Revista Digital de Ciencias Penales de Costa Rica, número 5 (36) (17). Año 5.
ISSN 2515-6704. RDCP- UCR. 2025.
https://revistas.ucr.ac.cr/index.php/RDMCP

LOS DELITOS INFORMÁTICOS Y LAS MEDIDAS DE INVESTIGACIÓN EN LOS DELITOS INFORMÁTICOS: EL AGENTE ENCUBIERTO EN EL CÓDIGO PROCESAL PENAL Y LA PRÁCTICA DE LA PRUEBA

INFORMATION CRIMES AND THE INVESTIGATION OF INFORMATION CRIMES: THE UNDERCOVER AGENT IN THE CRIMINAL PROCEDURE CODE AND THE PRACTICE OF EVIDENCE

Rommell Ismael Sandoval Rosales[1]

Fecha de recepción: 6 de octubre del 2025.

Fecha de aprobación: 30 de noviembre del 2025

RESUMEN: El artículo explora los cambios normativos en El Salvador, tanto de la Ley Especial contra los Delitos Informáticos y Conexos y en el Código Procesal Penal. Se establecen nuevos delitos y se incorpora en la ley salvadoreña la figura del agente encubierto digital y los procesos de presentación y práctica de la prueba electrónica en la vista pública.

PALABRAS CLAVE: Delitos informáticos; Código Procesal Penal; agente encubierto digital; prueba electrónica.

ABSTRACT: This article explores the regulatory changes in El Salvador in the Special Law Against Cybercrimes and in the Criminal Procedure Code. New crimes are established, and the figure of the digital undercover agent is incorporated into Salvadoran evidence rules, along with the procedures for the submission and presentation of electronic evidence at trial.

KEYWORDS: Cibercrimes; Criminal Procedure Code; digital undercover agent; electronic evidence.

ÍNDICE: 1. Introducción; 2. La Ley Especial Contra los Delitos Informáticos y Conexos; 3. Los actos de investigación del delito y los responsables; 4. El uso

[1] Abogado, notario y árbitro. Doctor en Derecho por la Universidad Autónoma de Barcelona, licenciado en Ciencias Jurídicas por la Universidad Centroamericana "José Simeón Cañas" de El Salvador. Docente y capacitador en Derecho en universidades y escuelas judiciales en México, República Dominicana, Panamá y Centroamérica. Investigador independiente, El Salvador.

de las técnicas especiales de investigación; 5. El agente encubierto digital y las otras técnicas de investigación informática; 5. Conclusiones; 6. Bibliografía.

1. Introducción

El Salvador ha adoptado una diversidad de normas para la gestión del gobierno digital, también ha emitido disposiciones para la atracción de inversiones y desarrollo de la economía por medio de la implementación de las tecnologías de comunicación. Previamente, la banca comercial con autorización de las normas técnicas del Banco Central de Reserva y la supervisión de la Superintendencia del Sistema Financiero estableció sus propias plataformas de banca electrónica, de transferencias de dinero, pago de compras de bienes o servicios, y pago de impuestos.

Por supuesto que la innovación y las tecnologías han precedido con increíble rapidez debido a que las personas y las empresas ya se comunicaban a través de estas, realizaban negocios o inversiones. Los particulares, las empresas y el Gobierno han utilizado plataformas para el comercio electrónico o de la banca, las redes sociales de cualquier aplicación electrónica, plataformas (exchanges) para el intercambio, inversión, gestión o custodia de criptomonedas o bitcoins.

Así, se puede mencionar a la Ley de Procedimientos Administrativos (LPA) que dispone que los órganos de la Administración Pública e instituciones públicas están facultados para emplear tecnologías de la información y la comunicación en la realización de trámites, diligencias, notificaciones, citatorios y requerimientos, siempre que dichos medios garanticen autenticidad, confidencialidad, integridad, eficacia, disponibilidad y conservación de la información, y resulten compatibles con la naturaleza del trámite. Esta obligación implica que la Administración Pública debe implementar mecanismos tecnológicos adecuados para mejorar sus funciones y los derechos de los ciudadanos, mediante el diseño de estrategias de gobierno electrónico.

De acuerdo con los arts. 18 a 20 de la LPA, los documentos generados electrónicamente por la Administración Pública se considerarán válidos como

originales, siempre que se garantice su autenticidad, integridad y conservación, y se cumplan los requisitos legales. Para tal efecto, se permite el uso de cualquier forma de firma electrónica o mecanismo de autenticación autorizado por la legislación.

La LPA establece la obligación de intercambio de información entre instituciones públicas mediante el uso de TIC, con el fin de facilitar la verificación de datos o circunstancias necesarias en los procedimientos administrativos y el cumplimiento de sus funciones. Este intercambio deberá respetar las limitaciones legales y concretarse mediante convenios o acuerdos institucionales que aseguren la coordinación, compatibilidad tecnológica e interconexión entre los sistemas utilizados.

Por su lado, la Ley de Firma Electrónica y la Ley de Comercio Electrónico fueron las primeras en establecer la regulación de las Tecnologías de Información y Comunicaciones (TIC) para las relaciones económicas entre los particulares, y entre los particulares y la administración pública (vinculada a la LPA y a la Ley de Compras Públicas). La Ley de Firma Electrónica estableció que el propósito de esta es equiparar la firma electrónica, ya sea simple o certificada, con la firma autógrafa, reconociéndoles valor legal. Además, otorga eficacia jurídica a los sellos electrónicos, sellos de tiempo, documentos electrónicos y mensajes de datos, y regula a los proveedores de servicios de certificación y almacenamiento de documentos electrónicos. Dispuso que la ley es tecnológicamente neutral y se aplica a cualquier tipo de firma o comunicación electrónica, sin importar su formato o desarrollo técnico, y debe interpretarse conforme al principio de equivalencia funcional.

La Ley de Comercio Electrónico instituye el marco legal aplicable a las relaciones comerciales y contractuales realizadas por medios digitales, electrónicos o tecnologías equivalentes. Se aplica a todo contrato o relación comercial que implique un beneficio económico y que se celebre electrónicamente. Asimismo, establece las reglas para la factura electrónica por lo que se vincula con las disposiciones tributarias. La ley obliga tanto a personas naturales como jurídicas, públicas o privadas, que estén establecidas

en El Salvador y que realicen transacciones comerciales o intercambios de bienes o servicios mediante tecnologías o redes de comunicación.

En el marco de la actividad económica e inversión recientemente El Salvador adoptó e implementó la Ley del Bitcoin y la Ley de Activos Digitales. Es decir, el marco jurídico va evolucionando hacia una economía digital y por lo tanto, la infraestructura tecnológica, las fuentes de energía, las plataformas de transacciones, la buena fe de las personas y empresas, así como los derechos fundamentales deben ser protegidas por la ley penal y las investigaciones de los hechos delictivos deben incorporar técnicas especiales.

El uso de esa tecnología para la realización de las actividades criminales ya no es un desafío para un delincuente ni para las organizaciones criminales. En algunos casos menos sofisticados, basta desarrollar habilidades y destrezas para su uso y su interacción con las víctimas. Es decir, en algunos delitos los delincuentes solo precisan unas habilidades básicas para la comisión de ilícitos como estafas, hurtos, apropiaciones indebidas, amenazas, mensajes de odio o robo de identidad, captación de víctimas de tráfico de personas o de trata de personas.

Los delincuentes utilizan las mismas tecnologías de la información (TIC) que utilizan las personas y empresas en las actividades lícitas de cualquier naturaleza como las relaciones sociales, la publicidad o la actividad económica. Para la comisión de delitos se pueden utilizar las plataformas electrónicas, los medios o las fuentes electrónicas para lesionar o poner en riesgo los derechos de la víctima o el objetivo del criminal, de la organización o del grupo terrorista.

En efecto, el desarrollo progresivo de las tecnologías de la información y comunicación ha generado nuevas formas de criminalidad que afectan de manera directa a la integridad de la infraestructura o de los sistemas informáticos, a la intimidad de las personas, a la propiedad intelectual y, en general, a los bienes jurídicos protegidos por el ordenamiento penal[2].

[2] C. Roxin, *La Evolución de la Política Criminal, el derecho penal y el proceso penal,* (Valencia, España: Tirant lo Blanch, 2000), 57.

En el plano procesal y probatorio, el Estado salvadoreño ha tenido que crear mecanismos de investigación técnica que limita derechos de los sospechosos, siempre que exista una causa fundada y la autorización del fiscal del caso o de un juez, como la intervención de las comunicaciones telefónicas o electrónicas, la captación de imágenes y seguimiento de personas, bienes o medios, el acceso a cuentas bancarias limitando el secreto bancario; estableciendo nuevos procedimientos civiles especiales como la extinción de dominio para desmantelar los bienes de las organizaciones criminales.

En las siguientes páginas se hará una descripción general de los contenidos de la Ley Especial contra los Delitos Informáticos y Conexos y de la reforma en materia de prueba digital y del investigador digital del Código Procesal Penal. Es decir una visión panorámica de la legislación recién aprobada.

2. La Ley Especial Contra los Delitos Informáticos y Conexos

En este contexto que se ha narrado, El Salvador ha adoptado e implementado un marco jurídico para la represión del ciber delito, específicamente a través de la Ley Especial contra los Delitos Informáticos y Conexos (LEDIC), reformada en el mes de junio de 2025, así como reformas al Código Penal (CP) y la legislación sobre crimen organizado y violencia de género. En este apartado se describirán por cada capítulo cada una de las conductas típicas contenidas en la ley especial[3].

La LEDIC define al delito informático como un hecho típico y antijurídico por medio del cual el sujeto activo hace uso de las tecnologías de información y comunicación para la obtención, manipulación o perjuicio de la información. Es decir que el uso o manipulación de la tecnología de forma dolosa se despliega con los elementos objetivos de la conducta prohibida[4].

[3] MC Rayón Ballesteros et al., *Cibercrimen: particularidades en su investigación y enjuiciamiento,* (*Anuario Jurídico y Económico Escurialense,* XLVII (2014) 209-234 / ISSN: 1133-3677)
[4] J. R Serrano Piedecasas Fernández y JM, Terradillos Basoco*, Manual de teoría jurídica del delito* (1a. ed, San Salvador, El Salvador, Consejo Nacional de la Judicatura, Escuela de Capacitación Judicial, 2003), 58.

