Fondo Editorial de la Universidad Bicentenaria de Aragua
Revista Arbitrada de la Facultad de Ciencias Jurídicas y Políticas | Escuela de Derecho.
Nro.16. 2024 (julio-diciembre)
Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

DELITOS INFORMÁTICOS: ANÁLISIS FORENSE DE LA CIBERSEGURIDAD EN VENEZUELA

Abog. Rodríguez Mileskii
Universidad Bicentenaria de Aragua

Enviado: marzo 2024 • Aprobado: septiembre 2024 • Publicado: diciembre 2024

Resumen

El presente artículo académico plantea como propósito general analizar los riesgos legales de la Ciberseguridad en Venezuela, el marco normativo de los delitos informáticos y la eficacia de la criminalística forense para investigar y analizar los incidentes que atenten contra la seguridad informática; en el entendido que el avance de la tecnología ha cambiado nuestra realidad en todos los ámbitos, aparejando no solo beneficios a nivel social y económico, sino situaciones negativas que se constituyen en una serie de prácticas maliciosas o ataques informáticos, destinados a afectar no los datos, ya sean personales, empresariales o gubernamentales, sino la confidencialidad, lo cual ha generado la imperiosa necesidad del tratamiento legal de la ciberseguridad en nuestro país a los efectos de evitar la pérdida, divulgación o accesos no autorizados a la data en servicios digitales, tecnológicos y/o internet, lo que se traduce en usos ilegales de las tecnologías de la comunicación y la información. De igual forma, siendo que la criminalística forense desempeña un papel crucial en la recolección y manejo de las evidencias del ámbito cibernético, su papel preventivo permite identificar y mitigar los riesgos para detectar patrones delictivos y anticiparse a posibles ataques. En virtud de lo indicado, se empleó como metodología el diseño de una investigación documental, apoyado en un nivel explorativo-descriptivo y como técnica de procesamiento de datos el análisis crítico interpretativo a los efectos de comprender el fenómeno de la ciberseguridad en los aspectos señalados, considerando sus implicaciones y las garantías de los derechos sociales, económicos y culturales en nuestro país.

Palabras Clave: Ciberseguridad, delitos informáticos, criminalística, ataques informáticos, privacidad de datos.

CYBERCRIMES: FORENSIC ANALYSIS OF CYBERSECURITY IN VENEZUELA

Abstract
The present academic article proposes as a general purpose to analyze the legal risks of Cybersecurity in Venezuela, the regulatory framework of computer crimes and the effectiveness of forensic criminalistics to investigate and analyze incidents that threaten computer security; in the understanding that the advancement of technology has changed our reality in all areas, bringing not only benefits at a social and economic level, but negative situations that constitute a series of malicious practices or computer attacks, intended to affect not the data, whether personal, business or governmental, but confidentiality, which has generated the imperative need for the legal treatment of cybersecurity in our country in order to avoid the loss, disclosure or unauthorized access to data in digital, technological and/or Internet services, which translates into illegal uses of communication and information technologies. Similarly, since forensic criminalistics plays a crucial role in the collection and management of evidence in the cybernetic field, its preventive role allows to identify and mitigate risks to detect criminal patterns and anticipate possible attacks. Based on the above, the design of a documentary investigation was used as a methodology, supported by an exploratory-descriptive level and as a data processing technique, critical interpretative analysis in order to understand the phenomenon of cybersecurity in the aspects indicated, considering its implications and the guarantees of social, economic and cultural rights in our country.
keywords: Cybersecurity, computer crimes, criminalistics, computer attacks, data privacy.

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

Introducción

En el sector jurídico, la Ciberseguridad es una necesidad apremiante debido a la confidencialidad y privacidad de la información que manejan. En este sentido, un incidente de seguridad puede tener graves consecuencias económicas, legales y reputaciones a nivel personal u organizacional. La ciberseguridad, tiene importantes implicaciones jurídicas en Venezuela, desde la tipificación de delitos hasta la necesidad de adaptación constante de las leyes y la capacitación de los operadores de justicia.

