Fundación por la Libertad de Expresión y Democracia

Informe Regional Derechos Digitales y Ciberdelincuencia en Centroamérica

Análisis comparado 2018–2025

Informe Regional Derechos Digitales y Ciberdelincuencia en Centroamérica

Análisis comparado

2018-2025

FLED

https://fled.ong/

https://www.facebook.com/fledONG

@FLED_ong

Autor: Alexa Zamora.

Índice de Contenidos

Introducción

Este informe ofrece un análisis comparado sobre la legislación y las prácticas en materia de derechos digitales, ciberdelitos, privacidad, retención de datos y uso de biometría en Centroamérica. Se considera que los derechos digitales son una extensión de los derechos humanos a los entornos digitales, abarcando el acceso a internet, la libertad de expresión en línea, la privacidad, el derecho al olvido, el acceso a la información y la neutralidad de la red. Estas garantías son fundamentales para preservar la dignidad humana y la libertad individual en el ciberespacio, y forman parte de la llamada cuarta generación de derechos humanos.

En Centroamérica, la protección de los **derechos digitales** y el combate al cibercrimen han motivado diversas leyes y políticas en los últimos años. Cada país de la región –Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica y Panamá– ha adoptado marcos normativos con enfoques y alcances distintos, el andamiaje jurídico sobre ciberdelitos, protección de datos y telecomunicaciones se ha expandido con rapidez. Sin embargo, junto con avances puntuales, varios Estados han introducido **tipos penales vagos, competencias amplias de interceptación** y **regímenes de retención/entrega de datos** que facilitan prácticas de vigilancia y censura.

A través del presente informe introduce una recopilación de las principales normativas de cada país, incluyendo proyectos de ley recientes, reformas relevantes, normativa al nivel del Sistema de Integración Centroamericana y jurisprudencia destacada, continuando con un breve análisis de su contenido y posibles implicaciones en materia de libertad de expresión, privacidad y seguridad cibernética, enfatizando **usos prácticos** que afectan la libertad de expresión y la privacidad en el entorno digital, además de realizar una comparación de cómo estas cumplen o no con los compromisos internacionales en materia de **Derechos Digitales**.

En este análisis incluiremos además estudios de casos emblemáticos por país, así como las perspectivas de expertos, periodistas y activistas de Centroamérica con respecto al estado actual de los derechos digitales en la región y recomendaciones dirigidas a los tomadores de decisiones y profesionales en el tema para garantiza la salvaguarda de los **Derechos Humanos** en línea.

Objetivo del Informe	Alcance	Metodología
Recopilar y analizar las principales normativas de cada país, incluyendo proyectos de ley recientes, reformas relevantes y jurisprudencia destacada.	Análisis de contenido y posibles implicaciones en materia de libertad de expresión, privacidad y seguridad cibernética.	Comparación de cumplimiento con compromisos internacionales en materia de Derechos Digitales, incluyendo estudios de casos emblemáticos.

Derechos digitales como una extensión de los derechos humanos en el entorno digital.

Los derechos digitales se consideran parte de los llamados **derechos humanos de cuarta generación**, orientados a garantizar la protección de las personas en el entorno digital. El ciberespacio se reconoce como un espacio de interacción humana sujeto a riesgos y amenazas similares a los del mundo físico, por lo que resulta esencial salvaguardar en él los principios democráticos, la convivencia pacífica, el respeto y la equidad entre quienes lo utilizan. En este sentido, los derechos digitales funcionan como un puente que asegura la vigencia de los derechos humanos tradicionales dentro de los entornos tecnológicos emergentes (Pacto Mundial, 2023).

Los derechos digitales constituyen la adaptación de los derechos humanos fundamentales al ámbito tecnológico. Estos abarcan dimensiones como la libertad de expresión, la privacidad, el acceso a la información y la libertad de reunión, todas reinterpretadas para el contexto digital. Su propósito es proteger a las personas dentro de los espacios virtuales, asegurando que el desarrollo y uso de tecnologías se realice con pleno respeto a la dignidad humana y a la libertad. En términos prácticos, los derechos digitales garantizan a las personas la posibilidad de acceder, usar, crear y difundir contenidos en los medios digitales, así como utilizar dispositivos electrónicos y redes de comunicación, siempre en concordancia con principios esenciales como la privacidad y la libertad de expresión (Pacto Mundial, 2023).

