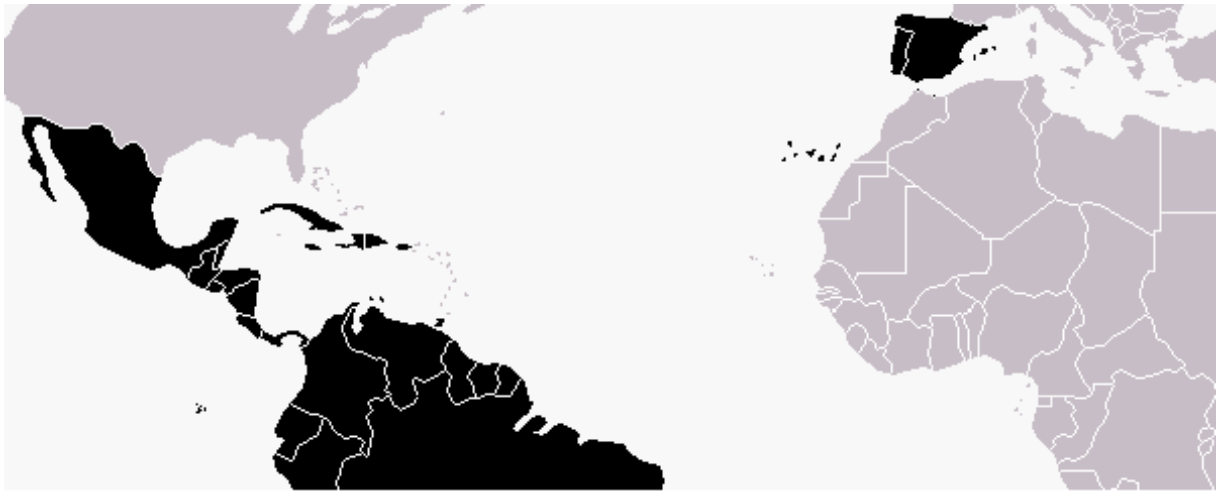

Declaración de Barranquilla, hacia la unificación de instrumentos jurídicos para la protección de la privacidad en Iberoamérica [1]

Los avances de las tecnologías de la información y la comunicación han cambiado radicalmente nuestro día a día tanto a nivel personal como a nivel profesional. Son muchas las ventajas y utilidades que nos aportan, pero como toda herramienta usada por el ser humano, también es susceptible de ser utilizada con fines ilícitos de toda clase, delitos electrónicos que tienen su razón de ser a través de la red, así como cualquier tipo de delito informático, relacionado con la información y los datos.

Diariamente conocemos casos de amenazas a través de virus o programas informáticos dañinos (malware) que circulan libremente por Internet instalándose en nuestros dispositivos. Unas veces tratan de provocar daños en los equipos y redes informáticas, otras veces tratan de robarnos información o espiarnos (Spyware). Estas mismas amenazas se reproducen por ataques dirigidos por humanos (hackers) que los realizan con idénticas finalidades. Las motivaciones y finalidades de estos actos delictivos pueden ser tantas como autores las lleven a cabo, puesto que en algunos casos será

[1] *La Declaración de Barranquilla, hacia la unificación de instrumentos jurídicos para la protección de la privacidad en Iberoamérica, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en la ciudad de Barranquilla (Colombia), el 1 de junio de 2013, por el Juez Alexander Díaz García, en el transcurso del Congreso en Seguridad Informática y Telecomunicaciones.*

para obtener información para vender, plagiar o chantajear y en otros casos será para satisfacer un mero ego "intelectual".

De la misma manera, los delitos tradicionales han encontrado en las nuevas tecnologías una vía de ampliar el número de actos delictivos o simplemente quedar amparados en un supuesto "anonimato". Las tradicionales estafas y suplantaciones de identidad han encontrado nuevas variables como el phishing. La obtención de material sexual de menores llegando incluso al acoso o abuso sexual (grooming), ha encontrado un terreno propicio ya que a través del correo electrónico, mensajería instantánea o redes sociales se puede contactar con los mismos induciendo al error por medio de perfiles falsos y, lo que resulta mas preocupante, sin que pueda llegar a percatarse un adulto. Tampoco hay que olvidar que estas tecnologías también facilitan el intercambio de material sexual de menores por parte de los pederastas. Pese a ser los mismos delitos, pero la cantidad de víctimas potenciales es peligrosamente mayor, por la facilidad en el acceso a las mismas y la posibilidad de mantenerse, el delincuente, en el anonimato.