Esta normativa dispone conductas que tipifican acciones antijurídicas dirigidas contra sistemas y datos, aquellos que utilizan las TIC para facilitar la comisión de delitos "convencionales", y los que van dirigidos a lesionar un bien jurídico o un derecho fundamental[5].

La LEDIC formula los delitos en 5 capítulos en el titulo II:

> "(...) delitos contra los sistemas tecnológicos de información, delitos informáticos, delitos informáticos relacionados con el contenido de los datos, delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad, y, delito contra el orden económico. Cada grupo encuentra respaldo jurídico en los textos legales vigentes y se relaciona con fenómenos de creciente complejidad y daño[6]."

Se pueden clasificar los tipos penales establecidos en la LEDIC, sin ánimo de agotar la temática, de la forma siguiente:

a) Delitos en los cuales los delincuentes u organizaciones criminales, utilizan y se benefician del uso de las TIC para la comisión de delitos convencionales, pero no se precisa el medio tecnológico para su comisión como los que están contenidos en el Código Penal (CP), la Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV) y otras leyes especiales penales y otras leyes que prohíben conductas antijurídicas para la protección de grupos vulnerables como la en la Ley Crecer Juntos para la Protección Integral de la Primera Infancia, Niñez y Adolescencia. En este caso se trata de delitos comunes cometidos por medio de las herramientas digitales, aunque no sean un medio directo ni un elemento objetivo del tipo, como la estafa, fraude, hurto, robo, amenazas, extorsiones, organización de

[5] JC Fuentes Real, *Contribuciones del Funcionalismo normativo en la teoría del delito,* (Comisión Coordinadora del Sector de Justicia, Unidad Técnicas Ejecutiva del Sector de Justicia, 2024), 133 y siguientes.
[6] RA, I. Parada, *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos Aires: Erreius, 2018.)

agrupaciones criminales o la concertación o planificación de actividades criminales.

b) Delitos en los que sus elementos objetivos requieren la tecnología para su realización. Este grupo incluye la falsificación de documentos electrónicos, la suplantación de identidad digital, el discurso de odio en plataformas digitales, la difusión de injurias y calumnias, el hostigamiento agravado con daño reputacional, el ciberacoso.

c) Delitos cuyo objetivo son acceder sin autorización, de forma indebida o dañar la integridad de los sistemas o plataformas informáticas. Los delitos cuyo objetivo principal son las páginas web, la infraestructura, las plataformas o los sistemas informáticos que comprenden conductas como el sabotaje digital, el daño informático y el acceso indebido a redes y bases de datos. Estas figuras delictivas afectan directamente la confidencialidad, integridad y disponibilidad de los datos, los sistemas y plataformas y generan la desconfianza del público (además del daño producido).

2.1. Delitos contra los sistemas tecnológicos de información

El capítulo I del título II de la LEDIC se enuncian los delitos contra los sistemas tecnológicos de información. En los delitos de carácter informático los bienes jurídicos que la ley penal protege es la información, la privacidad personal, el honor o la integridad psíquica de las personas, niños y adolescentes u otros grupos vulnerables. Pero, también se protege la infraestructura; los datos personales, de las empresas o de la administración pública; la integridad y disponibilidad de los sistemas informáticos, el correcto funcionamiento de estos, y la seguridad de la información, entre otros valores individuales y colectivos que el Estado busca salvaguardar frente a las nuevas formas de delincuencia en el ámbito digital.

En la LEDIC se establece que toda acción de acceso, interferencia, que altere, destruya o inutilice datos o sistemas debe ser castigada. Asimismo, el legislador dispone en la LEDIC que se sancionará el daño agravado cuando se afecta infraestructura crítica, lo cual permite imputar con mayor severidad los

ataques a plataformas estatales, bancarias u otras. De igual manera, la tipifica el acceso ilícito, es decir, el ingreso a sistemas o datos sin autorización, conducta que afecta directamente el principio de seguridad de la información.

La ley penal protege en el capítulo I del título II de la LEDIC a los bienes jurídicos de las personas y sus derechos, la infraestructura, la información, los datos y la confianza pública en los sistemas tecnológicos que sostienen la actividad económica, bancaria, personal, de las empresas y del Gobierno.

Esta categoría comprende aquellas acciones ilícitas tales como los ataques directos contra la infraestructura informática, interferencia, sabotajes, daños, accesos no autorizados y divulgación de información confidencial, por lo que se han establecido delitos por *acceso indebido a sistemas informáticos* (art. 4), *acceso indebido a los programas o datos informáticos* (art. 5), *interferencia del sistema informático* (art. 6), *daños a sistemas informáticos* (art. 7), *posesión y uso de equipos o prestación de servicios para la vulneración de la seguridad* (art. 8) o la *violación de la seguridad del sistema* (art. 9).

El delito de *Acceso indebido a sistemas informáticos* (art. 4), implica que una persona u organización criminal accede, intercepta o utiliza parcial o totalmente un sistema informático que utilice tecnologías de la información o comunicación sin autorización o excediendo los permisos de forma intencional en los sistemas informáticos, o excediendo la que se hubiese concedido, mediante el uso de tecnologías de la información o la comunicación. Esta conducta se penaliza con cárcel a quien, con conocimiento y propósito, acceda a programas o datos informáticos con la intención de apropiarse de ellos o de cometer un delito.

El Estado reprime la interferencia o alteración del funcionamiento de un sistema o programa informático, ya sea de forma temporal o permanente, y esta sanción se agrava si el daño afecta servicios públicos esenciales, servicios financieros o sistemas de criptomonedas, incrementándose la pena.

El *Acceso indebido a los programas o datos informáticos* (art. 5) dispone que se sancionará a quien, con conocimiento y con intención, accede parcial o totalmente a programas o datos almacenados en ellos, para apropiarse de la

información o cometer otro delito. De acuerdo con el tipo penal el sujeto activo puede cometer el ilícito mediante la utilización de cualquier dispositivo tecnológico, red, o mecanismo de conexión que permita el acceso indebido.

El delito de *Interferencia del sistema informático* (art. 6), de acuerdo con la ley se sanciona a toda persona que intencionalmente interfiera o altere de forma temporal o permanente el funcionamiento de un sistema o programa informático. Se agrava la pena si se trata de sistemas públicos o de servicios esenciales como salud, energía, comunicaciones, transporte, financieros o transacciones en criptomonedas.

La LEDIC dispone que se configura como delito a los *daños a sistemas informáticos* (art. 7). Es decir, que, en casos de daños causados a sistemas informáticos mediante destrucción, modificación o cualquier acto que altere o inhabilite total o parcialmente su funcionamiento, si estos sistemas están destinados a servicios públicos, financieros o contienen información sensible. Igualmente, se sanciona a quien posea, fabrique, distribuya o comercialice equipos, programas o códigos maliciosos para vulnerar sistemas informáticos. Si tales medios se utilizan, aunque no se logre el objetivo delictivo.

El art. 8 de la LEDIC establece el delito de *posesión y uso de equipos o prestación de servicios para la vulneración de la seguridad*. En esta figura delictiva el legislador sanciona a quien posea, produzca, facilite, venda equipos, programas, códigos maliciosos, virus, contraseñas o códigos de acceso para vulnerar la seguridad informática o preste servicios destinados a cumplir estos fines.

La ley especial penaliza con cárcel a quien viole la seguridad de sistemas informáticos restringidos o protegidos, incluso cuando induzca a otro a ejecutar programas o instrucciones que transgredan tales medidas. No se incurre en delito si estas acciones se realizan con autorización, para la ejecución de pruebas técnicas o auditorías de seguridad. El tipo penal en la LEDIC se denomina *violación de la seguridad del sistema* (art. 9).

En estos delitos, de especial complejidad para su ejecución, se pueden requerir conocimientos avanzados de los criminales para la manipulación de

sistemas TIC. Esta categoría de delitos informáticos requiere habilidades desarrolladas de manipulación tecnológica y tiene una connotación altamente lesiva para la confianza social, la seguridad e integridad de los sistemas, la administración pública y la convivencia democrática.

2.2. Los delitos informáticos

Hay conductas delictivas establecidas en la LEDIC que, si bien no se dirigen directamente contra los sistemas informáticos, encuentran en las TIC un medio idóneo para su comisión. En el capítulo II de la LEDIC les denomina como “delitos informáticos”.

De acuerdo con el art. 3 de la LEDIC, el delito informático es definido por el medio utilizado para la afectación de los bienes jurídicos, así estableció el legislador que “se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información” cuando se afecten los bienes jurídicos protegidos como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, y como el legislador dejó abierto los derechos fundamentales a ser protegidos, se puede agregar la protección de los datos personales.

El entorno digital ha potenciado modalidades como el *phishing*[7], el *carding*[8] y las estafas en plataformas de comercio electrónico, bancos o plataformas de criptomonedas, cuya frecuencia va en aumento.

Así se pueden mencionar a los delitos informáticos con una finalidad de enriquecimiento para sí o para un tercero afectando la buena fe y el patrimonio de las personas. En el capítulo II de *delitos informáticos* del título II de la LEDIC el legislador dispone el catálogo incluye la *estafa informática* (art. 10), el *fraude informático* (art. 11), *falsedad de documentos y firmas* (art. 11 A), *espionaje*

[7] Bajo esta figura se suplanta la web o la URL de la página de instituciones bancarias o cooperativas extrayendo la información, claves o tokens de los clientes. Son páginas web fraudulentas.

[8] Esta es una modalidad de estafa en línea donde los delincuentes obtienen y usan de forma ilegal los datos de tarjetas de crédito o débito para realizar compras no autorizadas, a menudo de escaso monto para pasar desapercibidas. En esta modalidad el estafador roba información de las tarjetas de crédito (número de tarjeta, fecha de expiración y CVV), a través de ataques de phishing, páginas web fraudulentas, o software malicioso.

informático (art. 12), *hurto por medios informáticos* (art. 13), y, *técnicas de denegación de servicio* (art. 14).