El sector jurídico en particular, debe priorizar la protección de la información confidencial que maneja y las garantías de los derechos a la privacidad y libertad de expresión, en el entendido que los ciberataques son intentos maliciosos de acceder, dañar o interrumpir sistemas informáticos, redes o dispositivos electrónicos, en consecuencia, para analizar el escenario descrito la criminalística desempeña un papel crucial para resolver estos incidentes de seguridad informática. Es sabido, que este fenómeno ha evolucionado notablemente desde sus primeros días, en la década de 1980, cuando los ataques digitales eran menos frecuentes y solían ser realizados por individuos o pequeños grupos con habilidades técnicas avanzadas. Con el tiempo, los ciberataques se han transformado en amenazas más sofisticadas y organizadas, perpetradas por actores estatales, grupos criminales y hacktivistas. Por ello, actualmente se sostiene que la seguridad en internet es una de las mayores preocupaciones entre usuarios y empresarios del país, dado que Venezuela es uno de los lugares con mayores ciberataques, razón por la que se ha convertido en todo un negocio para empresas de seguridad, tanto que las compañías encargadas de mejorar la ciberseguridad han tenido un gran crecimiento en los últimos años.

Así pues, abordar una revisión documental del estatus de la ciberseguridad en Venezuela, describir su realidad y las tendencias en la materia y su relación con la criminalística, implica desarrollar la noción general de este término a la luz de su regulación jurídica y mitigación de riesgos. Conforme a lo referido por Urdaneta (2016), la Ciberseguridad constituye un conjunto de prácticas, tecnologías y procesos diseñados

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

para proteger sistemas, redes y datos de amenazas cibernéticas, y cuyo objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de la información digital, lo que implica prevenir el acceso no autorizado, la alteración o la destrucción de datos. Ello considerando que la protección de los sistemas y la información frente a las amenazas cibernéticas, es crucial para garantizar la integridad y confidencialidad de los datos. Aunado al desempeño de la criminalística forense como disciplina para investigar y analizar incidentes que atenten contra la seguridad informática, es decir, determinar qué pasa si a nivel organizacional se producen ataques cibernéticos, y cómo determinamos la naturaleza del ataque.

En este sentido, se analizaron aspectos técnicos y legales que conforman un marco jurídico regulatorio que está en desarrollo con la interacción de la criminalística y criminología, con leyes claves que establecen un fundamento, pero que necesitan ser fortalecidas y actualizadas para enfrentar los desafíos actuales del ciberespacio, en el entendido que ha enfrentado críticas por su falta de actualización y por no abordar de manera integral las nuevas amenazas cibernéticas. Ello así, muchos expertos consideran que las normas en esta materia deben ser revisadas para adaptarse a la evolución rápida de la tecnología y las tácticas de los cibercriminales, tales como: Ley Especial contra Delitos Informáticos (LECDA) (2001), Ley Orgánica de Telecomunicaciones (2000), Ley de Infogobierno (2013). Además, se ha señalado que algunas regulaciones vulneran derechos fundamentales, como la libertad de expresión, lo que requiere un balance entre seguridad y derechos individuales, tal es el caso del reciente del Decreto N° 4.975 de la presidencia de la República, de fecha 20 de agosto de 2024, publicado en la Gaceta Oficial N° 42.939, que regula la creación del Consejo de Ciberseguridad.

