El Derecho Penal aplicado a los delitos informáticos: Una política eficiente para el cibercrimen?

por **GUSTAVO SAIN**
18 de junio de 2013
www.infojus.gov.ar. 18/6/2013
Id Infojus: DACF130148

Derecho y nuevas tecnologías Históricamente, diferentes bienes inmateriales o intangibles fueron considerados por las legislaciones penales como un bien jurídico a proteger. Así sucedió con la materia y la energía, contempladas en los códigos modernos de occidente. Con el surgimiento y auge de disciplinas como la cibernética, la informática y expansión de las tecnologías de la información y la comunicación (TICs) y las redes de comunicación como Internet, el valor de la información como bien intangible adquirió una nueva dimensión. Tal como se describe en el Manual de las Naciones Unidas sobre prevención y Control de Delitos Informáticos de 1994, "Hasta ahora, los códigos penales de todos los países se ha protegido de forma preponderante a los objetos tangibles y visibles. Aunque la protección de la información y de otros objetos o valores intangibles existía ya a mediados del siglo XX, lo cierto es que hasta muy recientemente no ha revestido importancia. En los últimos decenios se han producido cambios importantes: de una sociedad industrial se ha pasado a una sociedad postindustrial, el valor de la información ha aumentado en las esferas económica, cultural y política, y se ha incrementado la importancia de la tecnología informática, cambios que han planteado nuevos problemas jurídicos y han requerido nuevas respuestas jurídicas a la legislación en materia de información" (1).

Con la incursión de la informática en la vida cotidiana de las personas, el Derecho tuvo que adaptar su teoría no sólo para la protección de la información y los dispositivos sino para el mejoramiento de procesos jurídico-administrativos. Para este último caso se creó una nueva área, la informática jurídica, donde la tecnología es puesta al servicio del Derecho. La misma se divide en Informática Jurídica Documental, orientada a la compilación y búsqueda de documentos jurídicos; Informática Jurídica Administrativa o de Gestión, concebida como ayuda a los procesos jurídico-administrativos tradicionales; y la Informática Jurídica Decisional, que busca suplantar decisiones humanas mediante el uso de programas automatizados de software. En cuanto a la informática como objeto de estudio, es a través del Derecho Informático o Derecho de Alta Tecnología es donde se aplica las reglas jurídicas con los problemas vinculados con la tecnología. Dentro de este campo existe un área relacionada con el derecho penal, que consiste en el estudio de aquellos delitos donde la informática desempeña un papel condicionante, tanto como medio para la comisión de un ilícito. Así, estos tipos de ilícitos son entendidos como delitos informáticos, delitos de alta tecnología o delitos cibernéticos, entre otros.

Desde la incorporación de mecanismos electrónicos en la vida cotidiana, muchos países comenzaron a modernizar su legislación de acuerdo a las nuevas modalidades ilícitas. Algunos países incorporaron los delitos informáticos a su normativa mediante la promulgación de leyes específicas en

el área, mientras que otros modificaron su legislación para incorporar nuevas figuras que incluyan a la información como un bien jurídico a proteger. Otros, sin embargo, trataron de aplicar los tipos penales convencionales para la protección de la misma, como por ejemplo los delitos contra la propiedad, cuando el bien afectado eran las computadoras personales; o los delitos contra la intimidad, para el caso de la interceptación del correo electrónico como correspondencia personal. En este caso se presenta el problema de que a medida que evoluciona la tecnología, las figuras penales tradicionales de los antiguos códigos no alcanzan para ser cubiertas por las mismas. En este caso, resulta fundamental realizar un estudio particular sobre el tipo de bien o interés lesionado para adecuar la normativa o promulgar una nueva legislación específica.

Cabe señalar, resulta apropiado que las leyes penales establezcan diferenciaciones conceptuales de las expresiones "uso abusivo de computadoras", "uso indebido de computadoras" y "delitos informáticos", aunque en algunos documentos de referencia se los utilice como sinónimos. Existen usos abusivos de dispositivos informáticos que se producen en forma accidental, negligente y en forma deliberada y/o no autorizada, que en este último caso implica un uso indebido. De la misma manera se debe hacer una distinción de lo que no es ético y no es legal, es decir, la diferenciación entre una conducta vinculada con cuestiones reñidas con la moral pero lícita; y otras que constituye una conducta lisa y llanamente ilegal. Por último, el establecimiento de medidas sancionatorias -sean de tipo penal, administrativa, civil o comercial- debe ser proporcional al hecho que se ha cometido.