El delito de *Estafa informática* (art. 10 de la LEDIC) consiste en manipular o influir de manera fraudulenta en los datos o el procesamiento de un sistema informático para obtener un beneficio patrimonial indebido. Esto puede lograrse mediante el engaño o ardid a una persona o entidad, el uso de datos falsos en la propia web o comunicación pública o privada a la víctima, u otras acciones que alteren la información generada por el sistema con el objeto de obtener un beneficio patrimonial para sí o para un tercero. Si estas conductas afectan a entidades públicas o financieras, o son cometidas por empleados con acceso privilegiado, se consideran especialmente graves por la vulnerabilidad de las instituciones y los perjuicios causados.

La LEDIC dice que el fraude informático se produce cuando se insertan instrucciones falsas o manipulaciones en sistemas digitales como sus componentes, datos, metadatos o cualquier información para obtener beneficios en perjuicio de terceros. El delito se agrava si los sistemas afectados son financieros, bancarios o relacionados con criptomonedas, o si quien comete el acto tiene funciones de soporte o administración sobre dichos sistemas. También se sanciona cuando se utilizan estos accesos para alterar registros, crear datos falsos o conceder beneficios no autorizados.

El art. 11 A de la LEDIC relativo a la *Falsedad de documentos y firmas* en formato digital implica la falsificación, desciframiento o divulgación no autorizada de documentos o certificados electrónicos, sean públicos o privados. Esta conducta afecta la integridad y confiabilidad de los sistemas de certificación digital y pone en riesgo la autenticidad de las transacciones electrónicas y la fe pública.

El *Espionaje informático*, establecido en el art. 12 de la LEDIC, se configura cuando una persona accede, sin justificación, a datos confidenciales o reservados almacenados en sistemas digitales. El delito se torna más grave si conlleva beneficios para el autor, afecta la seguridad del Estado, o provoca

daños a personas o instituciones mediante la exposición de información protegida o sujeta a secreto bancario.

En cuanto al *Hurto por medios informáticos*, según el art. 13 de la LEDIC, consiste en apropiarse indebidamente de bienes o valores utilizando tecnologías de la información. El acto puede implicar el desvío de fondos, la utilización ilícita de cuentas electrónicas o tarjetas, o el ocultamiento de transacciones para beneficio económico propio o de terceros, vulnerando así la propiedad patrimonial.

El uso de *Técnicas de denegación de servicio* busca impedir deliberadamente que los usuarios legítimos accedan a una red o sistema informático de un proveedor de plataformas o servicios, art. 14 LEDIC. Esta conducta afecta la disponibilidad de servicios digitales, interrumpe operaciones implicando un bloqueo en el acceso y puede generar pérdidas económicas o institucionales, comprometiendo la estabilidad de servicios esenciales.

2.3. Delitos informáticos relacionados con el contenido de datos

El capítulo III del título II de la LEDIC establecen los *delitos informáticos relacionados con el contenido de datos*, establece conductas relacionadas con la manipulación de datos, que puede ocurrir en aquellas plataformas de las instituciones públicas o privadas provocándolas por el personal de dichas entidades. Es decir, la ley penal en este caso pretende proteger la confianza del público en la gestión de datos y servicios.

En cuanto al delito de *Manipulación de registros*, establece art. 15 de la LEDIC que ocurre cuando los administradores de plataformas tecnológicas modifican, destruyen u ocultan información contenida en registros informáticos. Esto representa un riesgo directo para la transparencia institucional, la integridad y certeza de la información o data, y puede facilitar la comisión de otros delitos, como fraudes o actos de corrupción.

En relación con el art. 16 de la LEDIC, se dispone que la *Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares* se presenta cuando se alteran, duplican o eliminan datos de tarjetas electrónicas con el propósito

de modificar cuentas, registros o consumos. El delito también abarca la comercialización y tenencia ilícita de estos instrumentos, lo que incrementa los riesgos de fraude financiero.

El art. 17 de la LEDIC tipifica el delito de *Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares* y se produce cuando una persona utiliza sin autorización una tarjeta inteligente ajena, o manipula sistemas informáticos para obtener productos, servicios o pagos sin cumplir con la contraprestación. Este acto viola los derechos del propietario del instrumento y compromete la legalidad de las transacciones.

En referencia al delito del art. 18 de la LEDIC denominado como la *Provisión indebida de bienes o servicios* ocurre cuando se prestan servicios o bienes mediante sistemas informáticos prestados por tarjetas inteligentes o instrumentos similares si la vigencia estaba caducada, revocada o suplantada para otorgar productos o beneficios económicos. También incluye la falsificación de datos con el fin de entregar dinero o servicios sin autorización, afectando el sistema financiero.

Según el art. 19 de la LEDIC, el delito de *alteración, daño a la integridad y disponibilidad de los datos* penaliza la acción de destruir, modificar o hacer inaccesible información almacenada en sistemas informáticos. Esta conducta pone en riesgo la confidencialidad, disponibilidad e integridad de los datos, esenciales para la operatividad y confianza en los sistemas digitales.

El delito de la *interferencia de datos* se configura cuando se obstruye o altera el uso legítimo de datos con el fin de inutilizarlos o dañarlos (art. 20 LEDIC). El delito se agrava si afecta servicios públicos esenciales como salud, energía, comunicaciones o transporte, debido al impacto que puede generar en el interés colectivo.

La ley salvadoreña tipifica que la *interceptación de transmisiones entre sistemas de tecnologías de la información y la comunicación* (art. 21 LEDIC) se penalizará cuando se acceda sin autorización a comunicaciones electrónicas que no están disponibles al público. Esto representa una grave invasión a la

privacidad y pone en peligro la confidencialidad de la información transmitida entre sistemas.

La LEDIC expresa que el *hurto de identidad* (art. 22) se da cuando una persona suplanta o se apodera de la identidad de otra a través de medios informáticos. Si esta suplantación se utiliza para dañar, injuriar, extorsionar, defraudar o difamar, o si los datos involucrados son personales, sensibles o confidenciales, el acto se considera más grave por su afectación directa a los derechos individuales.

El art. 23 de la LEDIC dispone que el delito relacionado en la *obtención y divulgación no autorizada* por el propietario de las contraseñas, códigos o información confidencial con fines lucrativos o delictivos constituye un atentado contra la seguridad digital. El delito se agrava si compromete la seguridad del Estado o de instituciones públicas o empresas del Estado, o si provoca daño a personas naturales o jurídicas.

El art. 24 de la LEDIC establece el delito de *utilización de datos personales*, este tipo penal dispone que el uso no autorizado de datos personales o datos sensibles mediante sistemas informáticos, violando mecanismos de confidencialidad, representa una afectación directa al derecho a la privacidad de las personas. Esta conducta se agrava si quien los revela tenía la obligación legal o contractual de preservar su secreto, o si la vulneración se debe a negligencia en el control de seguridad de los datos.

Según el art. 25 de la LEDIC es delito la *obtención y transferencia de información de carácter confidencial*, en este ilícito el legislador establece que quién obtenga o transfiera sin consentimiento del titular de dicha información mediante tecnologías digitales vulnera los derechos de los titulares y por lo tanto será sancionado. La confidencialidad, regulada por ley o por acuerdo entre partes, constituye un pilar del entorno digital y su violación conlleva consecuencias jurídicas severas.

El art. 26 de la LEDIC establece que es delito la *revelación indebida de datos personales* o *de información de carácter personal*, ocurre cuando se difunden, sin autorización, contenidos de carácter privado obtenidos mediante

medios digitales. Esta conducta puede volverse aún más grave si tiene fines lucrativos, si persigue otros delitos o si involucra la difusión de material sexual explícito.

La LEDIC establece en el art. 26-A que es delito el *secuestro de sistemas, programas o datos informáticos* el cual se produce cuando un individuo, por cualquier medio, restringe el acceso a dichos sistemas o a los datos informáticos almacenados (independientemente del soporte o medio de almacenamiento) con la intención de exigir un beneficio a cambio de liberarlos. Este delito compromete la funcionalidad y seguridad de los sistemas afectados y puede causar graves perjuicios económicos o institucionales.

El *acoso a través de tecnologías de la información y la comunicación* es un delito tipificado en el art. 27 de la LEDIC que consiste en realizar conductas de naturaleza sexual no deseadas mediante medios electrónicos. Esta modalidad de acoso representa una forma de violencia digital que vulnera la dignidad y los derechos de las personas afectadas.

2.4. Delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad

Es relevante mencionar que existe una protección reforzada a la integridad de la mujer en la LEIV. Si la víctima es mujer, el legislador ha establecido que se aplicarán los artículos 49 a 51 de la Ley Especial Integral para una Vida Libre de Violencia para las Mujeres (LEIV), que reconocen la violencia digital como una manifestación de violencia simbólica y estructural. El art. 49 (*Difusión Ilegal de Información*), el art. 50 (*Difusión Ilegal de Información*) y el art. 51 (*Difusión de Pornografía*) sancionan conductas relacionadas con la vulneración de la intimidad y dignidad de las mujeres mediante el uso de medios informáticos o electrónicos.

La LEIV castiga con penas de prisión a quien promueva o facilite la participación de mujeres mayores de edad, sin su consentimiento, en actos sexuales o eróticos a través de tecnologías digitales. Asimismo, el legislador establece una pena para quien difunda información personal que afecte el honor, la intimidad o imagen de una mujer sin su consentimiento, ya sea por

medios tradicionales o tecnológicos. Se penaliza con prisión la difusión de pornografía sin consentimiento que utilice la imagen o identidad real o simulada de una mujer, aumentando la pena si el material fue obtenido mediante relaciones de confianza, poder o afectivas.

En lo que respecta a la protección de la niñez y adolescencia de la ley penal es completada por las disposiciones de la Ley Crecer Juntos para la Protección Integral de la Primera Infancia, Niñez y Adolescencia, que refuerzan la protección de la niñez frente a contenidos digitales nocivos.

El capítulo IV de la LEDIC denominado como *delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad.* Los bienes jurídicos protegidos por la LEDIC para la integridad personal, moral, psíquica y la libertad de los niños, niñas y adolescentes También en esta categoría se ubica el castigo del Estado hacia el ciberacoso y el hostigamiento en línea, que sanciona a quien afecte la integridad psíquica mediante ataques reiterados por medios electrónicos.