Igualmente, otros tipos delictivos han comenzado cometerse a través de las nuevas tecnologías. Amparados en un "falso anonimato" y una falsa creencia de "impunidad", comienzan a proliferar los delitos de calumnias, injurias o revelación de secretos en sistemas de mensajería instantánea, foros o redes sociales, con una difusión y repercusión mediática antes desconocida, al igual que la amenaza o chantaje de difusión de material sexual (sextortion) que previamente había sido compartido (sexting). Otra modalidad de nueva creación es el acoso entre menores utilizando estas tecnologías (ciberbullying), que lamentablemente en algunas ocasiones ha acabado de forma trágica con un fatal desenlace. También el denominado espionaje industrial y robo de carteras de clientes encuentran en estas tecnologías posibilidades antes desconocidas.

Otra particularidad de este tipo de delitos es su repercusión y perdurabilidad en el tiempo. Además de los sistemas de mensajería instantánea que permiten los envíos masivos, la difusión por estos medios es universal y, con la llegada de los buscadores la información es fácilmente localizable y puede permanecer accesible de por vida, sin posibilidad de control por parte del afectado. También se multiplican los daños causados puesto que se pueden multiplicar los afectados, no sólo porque con un sólo click se llegue a multitud de destinatarios, sino porque además los daños pueden paralizar a una empresa, organismo público, infraestructura o servicio crítico.

Todas estas situaciones que se ven afectadas por un componente de internacionalidad que va ligado intrínsicamente a las nuevas tecnologías. Información, medios tecnológicos y actores pueden encontrarse en ubicaciones muy diferentes y verse afectados por legislaciones distintas, la información puede ser almacenada o reproducida desde cualquier parte del mundo.

A esta circunstancia podemos sumarle la aplicación extrajurisdiccional de las leyes. En efecto, las empresas que explotan las redes sociales, establecen sus propias polìticas de uso y de privacidad, que son aceptadas por los usuarios como una adhesión, sin posibilidad de modificarlas. Y una de las principales consecuencias de esta adhesión es la aceptación que la ley que se aplica en caso de controversias con, por ejemplo, los datos personales. Un usuario de cualquier parte del mundo si quiere litigar contra alguno de los principales buscadores o redes sociales debe enderezar su litigio en el país de origen de estas empresas, sin perjuicio que los efectos de la actividad se produzca en su país o en otros países.

Más compleja aún resultará la prueba de estos delitos, las más que polémicas "evidencias electrónicas", aquellos datos que de manera digital se encuentran almacenados o fueron transmitidos mediante equipos informáticos y que son recolectados mediante herramientas técnicas especializadas empleadas por un perito en una investigación informática

Las legislaciones e instrumentos jurídicos de los Estados deberán atender a los principios de la International Organization on Computer Evidence, sobre la adquisición y el tratamiento de la evidencia electrónica, garantizando su veracidad, integridad y correcto tratamiento de forma segura.

Ante este panorama expuesto, las medidas de respuesta por parte de los poderes públicos deben ser tan novedosas e innovadoras, como lo son estas tecnologías, la Administración, su funcionamiento, las normas y el poder judicial deben adaptarse a los nuevos tiempos.

Los ordenamientos jurídicos de los países iberoamericanos deben contemplar nuevos tipos penales, y establecer mecanismos de defensa de los derechos de las personas sobre su propia información, garantizando el derecho al honor y la intimidad, articulando y dotando de medios a la instituciones, generando información accesible y concienciando a los ciudadanos sobre sus derechos y como denunciar conductas ilegales.

Igualmente la tendencia internacional deberá de pasar por armonizar los conceptos relacionados con este tipo de delitos, pues si bien en la mayoría de las legislaciones nacionales están

protegidos, aún hay grandes diferencias conceptuales, desde los países que crean un nuevo bien jurídico tutelado "De la Protección de la información y de los datos" (Colombia), pasando por aquellos que determinan como bien jurídico "la protección de los sistemas informáticos"(Venezuela), terminando por aquellos países Europeos en los que no existe diferenciación entre "delitos electrónicos" y "delitos informáticos". La unificación de criterios normativos en los diferentes países, su tipificación y las penas parejas deben ser prioridad legislativa en el ámbito internacional.

La cooperación y coordinación entre Estados y organizaciones internacionales debe ser un pilar básico, las tecnologías no entienden de fronteras. Las Organizaciones Iberoamericanas e Internacionales deben establecer puentes de colaboración entre Estados, Instituciones, empresas y particulares. Sólo un compromiso de los actores implicados y una homogenización de criterios, normas y consecuencias pueden erradicar las situaciones de ilegalidad y vulneración de derechos.