Los delitos que involucran dispositivos informáticos presentan algunas características diferenciales en relación a otros delitos. Se destacan la transnacionalidad, a partir de la posibilidad de su comisión a distancia desde cualquier parte del mundo; las dificultades probatorias en función de la volatilidad de los rastros del crimen; su atemporalidad, ante la posibilidad de programar su ejecución automática para determinada fecha y hora -para el caso de los virus-, el anonimato que permite determinados entornos virtuales y la inadecuación legal de determinadas conductas ilícitas a las normas penales vigentes, entre otros. A su vez, el delito informático tiene una importante cifra oculta en función de la cantidad de hechos denunciados a la Justicia. Asimismo de la cantidad de hechos denunciados un porcentaje muy ínfimo tiene resolución penal en términos de identificación de los responsables. Existen varios factores que explican este fenómeno: la velocidad y complejidad de funcionamiento de las tecnologías modernas hacen que sean difíciles de descubrir, los investigadores carecen de pericia suficiente para encarar el proceso de examen y por último el desconocimiento de las víctimas de que fueron víctima de un delito informático.

Esfuerzos en materia de cooperación internacional Por la naturaleza transnacional del delito informático, los organismos internacionales intentan fortalecer la cooperación entre países no solo en materia de legislación penal, sino también en derecho procesal, la creación de organismos especializados y la asignación de facultades específicas para las autoridades de aplicación de la ley. Algunos problemas relacionados con la cooperación entre países en materia de delito informático son; la ausencia de consenso acerca de una definición jurídica de la conducta delictiva, la falta de conocimientos técnicos por parte de las autoridades de aplicación de la ley, la inadecuación de las facultades legales de investigación, la falta de armonización de los procedimientos de investigación y la ausencia de tratados de extradición y asistencia recíproca, entre otros.

En este proceso, diferentes organismos internacionales desempeñaron un rol fundamental para la definición de figuras penales y la armonización legislativa en relación a este tipo de conductas. Uno de los primeros intentos a nivel internacional se dio en 1983, cuando la Organización para la Cooperación y el Desarrollo Económico (OCDE) inició un estudio para la armonización de leyes penales en la materia para los países miembros. Tres años después, en 1986, publicó un informe titulado "Delitos de Informática: Análisis de normativa jurídica" donde se hacía un recorrido por la

legislación vigente y brindaba una serie de recomendaciones para la reforma penal. A partir de la elaboración de una lista mínima de ejemplos, se describían modalidades ilícitas tales como el fraude, la falsificación, la alteración de datos y programas, los derechos de autor y la interceptación de las comunicaciones, entre otras.

En línea con las propuestas de la OCDE, el Consejo de Europa elaboró una serie de directrices orientadas a los parlamentos de los países miembros en relación a los tipos de conductas punibles para su incorporación a la legislación penal. Mediante la conformación de un Comité Especial de Expertos sobre Delitos Relacionados con el Empleo de Computadora se abordaron temas como la prevención de riesgos, represión de este tipo de delitos, diferentes procedimientos de investigación, métodos de confiscación internacional y cooperación internacional. Tras la aprobación en 1989 de la resolución R(89)9 sobre delitos informáticos, recomienda a los gobiernos de los Estados Miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva el informe sobre la delincuencia relacionada con las computadoras y el particular las directrices para los legisladores nacionales. La resolución fue aprobada por el Comité de Ministros del Consejo de Europa en septiembre de ese año.

En este sentido, en el marco del Octavo Congreso de Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente realizado en 1990 en la Habana, Cuba, se adoptó una resolución donde se recomendaba elaborar un documento en el seno del la organización con el fin de aumentar los esfuerzos en el plano internacional en materia de prevención y represión de delitos relacionados con la informática. Tras esa resolución, el Gobierno de Canadá propuso realizar un manual en materia de delitos informáticos. El mismo fue presentado dos años más tarde en una reunión de expertos convocada por el Dr. Ulrich Sieber y organizada por la Asociación Internacional de Derecho Penal -una ONG reconocida mundialmente - con organización conjunta de la Organización de las Naciones Unidas, el Consejo de Europa y la Unión Europea en Wurzburgo, Alemania, en octubre de 1992.