En cuanto al ciberacoso la lesión que produce el criminal dependerá del bien jurídico tutelado. El acoso digital no puede reducirse a una extensión del acoso tradicional, sino que la lesión en la integridad moral o psicológica de la persona se basa en la afectación producida por la intensidad y permanencia agravada ante la omnipresencia de las tecnologías, así como el desarrollo y madurez de la víctima. El ciberacoso no es simplemente la figura del acoso con otro medio, sino una modalidad con autonomía propia y efectos psicosociales profundos en las personas.

El capítulo IV de la LEDIC establece los siguientes delitos: el art. 28 con el delito de *Pornografía a través del Uso de Tecnologías de Información y la Comunicación;* el art. 28 A) *Seducción de niñas, niños y adolescente o personas con discapacidad por medio de las tecnologías de la información y la comunicación*; art. 28 B) *Intercambio de mensajes de contenido sexual con niñas, niños y adolescentes o personas con discapacidad por medio de las tecnologías de la información y la comunicación*; art. 28 C) *Extorsión sexual de niñas, niños y adolescentes o personas con discapacidad por medio de las*

tecnologías de la información y la comunicación; art. 29 Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía a través del Uso de las Tecnologías de la Información y la Comunicación; art. 30 Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación; art.31 Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación; art. 32 Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación; y, art. 33 Condiciones Agravantes Comunes.

El art. 28 de la ley describe al delito de *Pornografía a través del uso de Tecnologías de la Información y la Comunicación,* como aquel cometido por quien, utilizando cualquier medio que involucre Tecnologías de la Información y la Comunicación, fabrique, transfiera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute, exhiba o muestre material pornográfico o sexual en el que intervengan niñas, niños, adolescentes o personas con discapacidad. Asimismo, incurre en delito quien, transmitiendo material pornográfico o sexual mediante dichas tecnologías, no advierta de manera visible que su contenido no es apto para niñas, niños, adolescentes o personas con discapacidad.

En cuanto al art. 28 A denominado *Seducción de niñas, niños, adolescentes o personas con discapacidad mediante Tecnologías de la Información y la Comunicación*, establece que incurre en delito la persona que, a través del uso de las Tecnologías de la Información y la Comunicación, establezca o entable una relación con una niña, niño, adolescente o persona con discapacidad con el propósito de sostener contacto sexual, ya sea mediante esas mismas tecnologías o de forma personal.

El art. 28 B establece el delito de *Intercambio de mensajes de contenido sexual con niñas, niños, adolescentes o personas con discapacidad mediante Tecnologías de la Información y la Comunicación* indicando que comete delito quien, utilizando Tecnologías de la Información y la Comunicación, envíe,

solicite, intercambie o transmita con una niña, niño, adolescente o persona con discapacidad audios, imágenes o videos de contenido sexual o que sexualmente sea explícito, real o simulado.

El art. 28- C denominado como *Extorsión sexual de niñas, niños, adolescentes o personas con discapacidad mediante tecnologías de la información*, se configura cuando una persona, valiéndose de medios tecnológicos, obliga, chantajea, amenaza o coacciona a una niña, niño, adolescente o persona con discapacidad, con el fin de que envíe, remita o transmita audios, imágenes o videos que representen contenido sexualmente explícito, ya sea real o simulado, o que muestren su cuerpo desnudo, con el propósito de obtener satisfacción sexual o algún provecho, utilidad, beneficio o ventaja, ya sea para sí mismo o para un tercero.

La pena será la máxima del rango si, además, el autor de los hechos amenaza con causar daño a los amigos o familiares de la víctima como represalia por no cumplir con sus exigencias, o si solicita una remuneración económica a cambio de no compartir, difundir o publicar el contenido sexualmente explícito (real o simulado) que tiene en su poder, incluso si dicho contenido muestra el cuerpo desnudo de la víctima.

La LEDIC describe en el art. 29 el delito de *Utilización de niñas, niños, adolescentes o personas con discapacidad en pornografía mediante tecnologías de la información*, describiendo el legislador que será sancionado con prisión quien, utilizando medios tecnológicos, produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda cualquier imagen, video o representación en la que se involucren actividades sexuales, eróticas o de naturaleza sexual inequívoca (explícitas o no, reales o simuladas) en las que se utilice la imagen, voz o participación de niñas, niños, adolescentes o personas con discapacidad.

El mismo castigo se aplicará a quien, a través de medios digitales, organice o participe en espectáculos públicos o privados que involucren a estas personas en actos de carácter pornográfico o erótico.

El art. 30 de la LEDIC dice que es delito la *Adquisición o posesión de material pornográfico de niñas, niños, adolescentes o personas con discapacidad mediante tecnologías de la información,* por el cual la persona que cualquier medio que implique el uso de tecnologías de la información, adquiera o posea material pornográfico que involucre la utilización de la imagen de una niña, niño, adolescente o persona con discapacidad, ya sea para sí mismo o para un tercero.

Esta sanción también se aplicará a quien mantenga en dispositivos de almacenamiento digital o por cualquier medio tecnológico, material pornográfico en el que se haya utilizado la imagen de las personas protegidas por esta norma.

En el art. 31 de la LEDIC se establece el delito de *Corrupción de niñas, niños, adolescentes o personas con discapacidad mediante tecnologías de la información,* que será sancionado con prisión quien, por medio de tecnologías de la información y la comunicación, mantenga, promueva o facilite la corrupción de una niña, niño, adolescente o persona con discapacidad, con fines eróticos, pornográficos u obscenos, incluso si la víctima ha dado su consentimiento.

La misma pena se impondrá a quien realice propuestas implícitas o explícitas para sostener encuentros sexuales o eróticos, o para la producción de pornografía digital, con alguna de las personas señaladas, ya sea para sí mismo, para un tercero o para grupos.

Dice el art. 32 que se considera como delito el *Acoso por medios tecnológicos a niñas, niños, adolescentes o personas con discapacidad*, la persona que, utilizando tecnologías de la información o la comunicación, atormente, hostigue, humille, insulte, denigre o realice cualquier conducta que afecte el desarrollo psicológico, emocional o personal de una niña, niño, adolescente o persona con discapacidad, incluyendo actos que pongan en peligro su vida o su integridad física.

La pena será agravada con prisión si los actos consisten en frases, señas o acciones inequívocas de naturaleza o contenido sexual dirigidas a la víctima por medio de tecnologías digitales.

Se consideran agravantes comunes a las penas previstas en los delitos del capítulo IV cuando el delito sea cometido por:

a) Parientes cercanos, como ascendientes, descendientes, hermanos, adoptantes, adoptados, cónyuges, convivientes, o familiares hasta el cuarto grado de consanguinidad o segundo de afinidad;

b) Funcionarios o empleados públicos, municipales, autoridades o agentes de autoridad;

c) Personas que ejerzan tutela, protección o vigilancia sobre la víctima;

d) Cualquier persona que se aproveche de una relación de confianza, ya sea doméstica, educativa, laboral o de cualquier otra índole.

Se incrementará la pena, establece el legislador, hasta en una tercera parte del máximo establecido y se impondrá, además, la inhabilitación para el ejercicio profesional durante el tiempo de la condena.

2.5. Delito contra el orden económico

El capítulo V de la LEDIC establece solo un tipo penal, es el delito la *Suplantación en Actos de Comercialización,* que toda persona que, sin contar con autorización, utilice las Tecnologías de la Información y la Comunicación para vender o comercializar bienes o servicios a nombre de un tercero, suplantando la identidad del productor, proveedor o distribuidor legítimamente autorizado.

La sanción de la pena de prisión será agravada por la venta o comercialización indebida de medicamentos, suplementos, productos alimenticios, bebidas u otros bienes destinados al consumo humano.

3. Los actos de investigación del delito y los responsables

No hay duda de que los ciudadanos, las empresas, las instituciones bancarias y otros sujetos han sido víctimas del cibercrimen. Ante esta realidad, el Estado ha respondido con herramientas investigativas sofisticadas, que incluyen la evidencia digital y la figura del agente encubierto digital agregando un capítulo X al Título V de la Prueba. Es importante aclarar que este Título X del CPP desarrolla las disposiciones sobre actos de investigación, fuentes o elementos de prueba y procedimientos para la práctica de la prueba[9].

En ese contexto normativo salvadoreño, el legislador agregó en el art. 35 A de la LEDIC que la Policía Nacional Civil (PNC) y la Fiscalía General de la República (FGR) deberán actualizarse constantemente en el combate de los delitos informáticos y en el art. 35 de la LEDIC establece la creación de unidades de investigación científica de los delitos informáticos, tratamiento y análisis de la evidencia digital para pericias de informática forense.

El legislador modificó el Código Procesal Penal para introducir la figura del agente encubierto digital y las técnicas especiales informáticas, junto con el conjunto de medidas procesales que abarcan actos de investigación como la vigilancia, incautación, operaciones técnicas, obtención de información electrónica, custodia de pruebas, prueba testimonial y pericial, conforman un único sistema orientado a confrontar la criminalidad digital con eficacia, legalidad y respeto al debido proceso. Para comprender su legitimidad y aplicación, resulta ilustrativo examinar cómo esta figura se ha desarrollado doctrinalmente en otros sistemas jurídicos, como el español, el colombiano y el estadounidense.

El CPP diferencia los actos de investigación de los actos de prueba por razón de la etapa procesal en que se llevan a cabo, por los requisitos formales que han de cumplir, por los sujetos que realizan las funciones asignadas por la ley en cada etapa del proceso y por su valor procesal. Para convertir los actos de investigación en actos de prueba se debe partir del principio general que nada llega probado a las audiencias, y mucho menos al plenario.

[9] RI Sandoval Rosales et al., *Código Procesal Penal comentado V. 1 y V. 2 (*1ª Ed. San Salvador, Consejo Nacional de la Judicatura: 2018). Es la fuente que puede explicar los actos de investigación y de prueba.