Se debe dotar de medios a las instituciones ya existen y se deberá avanzar en cuerpos de seguridad ultra nacionales, entendida como unidad especializada cuyo objetivo sería la prevención y el combate de los delitos electrónicos e informáticos encargados de establecer estrategias y de diseñar mecanismos que contrarresten los efectos de las conductas delictivas surgidas del Internet, junto a una clara cooperación de las fuerzas de seguridad nacionales. La definición internacional clara del concepto de ciberdelito debe ser materia a abordar por los foros internacionales.

Los Estados deben avanzar en el fortalecimiento de las "redes de alerta temprana", reforzando la información temprana sobre amenazas, en tiempo real por los instituciones, empresas y los ciudadanos que utilizan estas tecnologías.

Las nuevas formas de transmisión de datos posibilitados a través de redes informáticas y electrónicas tales como los sistemas inalámbricos, dispositivos de geolocalización, sistemas de radiofrecuencia y sensores, deberán ser temas prioritarios para el desarrollo de estudios e investigación a fin de conocer y prevenir las nuevas formas de procesamiento de datos.

Los Estados deben armonizar sus normativas, evitando la creación de "paraísos cibernéticos" a través de los cuales los ciber delincuentes puedan actuar impunemente. Para ello, se deben clarificar las reglas sobre competencia judicial, legislación aplicable y reconocimiento, así como la ejecución de resoluciones judiciales o administrativas, en aras de evitar lagunas legales que puedan

favorecer estas conductas delictivas, con independencia del lugar donde se cometan dichas conductas, protegiendo la intimidad y la información de las personas.

Se deben reforzar los mecanismos de auxilio judicial y colaboración administrativa, intercambio de información y reconocimiento y ejecución de sentencias, sentencias en el marco de la Convención (NU) de Nueva York de 1958 relativa al reconocimiento y ejecución de laudos y sentencias judiciales, y actos administrativos entre estados y entre estos y sus empresas y ciudadanos, de manera que una decisión judicial o administrativa en otro estado se acabe ejecutando aunque el autor o "arma del delito", se encuentren ubicados en otro.

Particularmente se deben facilitar mecanismos inmediatos, sencillos y universales para la tutela de los derechos de los usuarios, de manera que se minimicen los daños que puedan provocar en las "víctimas" la expansión viral, incontrolada y universal que posibilita las nuevas tecnologías. Para ello han de articularse instrumentos de colaboración con los distintos agentes intervinientes, muy especialmente con los prestadores de servicios de comunicaciones electrónicas, prestadores de servicios de intermediación y proveedores de contenidos.

Reforzar los mecanismos de identificación de los usuarios de las TIC,s ante la posible comisión de ilícitos, siempre de manera proporcionada y adecuada a los distintos escenarios posibles, procurando evitar así que el anonimato sirva como amparo y paraguas para la comisión de este tipo de actos, y siempre garantizando la protección del derecho a la intimidad del usuario.

Los tipos penales y las infracciones administrativas, deben ser claros, correspondiendo al poder legislativo de cada uno de los estados el ser dinámicos ante unas amenazas en proceso de continuo cambio, al objeto de evitar que unos hechos puedan quedar sin sanción por falta de cobertura legal, el derecho debe adaptarse a los tiempos actuales y ser dinámico.

Los estados y organizaciones internacionales deberán tener en sus plantillas, personal suficientemente formado para combatir estas amenazas y asistir a las victimas (jueces, fiscales, unidades especiales de policía informática, expertos en hacking ético y ciber seguridad, asistentes sociales, profesores, psicólogos…), en la protección de la privacidad, de los datos y la información, se deben contar con medios humanos y tecnológicos, asignando eficientemente recursos a la protección de las personas.

Los poderes públicos en colaboración con la sociedad civil, deben realizar campañas de concienciación sobre ciber amenazas en diferentes ámbitos sectoriales. Sólo mediante una formación de menores, padres o tutores, profesores y la ciudadanía en general se pueden prevenir situaciones de riesgo, la seguridad de la información y la privacidad, la protección de los datos debe empezar por uno mismo, educando a los menores en una sociedad tecnológica, en la que las relaciones encuentran un nuevo medio de desarrollo, las redes sociales e Internet.