Por otro lado, en Abril de 2001, el Comité de Ministros del Consejo de Europa -el organismo internacional más antiguo del viejo continente- adoptó un proyecto orientado a armonizar las legislaciones de los 47 estados miembros en la materia. Ante "la necesidad de aplicar una política penal común a los estados miembros y fortalecer la cooperación internacional" y "prevenir actos que pongan en peligro la confidencialidad, la integridad y disponibilidad de los sistemas, redes y datos informáticos tanto así como su abuso, la tipificación penal de los actos, mecanismos y procedimientos para su detección, investigación y sanción y fortalecimiento de la cooperación internacional" (2), el acuerdo se constituyó de carácter abierto, para que pueda ser suscripto por otros países fuera de la Unión. "The Convention on Cybercrime" o "Convenio sobre Cibercriminalidad de Budapest" -por la ciudad donde se terminó firmando en noviembre de 2001-, representa en la actualidad el documento de referencia internacional más importante en términos de Derecho Penal, Derecho Procesal Penal y cooperación internacional en materia de delitos informáticos. Su entrada en vigencia se produjo el 1 de julio de 2004, y a la fecha posee la adhesión de países como Australia, Japón, Canadá y Sudáfrica, entre otros.

Administración de Internet Internet es un medio descentralizado en cuanto a sus comunicaciones, donde el flujo de información circula por diferentes vías de comunicación desde una computadora hasta un punto de destino. En tanto conjunto de redes individuales, cada una de ellas posee su propia estructura tecnológica y es administrada en forma individual por sus propietarios. Por su arquitectura de red, resulta imposible que Internet pueda ser controlada por un ente que supervise el flujo total de comunicaciones, motivo por el cual la red de redes global no posee una autoridad central. Así, la administración de Internet es llevado a cabo por una serie de organizaciones no gubernamentales interesadas en el desarrollo y evolución tecnológica de la red.

La más importante es la Internet Society (ISOC) creada en 1992 y conformada por un conglomerado de empresas, organismos gubernamentales y fundaciones interesadas en las posibilidades comerciales que ofrece la red. Con una fuerte presencia de las empresas del sector de telecomunicaciones, los principios fundamentales que promueve están basados en el autogobierno de la red por parte de los usuarios y las empresas del sector fundados en la utilización de Internet en forma abierta y no gravada; la autorregulación de los proveedores de contenido, la no censura previa de las comunicaciones en línea, la no restricción a la libertad de expresión por medios indirectos como normativas gubernamentales o privadas; y la posibilidad de que los usuarios de Internet puedan cifrar sus comunicaciones y la información sin restricción alguna, entre otras. Las diferentes resoluciones adoptados por este organismo no son vinculantes, ya que ofician a modo de recomendaciones para los diferentes administradores de las diferentes redes que componen Internet.

La otra organización significativa es el World Wide Web Consortium (W3C), creada en 1994 en el seno del Instituto de Tecnología de Massachusetts. Esta organización es un consorcio internacional donde las organizaciones miembros trabajan conjuntamente para el desarrollo de estándares tecnológicos para el uso de la Web. Al igual que lo que sucede con la Internet Society, las normas aprobadas por la organización no son de carácter vinculantes por su inaplicabilidad universal. Los diferentes documentos oficiales elaborados por la organización son presentadas públicamente bajo el nombre "recomendaciones de la W3C".

En relación al gobierno de Internet, Ed Krol señala; "Internet se parece a una iglesia: cuenta con un grupo de consejeros, cada miembro tiene una opinión acerca de cómo deben hacerse las cosas y puede decidir tomar parte o no. Es una elección personal. Internet no tiene presidente, director ejecutivo o mandatario. Las redes que componen Internet pueden tener presidentes o directores ejecutivos, pero en Internet, eso es distinto, no existe la figura de autoridad máxima como un todo" (3).