De acuerdo con la Constitución y a la Ley Orgánica de la Fiscalía General de la República, el Fiscal es autónomo e independiente en sus investigaciones. El Fiscal General de la República por medio de sus fiscales auxiliares dirige funcionalmente a los miembros de las áreas de investigación de la Policía Nacional Civil en la etapa de diligencias iniciales como en la instrucción. El Fiscal puede examinar en cualquier momento las actuaciones que ha realizado y ordenar que se lleven a cabo actuaciones que sean relevantes y pertinentes, resguardando la legalidad de estos.

Los resultados o hallazgos de los actos de investigación le dan la pauta al acusador, Fiscal, de presentar tanto el requerimiento en el proceso penal común o en los procesos penales especiales para la audiencia inicial (o audiencia de medidas cautelares) como el dictamen Fiscal para celebrar la audiencia preliminar y la acusación para llevar a cabo el juicio. Es necesario, entonces, acreditar, en la audiencia de prueba o vista pública a través de los medios probatorios pertinentes los elementos de prueba.

De allí que los actos de investigación tengan una función preparatoria para recoger los elementos que permitirán evaluar al Fiscal si procede o no la promoción de la acción penal. A lo largo del Código Procesal Penal el legislador salvadoreño denomina indistintamente a los actos de investigación como “diligencias de investigación”, diligencias para la “averiguación de la verdad”, “diligencias policiales” o “diligencias iniciales de investigación”.

La finalidad de la etapa de instrucción en el proceso penal es la preparación del juicio oral. Se entiende que tanto las actividades policiales y de la Fiscalía pretenden en la etapa de la instrucción, por una parte, confirmar los hechos contenidos en el requerimiento fiscal y, por la otra, recopilar los elementos que demuestren la posible responsabilidad del sujeto imputado en el juicio. En El Salvador, el Juez de Instrucción, pese a su denominación similar al utilizado en el derecho procesal de Europa continental y de Iberoamérica, no realiza actos de investigación, coordina la etapa de instrucción, pero no ordena actos de investigación ni a la Policía ni a los sujetos procesales como el acusador o Fiscal o al defensor.

Las actuaciones realizadas por los órganos de investigación no están sometidas a requisitos rigurosamente formales exigidos en las audiencias judiciales, pero sí a los procedimientos legalmente establecidos y se deberá tener de forma previa del fiscal o del juez, en aquellos actos que requieran la autorización. Sin embargo, se exige un rigor procedimental en los elementos u objetos de prueba materiales (objetos, documentos, sustancias controladas, fluidos o similares) y la evidencia digital que por su propia naturaleza requiera un resguardo de cada uno de los eslabones de la cadena de custodia y que se deje constancia formal de los mismos.

Es así como para el derecho procesal salvadoreño (CPP) el aspecto critico de la cadena de custodia lo constituyen las evidencias físicas, sustancias, fluidos o cualquier elemento fungible, que se pueda destruir o contaminar y la evidencia digital, obtenidas mediante su recolección en la escena del delito, durante la práctica de un registro o requisa, recibidas de la víctima, el sospechoso o un testigo. En el caso de la evidencia digital, la escena del delito es la web pública, chats públicos o privados, sistemas, plataformas o dispositivos electrónicos.

El procedimiento y protocolo técnico y científico que debe dársele a la recolección, análisis y custodia de las evidencias deberá atender a sus propias características sustanciales para conservarlas, independientemente de la forma en que se obtienen. La diferencia radica en el momento en que se inicia la cadena de custodia y la manera en que se hace constar la obtención, así como la naturaleza del objeto o sustancia que requiere un tratamiento científico por los peritos permanentes o no permanentes de la División de Policía Técnica y Científica (el Instituto de Ciencias Forenses), el Instituto de Medicina Legal, o la unidad de análisis de la FGR.

La escena del delito, de acuerdo con el CPP, se documenta a través de un acta preparada y redactada por el investigador a cargo de la inspección, y en ella se debe hacer constar una descripción detallada del lugar, el estado de las cosas, los rastros, huellas y demás objetos que fueron encontrados, así como un detalle de la recolección de las evidencias, el técnico a cargo de estas

y el lugar al que serán trasladadas para la práctica de los análisis periciales que sean requeridos. Asimismo, debe contener los nombres y cargos de las personas que, por alguna razón, participaron en el procesamiento de la escena, por ejemplo: el médico forense, técnicos del laboratorio de la Policía, socorristas, bomberos, etc.

En cuanto a los actos de prueba, se entienden que son únicamente los practicados en las audiencias, en la vista pública o juicio, bajo la inmediación del Juez o tribunal y mediante una actividad confrontativa de las partes, tanto en las aportaciones que realizan como en los medios de defensa que despliegan (contrainterrogatorio u objeciones) ante la práctica de la prueba de la parte contraria en ejercicio del derecho de confrontación.

La decisión judicial restrictiva de la libertad de un individuo únicamente puede fundarse en un auténtico medio de prueba (no atestado o acto de investigación) practicado de acuerdo con las garantías y principios procesales oportunos y siempre con el máximo respeto a los derechos fundamentales que la Constitución enuncia en el art. 11 y 12.

En efecto los actos de prueba se pueden definir como la actividad de las partes procesales en audiencia, dirigida a practicar la evidencia necesaria para obtener la convicción del Juez o Tribunal sobre los hechos por ellas afirmados. La actividad en audiencia se desarrolla bajo los principios de inmediación, confrontación, igualdad y de las garantías constitucionales. Se exceptuaría el cumplimiento de estos requisitos a las situaciones en que es admisible la prueba anticipada y bajo las concepciones de la admisibilidad excepcional de la prueba de referencia que fueren aplicables al sistema procesal penal salvadoreño.

Esta definición, sin embargo, dada la plenitud de los principios de inmediación y contradicción o confrontación en el régimen procesal salvadoreño, también debe ser aplicable a las audiencias inicial y preliminar. Es decir, que para los propósitos que las partes prevén en esas audiencias inicial y preliminar y que estén permitidos por la ley, se entenderá que se estaría efectuando una “mínima actividad probatoria”.

De acuerdo con esta doctrina, si bien los jueces tienen libertad en ponderar los distintos elementos probatorios para tomar una decisión, ello no le autoriza para prescindir de la exigencia de la ley y de la Constitución para que las partes practiquen la prueba mínima y suficiente en la respectiva audiencia. Puesto que en esta mínima y suficiente actividad probatoria, el Juez podrá descansar y encontrar fundamento para la aplicación de su sana crítica. Cualquier decisión sin base en esa mínima y suficiente actividad probatoria vulneraría el derecho a la presunción de inocencia del inculpado.

La prueba, consecuentemente, debe ser entendida como la actividad de verificación o comprobación de las afirmaciones de las partes en un "juicio" con todas las garantías ante un juez o tribunal independiente.

Es así como se pueden distinguir los caracteres entre los actos de investigación y los actos de prueba:

a) El acto de investigación está orientado a averiguar los hechos criminales y los responsables, el acto de prueba está orientado a convencer al juez sobre las afirmaciones de parte. La actividad probatoria es responsabilidad de las partes, como resultado del principio de aportación del sistema acusatorio.

b) La prueba tiene por finalidad convencer al juez o a los miembros del Tribunal, bajo las reglas de la sana crítica, sobre la existencia del hecho punible y la responsabilidad del autor (o la falta de tipicidad, antijuridicidad o culpabilidad, exclusión de responsabilidad o causa de justificación).

c) Los actos de prueba deben recaer sobre los hechos afirmados por las partes en la audiencia preliminar.

d) La prueba exige la intervención de un órgano jurisdiccional imparcial e independiente, y que se produzca en un juicio –o audiencia- oral y público, bajo los principios de inmediación y confrontación de partes –de allí la importancia del contrainterrogatorio). Los actos de investigación no requieren la contradicción hasta que ofrecidos en audiencia; y,

e) La actividad probatoria debe realizarse por los medios lícitos, es decir, respetando los derechos fundamentales.

Por lo que la prueba es un fenómeno diferente de la averiguación o investigación de los hechos. Esta diferencia no radica, como se ha señalado, sólo por su distinta naturaleza sino también porque ambas se llevan a cabo en momentos procesales diferentes, y puede darse el caso que sea realizada o atribuida a órganos o partes procesales distintas, dependiendo lo establecido en la ley.

Algún sector de la doctrina ha intentado definir la prueba a partir de la actividad procesal que realizan los sujetos procesales. Es decir, las partes y el Juez. Es así como distinguen entre las actuaciones de uno y de otro, pero únicamente nos indican este concepto de prueba a los actos procesales que se llevan a cabo durante el procedimiento probatorio.

Del concepto mencionado se puede destacar como características fundamentales que la prueba es una actividad procesal y que es realizada por las partes en una audiencia ante un juez, sujeta a confrontación. La finalidad de la prueba es convencer al juez de la veracidad de las alegaciones de las partes. La actividad investigadora realizada fuera del procedimiento judicial permite ofrecer las fuentes o elementos de prueba que sean pertinentes para su producción en la audiencia. La actividad de los actos de investigación está bajo la responsabilidad de la policía y del agente fiscal.

4. El uso de las técnicas especiales de investigación

En el Código Procesal Penal vigente, y leyes especiales, el legislador salvadoreño ha establecido procedimientos convencionales y no convencionales para la investigación de delitos. Algunos procedimientos de investigación son responsabilidad de la Policía bajo la dirección funcional de la FGR. Es decir, por su naturaleza no requieren la autorización judicial, sino el control del agente fiscal. Hay algunos actos de conocimiento y de averiguación inicial contenidos en el aviso o denuncia que los puede realizar la policía para un posterior control de la Fiscalía. En otras actuaciones el policía requerirá la dirección fiscal, su coordinación y autorización. La misma Fiscalía puede

ordenar la limitación de libertades en los actos de investigación o de la privación de algunas libertades.

Otras intervenciones establecidas en el CPP requerirán la previa autorización del juez. El grado de la autonomía de los actos de investigación tanto convencionales como no convencionales son establecidos por el legislador.