Así mismo se debe promover una alfabetización digital, con especial hincapié en la privacidad y la protección de datos entre los "inmigrantes digitales", ya que habiendo nacido en un mundo anterior a la era de las TIC se han visto obligados a introducirse en este ámbito. De esta forma consideramos como un punto vital la formación a lo largo de la vida para reciclar los conocimientos y fortalecer diferentes conductas y actitudes que aseguren la máxima privacidad de los individuos.

Los estados en colaboración conjunta deben llevar adelante políticas educativas y de prevención que tengan como finalidad la reducción de la brecha digital en materia de datos personales y protección de la privacidad, no sólo en el uso de los computadores portátiles sino también en las nuevas tecnologías que involucren –directa o indirectamente- la posibilidad de tratamiento de datos.

Se debe concienciar a las empresas sobre buenas prácticas en la salida al mercado de sus productos. Las empresas deben procurar que sus productos o servicios cumplan unos estándares mínimos en seguridad y privacidad, dejando la posibilidad al consumidor de optar por la configuración que desea implantar, garantizando la seguridad de sus datos.

En este sentido, en relación a la responsabilidad que las empresas y organizaciones tienen sobre la información y datos personales que tratan, se deberá apostar por un modelo de privacidad empresarial y corporativo, incorporando responsables de privacidad a la toma de decisiones, elaborando informes de impacto y, tomando las medidas técnicas y organizativas necesarias para garantizar la privacidad y derechos de las personas.

Los Estados Iberoamericanos, las organizaciones internacionales y empresas, deben invertir en Programas de i+d+i, que doten de contenido económico el estudio e implantación de estas medidas. Se deben habilitar partidas presupuestarias tanto en las empresas como en los poderes

públicos, así como establecer los correspondientes beneficios fiscales para las empresas que pongan en marcha estos programas.

La transnacionalidad y universalidad de estas tecnologías requieren la urgente armonización internacional del "derecho al olvido". De no ser así, numerosos casos pueden recibir una respuesta estimatoria por de los juzgados y tribunales, o incluso una persecución por parte de los órganos de la Administración cuando no exista tipo penal y si infracción administrativa, y quedar en papel mojado al encontrarse el causante del perjuicio o su infraestructura tecnológica ubicados en un país que no sea sensible al derecho de toda persona a poder borrar la información que le sea desfavorable o que simplemente, no desee compartir cuando una ley no obligue a su publicación o mantenimiento.

Junto con la armonización e internacionalización de las normas de los Estados, se debe avanzar en la capacitación de las personas, empresas e instituciones, sobre la utilización correcta de las herramientas informáticas. En un mundo tecnológico e interconectado la educación y formación desde la infancia se constituyen un valor necesario para la prevención de conductas delictivas y la correcta privacidad de los usuarios.

La libertad de expresión en los nuevos medios de comunicación debe asegurar los derechos fundamentales de la persona a la intimidad, al honor, a su privacidad y a la protección de sus datos personales. Las normas jurídicas, equilibradas y sociales, deben proteger esos principios fundamentales recogidos en las diferentes Constituciones nacionales de los Estados Iberoamericanos.

El hombre es un ser libre, que goza de su libre albedrío en la sociedad democrática, tal como es concebida, se debe procurar que la tecnología contribuya a su desarrollo, y le permita gozar más de su vida personal, expresarse, crear y disfrutar del ocio, sin ser un verdadero esclavo de ella. Se debe utilizar las herramientas informáticas y nuevos canales de comunicación para mejorar la calidad de vida y los avances científicos; no para ser dominado por las mismas. La seguridad de la información, la protección de la privacidad debe ser un compromiso de todos: los usuarios, las empresas e instituciones, y los propio Estados y Organizaciones Internacionales.

Por ello, desde la iniciativa del Observatorio Iberoamericano de Protección de Datos hace un llamado a la comunidad general y en particular a los diferentes estados iberoamericanos a que se fortalezcan decididamente los mecanismos de protección en materia de datos personales y seguridad de la información, adoptando medidas urgentes para contrarrestar los efectos del fenómeno criminal

internacional. Estas medidas deberán incluir, sin limitarse a ello, redes de alertas tempranas en materia de delitos transnacionales, armonización de reglas de tratamiento de datos personales, adopción de mecanismos eficaces en materia judicial y administrativa internacional, programas de sensibilización y adopción de currículos académicos en protección de datos, seguridad de la información y delitos informáticos, así como programas de formación en la materia como elemento de prevención de conductas ilícitas con la información personal.