La respuesta penal frente a las nuevas tecnologías (Parte III)

Por Uriel Bekerman, Guido Damián Cresta y Federico Pérez Millán

El uso indebido de la tecnología ya no debe comprenderse como únicamente propio de un hacker o especialista en la materia, sino que la delincuencia ha sido expandida respecto de su sede de operaciones, por lo que cualquiera puede lograr delinquir con acceso y creatividad delictiva.

Por otro lado, vemos que tradicionalmente la dogmática ha utilizado el paradigma histórico-delictivo de delitos de comisión por mano propia (robos, homicidios, etc.) para lo cual el autor debía trasladarse a un lugar físico determinado para la comisión de una conducta reprochada, mientras que en la actualidad, el ciberdelincuente, desde su propia computadora, celular o hasta a través de un software automatizado, puede afectar bienes jurídicos en cualquier lugar del mundo, cometiendo hechos con características delictivas a través de medios tecnológicos, muchas veces carentes de tipificación.

Es aquí donde aparece y debe aparecer el derecho trasnacional, dando respuesta a esta incertidumbre sobre la seguridad de la información y regulando a través del Convenio de Budapest[1] "Sobre la Ciberdelincuencia", la obligación de los Estados partes para que dicha incertidumbre desaparezca; legislándose los principales delitos informáticos, y por ende, pasando a estar tipificados y definidos.

El Convenio de Budapest, a pesar de haberse redactado en el año 2001, contó con la adhesión del Estado argentino recién en noviembre del año 2017, a través de la Ley 27.411[2] sancionada por el Congreso Nacional. El principal objetivo del instrumento fue prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos[3].

El Estado argentino ha atravesado un largo proceso legislativo hasta llegar a la adhesión del Convenio de Budapest. Inicialmente, la Ley 24.766, conocida como "Ley de secretos comerciales", tipificó en 1996 la sustracción de Secretos Comerciales contenidos en soportes electrónicos; luego en 1998, la Ley 11.723 de Propiedad Intelectual trató la copia ilegítima de cualquier programa de software y base de datos informática; y en el año 2000 se dictó la Ley 25.326 de Protección de los Datos Personales[4].

Sin embargo, la laguna normativa en materia penal relacionada con la delincuencia informática permaneció intacta durante años sin su debido tratamiento, hasta la llegada de la Ley 26.388, conocida

[1] Convenio de Budapest sobre la ciberdelincuencia; Budapest, 23/11/2001.
[2] Ley 27.411: "Convenio sobre Ciberdelito. Aprobación".
[3] Preámbulo del Convenio de Budapest sobre la ciberdelincuencia.
[4] Una aproximación a la estadística criminal sobre delitos informáticos. Primer muestreo de denuncias judiciales de la República Argentina. 1ra. edición - septiembre de 2016. Editorial Ministerio de Justicia y Derechos Humanos de la Nación

ISSN 2362 - 3217

como “Ley de Delitos Informáticos”, la cual modificó en el 2008 el Código Penal de la Nación. Posteriormente, para aumentar aún más el campo normativo, se legisló la Ley 26.904, que en el año 2013, reguló el ciberacoso, denominado en la regulación bajo el nombre de “Grooming”.

La Ley 26.388, tipificó una serie de delitos informáticos en plena concordancia con lo establecido por el Convenio de Budapest, independientemente de no haberse encontrado el Estado argentino adherido a dicho instrumento en aquél entonces. Esta ley, marcó un antes y un después en la materia criminal-informática. Específicamente, estableció las siguientes figuras penales derivadas del Convenio y de recomendaciones internacionales para contrarrestar la principal laguna normativa:

a) Se amplió el alcance de los términos “Documento”, “Firma”, “Suscripción”, “Instrumento privado” y “Certificado”, las cuales, si bien no son conductas reprochadas por la ley, norman las acciones digitales que oportunamente podrían verse afectadas por los tipos de conductas criminales.

b) Delito de producir, financiar, ofrecer, comercializar, publicar, facilitad, divulgar o distribuir pornografía infantil.