Ahora bien, es sabido y por todos conocidos que la sociedad está dominada por la tecnología, el valor de la información y del conocimiento ha alcanzado niveles muy altos, por lo que personas, entes públicos y organizaciones deben promover una efectiva gestión de la seguridad de la información para proteger este activo y minimizar el impacto en los servicios causados por vulnerabilidades o incidentes de seguridad en esta materia. Es decir, los avances tecnológicos acarrean un alto riesgo para personas, empresas y

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

gobiernos, ya que se puede exponer la privacidad y datos importantes de las personas. A nivel organizacional a pesar de que todo el riesgo es de manera intangible, impacta en lo tangible, entiéndase, que generan pérdidas económicas, daño a la imagen, inclusive la pérdida de confianza, y a nivel de gobierno se ven expuestos a la fuga masiva de información sensible, ataques a plataformas, sistemas vulnerables de servicios, por lo que deben evaluar constantemente sus brechas de seguridad mediante protocolos previstos en ley para atender de forma preventiva cualquier crisis o ataques imprevistos.

Metodología

La metodología empleada en este estudio es la cualitativa, orientada hacia un tipo de investigación documental, considerando que se buscó comprender el fenómeno de la Ciberseguridad y su marco regulatorio en el contexto jurídico venezolano; se consideró fuente principal de información la revisión documental relativa al impacto de las amenazas y riegos en la materia de ciberseguridad, cuando hablamos de la protección de datos personales, la privacidad y la libertad de expresión se trata. La técnica empleada para este tipo de investigación se denomina “técnica de la observación documental” o “guías de observación documental”.

Resultados

Los Delitos Informáticos

Primeramente, hagamos referencia al concepto de delito, según refiere Aveledo (2010), el Código Penal Venezolano (2021), no da una definición expresa del delito, por lo que indica que un delito comprende: “las acciones u omisiones prevista por la ley y castigada por ella por una pena”. Ello así, el delito informático, es aquel donde el sujeto activo comete una acción o actividad que debe encuadrar en la norma jurídica y debe ir en contra del ordenamiento jurídico establecido para dar castigo al que cometa el hecho punible, el que cometa este delito debe tener la capacidad para ser responsable y tener la culpabilidad.

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

En este orden de ideas, es importante resaltar que los delitos informáticos en Venezuela han ido en aumento en los últimos años, impulsados por la crisis económica y el uso creciente de plataformas digitales. Por ello, a continuación, se presentan los tipos de delitos informáticos más comunes en nuestro país, cuyas penalidades oscilan de cuatro (4) a diez (10) años con sanciones pecuniarias, regulados por la Ley Especial contra los Delitos Informáticos (2001), publicada en Gaceta Oficial Nº 37.313, en fecha 30 de octubre de 2001, cuyo objetivo es ser utilizada como herramienta o instrumento legal para proteger a todas las personas que empleen la utilización de la tecnología de información. Sin embargo, no aborda de manera directa la protección de datos personales, sino que clasifica estos delitos en cinco categorías: contra el orden económico, la propiedad, la privacidad de las personas y las comunicaciones, y contra niños y adolescentes.

Más allá de lo referido anteriormente, la Constitución de la República Bolivariana de Venezuela (1999), prevé la intención política del Estado venezolano de valorar y utilizar la ciencia y la tecnología e innovación como pilar fundamental para el desarrollo. De igual forma, nuestro texto constitucional, establece un marco regulatorio que protege tanto la confidencialidad de datos como la libertad de expresión (artículos 28, 43, y 60), aunque la falta de una ley específica sobre protección de datos personales plantea desafíos en la práctica. La interrelación entre estos derechos es crucial para el respeto y la promoción de la dignidad humana en el país.

Aunado a ello, la Ley Orgánica de Telecomunicaciones publicada el 12 de junio de 2000, en la Gaceta Oficial de la República Bolivariana de Venezuela No. 36.970, creó un marco legal moderno y favorable para la protección de los usuarios y operadores de servicios de telecomunicaciones en un régimen de libre competencia, así como para el desarrollo de un sector prometedor de la economía venezolana. En esta misma orientación, se promulgó en fecha 30 de abril de 2012, una nueva Ley Orgánica contra la delincuencia organizada y financiamiento al terrorismo (LOCDOFT), y la cual tiene por objeto prevenir, investigar, perseguir, tipificar y sancionar los delitos relacionados con la delincuencia organizada y el financiamiento al terrorismo de conformidad con lo dispuesto en la Constitución de la República y los tratados internacionales relacionados con la

materia, suscritos y ratificados por la República Bolivariana de Venezuela. De manera tal, ofrece el marco jurídico para sancionar el acceso indebido a datos personales en Venezuela y la incursión directa en las prácticas de robo de información.

