Por: Désirée Barinas
Master en Derecho multimedia e informático
(Université Panthéon-Assas Paris II).

ACONTECER

PROTECCIÓN DE DATOS PERSONALES Y CIBERCRIMINALIDAD

Extracto de ponencia realizada durante el Congreso Internacional sobre Cibercriminalidad y Evidencia Digital, organizado por la Escuela Nacional de la Judicatura en octubre del año 2018

Introducción: comprendiendo la realidad actual

El Internet, y junto a éste el desarrollo de las tecnologías de la información y la comunicación (TICs), ha sido sin duda un invento revolucionario, encontrándose en la actualidad más del cincuenta por ciento (50%) de la población mundial conectada al llamado ciberespacio. Hoy en día hablamos de comercio electrónico, banca en línea, gobierno digital, del uso de ***big data***, redes sociales y de perfiles en línea, como parte de nuestra cotidianidad, sin olvidarnos de que ya tiene presencia la inteligencia artificial y el Internet de las cosas (IoT), con los dispositivos inteligentes e interconectados, que sin duda nos llevará a un "Internet de las personas", encaminandonos a una web de la predictibilidad. Las personas se encuentran representadas a través de sus datos en el mundo digital, coexistiendo con nuestra realidad "física" una realidad "virtual" que también debe ser protegida.

Dentro del contexto actual resulta relevante la protección de los datos, y muy particularmente de los datos personales, los que se han vuelto un blanco codiciado y casi primario de la ciberdelincuencia. No es vano el Reporte de Riesgo Global de 2018 realizado por el Foro Económico Mundial, muestra como el riesgo a sufrir ciberataques, así como al fraude y robo masivo de la información se ha intensificado, apareciendo en la lista de los cinco principales riesgos globales por probabilidad de ocurrencia y los ciberataques dentro de los diez de mayor impacto, transformándose en una preocupaciones de carácter mundial junto a los desastres naturales y el cambio climático.

En una investigación realizada por Verizon se revela que tan sólo en el año 2017 se reportaron más de 53,000 incidentes de seguridad de los cuales 2,216 fueron exitosos, siendo la tendencia el sufrir ciberataques de denegación de servicios (DoS), marcados por la ingeniería

Volumen 1 • Número 15 • Junio 2019 • ISSN: 2305-2589

social y programas maliciosos como los ***ransomware***, donde ya no se habla del secuestro de personas sino de datos, estando a la cabeza los ataques realizados por ***hackers*** y los resultantes de descarga de archivos y/o programas maliciosos.

La cibercriminalidad no para de evolucionar, enfrentándonos no a aficionados que intentan probar sus habilidades técnicas, sino a bandas de crimen organizado las que llevan a cabo el 50% de los ciberataques y al cibercrimen ofrecido como "un servicio" en línea (CaaS), poniendo disponibles herramientas y plataformas a personas sin conocimiento técnico especializado para fines delictivos, siendo la motivación principal el obtener beneficios económicos y estimándose el costo de la misma en unos seiscientos mil millones de dólares.

El robo masivo de información se ha convertido en una preocupación de todos, yendo de la mano con la necesidad de salvaguardar los datos personales y la privacidad en la línea, frente a una cibercriminalidad creciente.

Igualmente, vemos cada vez más la monetización de la información y como los casos de robo masivo de data se han multiplicado, sumándose al ya conocido caso de Yahoo donde se vieron expuesto datos de miles de millones de sus usuarios, tales como nombres, números de teléfono, fechas de nacimiento, contraseñas cifradas y preguntas de seguridad, sucesos como el de Ticketfly, una empresa de distribución de tickets, que en el año 2018 fue víctima de un ciberataque siendo accedida información personal de más de 26 millones usuarios, incluyendo nombres, direcciones e mails; o el del Banco de Montreal y Simplii Financial, dos bancos canadienses, que vieron comprometida información financiera de aproximadamente 90 mil de sus clientes; en el año 2017, Equifax, un buró de crédito vio expuestos datos crediticios e información personal de más de 143 millones de sus usuarios; o en 2016 el 21st Century Oncology, donde el proveedor de servicios de salud vio accedida información personal y de salud de más de 2 millones de sus pacientes, incluyendo los números de seguro social, los nombres de los médicos, los diagnósticos, el tratamiento y la información del seguro; en 2015 el caso de Athem, el segundo asegurador de Estados Unidos, vio comprometida información de 80 millones de sus clientes, incluyendo nombres, fechas de nacimiento, números de seguridad social, direcciones, teléfonos, email, información laboral, o en 2012 donde se descubrió que había sido orquestado un ataque masivo obteniendo informaciones de tarjetas de crédito, debito y cuentas bancarias de más de 160 millones de compradores. La lista parece interminable apareciendo casos relacionados con empresas como Ebay, Target, Home Depot, Heartland, Adobe, Uber, Sony's PlayStation Network hasta con la Agencias de Transporte Sueca y con la Milicia, la Fuerza Armada, el Departamento de Defensa y la Oficina de Gestión del Personal estadounidense, siendo preocupante no solo la cantidad de personas afectadas, sino la sensibilidad de los datos involucrados y la capacidad de los individuos de tener conocimiento de que sus datos han sido expuestos y la pérdida de control sobre ellos.

