Revista Mexicana de Ciencias Penales

ISSN 0187-0416

Año 3 • Número 10 • enero-abril de 2020 • $100.00

Ciberdelitos

- Tecnología, derecho y conflictos
  Bibiana Beatriz Luz Clara
- Convertir una debilidad en fortaleza. Primeras experiencias acumuladas
  Damián Paret Francia
- Los Estados, las criptomonedas y la ciberseguridad
  Humberto Martín Ruani
- Las operaciones con recursos de procedencia ilícita y las *fintech*: responsabilidad penal de las personas morales
  Alberto Enrique Nava Garcés

INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

TECNOLOGÍA, DERECHO Y CONFLICTOS

Bibiana Beatriz Luz Clara*

* Profesora e investigadora de la Universidad FASTA; Presidenta del Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata.

PALABRAS CLAVE *KEYWORDS*

Tecnología	*Technology*
Derechos	*Rights*
Riesgos	*Risks*

Resumen. La tecnología ha impactado fuertemente en nuestra sociedad, modificándola y creando nuevos procesos disruptivos que traen aparejados cambios profundos también en la forma de relacionarse en lo social y comercial, entre otros ámbitos, que requiere del derecho un análisis para su adecuación y tutela efectiva frente a las nuevas situaciones conflictivas y delictivas que, facilitadas por las nuevas tecnologías, pueden producirse. En este articulo analizaremos algunos posibles riesgos y la necesidad de tomar conciencia y acciones para la protección y solución.

Abstract. Technology has strongly impacted our society modifying it and creating new disruptive processes that bring about profound changes also in the way of relating socially and commercially, among others subjects, which requires an analysis from the Law for its adequacy and effective protection against new conflictive and criminal situations that, faciliatated by new technologies, can occur. In this article we will analyze some possible risks, and the need to take awareness and actions for protection and solution.

SUMARIO:

I. INTRODUCCIÓN

Los procesos de cambio en nuestra sociedad permiten comparar la evolución de las personas en el espacio y tiempo y su actitud frente a los nuevos desafíos. En el caso de la sociedad actual, frente a las tecnologías de la información y las comunicaciones, que se encuentran transformando vertiginosamente el mundo, en comparación a como era conocido hace algunos años.

Según indicaba el filósofo Javier Echeverría,[2] se reconocen tres entornos: el primero es el de la naturaleza, en el que transcurre la sociedad rural agraria basada en el trabajo del campo (*physis*), donde los tiempos son los de las estaciones y, por ende, se trata de tiempos largos; el segundo es el entorno de la ciudad (*polis*), de la industria y del mercado, donde los tiempos ya se aceleran y se fabrica en masa; y el tercer entorno es el electrónico, el espacio de la sociedad de la información, que se superpone a los dos anteriores y coexiste con ellos, aquí el poder económico lo tienen quienes manejan la conectividad y las redes.

Los elementos de este tercer entorno son muy diferentes a todo lo anteriormente conocido, ya que la distancia entre las personas se vuelve irrelevante, se confluye en las redes y requiere adaptación a este nuevo espacio para quienes no son nativos digitales.[3] Esto debido a que estos últimos están rodeados desde la más temprana edad por las tecnologías[4] de información y las telecomunicaciones, lo que los mantiene familiarizados con habilidades tecnológicas desconocidas a esa edad por las generaciones anteriores. El lenguaje digital se vuelve su segundo lenguaje.

[1] Acrónimo proveniente del inglés: *Internet of Things*.

[2] En su conferencia del 17/01/2001 en Málaga, "Sociedad y nuevas tecnologías en el siglo XXI".

[3] Término acuñado y divulgado por Marck Prensky en su libro *Inmigrantes digitales* (2001) para indicar a los niños nacidos desde 1990 en adelante, para quienes utilizar los elementos tecnológicos es muy sencillo, a diferencia del resto de las personas que tienen que aprender y esforzarse.

[4] Videocámaras, celulares, computadoras, tabletas, videojuegos, etcétera.

II. INICIO DE UNA NUEVA ETAPA: EL ENTORNO ELECTRÓNICO

Este nuevo escenario fue propiciado por la aparición de internet,[5] que permite nuevos tipos de comunicación mediante el acceso a redes, y por el cual se pueden desarrollar actividades comerciales, educacionales, médicas, laborales, de gobierno, entre otras.

El entorno electrónico es un espacio internacional y eminentemente visual. Es más complejo que la propia internet, donde se hacen nuevas relaciones, basadas en intereses comunes, y que impacta en la estructura económica y social.[6] Su inmediatez y velocidad permiten que las personas estén conectadas a amplias redes de contactos en tiempo real, de acuerdo con afinidades.