De igual modo cabe precisar, que la Ley de Infogobierno (2013), tiene por objetivo desarrollar aplicaciones informáticas en tecnologías libres que soporten los procesos que requieran los servicios públicos para una interacción ágil y eficiente con la ciudadanía, mediante operaciones automatizadas y auditables. Asimismo, protege los derechos y libertades de las personas al garantizar que el uso de las tecnologías de información por el Estado se ajuste a los principios, límites y garantías establecidos en la Constitución, las leyes y demás actos formales.

En este mismo orden, especial mención merece la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (2011), la cual incorpora en su art. 27, algunas consideraciones respecto a la publicación de mensajes, que dejan abierta la ventana para la tipificación de los supuestos de hechos no permitidos, como por ejemplo la incitación al odio y la intolerancia por razones religiosas, políticas por diferencia de género, por racismo o xenofobia, la propaganda de guerra, fomentar zozobra en la población, inducir al homicidio, etc.

Ahora bien, por último y no menos importante la Ley de Mensajes Datos y Firmas Electrónicas (2001), y la ciberseguridad están interrelacionadas y se complementan para garantizar la seguridad y privacidad de la información en el entorno digital. Esta ley, juega un papel crucial en la ciberseguridad al establecer un marco normativo que promueve la autenticación, el cifrado, la implementación de políticas de seguridad y la protección de datos sensibles. Estas medidas, no solo aseguran la integridad y confidencialidad de la información, sino que también fortalecen la confianza en las transacciones digitales en un entorno cada vez más complejo y amenazante.

Aunado a lo anterior, y en consonancia con lo referido, en el año 2019, se publicó un texto de un anteproyecto de Ley Constitucional del Ciberespacio cuya aprobación pretendía la Asamblea Nacional Constituyente (AN) venezolana, el cual despertó alertas

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

en la sociedad civil y los medios de comunicación locales. Este nuevo instrumento legislativo, expandía e incrementaba los poderes del Ejecutivo Nacional para la vigilancia sobre el internet, se convertiría así en una nueva herramienta de control que pudieran caracterizar políticas públicas de restricción del flujo de información y de la libertad de expresión en la web.

Por otra parte, respecto a los avances de la seguridad en el internet Venezuela se puede afirmar que no cuenta con una estrategia nacional clara de seguridad en internet. Aunque si existe un sistema de seguridad nacional informática, con el objetivo de implementar medidas que generen confianza, proporcionando niveles óptimos de ciberseguridad. El organismo responsable de este sistema es la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). Este organismo es además parte de la sede del VenCERT (Sistema Nacional de Gestión de Incidentes Telemáticos), encargada de prevenir y gestionar posibles incidentes en los sistemas informáticos de la administración pública del país. VenCERT también tiene entre sus tareas, formar a personas en temas de seguridad cibernética. Aunque todavía queda mucho más por avanzar en cuanto a educación en estos temas.

Sin embargo, no puede dejar de mencionarse como un aspecto relevante, la reciente creación del Consejo Nacional de Ciberseguridad a través de Gaceta Oficial N° 42.939, Decreto N° 4.975 de la Presidencia de la República, de fecha 20 de Agosto de 2024, en un contexto socio político determinante, y el cual funcionará de manera permanente como un órgano consultivo y de asesoría bajo la autoridad del jefe de Estado, “enfocado en la prevención de los usos ilegales de las tecnologías de la comunicación y la información” y cuya función principal es el establecimiento de una red de monitoreo constante para incidentes telemáticos, “con el objetivo de prevenir, mitigar y gestionar los delitos informáticos de forma más eficaz. A su vez, el organismo podrá solicitar información a entidades tanto públicas como privadas”. Asimismo, este Consejo Nacional de Ciberseguridad, tiene 13 atribuciones específicas, incluyendo la creación de una red de vigilancia, que podrían ser útiles para contrarrestar los "ataques cibernéticos".