El robo masivo de información se ha convertido en una preocupación de todos, yendo de la mano con la necesidad de salvaguardar los datos personales y la privacidad en la línea, frente a una cibercriminalidad creciente. Datos que tienen un valor en el mercado negro y en la ***dark web,*** viabilizando la comisión de otros ciberdelitos, como la suplantación de identidad, el fraude informático, el acceso no autorizado y la transferencia de fondos, entre otros. Como bien señala el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos "***Si no se toman***

La protección de los datos personales va de la mano con la salvaguarda del derecho a la privacidad, derecho humano internacionalmente reconocido y protegido en nuestra Constitución en su artículo 44, prerrogativa que se extiende a tener control sobre la recolección, acceso, uso, calidad y anonimidad de los mismos, partiendo nuestra Carta Magna de que todo tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad.

a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión".

Datos personales y cibercriminalidad: la respuesta legislativa dominicana

La protección de los datos personales va de la mano con la salvaguarda del derecho a la privacidad, derecho humano internacionalmente reconocido y protegido en nuestra Constitución en su artículo 44, prerrogativa que se extiende a tener control sobre la recolección, acceso, uso, calidad y anonimidad de los mismos, partiendo nuestra Carta Magna de que todo tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad.

A este respecto la República Dominicana cuenta con la Ley 172-13, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados del 15 de diciembre de 2013, la cual deja mucho que desear, y la que, si bien busca la protección integral de los datos personales de las personas naturales, siendo indiferente si son digitales o manuales, reconociéndoles los derechos de acceder, rectificar, actualizar y solicitar la destrucción de sus datos, no establece un órgano regulador, excepto para las informaciones financieras que se infiere será la Superintendencia de Bancos, lo que dificulta su correcta aplicación. Igualmente el texto no prohíbe la toma de decisiones basados únicamente en tratamiento automatizado de datos, ni establece como condición para la transferencia internacional de datos que la misma se realice a países que contemplen un nivel de protección similar al definido por la ley, lo cual no deja de ser cuestionable.

Cabe también acotar que la misma no contempla aspectos como el reconocimiento de un derecho al olvido, el derecho a la limitación del tratamiento y, por qué no, a la generación misma de la información, el derecho de ser informado en caso de que su información se haya visto comprometida, entre otros nuevos elementos que se han revelado como necesarios para proteger a las personas en el mundo digital, y muchos de los cuales van siendo reconocidos a nivel internacional, tomando como ejemplo el Reglamento General de Protección de Datos de la Unión Europea. Ni hablar de que en ella se planteen conceptos como el ***privacy by desing***.

Volumen 1 • Número 15 • Junio 2019 • ISSN: 2305-2589

La Ley 172-13 de protección de datos personales contempla sanciones penales, estableciendo en su art. 84 como pena excepcional una multa de diez (10) a cincuenta (50) salarios mínimos vigentes la violación a la vida privada en caso de "1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe. 2. Proporcionara, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales. 3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales. 4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley", como si todos estos hechos tuvieran la misma gravedad y consecuencias similares para los afectados, y obvia penalizar el uso y tratamiento no autorizados de de esos datos, así como su recolección no autorizada.

A esto se suman las sanciones establecidas en los artículos 86 y 87, las cuales están orientadas a los datos tratados por una Sociedad de Información Crediticia (SIC), donde se establece multa que van desde los diez (10) a cincuenta (50) salarios mínimos la violación a la vida privada en caso acceso de un subscriptor a informaciones personales sin autorización del titular; de diez (10) a cien (100) salarios mínimos vigentes en caso de uso distinto al consignado; veinte (20) a cien (100) salarios mínimos vigentes cuando se acceda de manera fraudulenta usando claves de acceso que no le pertenecen; prisión de seis (6) meses a un año en caso que utilice o facilite un reporte de crédito proveniente de una Sociedad de Información Crediticia (SIC) con la finalidad de la comisión de un delito y en caso de que haya tenido como finalidad facilitar la comisión de un crimen, será sancionado con la prisión que establezca el Código Penal vigente para los cómplices. A lo que añade el art. 88 sanciones de seis (6) meses a dos (2) años, y una multa de cien (100) a ciento cincuenta (150) salarios mínimos vigente, a quien, fuera de los fines establecidos en esta ley, divulgue, publique, reproduzca, transmita o grabe el contenido parcial o total de un reporte de cualquier tipo proveniente de una Sociedad de Información Crediticia (SIC), referente a un titular de los datos, en cualquiera de sus manifestaciones, en cualquier medio de comunicación masiva, sea impreso, televisivo, radial o electrónico.