Los procedimientos convencionales autorizados por el legislador en los actos de investigación:

a) Entrevistas a las víctimas y testigos.

b) Indagaciones en la escena del delito o lugares en dónde se encuentre un sospechoso o material ilícito.

c) Procesamiento de una escena del delito, bajo la dirección Fiscal.

d) Vigilancias y seguimiento a sospechosos o movimientos de material ilícito, o de personas, como en los delitos de tráfico de migrantes, trata de personas[10], "mulas" en el caso de drogas, estafas o extorsiones.

e) Individualización de sospechoso.

f) Perfilación de víctimas.

g) Perfilación de sospechosos.

Ahora, bien, se pueden utilizar las técnicas especiales para cualquier tipo de hechos delictivos, no solo los de crimen organizado. Así dispone en el art. 282 del CPP las siguientes técnicas de investigación policial: "Art. 282.- Cuando la fiscalía tuviere razones fundadas, para inferir que una persona está participando en la comisión de un hecho delictivo de gravedad o pudiere conducirlo a obtener información útil para la investigación, podrá disponer:

[10] R. Sandoval, *Manual para la Investigación de los Delitos de Trata de Personas y Tráfico Ilicito de Migrantes*, OEA-OIM-ACNUR, Programa de Prevención de los Delitos Vinculados a la Migración Irregular en Mesoamérica, 2017, 29 y ss.

a) Que al imputado o investigado, sus familiares, socios comerciales o cualquier otra persona con la que tenga relación permanente, se les realice vigilancia y seguimiento.

b) Que se vigile un lugar, inmueble, vehículo, nave, aeronave o cualquier otro objeto que se considere puede ser utilizado para realizar una actividad ilícita.

c) Que se analicen las actividades y ramificaciones de una estructura, asociación u organización criminal.

d) Que se utilicen técnicas especiales de investigación, como agentes encubiertos, entregas vigiladas o compras controladas para la comprobación de la existencia y participación en delitos.

e) Que se realicen cotejo de bases de datos de acceso público o cruce de información.

f) Cualquiera otra actividad que la técnica policial aconseje”

Se pueden considerar como técnicas especiales de investigación el manejo y gestión de informantes o eventuales co-imputados a los que se les podría otorgar la calidad de “testigo bajo criterio de oportunidad” (que ha sido fundamental para desarticular organizaciones criminales como pandillas o maras o para el hallazgos de restos de personas desaparecidas), la entrega vigilada, operaciones encubiertas y la intervención de las comunicaciones, así como la figura del agente encubierto digital y otras técnicas, que dispone el art. 259 D del CPP.

5. El agente encubierto digital y las otras técnicas de investigación informática

5.1. El seguimiento en sitios públicos de internet

Internet ha sido una gran revolución tecnológica que ha cambiado la vida de todas las personas, relaciones sociales y economía global. Facilita realizar investigaciones académicas, facilita la comunicación y permite la realización de emprendimientos y negocios. En efecto, la delincuencia convencional y la

transnacional no ha sido ajena al uso de la tecnología para cometer delitos, mediante el uso de redes sociales, blogs, sitios en donde aparentemente son lícitos los negocios o las oportunidades de empleo o de negocios.

En la investigación del delito, los agentes investigadores siempre han dado seguimiento a los sospechosos en la internet pública a través de motores de búsqueda u otras redes sociales accesibles, en realidad no ha habido limitaciones explícitas a las investigaciones de actos delictivos o de sospechosos en plataformas de acceso público (web libre o en la misma internet oscura o dark) o que estos hubieran hecho público en las redes sociales, previamente a la reforma adoptada del agente digital.

Los investigadores de las unidades de delitos comunes y en los especializados de cibercrimen están acostumbrados a trabajar rastreando en la red abierta. En algunos casos orientan a los investigadores sobre el estilo de vida o movimientos de los sospechosos que son investigados. En los delitos en los que se ha usado el internet, los agentes están acostumbrados al reconocimiento de los protocolos IP de internet, con lo que la red pública ofrece información relevante.

Esta reforma al CPP representa un paso significativo hacia la modernización del sistema de justicia penal frente a las amenazas que surgen en el ciberespacio, y cuya naturaleza demanda respuestas técnicas, legales y estratégicas acordes a su complejidad. Por supuesto, que el seguimiento en internet abierta siempre planteará dudas sobre la protección de la intimidad y privacidad personal[11].

5.2. La evidencia digital

En el marco del desarrollo tecnológico y la evolución de las formas delictivas, los Estados se han visto en la necesidad de adaptar sus marcos normativos y herramientas procesales a las nuevas realidades del cibercrimen.

El art. 259 A y siguientes del CPP reconoce la existencia de la evidencia digital, así expresa que:

[11] J.I, Reyes, *Los registros y allanamientos en la era digital: la renuncia a nuestra privacidad,* (Revista UIPR, Vol XLIX: 3: 467, 2014-2015), 467 a 482.

> "(...) los documentos digitales, mensajes electrónicos, imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las Tecnologías de la Información y Comunicación o por medio de cualquier dispositivo electrónico, serán admisibles como prueba y valorados conforme a las reglas de la sana crítica establecidas en este Código y en el Código Penal (…)"

sigue manifestando que;

> "(…) las Tecnologías de la Información y Comunicación establecidas en el Art. 3 letra l) de la Ley Especial contra los Delitos informáticos y Conexos o cualquiera que la ciencia y tecnología haya desarrollado o lo haga en el futuro, tendrán carácter de prueba de acuerdo a las reglas de incorporación de la evidencia establecidas en este Código (Procesal Penal) (…)";

y finaliza afirmando que:

> "(…) En los procesos referentes al delito de Disposición Indebida de Residuos o Desechos, el juez deberá admitir y valorar toda la evidencia digital que sea presentada de conformidad a las reglas de la sana crítica".

Por lo tanto, considera que la evidencia digital puede provenir de diversas fuentes, formatos y tecnologías de la información y comunicación[12].

5.3. El agente encubierto

En cuanto al artículo 259-D sobre el agente encubierto digital, se reconoce por primera vez en la legislación salvadoreña la posibilidad de realizar operaciones encubiertas en ambientes virtuales, como parte de la investigación de delitos informáticos o conexos. Esta técnica, autorizada expresamente por el Fiscal General de la República y ejecutada por la Policía, se corresponde con modelos comparados como el de España, donde la Ley de

[12] P.R. Jennetten, *From E-Discovery to E-Evidence: Lorraine v Markel American Ins. Co,* (Illinois Association fo Defensa Trial Counsel, Springfield, Illinois, V. 18, No. 1), 1 a 3.

Enjuiciamiento Criminal (reformada por la Ley Orgánica 41/2015)[13] permite el uso de agentes encubiertos para interactuar con los investigados a través de redes sociales o plataformas digitales[14].

En los Estados Unidos, si bien no existe una doctrina única sobre el "agente encubierto digital", las prácticas de investigación encubierta en entornos digitales están sustentadas en mandatos judiciales precisos: las órdenes de registro deben autorizar la búsqueda de indicios de control o uso del dispositivo, incluyendo correos, historial de navegación, imágenes, registros del sistema, elementos que permitan identificar al autor del delito[15].

En Estados Unidos, el uso de agentes encubiertos en línea ha sido validado por múltiples decisiones judiciales, como en United States v. Gagliardi, 506 F.3d 140 (2d Cir. 2007), donde se estableció que no se infringe la Cuarta Enmienda cuando el agente accede a información disponible públicamente en internet o se hace pasar por un interlocutor en redes sociales, siempre que no se induzca al delito.

Además, instituciones como el Departamento de Justicia han desarrollado capacidades especializadas, como el National Cryptocurrency Enforcement Team (NCET) y el Virtual Asset Unit (VAU), que combinan pericia técnica con investigación encubierta en entornos digitales sofisticados como criptomonedas[16]. Estos modelos enfatizan una estrategia investigativa basada en capacitación técnica avanzada, mandatos judiciales sólidos y protección de las garantías constitucionales.

En Colombia, el artículo 242 y siguientes del Código de Procedimiento Penal regula las operaciones encubiertas digitales, exigiendo autorización

[13] A Soriano Guillamón et al, *Agente encubierto informático. Informe de derecho comparado*, (Cuadernos de RES PUBLICA en derecho y criminología, ISSN: 2990-0697 DOI: Nº En prensa 10.46661/respublica.12120, Universidad Pablo de Olavide).
[14] MP, Pérez, *El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española (*Criterio Jurídico Santiago de Cali V. 6 2006 pp. 267-310 ISSN 1657-3978)
[15] United States v. Gagliardi, No. 06-4541 (2d Cir. 2007)
[16] Federal Bureau of Investigation, *2020 Cryptocurrency Fraud Report Released*, 10 de septiembre, 2024. https://www.fbi.gov/news/stories/2023-cryptocurrency-fraud-report-released

judicial y reserva[17]. Se ha utilizado el agente encubierto para la investigación de la corrupción, además del cibercrimen u otras actuaciones ilícitas de las organizaciones criminales.

En este contexto, el artículo 259-D del CPP introduce la figura del agente encubierto digital y autoriza otras técnicas especiales de investigación informática, regulando así la posibilidad de que las autoridades policiales, bajo autorización del Fiscal General de la República, realicen operaciones encubiertas en entornos digitales cuando se trate de delitos previstos en la Ley Especial contra los Delitos Informáticos y Conexos, o en otras leyes penales especiales. Esta disposición representa un paso significativo hacia la modernización del sistema de justicia penal frente a las amenazas que surgen en el ciberespacio, y cuya naturaleza demanda respuestas técnicas, legales y estratégicas acordes a su complejidad.

La figura del agente encubierto digital encuentra su justificación en el principio de necesidad en la investigación penal de fenómenos criminales que difícilmente pueden ser detectados a través de métodos tradicionales. Así, en lugar de restringirse a un espacio físico determinado, el agente encubierto digital actúa en plataformas virtuales (foros, redes sociales, servicios de mensajería y otros entornos en línea) simulando ser parte de una red delictiva, con el objetivo de recabar información probatoria sin revelar su verdadera identidad. Esta práctica, si bien invasiva, se considera legítima siempre que esté legalmente autorizada y sea proporcional al fin perseguido.