Los principios básicos de Internet tienen una impronta liberal y fueron claramente definidos a partir a partir de la apertura comercial de Internet por parte del gobierno de los Estados Unidos a mediados de los años 90. Durante la presentación mundial de la Infraestructura Global de Información (GII) por parte del Vicepresidente estadounidense Albert Gore en la Asamblea Anual de la Unión Internacional de las Telecomunicaciones (UIT) de 1994, se estableció que las llamadas autopistas de la información representaban el requisito indispensable para el desarrollo y crecimiento económico sostenible y la construcción de una democracia plural a nivel global. El servicio universal debía estar garantizado por el mercado, el factor determinante para la creación de las infraestructuras nacionales de la información. Los objetivos estaban puestos en promover la inversión privada, incentivar la competencia y crear un marco regulatorio flexible para el sector de las telecomunicaciones. En este proceso, el Estado debía tener un rol mínimo en términos de diseño de políticas públicas para el sector.

Gobernanza de la red En la actualidad, cada vez que un delito informático adquiere relevancia pública a partir de un caso resonante, diferentes expertos en materia de derecho aluden a la necesidad de tipificación penal de determinadas conductas, la concordancia legislativa a nivel internacional, la necesidad de la firma de acuerdos comunes entre países en materia extradición o investigación criminal, y la reforma de códigos procesales penales para la admisión de pruebas informáticas en el marco de un proceso judicial, entre otras medidas. Al igual que cualquier otra política o estrategia en materia de seguridad ciudadana donde cualquier acto deliberado que afecta y/o vulnera de derechos y libertades individuales, si bien la solución penal resulta una parte importante de este proceso, no resulta ser la única opción para el abordaje de este tipo de criminalidad. En este sentido, el derecho

brinda una perspectiva meramente sancionatoria, ya que el abordaje se encuentra focalizado en la conjuración y represión de este tipo de delitos y no así en su prevención y gestión de conflictividades.

La incursión de Internet en la vida cotidiana de las personas hace que diferentes organismos encargados de elaborar políticas públicas incorporen a su agenda diaria la necesidad de contemplar diferentes actividades que tienen lugar en el ciberespacio. Asi, por ejemplo, una agencia gubernamental encargada de regular la venta de medicamentos dentro de un país debe poseer un equipo especializado como parte del mismo para la fiscalización de venta de drogas controladas por Internet dentro de su territorio, tanto así como las fuerzas de seguridad deben poseer unidades especializadas para la venta de drogas prohibidas. Asimismo, un organismo que recibe denuncias sobre discriminación o actos de violencia simbólica debe estar atento a las diferentes denuncias recibidas por personas que se sienten agraviadas por publicaciones en sitios web o redes sociales que afectan su sensibilidad u honor, elaborando una serie de mecanismos de acción para abordar esta problemática en entornos digitales. A su vez, una agencia encargada de fiscalizar las diferentes operaciones financieras para evitar el lavado de dinero proveniente de actividades ilícitas debe tener una mirada por sobre los transacciones online a partir de los movimientos de flujo de dinero través de la banca online o sistemas de pago electrónico, por ejemplo.

Estas cuestiones de política pública que escapan a la cuestión meramente sancionatoria establecida por el derecho penal abarca el debate actual en términos de supervisión de las actividades en el ciberespacio. En este sentido, diversos organismos y países han iniciado una discusión acerca de la intervención de los gobiernos en la red desde el punto de vista de la regulación de contenidos. Una primer iniciativa se dio en el año 2003, donde la Organización de las Naciones Unidas reunió en Ginebra, Suiza, a los representantes de 153 países para la elaboración de un plan de acción para el desarrollo de la sociedad de la información del siglo XXI. En la primera reunión de la Cumbre Mundial de la Sociedad de la Información (CMSI) se establecieron los principios de lo que se denomina "la gobernanza de Internet", donde el grupo solicita al Secretario General de las Naciones Unidas "elaborar una definición de trabajo del gobierno de Internet" e "identificar las cuestiones de política pública que sean pertinentes para el gobierno de Internet"(4), entre otras.