Estas comunidades crecen virtualmente y en forma constante. Es un ambiente multicultural y electrónico, en el que se generan, como en cualquier otro, situaciones conflictivas, que muchas veces no se sabe cómo atender o no se encuentran las personas idóneas para gestionarlas eficientemente, pero lo importante, que debemos tener en la mira, es tratar de lograr un ambiente de paz para las relaciones virtuales.

También la dinámica comercial ha cambiado desde que es posible hacer compras y otras operaciones en línea. Aquí uno de los mayores inconvenientes es el problema de la deslocalización y el acceso a la justicia, marcado por la falta de información y conocimiento de los usuarios, los altos costos a enfrentar ante una demanda que debe hacerse en ajena jurisdicción, sobre todo cuando el monto de la reclamación es pequeño. Ante estas dificultades es posible que dichas personas decidan no hacer nada, quedando de este modo sus derechos vulnerados sin la correspondiente reparación.

[5] Los orígenes de internet se remontan a finales de los años sesenta (1969). En plena Guerra Fría, un proyecto de investigación en redes de conmutación de paquetes, dentro del ámbito militar (ARPA) desarrolló una tecnología de conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud, llamados paquetes. Cada uno de ellos lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etcétera. El paquete contiene información suficiente como para dirigirse a su destino. El camino a seguir no se encuentra preestablecido, así, si una parte de la red cae o es destruida, el flujo de paquetes será automáticamente desviado a otros nodos alternativos.

[6] La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha trabajado —desde comienzos de este siglo— con el Grupo de Trabajo de Indicadores de la Sociedad de la Información (WPIIS, por sus siglas en inglés) para controlar las estadísticas de dichos indicadores, mediante cuestionarios modelo en hogares, empresas y gobiernos sobre el uso y aplicaciones de las TIC.

III. CONFLICTOS EN EL ENTORNO ELECTRÓNICO Y MEDIOS PARA RESOLVERLOS

Los métodos de resolución de disputas en línea (ODR)[7] aparecen aquí como una opción que puede aportar grandes beneficios, sobre todo cuando de relaciones de consumo se trata. Estas modalidades comerciales van en avance, y por ello es necesario dar respuesta rápida a sus necesidades por medio de mecanismos de resolución extrajudicial que complementen al sistema tradicional de administración de justicia, por su flexibilidad y pertenencia al medio electrónico, y permitan a los usuarios resolver sus conflictos en el mismo medio en el que se produjo el conflicto y con las herramientas electrónicas necesarias, reduciendo con ello los costos de la tramitación.

Los métodos ODR aprovechan la experiencia de los ADR[8] y le suman todas las posibilidades que brinda la tecnología para solucionar los conflictos que en el entorno electrónico se produzcan de modo ágil, y aun en otras situaciones que, habiéndose suscitado en el trato presencial, deciden optar por ellos para su resolución por las ventajas que implican, siendo los métodos principales:

- La negociación: aquí las partes actúan personalmente en la búsqueda de una solución al conflicto mediante sistemas que están automatizados y donde la comunicación puede ser sincrónica o asincrónica.[9] Se utilizan programas que facilitan la comunicación, identifican las posibles alternativas de solución y arman los acuerdos, emulando las funciones de un tercero neutral. Se utiliza mayormente para determinar los valores económicos en discusión. El éxito de estos sistemas depende de la naturaleza del conflicto, la precisión de la información que se suministra y la capacidad del *software* utilizado. La negociación puede ser totalmente automatizada[10] o negociación asistida,[11] según se tenga o no intervención humana en la negociación.

[7] *Online Dispute Resolution*: el término ODR es producto de las ciencias de la computación, donde se utiliza *on line*, que proviene del siglo pasado y es usado para hacer referencia al algoritmo que procesa sus entradas (*input*) de forma secuencial a medida que las recibe. Hace alusión a un servicio que se brinda a medida que se está produciendo una actividad. En su inicio los ODR eran métodos ADR conducidos *on line*, pero con el tiempo y el avance tecnológico fueron demostrando capacidades propias superadoras.

[8] ADR es el acrónimo inglés de *Alternative Dispute Resolution*. Se trata de los sistemas alternativos de resolución de conflictos, tales como el arbitraje, la mediación y la conciliación.

[9] Según sea que las partes estén en línea en el mismo momento, o no.