Este esquema de sanciones deja mucho que desear, pues establece mayor peso a las violaciones relativas a datos personales gestionados por las Sociedad de Información Crediticia, como si éstos tuviesen mayor importancia que otros de datos personales, limitando incluso solo a estos casos la penalización para usos delictivos, no planteándose el castigar el uso de datos personales con fines discriminatorios o la manipulación de los datos de sensibles, ni la penalización de la recolección ilegítima de datos. Aun más sorprendente es la divergencia de las penas, que no parecen seguir ninguna lógica ni siguiera entre ellas y que resultan incluso inferiores a las contempladas en la Ley 53-07 de crímenes y delitos de alta tecnología, que contempla casos similares con sanciones más importantes.

Por último establece en su art. 88 una sanción general a quienes viole las disposiciones contenidas en la ley de prisión correccional de seis (6) meses a dos (2) años, y una multa de cien (100) a ciento cincuenta (150) salarios mínimos vigente, quedando por ver que entraría dentro de este tipo penal de amplia definición ¿la recolección de datos no consentida?, ¿la violación de la finalidad?, ¿la vulneración al deber de seguridad?

Ahora bien, podemos considerar que la protección de los datos personales frente a la cibercriminalidad no se limita a un tratamiento "adecuado" y "legítimo", sino que va mucho más allá, surgiendo la creciente necesidad de garantizar su ciberseguridad. Se habla entonces de la proteger la confidencialidad, integridad, y disponibilidad de los datos, incluyendo no solo los datos personales sino también de los negocios e incluso información estatal y los sistemas relacionados. Se busca garantizar que sólo las personas apropiadas tengan acceso a la información según su nivel

de autorización (confidencialidad), que los datos sean confiables y correctos, conservando su forma original al ser transmitido, tratado o almacenado (integridad) y que las personas autorizadas puedan acceder de manera segura y oportuna a las informaciones y sistemas (disponibilidad).

No en vano el Convenio sobre la Ciberdelincuencia, del 23 de noviembre de 2001, también conocido como el Convenio de Budapest, principal instrumento internacional en la materia, aborda en su parte sustantiva los denominados delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Convenio de aplicación en nuestro país, pues fue ratificado por República Dominicana el día 7 de febrero de 2013, y al que responde la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología del 23 abril de 2007. Esta pieza normativa establece en sus considerandos que las tecnologías de la información y de la comunicación (TICs) se erigen como un nuevo soporte para la comisión de delitos tradicionales e introduce nuevas conductas antisociales a sancionar, así como la agravación de otras ya tradicionalmente reconocidas, por la magnificación del daño que implica su utilización, como sucede por ejemplo con el caso de la difamación o la injuria, señalando esta norma que las TICs brinda "un nuevo soporte para la comisión de delitos tradicionales" y crea "nuevas modalidades de infracciones y hechos no incriminados" .

Nuestro legislador opta así por incorporar al Derecho Penal sustantivo nuevos bienes jurídicos que podrían considerarse intermedios. Así, la confidencialidad, la integridad y la disponibilidad de los datos se transforman en valores a ser protegidos en sí mismos, al margen de que con ello se garanticen, directa o indirectamente, otros bienes jurídicos tradicionalmente reconocidos como la privacidad, sin por ello dejar de ponderarlos dentro de otros tipos penales.

La Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología contempla un capítulo para los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, con un catalogo más amplio que el de la Convención de Budapest, donde se tipifican como conductas a ser sancionadas la utilización de códigos de acceso (Art. 5), la clonación de dispositivos de acceso (Art. 5, párrafo), el acceso ilícito en sí mismo (Art. 6), el uso de datos por acceso ilícito (Art 6, párrafo I), la explotación ilegítima del acceso inintencional (Art. 6, párrafo II), el acceso ilícito para servicios a terceros (Art. 7), el beneficio de actividades de un tercero (Art. 7, párrafo), el uso de dispositivos fraudulentos (Art. 8), la interceptación e intervención de datos o señales (Art. 9), el daño o alteración de datos (Art. 10) y el sabotaje a los sistemas (Art. 11), estableciendo penas que pueden alcanzar hasta los 10 años de prisión y quinientas (500) veces el salario mínimo.