En la segunda parte de cumbre, realizada en Túnez en 2005, el plan de acción establece claramente que "la designación del organismo encargado de las cuestiones de política pública de Internet es el derecho soberano de los Estados. Estos tienen derechos y responsabilidades en lo que concierne a las cuestiones de política pública que suscita internet en el plano Internacional"(5) y especifica que el sector privado, la sociedad civil las organizaciones intergubernamentales y los organismos internacionales deben desempeñar un papel importante para la definición de las mismas. Si bien estos principios sientan las bases para la intervención de los Estados sobre la red, la mayoría de las medidas propuestas estaban orientadas a generar un entorno propicio de inversiones financieras y corregir las imperfecciones del mercado en aras de disminuir la brecha digital entre países. Así, en la declaración de principios de Ginebra se señala; "Los gobiernos deben intervenir, según proceda, para corregir los fallos de mercado, mantener una competencia leal, atraer inversiones, intensificar el desarrollo de infraestructura y aplicaciones de las TIC, aumentar al máximo los beneficios económicos y sociales y atender a las prioridades nacionales"(6).

En la actualidad, el debate acerca de la gobernanza de Internet llegó tuvo su corolario en la última reunión de la UIT realizada en Dubai, Emiratos Árabes en diciembre de 2012. En dicho marco, los 153 países miembros del organismo se dieron cita en el marco de la Conferencia Mundial de Telecomunicaciones para discutir, entre otras cosas, la intervención de los gobiernos en la red. En dicha oportunidad, la imposibilidad de firma de un nuevo tratado se dio a partir del lobby realizado por los Estados Unidos a la asignación de facultades al organismo en materia de regulación de Internet,

seguido por países como Gran Bretaña, Alemania, Japón, Canadá e India, entre otros, negándose a firmar el acta final si se incluía esta moción. Pese a esto, 89 de los 153 de los países firmaron una resolución anexa no vinculante donde se decide "invitar a los Estados Miembros a que detallen sus posturas respectivas sobre cuestiones técnicas, de desarrollo y de política pública internacional relacionadas con Internet que son competencia de la UIT..."(7).

Reflexiones acerca de la política de Internet Históricamente Internet fue producto de una serie de innovaciones de los años 60 y 70 que se produjeron en el seno de instituciones gubernamentales y centros de investigación de los Estados Unidos que proyectaban sus trabajos en ver como las computadoras podían comunicarse entre sí y compartir recursos entre los centros de informática y laboratorios académicos. Si bien la idea de creación de Internet parte de una necesidad estratégico-militar, su desarrollo y evolución tuvo un fin puramente práctico y experimental. ¿Pero cómo puede definirse Internet? Es una red electrónica que nuclea redes independientes de computadoras y otros dispositivos y permite el intercambio datos en forma digital a través de un protocolo de comunicaciones. En cuanto a su diseño es un medio de comunicación descentralizado, ya que no posee una unidad central que concentre el tráfico de información. Las redes que componen Internet poseen su propia configuración y se clasifican en diferentes tipos de acuerdo al área geográfica. En este sentido, la red no fue pensada y concebida en términos de seguridad de los contenidos sino en la seguridad física de las redes de telecomunicaciones que sustentan el tráfico de datos.

Como se señaló anteriormente, Internet no posee un Estado supremo ni existe un organismo internacional al estilo de Naciones Unidas o la Unión Europea que establezca políticas públicas globales. La Internet Society y el World Wide Web Consortium, con fuerte presencia de los gigantes de las telecomunicaciones, promueven el espíritu liberal no-intervencionista establecido en los principios básicos de la UIT en 1994, centrando sus funciones en el autogobierno de Internet. El debate actual esta puesto en la forma en que los Estados pueden intervenir en una red con presencia mayoritariamente privada, tanto a nivel de proveedores de acceso como empresas de servicios y contenidos. El estado de situación actual se encuentra empantanado en términos de la falsa dicotomía "regulación versus censura" impuesto por los defensores de los intereses comerciales de la red. Los partidarios de la censura argumentan que la intervención de los gobiernos siempre es arbitraria y que Internet es un medio libertario donde el intervencionismo estatal debe darse para corregir las fallas del mercado en el sector de las telecomunicaciones. Si bien es cierto que en la historia de Internet se sucedieron casos resonantes donde diferentes gobiernos vulneraron derechos y libertades de los usuarios, la discusión debe darse en un nivel más amplio.