[10] *Fully automated negotiation.*

[11] *On line assited negotiation.*

- La mediación: es un método donde un tercero neutral, el mediador, mediante sus técnicas, ayuda a las partes a recuperar el diálogo perdido o a mejorar su comunicación, a fin de que encuentren por ellas mismas alternativas de acuerdo al conflicto. Se desarrolla mediante las herramientas electrónicas en línea. Las partes se comunican con la ayuda del mediador, ya sea en forma sincrónica o asincrónica. En la mediación concurrente, cuando varias personas interactúan en línea, la comunicación debe ser sincrónica. En cambio, cuando no se requiere la presencia, la comunicación puede ser asincrónica.

- El arbitraje en línea: es un método extrajudicial de resolver conflictos por el cual las partes, mediante su libre voluntad expresada en un acuerdo en tal sentido,[12] confían a un tercero la solución de sus controversias, atribuyéndole autoridad para emitir una resolución.[13] El tercero neutral es generalmente un experto en la materia requerida, que inspira la confianza de las partes por sus conocimientos y experiencia. El arbitraje es vinculante y podrá solicitarse el auxilio de la fuerza pública para lograr la ejecución del laudo, en el caso de que el obligado no cumpla, ya que los árbitros carecen de *imperium*.

Asimismo, en este entorno existen otros mecanismos de estímulo al cumplimiento de lo acordado entre las partes de modo voluntario. Estos son:

- Los sistemas de puntuación y reputación: estos son los que están basados en las opiniones que indican los clientes una vez que han utilizado el servicio y que les permite calificarlos según su satisfacción, opiniones a las que el público puede acceder y le permiten una mejor toma de decisiones.

- Sellos de confianza: donde se exhiben etiquetas de calidad que acreditan el cumplimiento de ciertos estándares.

- Los reembolsos, o chargeback: que permiten recuperar la suma pagada cuando las expectativas que tuvieron durante la transacción se han visto frustradas, especialmente cuando el pago ha sido realizado con tarjeta de o pasarelas de pago, a quienes se les solicitará la retención de lo pagado.

[12] La cláusula arbitral o cláusula compromisoria que las partes deciden insertar en los contratos para acudir al arbitraje en caso de conflicto.

[13] El laudo arbitral.

- Las cuentas de garantía: el dinero es entregado al comerciante cuando el cliente ha recibido el producto de conformidad, mientras tanto permanece depositado en una cuenta de un tercero al efecto.

- La suspensión del acceso: en este caso, se le suspende por su inconducta el acceso al sitio como usuario en el que se encontraba registrado o era miembro.

- Las *black lists*: son listas de comerciantes de riesgo para los usuarios, que se forman con los incumplidores y sirven para prevenir al público.

Todos estos sistemas son complementarios y ayudan a la desjudicialización, pero no impiden que el usuario haga uso de las acciones ante los tribunales si lo considera necesario.

Debemos agregar, además, a los *smart contracts*[14] o contratos inteligentes, que son negocios jurídicos programados gracias a las posibilidades que brinda el internet de las cosas (IoT).[15] Se trata de programas en la nube que siempre actúan del mismo modo y permiten guardar información que no puede ser modificada. El *software* autorizará y corroborará que el contrato sea válido y registrará la operación de modo transparente en un registro contable digital que no podrá luego ser modificado, lo cual ayuda a la transparencia de las transacciones y ahorra costos. Utilizan *blockchain*[16] para garantizar que nadie podrá modificar las condiciones contractuales. En este caso, es el mismo protocolo de confianza del código el que hace cumplir las pautas programadas a ambas partes. Al encontrarse escritos en lenguajes de programación, no están sujetos a interpretación, con lo cual se evitan discusiones y diferencias.

El programa siempre actuará de la misma forma sin depender de la voluntad de un tercero. Asimismo, permite incorporar métodos ODR que integran a un sistema de verificación autónoma de las obligaciones que asumieron las partes, así como mecanismos de ejecución de las consecuencias indicadas en

[14] Se trata de un programa de *scripts* modulares que reproduce los acuerdos y las reglas pactadas y también las consecuencias de los incumplimientos.

[15] Interconexión de objetos de uso cotidiano. Se interconectan objetos heterogéneos a través de diferentes redes y métodos de comunicación, posicionando dispositivos que proveen información y realizan acciones en forma autónoma. Este ecosistema tiene tres partes: aplicaciones, *software* y sensores. Siempre por los sensores recibiremos la información, por eso deben ser especialmente cuidados, y cada día aumentan las aplicaciones para las distintas áreas.

[16] Cadena de bloques: es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores, y en esto se basa su seguridad.

el contrato. Mediante este tipo de contrato se pueden cerrar de modo automatizado transacciones electrónicas y reclamaciones.

