y la calumnia. Lo preocupante es que no hay un tipo penal adecuado que ponga freno a este fenómeno por la tensión de derechos que prevé. Sin embargo, en Colombia la Corte Constitucional hizo un llamado para que los ciudadanos pongan límites a sus publicaciones o denuncias en las redes sociales, tras señalar que cualquier tipo de afirmaciones "deben estar debidamente soportadas y corroboradas con el fin de que se cumplan los requisitos de veracidad e imparcialidad".

Este llamado de atención se hizo en abril de este año luego de analizar dos tutelas en los cuales a la víctima se le vulneraron sus derechos al buen nombre y honra. De acuerdo con la Corte, en el caso de información publicada en redes sociales debe existir la misma rigidez que en un medio de comunicación y "Deben aplicarse las mismas reglas para el correcto ejercicio de libertad de expresión". Y añade que "La libertad de expresión no es un derecho que carece de límites"; es por eso que el uso frases injuriosas, insultos, expresiones desproporcionadas y humillantes, pueden vulnerar los derechos fundamentales de terceros.

Separar los conceptos de intimidad y privacidad

Las técnicas de captación, tratamiento y almacenamiento de datos están en constante evolución y hacen de la esfera de la intimidad un ámbito susceptible de ser transgredido con facilidad, debate recurrente durante el Curso.

Intimidad y privacidad son conceptos diferentes con un régimen de protección distinto.

El concepto de privacidad es más amplio que el de intimidad cuyo alcance es más restringido, pues protege la esfera en la que se desarrollan las facetas más reservadas de la vida de una persona: su entorno familiar, su trabajo, su credo, sus preferencias sexuales y afinidades políticas, por ejemplo.

El artículo 18 de la Constitución española protege la intimidad a través del derecho al honor, a la intimidad personal y la propia imagen, la inviolabilidad de las comunicaciones, etcétera. Un dato privado por el contrario revela rasgos de nuestra personalidad que quizá queramos mantener en reserva y que merecen protección como gustos personales, pasatiempos, necesidades que, tomados en conjunto, arrojan un perfil de la persona. Las plataformas tecnológicas toman esos datos, los cruzan y mantienen en el tiempo, por lo que se hace necesaria la limitación y reglamentación de su uso. De allí surge la imperiosa necesidad de legislar en favor de la Protección de datos.

Protección de datos y derecho a la confidencialidad

"Una cosa es ceder el dato y otra captar el dato, que debe tener una finalidad específica":

La normativa respecto a la Protección de datos debe ser clara y precisa. Algo así como un tutorial. Trasciende la propuesta para la conformación de una agencia de Protección de datos para hacer cumplir la normativa local, (en España, existe la Agencia española se protección de datos).

Se cuestionó cómo en algún caso las empresas y entidades estatales negocian o mercadean con los datos de los ciudadanos. "En algunos países el tema está reglamentado pero no se cumple". Se propone firmar convenios con las empresas y organizaciones para tener acceso a los datos, pues uno de los inconvenientes a la hora de captar la evidencia electrónica para un proceso judicial como las escuchas telefónicas, es precisamente que los operadores no son proclives a colaborar, tal como pasa con las compañías transnacionales de mensajería instantánea.

Pero ¿Qué son datos personales? Es toda aquella información asociada a una persona y que permite su identificación. Su documento de identidad, lugar de nacimiento y residencia, estado civil, edad, trayectoria académica, laboral, o profesional. Existe también información de carácter privado como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros. Los datos, previo consentimiento, se recogen de diferentes maneras, a través del diligenciamiento de un formulario para adquirir un producto bancario, por ejemplo. Asimismo, se establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación: Dato Público, el que la Constitución determina como tal; el Semiprivado, que no tiene naturaleza

íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas; el Privado, es aquel que por su naturaleza íntima o reservada sólo es relevante para el titular de la información; y el Sensible, que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

En España recién se publicó en el Boletín Oficial del Estado, la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD), armonizado con la normatividad europea, que introduce nuevos derechos digitales que afectarán a las empresas, instituciones y ciudadanía en general. Uno de los componentes más relevantes es el 'Consentimiento expreso', acorde a las exigencias europeas, y en su artículo 6, reza textualmente, que cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades «será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas». Por otra parte, se amplían las albaceas digitales para que los familiares de usuarios fallecidos dispongan de su 'testamento digital'.

Y por último, uno de los más importantes y que tendrá mucho impacto en la sociedad española, por el conflicto que existe frente a la publicación de información falsa, injurias y calumnias en redes sociales que dañan la honra

y el buen nombre de las personas, es el derecho de rectificación y supresión: «Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en internet y el derecho a comunicar o recibir libremente información veraz». De esta manera, los medios de comunicación digitales deberán atender la solicitud de rectificación formulada contra ellos y proceder de inmediato a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo, la cual deberá aparecer en lugar visible junto con la información original.

LA INVESTIGACIÓN A TRAVÉS DE LOS DATOS ASOCIADOS A LAS COMUNICACIONES ELECTRÓNICAS. UNA HERRAMIENTA EN EL PROCESO PENAL

Los datos asociados a las comunicaciones electrónicas –DACE- son una herramienta fundamental en las investigaciones criminales y son invaluables para el Proceso Penal de cara a la valoración judicial como prueba durante el acto de juicio oral. EL DACE es el conjunto de datos que permiten identificar a los intervinientes en un proceso de comunicación, el lugar, tiempo, soporte y los dispositivos usados, pero nunca el contenido de la comunicación.

Al respecto surgen varios dilemas: Con la premisa de luchar contra la delincuencia, ¿Puede una norma nacional establecer que se conserven de manera generalizada e indiscriminada todos los datos de tráfico y localización de todos los abonados y usuarios registrados en relación con los medios de comunicación electrónica?, ¿en qué casos procede?, ¿acaso en casos de delincuencia grave o seguridad nacional?, ¿cómo actúa la conservación del DACE y cómo se resuelve una investigación con estos datos?

En la determinación de la ubicación espacio-temporal relativo de un homicida respecto de su víctima en un lugar de España, por ejemplo, el DACE ofreció únicamente una estimación pericial de la posición relativa de los teléfonos celulares de los actores del delito, que resulta de gran valor orientativo para la investigación y relativo como prueba para el proceso penal. Sirve también para refutar coartadas.

Al respecto, surgió un debate final en el Curso, en el sentido de la ponderación y balanceo de derechos fundamentales con relación al rastreo indiscriminado vía DACE de un sindicado, Se hace énfasis en señalar que "A la autoridad no se le puede permitir inmiscuirse indiscriminadamente en la intimidad de las personas", pues los "ciberdelitos son de complicado rastreo y se dilata la recolección de la prueba por el cumplimiento de los protocolos establecidos por el ordenamiento jurídico que realmente deben ser estrictos porque se está afectando la vida de un ciudadano que todavía tiene la presunción de inocencia incólume".
Es importante entonces insistir en que el proceso de recolección de la prueba digital o DACE, no lleve a la vulneración de derechos fundamentales de manera indiscriminada anteponiendo otros sin hacer un juicio ponderado". Para ello se aclaró en todo caso que cualquier cesión y autorización de uso de datos asociados contará siempre con la supervisión de las autoridades judiciales en sentido amplio, la garantía de jurisdiccionalidad ha sido incorporada aunque se tienen que explorar caminos para una cesión y utilización de esos datos en casos urgentes o en aquellos supuestos donde no está comprometida de manera evidente la defensa de un derecho fundamental de las personas.

GOBIERNO DE ESPAÑA
MINISTERIO DE JUSTICIA

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

aecid

Cooperación Española