Si bien las primeras respuestas por parte de los Estados ante la aparición de este nuevo tipo de criminalidad estuvieron centradas en reformas legislativas en materia penal y procesal penal para abarcar nuevas conductas indebidas e ilícitas, el lugar que ocupa Internet y la cantidad de actividades sociales, laborales y financieras intermediadas por el ciberespacio en la actualidad plantea la necesidad de una intervención por parte de los gobiernos. En este sentido, el punto de partida debe ser la facultad indelegable que poseen los Estados de garantizar y velar los derechos y libertades de las personas dentro de la sociedad. Internet es un medio de comunicación que se encuentra dentro de ella y ocupa un lugar indispensable en las actividades cotidianas de los ciudadanos. Partiendo de esta función, los principios más importantes por el que deben velar los gobiernos son la libertad de expresión y el derecho a la información de las personas, tal como lo señala la Declaración Universal de los Derechos Humanos en su Artículo 19, por el cual "todo individuo tiene derecho a la libertad de opinión y expresión, este derecho incluye el de nos ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión"(8).

Otra cuestión esencial que hace al diseño de la política pública de Internet es la llamada neutralidad de la red. Este principio incluye una serie de nociones relacionadas con la imposibilidad por parte de los proveedores de acceso a Internet y de servicios de contenido de obstaculizar o alterar en forma arbitraria las comunicaciones y la transferencia de datos. En este punto, los gobiernos deben actuar para el mantenimiento de la neutralidad de las comunicaciones a través de su intervención, regulando el servicio mediante el establecimiento de protocolos, la instrumentación de medidas administrativas o legislación que establezca reglas claras para las empresas. La actuación de los gobiernos por sobre la red debe establecerse mediante la más estricta legalidad y la intermediación de la Justicia, fundamentalmente para los casos que amerita la interceptación, seguimiento u observación de comunicaciones privadas. En este sentido, se puede trabajar conjuntamente con las empresas que brindan servicios de contenido en Internet mediante la firma de convenios de colaboración.

En conclusión, si bien resulta necesaria la tipificación de conductas indebidas, hechos ilícitos e ilegales por parte del derecho penal, civil o comercial; la cooperación internacional en este sentido y la reforma de los códigos procesales para la admisibilidad de pruebas electrónicas en el marco de una causa judicial, la solución penal resulta insuficiente en términos de diseño de una política pública para la red. En este sentido, resulta necesaria la creación en el seno de las administraciones centrales de un organismo gubernamental para el diseño de estrategias y políticas integrales en materia de cibercrimen. Las políticas resultantes deben estar fundadas en diagnósticos certeros basados en la realización de estudios y el acopio de información estadística sobre nuevas modalidades delictivas. A su vez, debe proponer legislación para la regulación del sector y brindar asistencia y asesoramiento a aquellos organismos que así lo requieran, brindando recomendaciones y líneas de acción estratégicas.

Notas al pie:

1) Organización de las Naciones Unidas (ONU): "MANUAL DE LAS NACIONES UNIDAS SOBRE PREVENCIÓN Y EL CONTROL DE DELITOS INFORMÁTICOS". En Revista Internacional de Política Criminal. Nueva York, Naciones Unidas, 1994, Nº 43 y 44.

2) Consejo de Europa, Convenio sobre la ciberdelincuencia. Estrasburgo, Consejo de Europa, 2001.

3) Krol, Ed: Conectate al mundo de Internet. México D. F., McGraw Hill, 1994.

4) Organización de las Naciones Unidas (ONU): Declaración de Principios de Ginebra de la Cumbre Mundial de la Información. Ginebra, Publicación de las Naciones Unidas, 2003.

5) Organización de las Naciones Unidas (ONU): Agenda de Túnez... (op. cit.)

6) Organización de las Naciones Unidas (ONU): Declaración de Principios de Ginebra... (op. cit.)

7) Unión Internacional de Telecomunicaciones: Actas Finales de la Conferencia Internacional de Telecomunicaciones 2012. Dubai, Publicación de la Organización Internacional de Telecomunicaciones, 2012.

8) Artículo 19 de la Declaración Universal de los Derechos Humanos.