Como vemos, todas estas herramientas ágiles presentan una visión transformadora de la realidad social y comercial, por ello es preciso entender el paradigma de desarrollo actual y aplicar, por tanto, las nuevas tecnologías como mecanismo que facilite el acceso a la justicia, fomentando la dignidad e igualdad de las personas en un acceso más equitativo que el uso de tales herramientas puede propiciar.

Podremos cumplir, así, con el objetivo número 16 de los Objetivos de Desarrollo Sustentable (ODS) de las Naciones Unidas, que indica: "Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles" (ONU, 2015), base de la sostenibilidad económica, social y ambiental de los 193 estados miembros firmantes.

Para que dichas políticas tengan éxito se requiere de alianzas entre los gobiernos, el sector privado y la sociedad civil, construidas sobre principios y valores comunes y metas compartidas de la agenda para el desarrollo.

IV. INTERNET DE LAS COSAS (IOT),[17] RIESGOS Y ACCIONES DE PROTECCIÓN

Otro de los fenómenos frente al cual nos encontramos es la interconexión de objetos heterogéneos de uso cotidiano a través de diferentes redes y métodos de comunicación, posicionando dispositivos que proveen información y realizan acciones en forma autónoma. La IoT lo conecta todo. Vivimos en un mundo hiperconectado que se potenciará aún más cada día.

Este ecosistema tiene tres partes: aplicaciones, *software* y sensores. Es por medio de los sensores que recibimos la información, por eso deben ser especialmente cuidados, ya que progresivamente aumentan las aplicaciones para las distintas áreas.

Las tendencias de mercado confluyen hacia la IoT desde la irrupción de IPV,[6] por lo cual se deben tener reglas claras para mantener la estabilidad de internet, pues cuantos más dispositivos conectados encontremos más riesgos a considerar:

- La interconexión entre dispositivos de alta y baja seguridad conforma un ambiente vulnerable, que puede facilitar los accesos indebidos, por lo cual se deberá contar con algoritmos

[17] Acrónimo proveniente del inglés: *Internet of Things*.

criptográficos y gestión de claves adecuadas.

- La privacidad de los datos obtenidos, sobre todo en los aspectos más sensibles, tanto los que genera el usuario como los que se brindan a terceros[18] o los que adquiere el sistema de modo automático. Será necesario concientizar a todos los actores del sistema para el resguardo adecuado de dicha información.

- Debida identificación de la identidad de cada objeto conectado y su función para circunscribir la acción de cada uno de ellos al contexto y usuario correspondiente y así poder definir los mecanismos de seguridad apropiados.

- Definir la confianza en la IoT en un entorno dinámico y colaborativo entre todos los componentes vinculados. Los usuarios deben confiar en el uso adecuado de los dispositivos conectados, con un marco legal respaldatorio.

- Todos los objetos deberían: i) ser seguros por sí mismos en cuanto al *hardware* y al *software*; ii) conocer el estado de la red y sus servicios; iii) poder defenderse contra ataques de intrusos y fallas.

La economía mundial se realiza en forma electrónica, por ello es fundamental considerar las distintas amenazas al sistema, dada la cantidad de dinero que fluye en este entorno y los nuevos negocios que generan.

Debemos prevenir el robo de la información y su acceso de forma ilegal, comprometida o atacada, poniendo en riesgo a la comunidad, y mantener indemnes sus derechos.

Por ello, es necesario realizar el análisis de los métodos preventivos, dado el impacto económico y social que pueden implicar, de acuerdo con los siguientes criterios:

- Tipo de acción: interceptación, sabotaje, robo de datos, denegación de servicios

- Tipo de perpetrador: quien está cometiendo las acciones: hackers, terroristas, gobiernos, delincuentes, revolucionarios.

- Tipo de objetivo: hacia donde o quien se quiere atacar, por ejemplo, sociedad civil, organizaciones, empresas, medios de comunicación, unidades militares, infraestructuras críticas, etcétera.

[18] Datos de geolocalización, claves de acceso, números de teléfonos, de tarjetas de crédito, entre otros.

Es necesario evitar que la cantidad de personas afectadas se multiplique, ya que las amenazas son múltiples: *malwere* (software malicioso); *ramsomwere* (para tomar control de los datos por un precio); *botnets* (redes o dispositivos secuestrados que realizan acciones sin conocimiento de sus usuarios); denegación de servicios (para demostrar que se puede tomar control de los sistemas o para obtener ganancias); *phishing* (mediante ingeniería social se obtiene información de las personas a quienes se engaña para que realicen algo).