Dentro de estos, llama particularmente nuestra atención el art. 9 de la Ley 53-07 que penaliza el hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, siendo un artículo de necesaria referencia, pues hace mención de la protección del secreto, la intimidad y la privacidad como elementos tipificantes.

Un dato interesante es que en el mismo se salvaguarda los datos o señales tanto de las personas físicas como de las personas morales, reconociéndose un cierto ámbito de secreto a las personas jurídicas, siguiendo la línea de la decisión de la Corte Europea de Derechos Humanos de 16 de abril de 2002 contra Francia, en la cual se consideró que las personas morales tienen derecho a la protección de su sede social bajo, debiendo ser respetada su "vida interior".

Asimismo, cabe destacar dentro de los llamados delito de contenido tipificados por la Ley 53-07 07 de

Volumen 1 • Número 15 • Junio 2019 • ISSN: 2305-2589

Crímenes y Delitos de Alta Tecnología, el art. 17 sobre suplantación de identidad, al ser una técnica muy utilizada para la obtención de datos personales, como es el ***phising*** o el ***baiting***, siendo el primero la modalidad imperante en la ingeniería social empleada por los cibercriminales, siendo sancionada con penas de tres meses a siete años de prisión y multa de dos a doscientas veces el salario mínimo.

Igualmente, no podemos dejar de mencionar el art. 19, que sanciona con la pena de seis meses a dos años de prisión y multa de cinco a quinientas veces el salario mínimo el uso, sin causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas. Su amplia definición nos hace preguntar qué los tribunales consideraran dentro de este tipo penal, ¿la recolección y tratamiento masivo no autorizado de información?, ¿proceso de ***data mining?,*** ¿la apropiación de informaciones residuales (***scavenging***) y su tratamiento?, ¿la implementación de cualquier tratamiento ilegítimo?, ¿el robo a gran escala de información?, ¿sería necesaria la creación de un tipo penal específico y agravado para estos casos a sabiendas de que los cibercriminales lo utilizan como parte de un eslabón primario en la comisión de otros ciberdelitos y por el impacto masivo de su comisión?

Se revela como un elemento importante el garantizar la seguridad de los datos y sistemas que son utilizados y/o gestionados, a sabiendas de que las personas siguen siendo el eslabón más débil de la cadena de protección. Ello requiere una toma de consciencia global sobre la importancia de la protección de los datos personales y de garantizar su ciberseguridad. Si bien hoy día se habla de mejorar la capacidad de resiliencia de los sistemas, no solo de prevenir y defenderlos, partiendo de que serán con certeza objeto de ciberataques, pero debemos tener claro que en el caso particular de los datos personales, una vez que ellos son expuestos difícilmente es reparable el daño causado. No todo es tan fácil como cambiar de número de tarjeta de crédito o cambiar de correo electrónico, con los inconvenientes que esto nos pueda traer, imaginen el tener que cambiar nuestro nombre, documento de identidad o de dirección para recuperar nuestra privacidad, a lo que se suma que en algunos casos resulta sencillamente imposible, como ocurre con los datos relativos a nuestras huellas digitales, las que nos acompañan de por vida. El garantizar y recuperar el control sobre nuestra información personal, con todo lo que puede implicar la pérdida del mismo en un mundo interconectado se revela como un gran reto actual y dentro del marco escenario de la cibercriminalidad.

Nos preguntamos así si la configuración normativa actual es suficiente. Si bien es cierto que la ley 53-07 de Delitos de Alta Tecnología viene a la defensa de los datos y sistemas, no es menos cierto que la protección integral de los datos personales y del derecho a la privacidad se tambalea frente a una legislación deficiente como es la 172-13 de Protección de Datos Personales, la que debió crear mecanismos que permitieran prevenir su mal uso y tratamiento y condicionar la utilización de la tecnología al respeto de tales derechos, pero que se quedó corta, y la que necesariamente deberá ser objeto de modificación si queremos responder a los retos actuales en la materia y garantizar una debida protección de los mismos.

No podemos dejar de destacar las palabras de Walter Peissel quien señala que la "discusión sobre la privacidad no es sólo sobre 'derechos'; es también sobre la filosofía de la autonomía y de la libertad (…)". Cabe entonces replantearse cuál sería la forma ideal para estructurar el funcionamiento de este mundo digital y de las tecnologías que lo soportan y atrevernos a cuestionar sus cimientos.