Al respecto, sería importante observar la evolución del Consejo Nacional de Ciberseguridad y su impacto en la seguridad digital del país, así como evaluar si realmente contribuye a la protección de la privacidad y los derechos digitales de los ciudadanos. En efecto, debe destacarse que la creación de este organismo administrativo surge en un contexto donde hay cientos de páginas web con el acceso bloqueado por las empresa proveedoras de Internet, incluyendo portales de noticias y la red social X (Twitter) ,después que el 9 de agosto de 2024, sujetos a presentar recaudos para establecer medidas administrativas definitivas. De igual forma, este Consejo de Ciberseguridad se crea motivado en la seguridad digital, destinado a resguardar los derechos de la población en el ámbito digital y de las estructuras informáticas del Estado, incluyendo la protección de datos, violencia de género, mecanismos para identificación de responsables de extorsiones, acoso, vulneración de información privada, así como otros delitos propios del entorno digital que afectan a las personas e instituciones.

Así las cosas, dados los avances de las tecnologías y técnicas de vigilancia, la falta de un marco sólido y actualizado del derecho a los datos personales en el espacio digital redunda en mayores brechas en la protección y desencadena una serie de perjuicios contra los derechos de las personas usuarias que pudieran minar su confianza en Internet, lo que también implicaría que dejen de utilizar de manera libre estos medios para expresar sus opiniones, exigir respeto a los derechos, y ejercerlos en línea sin miedo a represalias. Por ello, se ha afirmado que el referido Decreto Presidencial, en principio desprotege principalmente la privacidad en línea, lo que a su vez impacta negativamente en derechos conexos como la libertad de expresión y la garantía a los derechos económicos, sociales y culturales en el país.

Desafíos actuales de la Criminalística Forense

La criminalística forense, es fundamental para fortalecer la ciberseguridad en Venezuela al proporcionar las herramientas necesarias para investigar delitos informáticos, asegurar un marco legal adecuado y contribuir a la prevención de futuros incidentes. Sin embargo, es esencial abordar los desafíos existentes para mejorar su eficacia y capacidad operativa frente a los delitos informáticos. Para Muñoz (2024), la informática forense se consolida como una disciplina para prevenir e investigar delitos

cibernéticos. Con su técnica especializada, promueven la extracción de datos desde discos duros, dispositivos de almacenamiento, redes y otros medios digitales a los efectos de la recuperación de archivos eliminados, la identificación de malware y la reconstrucción detallada de los eventos. Así pues, la importancia del análisis forense digital en la era tecnológica es fundamental, pero enfrenta varios desafíos en Venezuela, como la falta de recursos, corrupción e inestabilidad política. Estos factores dificultan el trabajo efectivo de los profesionales en el campo forense y limitan su capacidad para combatir eficazmente la ciberdelincuencia.

Conclusión

Analizado el marco regulatorio venezolano en materia de ciberseguridad, en el contexto de la protección de los datos personales, el derecho a la confidencialidad y la libertad de expresión, se puede afirmar que se requiere mayor desarrollo legal, dado que este panorama constituye un aspecto crucial para la protección de los derechos humanos, a tenor de lo consagrado en nuestro marco constitucional. Así pues, aun cuando la Constitución de 1999, establece en su artículo 60 el derecho a la protección de la privacidad, confidencialidad y datos personales, actualmente no existe una Ley Orgánica de Protección de Datos Personales que regule de manera integral este ámbito.