Las categorías de ciberseguridad que deben considerarse para ver cómo se pueden proteger los usuarios son: i) *Link* o enlace; ii) Infraestructura de telecomunicación; iii) Seguridad de internet (ISP, rutas, nombres de dominio, comunicación misma, elementos de hardware); iv) Seguridad de los procesadores; v) Aplicaciones; vi) Seguridad de los datos; vii) Comprobación de identidad de usuarios; viii) Seguridad de los servicios esenciales.

Los posibles problemas de seguridad pueden provenir de:

- Usuario travieso: cuando accede al dispositivo, de manera desprevenida para el fabricante, e ingresa a utilidades limitadas del producto.
- Fabricante inmoral: el productor del dispositivo usa y explota las tecnologías para revelar información del usuario a extraños.
- Agresor externo: conocido también como "entidad ajena" porque no forma parte de la red de la IoT y no tiene autorización para acceder, aun así, intenta obtener información confidencial y puede causar el mal funcionamiento de las entidades con IoT.
- Programación deficiente: el desarrollador de software para la aplicación IoT o los dispositivos IoT, pueden escribir códigos no seguros que permitan reconocer los datos del usuario.

Las fuentes de amenazas pueden ser utilizadas como vía de acceso para vulnerar los sistemas de seguridad digital del usuario, estableciendo situaciones de extorsión, robo, secuestro u otros delitos informáticos. Las áreas que más pueden verse afectadas por la IoT son la privacidad y la seguridad de las personas.

Se debe tener cuenta la alta escalabilidad de los ataques. Debido a que los sistemas IoT utilizan la red de redes para la comunicación y desde un punto cualquiera de la red, el ataque se difunde rápidamente hacia nuevas conexiones de puntos no atacados inicialmente.

Todos los componentes conectados a internet están expuestos a la intrusión indebida.

Existen, por lo tanto, algunos desafíos en este ecosistema de responsabilidades donde cada uno tiene un importante papel: realizadores de aplicaciones, operadores de plataformas, desarrolladores que no se toman el tiempo para considerar las implicancias de sus creaciones. Todos debemos involucrarnos para esta regulación, incluidos los usuarios, que tenemos el poder de decidir qué queremos y qué no. En este sentido, deben regularse las exigencias mínimas para que el uso de IoT sea seguro,[19] sobre todo para quien lo utiliza.

V. CONCLUSIÓN

Advertimos que el entorno electrónico es el espacio que se encuentra atrayendo la mayor parte de actividades de nuestra sociedad digital. Que es un espacio nuevo, dinámico y visual en el que pueden ocurrir distintos tipos de conductas, algunas que generan conflictos que deben resolver rápidamente para evitar que escalen y mantener las relaciones pacíficas, y para ello existen mecanismos ODR y otros ágiles y alternativos lo favorecen. Pero por la irrupción de las tecnologías vinculadas al uso de IoT, se pueden generar también situaciones de riesgo y conductas delictivas que deben ser perseguidas y fijar reglas claras para minimizar los riesgos a los que se enfrenta toda una sociedad conectada y vulnerable. Esto requerirá el esfuerzo conjunto de los países, mediante la conformación de espacios de trabajo interdisciplinarios, para fijar pautas comunes en cuanto a las normas técnicas y legales, y perseguir determinadas acciones dañosas, pero sin perder de vista que, si se regula demasiado, Internet puede perder su naturaleza libre, ya que lo que necesitamos es que sea abierta, y segura para todos

[19] La Online Trust Alliance (OTA), desde 2004, desarrolla estándares de seguridad, analiza las buenas prácticas, el futuro programa de certificación de IoT: abordaje de amenazas y vulnerabilidades, y reporta los incidentes ocurridos.

VI. FUENTES DE CONSULTA

Alzate Sáez de Heredia, R. y Vásquez de Castro, E. (2013). *Resolución de disputas en línea*. España: Ed. Reus.

Betancourt, D., Gómez, G. y Rodríguez J. (2016). "Introducción a la internet de las cosas", En *Revista Tecnogestión. Una Mirada al Ambiente*, 3(1). Disponible en: https://revistas.udistrital.edu.co/index.php/tecges/article/view/12132. Consultado el 31 de agosto de 2019.

Osepa, S. (14 de junio de 2019). "Conferencia IoT y Políticas Públicas". Internet Society.

Ebner, N. y Zeleznikow, J. (2015). "Fairness, trust and Security in Online Dispute Resolution". En *Journal of Public Law and Policy*, 36(2). Disponible en http://digitalcommons.hamline.edu/jplp/vol36/iss2/6

Echeverria, J. (1999). *Los señores del aire*. Barcelona: Ediciones Destino.

Vilalta Nicuesa, A. (2013). *Mediación y arbitraje electrónicos*. España: Ed. Aranzadi.

ISSN 0187-0416