c) Delito de violación de correspondencia electrónica, con agravantes en el caso haber sido comunicada a un tercero o publicada dicha correspondencia, o de haber sido cometida por funcionario público.

d) Delito de acceso indebido a un sistema o dato informático, agravándose si éste es en perjuicio estatal o de un proveedor de servicios públicos o financieros.

e) Delito de publicación indebida de comunicaciones electrónicas, con el eximente de haber obrado bajo interés público.

f) Delito de revelación de secretos cometido por un funcionario público.

g) Delitos referidos a la protección de información en bancos de datos personales.

h) Delito de defraudación mediante cualquier técnica de manipulación informática.

i) Delito de alteración, destrucción o inutilización de datos

j) Delito de daño informático, que incluye la alteración, destrucción e inutilización de datos, la venta o distribución de sistemas informáticos para causar daños; los cuales cuentan con agravantes establecidos por la ley.

Por otro lado, La Ley 26.904 sancionada por el Congreso Nacional en el año 2013, modificó el Código Penal de la Nación tipificando el delito de ciberacoso o grooming, que estableció en el artículo 131 del Código Penal que: “Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio

de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

Según la autora Sandra María Pesclevi: "El "grooming" comprende básicamente, la realización de actos preparatorios a través de los cuales y mediante la utilización de las nuevas tecnologías, se pretende lograr comunicación e información para luego cometer delitos de índole sexual induciendo a que el menor dé datos sobre su persona o amistades, para luego –ya en un grado de mayor confianza- se le soliciten acciones tales como desvestirse ante la webcam, se masturbe o realice alguna práctica de tipo sexual. Sin embargo, algunos autores señalan que no es del todo correcta la etiqueta de "grooming" para designar las acciones tipificadas por resultar extremadamente difícil discernir "ex ante" qué conductas están siendo dirigidas a un abuso y cuáles son, simplemente, conductas de atenciones sinceras respecto de menores"[5].

III. Conclusión

El ordenamiento jurídico argentino ha tenido que adecuarse a una época que reclama cambios regulatorios en materia de derecho penal, principalmente por la expansión fáctica de la materia criminal hacia campos nunca antes previstos y que, por supuesto, se encontraban lejos de estar regulados (recordemos que nuestro actual Código Penal data del año 1921).

El delito a través del espacio cibernético ("Ciberdelito" o "Ciberdelincuencia") ha cobrado principal importancia. La incorporación de herramientas y servicios tecnológicos, la cual es constante e imparable en términos generales y progresivos, debe acompañarse con legislación acorde; en su defecto, nos encontraremos ante fallas estructurales que podrán dañar a la sociedad en su conjunto, abriendo paso hacia escalafones delictivos de gran magnitud operativa (como por ejemplo ciberataques a países enteros, a sistemas financieros, etc.).

Pero a su vez, como bien mencionamos previamente, la magnitud operativa no corresponderá siempre a grandes y rebuscadas organizaciones delictivas cómo es posible imaginar, sino que el campo criminal-informático ha abierto sus puertas a un sinfín de oportunidades de cometer ilícitos, que aún hoy en día no han sido recogidas por la legislación y que si bien no implican grandes daños a escala transnacional o financiera, afectan a personas individuales a veces de manera muy dañosa.

[5] Sandra María Pesclevi "Grooming. Una figura a modificar en el Código Penal", Editorial Albrematica S.A. - Ciudad Autónoma de Buenos Aires - Argentina

Será trabajo de los legisladores reducir el poder de interpretación que deban ejercer los jueces respecto de las leyes penales, tipificando nuevas conductas o adaptando las leyes penales a las nuevas formas de ejecución de las ya existentes conductas reprochadas, para así lograr abarcar los nuevos hechos delictivos que los intensos y veloces cambios tecnológicos permiten.

Por ello es importante ser cautos a la hora de sancionar leyes que criminalicen conductas, como así también en su aplicación por el sistema penal, para que no se produzcan violaciones a los derechos fundamentales de las personas y se resguarden las garantías constitucionales de los individuos.

ISSN 2362 - 3217