Las operaciones encubiertas constituyen medios excepcionales de investigación en sociedades democráticas que buscan preservar los derechos fundamentales, y que su admisibilidad depende de un equilibrio delicado entre eficacia penal y garantías procesales. La autorización previa y escrita del Fiscal General constituye en este sentido una salvaguarda básica para prevenir abusos, asegurando que la medida solo se emplee cuando sea indispensable para descubrir la verdad.

[17] J. R., Hernández Gómez, *La anticorrupción en Colombia, el agente encubierto y la función de inteligencia,* (Revista Prolegómenos - Derechos y Valores - pp. 99-114, 2018, I)

La legalidad y razonabilidad de esta técnica también debe analizarse en armonía con las reglas generales que rigen las técnicas de investigación policial. El CPP (arts. 272, 273, 276, y 282, entre otros) establece que el fiscal podrá disponer diversas medidas de vigilancia o técnicas especiales (como agentes encubiertos, entregas vigiladas o compras controladas) cuando existan razones fundadas para inferir la participación de una persona en un hecho delictivo grave, o cuando dicha persona pudiera proveer información útil para la investigación.

A estas facultades se suman la vigilancia de personas y objetos, el análisis de estructuras criminales, el cruce de bases de datos de acceso público, y otras actividades recomendadas por la técnica policial. En conjunto, estas herramientas constituyen un sistema normativo integrado que permite a la fiscalía y a la policía operar con eficiencia y dentro de un marco jurídico garantista. La inclusión del agente encubierto digital no debe verse como una figura aislada, sino como una extensión lógica de estas técnicas adaptadas al entorno virtual, en el que el anonimato, la descentralización y la velocidad de difusión dificultan la obtención de prueba por medios convencionales.

A su vez, la aplicación de estas técnicas debe integrarse sistemáticamente con las reglas sobre incautación, decomiso y custodia de evidencias, recogidas en los artículos 283 al 285. Estas disposiciones establecen que el fiscal debe ordenar la incautación de objetos relacionados con el hecho delictivo y, en caso de urgencia, la policía puede ejecutar dicha medida con obligación de rendir informe en ocho horas. Cuando los objetos incautados afectan derechos patrimoniales, el fiscal debe solicitar el secuestro judicial en un plazo de cuarenta y ocho horas. De esta manera, se garantiza un control judicial y fiscal adecuado sobre las medidas restrictivas que afectan bienes y derechos fundamentales, incluso en el contexto de delitos informáticos. En estos casos, la evidencia suele consistir en información digital almacenada en dispositivos tecnológicos, cuya preservación requiere protocolos especializados que aseguren la cadena de custodia[18].

[18] Fiscalía General del Estado, *Manual de actuación para la recolección, preservación, tratamiento y análisis de contenido digital,* (Código: CSEIIMLCF-MLCF-MAN-2025-002, Versión: 1.0)

La normativa salvadoreña reconoce también la necesidad de realizar operaciones técnicas y científicas como complemento de las inspecciones y pericias, conforme lo establece el artículo 186 del Código Procesal Penal (CPP). Estas operaciones pueden incluir análisis serológicos, pruebas ópticas, electrónicas, fonográficas, grafoscópicas, rayos X, análisis de ADN y cualquier otro examen disponible por la ciencia.

En delitos informáticos, estas técnicas se traducen en análisis forenses digitales, recuperación de archivos eliminados, extracción de metadatos, verificación de hash, autenticación de firmas electrónicas y reconstrucción de redes de comunicación. Estas prácticas permiten validar técnicamente la prueba obtenida por medio de agentes encubiertos digitales o en fuentes abiertas, otorgándole valor probatorio sólido ante el tribunal. El artículo 187 del CPP, por su parte, autoriza la realización de exámenes genéticos cuando existan rastros corporales en la escena del delito, lo cual permite extender la lógica del uso de perfiles biogenéticos al uso de perfiles digitales como mecanismo identificativo y de vinculación en la investigación penal contemporánea.

La obtención y resguardo de la información electrónica está regulada en el artículo 201 del vigente CPP, que exige autorización judicial cuando la información se encuentra en posesión de un particular y es necesaria para la investigación. No obstante, la norma permitía, mucho antes de la introducción del capítulo X de la reciente reforma al CPP, que, en las actuaciones de los policiales encubiertos, allanamientos o situaciones de flagrancia, y bajo la dirección funcional de la Fiscalía, el investigador policial estaba autorizado para adoptar medidas (técnicas) que garantizaran el resguardo inmediato de dicha información, sin perjuicio de la incautación posterior.

Esta disposición resulta coherente con las dinámicas propias del cibercrimen previa a la reforma al art. 259 D y siguientes del CPP, donde la velocidad de acción y la volatilidad de la información digital hacen indispensable la intervención oportuna para asegurar la prueba, sin que ello implique violación al debido proceso, siempre que se documente

adecuadamente la intervención y se garantice su control posterior por parte del fiscal y del juez competente.

El régimen de prueba testimonial también encuentra aplicación armónica en este esquema normativo. El artículo 215 permite que los agentes encubiertos puedan declarar testigos en juicio, con posibilidad de acogerse a medidas de protección. Esta previsión garantiza la validez procesal de la información recabada mediante operaciones encubiertas, y reconoce la necesidad de resguardar la integridad de quienes se exponen en estas tareas.

El CPP contempla además la posibilidad de incorporar testimonios de referencia en casos excepcionales, como en operaciones policiales encubiertas o cuando exista peligro grave para los testigos, según lo regulado en los artículos 220 y 221. Estos mecanismos refuerzan la protección del testigo y aseguran que la prueba no se vea frustrada por represalias o amenazas derivadas de estructuras criminales complejas.

La prueba pericial desempeña un rol esencial en este marco investigativo del cibercrimen. El artículo 226 CPP prevé, que los fiscales pueden requerir peritajes cuando sea necesario poseer conocimientos especializados para valorar una evidencia, y reconoce como peritos permanentes a los técnicos, analistas y especialistas de la Fiscalía y de la Policía Nacional Civil. Esta previsión permite que, por razones de eficiencia y especialidad, los peritos digitales de estas instituciones participen directamente en la obtención, validación y análisis de la evidencia tecnológica, contribuyendo con dictámenes que fundamenten las decisiones judiciales sobre su autenticidad, integridad y pertinencia.

El artículo 259-D faculta a la Policía a realizar búsquedas abiertas en sitios web y espacios públicos virtuales, así como a emplear software especializado para identificar evidencia digital. Esta facultad se enmarca en lo que la jurisprudencia estadounidense ha denominado “open-source intelligence” (OSINT), es decir, el uso de herramientas informáticas para extraer evidencia accesible al público.

De igual forma, la posibilidad de que Fiscalía y Policía celebren acuerdos con entes extranjeros para el intercambio directo de noticias criminales mediante TIC encuentra respaldo en los tratados internacionales como la Convención de Budapest sobre Ciberdelincuencia (que se encuentra pendiente de aprobación o ratificación en la Asamblea Legislativa de El Salvador), que fomenta la cooperación transfronteriza inmediata en casos que involucren evidencia digital. En este punto, la admisibilidad de dicha evidencia estará supeditada, como lo exige el artículo 259-C, al cumplimiento de los requisitos de autenticidad, obtención legal y cadena de custodia conforme a las reglas internas.

5.4. La acreditación de la prueba digital en la audiencia

El artículo 259-C del Código Procesal Penal establece un desarrollo técnico probatorio importante en cuanto a la autenticación de la prueba en la audiencia de la vista pública[19]. Lo relevante es garantizar al juez o tribunal que la evidencia digital no ha sido alterada, manipulada o transformada, por lo que se incorporan en la disposición criterios objetivos y prácticos similares a los que se exigen en la jurisprudencia estadounidense a la práctica probatoria[20]. De allí la aplicación de las reglas siguientes:

> "1) Acreditación de su autenticidad, lo cual puede ser realizado por cualquier de los medios siguientes:
>
> a) Prueba testimonial de la persona que intervino directamente en la elaboración, generación, transmisión o recepción de la evidencia digital por medio de las Tecnologías de la Información y Comunicación.
>
> b) Acreditación de los mecanismos técnicos informáticos idóneos utilizados para su generación, que aseguren esa autenticidad, como puede ocurrir en el caso de la firma electrónica u otros mecanismos semejantes.

[19] JA. Díaz Limón, *La incorporación de la prueba cibernética e informática: electrónica y digital,* (IUDICIUM, Revista de Derecho Procesal de la Asociación Iberoamericana de la Universidad de Salamanca, segundo semestre, 2019), 13-31.
[20] V.I. Neptune Rivera, *Los Retos de la Evidencia Electrónica,* (Revista Jurídica UPR, Vol 76, Número 3, 2007), 337 a 350.

c) Perito informático que haya intervenido en la obtención, resguardo o almacenamiento de la información o en el análisis de la evidencia digital, designado conforme a las reglas de este Código.“

Las reglas de acreditación de autenticidad de la evidencia digital, establecidas anteriormente pueden ser aplicadas de forma independiente entre sí, por lo que cada una será suficiente para tenerla por acreditada; sin embargo, en el caso de las contenidas en los literales a) y b), si alguna de las partes impugna de manera fundada el mecanismo de acreditación dentro de la fase de instrucción formal, la parte interesada en la admisión de evidencia deberá demostrar su integridad por medio de la intervención de un perito informático, designado conforme a las reglas de este Código.

1) El acceso al contenido de la evidencia digital, en virtud del derecho a la intimidad que se puede ver afectado, tal como lo regula el Art. 201 Procesal Penal, requerirá orden judicial, la cual podrá ser solicitada por la Fiscalía durante los actos urgentes de comprobación o diligencias iniciales de investigación al juez de paz competente, o durante la fase de Instrucción formal al juez de instrucción que conozca de la imputación. Lo anterior no será necesario cuando se obtenga el consentimiento informado del titular del derecho a la intimidad que podría verse afectado; así como sus consecuencias legales si las hay, lo cual deberá registrarse por escrito; en el caso del imputado, además de su defensor, deberá acreditar que ha informado las consecuencias de la realización de la diligencia.