En este estricto orden de ideas, se concluye lo siguiente:

- Venezuela carece de una ley específica que desarrolle los principios, derechos y obligaciones relacionados con la recolección, almacenamiento, procesamiento y transferencia de datos personales.

- La legislación vigente, como la Ley Especial Contra los Delitos Informáticos (LECDA) (2001), aborda el tema de manera limitada y no ofrece un marco legal completo para garantizar la protección de datos y la confidencialidad.

- La lucha contra la ciberdelincuencia requiere de una verdadera colaboración y capacitación entre diversas entidades nacionales e internacionales. Compartir

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

información y recursos es vital para una respuesta efectiva ante las amenazas cibernéticas

A la luz de lo indicado, la protección de datos personales en Venezuela enfrenta desafíos significativos debido a la ausencia de un marco legal integral y a los riesgos de exposición y vulneración de este derecho fundamental. En este sentido, la promulgación de una Ley Orgánica de Protección de Datos Personales, es una prioridad para garantizar la privacidad de los ciudadanos en el entorno digital, considerando que la falta de un marco legal adecuado expone a los ciudadanos venezolanos a diversos riesgos, como la exposición no autorizada de datos personales, su uso con fines inesperados y la venta o acceso por parte de terceros sin consentimiento. Así pues, urge la necesidad de garantizar el derecho de las personas a acceder, rectificar, actualizar, suprimir o mantener confidenciales sus datos personales, así como establecer sanciones efectivas ante incumplimientos. Por otra parte, respecto al derecho que consagra la libertad de expresión, algunas restricciones evidenciadas en cuanto a la publicación y manejo de las redes sociales actualmente, se evidencia la necesidad urgente de fortalecer la ciberseguridad en Venezuela para proteger los derechos fundamentales de los ciudadanos (as).

Referencias

Baez, E (2021). Ciberespacio y Cibermundo: delimitaciones conceptuales del materialismo sistémico. Ciencia y Sociedad, vol. 47, núm. 1, pp. 45-57, 2022. Instituto Tecnológico de Santo Domingo. https://www.redalyc.org/journal/870/87070563004/html/

Rodríguez, G (2016). Ciberseguridad, realidad y tendencias en Venezuela. https://www.redalyc.org/journal/1275/127550463012/html/#fn1

Asamblea Nacional Constituyente. Constitución de 1999. G.O. 36.860 de fecha 30 de diciembre de 1999.

Asamblea Nacional Bolivariana de Venezuela. Ley de Infogobierno Gaceta Oficial No. 40.274 de fecha 17 de octubre de 2013.

Asamblea Nacional Bolivariana de Venezuela. Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Reformada Gaceta oficial 39.610 de fecha 07 de febrero de 2011).

Asamblea Nacional Bolivariana de Venezuela. Ley especial contra los Delitos Informáticos. Gaceta Oficial No. 37.313 de fecha 30 de octubre de 2001.

Depósito Legal: ***pp 200203AR289*** *ISSN: 1317-6331*

Muñoz, A (2024). Informática Forense: Seis aspectos para investigar y resolver delitos cibernéticos. Disponible en: https://www.pwc.com/co/es/pwc-insights/informatica-forense-seis-aspectos.html

OEA. Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética, resolución aprobada en la cuarta sesión plenaria, celebrada el 10 de junio de 2003. En http://www.oas.org/juridico/spanish/agres_1939.pdf.

Presidencia de la República Bolivariana de Venezuela. Decreto- Ley N° 1.204 de fecha 10 de febrero de 2001, sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.

Presidencia de la República Bolivariana de Venezuela. Decreto No. 825 de fecha 22 de mayo del 2000, publicado en Gaceta Oficial N°36.955.

Presidencia de la República Bolivariana de Venezuela. Decreto-Ley Orgánica de Ciencia, Tecnología e Innovación. Gaceta Oficial del Decreto N° 1.290, en fecha 30 de agosto de 2001.