2) En caso que sea necesaria la realización de la prueba pericial en la evidencia digital, se deberán cumplir con los requisitos establecidos para este medio probatorio por este código; sin embargo, si el perito informático es de carácter permanente, los puntos de pericia podrán ser establecidos por el fiscal del caso, o solicitados al juez competente a requerimiento de las partes. Sin perjuicio de lo anterior las partes podrán acordar la estipulación de la evidencia digital, en los términos establecidos en este Código.

3) El secretario del Tribunal o quien disponga administrativamente la Corte Suprema de Justicia notificará de inmediato a las partes, citará a los testigos o peritos y solicitará los objetos y documentos y dispondrá cualquier otra medida necesaria para la organización y desarrollo de la vista pública. La producción de la evidencia digital podrá ser realizada en el proceso penal mediante el uso de cualquier método y recurso tecnológico, que sea idóneo para realizar la correcta presentación de la misma, inclusive con el apoyo de perito informático designado conforme a las reglas de este Código."

Esta previsión legislativa del art. 259-C del CPP se basa en la doctrina de Lorraine v Markel American Insurance[21], donde se establece que la prueba electrónica debe contar con una demostración de autenticidad conforme a las Reglas de Evidencia Federales (FRE por su acrónimo en inglés) la Federal Rule Evidence 901(a), pudiendo ser acreditada por medio del testimonio de una persona con conocimiento (Rule 901(b)(1)), por características distintivas (Rule 901(b)(4)), por un perito o por certificaciones técnicas como los *hash codes* o metadatos[22].

La fuente de prueba testimonial y pericial se introduce en la audiencia a través del interrogatorio si la ofrece quien tiene la carga de la prueba, sujeta a la confrontación mediante el contrainterrogatorio, de acuerdo con las reglas del CPP[23].

El art. 259-C del CPP reconoce la posibilidad de validar evidencia digital sin depender exclusivamente de la persona que la generó (como podría ser la víctima o el agente digital encubierto) en el caso de la acusación que tiene la carga de probar que la prueba ofrecida es lo que afirmo que es (parte fiscal), sino por medio de peritos informáticos o mecanismos técnicos informáticos idóneos como es la firma electrónica.

[21] Lorraine v. Markel American Insurance Company, 241 FRD 534 (D. Md. 2007).
[22] P.W. Grimm et al, *Authenticating Digital Evidence,* (Baylor Law Rewiew, Vol 69:1, 2017), 11-24.
[23] R.I. Sandoval Rosales, Las reglas de interrogatorio y el contrainterrogatorio adversativo en el proceso penal de El Salvador, (IUDICIUM, Revista de Derecho Procesal de la Asociación Iberoamericana de la Universidad de Salamanca, primer semestre, 2020), 61 a 86.

El artículo 259-C, numeral 4, refuerza el principio de oralidad y publicidad al exigir que la evidencia digital sea presentada (autenticada en audiencia pública) mediante los recursos tecnológicos adecuados y, de ser necesario, con el auxilio de perito informático[24]. Este principio refuerza la regla general de contradicción y permite al tribunal visualizar directamente el contenido, tal como lo permite la Regla 1001(3) de las Federal Rules of Evidence, que define el "original" en términos amplios para incluir la visualización legible en pantalla o la impresión que refleje fielmente el contenido digital. La carga probatoria no solo se limita a presentar el documento electrónico (la prueba digital), sino a demostrar su fidelidad, relevancia, autenticidad y admisibilidad bajo los estándares vigentes.

La disposición del art. 259 B permite la autenticación, reforzando el criterio de que no se trata de una prueba infalible, sino de una evidencia que debe ser verificada conforme a los medios técnicos y las garantías del debido proceso.

Asimismo, el artículo 259-B introduce la obligación de respetar la cadena de custodia aun en los casos donde la evidencia haya sido obtenida por medios oficiosos, lo cual resulta esencial para sostener la integridad de la prueba digital. Esta disposición coincide con la regla de cadena de custodia del CPP que exige trazabilidad en la manipulación de la evidencia electrónica.

En la práctica judicial salvadoreña, la cadena de custodia digital no solo implica asegurar que la evidencia no ha sido alterada, sino también documentar con precisión cada paso desde su adquisición hasta su presentación judicial, lo que implica peritaje en algunos casos por la naturaleza de la evidencia material. En el caso de la evidencia digital, analizada por un perito se requerirá autenticar el log in de acceso, hash de verificación, y sistemas de respaldo confiables. Esta necesidad se vuelve más crítica en los entornos digitales donde la información puede ser fácilmente modificada sin dejar rastros físicos visibles. En Lorraine, el juez Grimm advierte que la ausencia de estas

[24] L. Rivera Román, *Presentación del Libro La Evidencia Electrónica de la licenciada Vivian I Neptune Rivera, Decana de la Escuela de Derechos de la UPR.* (Revista Jurídica UPR, Vol 87, Número 4, 2018), 1427.

precauciones puede hacer inadmisible la *evidencia digital* no por su contenido sino por el quebrantamiento de los procedimientos de autenticación y conservación de su integridad[25].

6. Conclusiones

El legislador, con la reforma del 2025 a la LEDIC y al CPP, está adaptándose a las nuevas amenazas del crimen común y del crimen organizado a las conductas delictivas que lesionan o ponen en riesgo a los ciudadanos frente al cibercrimen. Además, el legislador reconoce que la actividad social, económica y gubernamental se lleva a cabo a través de las tecnologías de información.

La vida de las personas se encuentra vinculada a las bases de datos, a las redes sociales y a la navegación en el internet, lo cual genera preguntas desde la protección a la intimidad, el derecho al olvido, la propia imagen, y la seguridad de la información. Sin duda la ley es un punto de partida, pero no de llegada, debido a la rápida evolución de las tecnologías, la inteligencia artificial y la creatividad de los criminales.

Asimismo, el legislador creo en la LEDIC y en el CPP unidades y herramientas de investigación de los ciberdelitos. La legislación salvadoreña en materia de evidencia digital, tal como lo reflejan los artículos 259-A a 259-D del Código Procesal Penal, no solo establece un marco integral para la admisión, autenticación y valoración de la prueba electrónica, sino que permite a jueces y partes actuar con previsibilidad y coherencia técnica ante los retos de la criminalidad digital, reforzando así el principio de legalidad procesal y la protección judicial.

7. Bibliografía

Capra DJ., *Deepfakes reach the advisory Committee on evidence rules*, (FORDHAM LAW REVIEW, Vol. 92, 2024).

[25] DJ. Capra, *Deepfakes reach the advisory Committee on evidence rules,* (FORDHAM LAW REVIEW, Vol. 92, 2024), 2491-2505.

Díaz Limón, JA., *La incorporación de la prueba cibernética e informática: electrónica y digital,* (IUDICIUM, Revista de Derecho Procesal de la Asociación Iberoamericana de la Universidad de Salamanca, segundo semestre, 2019).

Fiscalía General del Estado, Manual de actuación para la recolección, preservación, tratamiento y análisis de contenido digital, (Código: CSEIIMLCF-MLCF-MAN-2025-002, Versión: 1.0)

Fuentes Real, JC, *Contribuciones del Funcionalismo normativo en la teoría del delito*, (Comisión Coordinadora del Sector de Justicia, Unidad Técnicas Ejecutiva del Sector de Justicia, 2024).

Grimm P.W. et al, *Authenticating Digital Evidence*, (Baylor Law Rewiew, Vol 69:1, 2017)

Hernández Gómez, J. R., *La anticorrupción en Colombia, el agente encubierto y la función de inteligencia,* (Revista Prolegómenos - Derechos y Valores - pp. 99-114, 2018, I)

Jennetten,P.R. *From E-Discovery to E-Evidence: Lorraine v Markel American Ins. Co*, (Illinois Association fo Defensa Trial Counsel, Springfield, Illinois, V. 18, No. 1).

Lorraine v. Markel American Insurance Company, 241 FRD 534 (D. Md. 2007).

Neptune Rivera V.I., *Los Retos de la Evidencia Electrónica*, (Revista Jurídica UPR, Vol 76, Número 3, 2007).

Parada. RA, I., *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (compilado por Ricardo Antonio Parada; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos Aires: Erreius, 2018.)

Pérez, MP, *El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española* (Criterio Jurídico Santiago de Cali V. 6 2006 pp. 267-310 ISSN 1657-3978)

Rayón Ballesteros, MC et al, *Cibercrimen: particularidades en su investigación y enjuiciamiento,* (Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234 / ISSN: 1133-3677)

Reyes, J.I, *Los registros y allanamientos en la era digital: la renuncia a nuestra privacidad*, (Revista UIPR, Vol XLIX: 3: 467, 2014-2015).

Rivera Román, L., *Presentación del Libro La Evidencia Electrónica de la licenciada Vivian I Neptune Rivera*, Decana de la Escuela de Derechos de la UPR. (Revista Jurídica UPR, Vol 87, Número 4, 2018).

Roxin, C. *La Evolución de la Política Criminal, el derecho penal y el proceso penal*, (Tirant lo Blanch, Valencia, 2000).

Sandoval Rosales, R.I. *Las reglas de interrogatorio y el contrainterrogatorio adversativo en el proceso penal de El Salvador*, (IUDICIUM, Revista de Derecho Procesal de la Asociación Iberoamericana de la Universidad de Salamanca, primer semestre, 2020)

Sandoval Rosales RI et al, *Código Procesal Penal comentado V. 1 y V. 2* (1ª Ed. San Salvador, Consejo Nacional de la Judicatura, 2018). Es la fuente que puede explicar los actos de investigación y de prueba.

Sandoval, R. *Manual para la Investigación de los Delitos de Trata de Personas y Tráfico Ilicito de Migrantes,* (OEA-OIM-ACNUR, Programa de Prevención de los Delitos Vinculados a la Migración Irregular en Mesoamérica, 2017)

Serrano Piedecasas Fernández J. R et al, *Manual de teoría jurídica del delito* (1a. ed, San Salvador, El Salvador, Consejo Nacional de la Judicatura, Escuela de Capacitación Judicial, 2003).

Soriano Guillamón A et al, *Agente encubierto informático. Informe de derecho comparado,* (Cuadernos de RES PUBLICA en derecho y criminología, ISSN: 2990-0697 DOI: Nº En prensa 10.46661/respublica.12120, Universidad Pablo de Olavide).