Los derechos digitales abarcan múltiples ámbitos de la vida en línea. Entre los más relevantes se encuentran:

1 Derecho de acceso a Internet

El acceso a Internet se posicionó como un elemento clave el 1 de junio de 2011, cuando diversos organismos internacionales de libertad de expresión emitieron la Declaración Conjunta sobre Libertad de Expresión e Internet. El documento destacó la obligación de los Estados de promover el acceso universal a Internet como medio indispensable para garantizar la libertad de expresión y otros derechos fundamentales, incluyendo la educación, la salud, el empleo, la libertad de reunión y la celebración de procesos electorales libres (Relatoría ONU et al., 2011).

2 Libertad de expresión digital

La libertad de expresión digital protege el derecho de toda persona a expresar ideas, opiniones y pensamientos mediante plataformas en línea sin temor a censura o represalias. Este derecho es esencial para la vida democrática, pues facilita el intercambio de información y la deliberación pública. No obstante, enfrenta desafíos como la censura en línea, la moderación de contenidos y el uso indebido de leyes de difamación para limitar la crítica o la disidencia (Pacto Mundial, 2023).

3 Privacidad en línea y derecho al anonimato

La privacidad en línea implica el control que las personas tienen sobre sus datos personales y la forma en que estos se utilizan en internet. Incluye la facultad de navegar de manera anónima, impedir el uso indebido de datos y proteger la información ante accesos no autorizados. La privacidad digital es esencial para garantizar la libertad en la red y prevenir prácticas de vigilancia que puedan poner en riesgo los derechos individuales (Pacto Mundial, 2023).

4 Derecho al olvido

El derecho al olvido fue reconocido por primera vez en la Unión Europea en 2014 a partir de una sentencia del Tribunal de Justicia de la Unión Europea. Este fallo estableció que las personas pueden solicitar a los motores de búsqueda eliminar resultados asociados a su nombre cuando la información sea inexacta, irrelevante, inadecuada o excesiva, sopesando siempre el interés público de mantener la información disponible (TJUE, 2014).

5 Acceso a la información digital

Este derecho se refiere a la posibilidad de buscar, recibir y difundir información a través de medios digitales. Su ejercicio es fundamental para la educación, la participación ciudadana y la toma de decisiones informadas. No obstante, se ve afectado por factores como la brecha digital, restricciones gubernamentales y limitaciones derivadas de la falta de neutralidad de la red (Pacto Mundial, 2023).

6 Neutralidad de la red

La neutralidad de la red establece que los proveedores de servicios de Internet deben tratar de manera igualitaria todos los datos que circulan por sus redes, sin bloquear, priorizar ni discriminar contenidos, aplicaciones o usuarios. Este principio garantiza un Internet abierto, competitivo e inclusivo, preservando el acceso equitativo a la información para toda la ciudadanía (Pacto Mundial, 2023).

¿Cómo están regulados los derechos digitales en centroamérica?

La regulación de los derechos digitales en Centroamérica es fragmentada y evidencia profundas diferencias entre los países de la región. Costa Rica y Panamá cuentan con los marcos más sólidos: ambos han adoptado leyes de protección de datos personales inspiradas en estándares internacionales y disponen de autoridades especializadas, mecanismos de control judicial y jurisprudencia que refuerza la privacidad, la libertad de expresión y la proporcionalidad en la intervención de comunicaciones (PRODHAB, 2011; ANTAI, 2021). En contraste, Guatemala y Honduras presentan rezagos significativos: carecen de leyes integrales de protección de datos y sus intentos de regulación en materia de ciberdelitos han enfrentado fuertes críticas por ambigüedad y riesgos a la libertad de expresión, generando vacíos legales que dejan sin adecuada protección derechos como la privacidad digital o la libertad de expresión en línea (Criterio.hn, 2019; Prensa Libre, 2022). Mientras tanto, El Salvador y Nicaragua ilustran un giro restrictivo: han promulgado leyes que, aunque presentadas como herramientas de seguridad digital, concentran poder en autoridades dependientes del Ejecutivo, habilitan amplias facultades de intervención y han sido denunciadas por facilitar censura, vigilancia y persecución del disenso (Human Rights Watch, 2024; Access Now, 2020).

Presentaremos los Marcos legales de los correspondientes países a continuación:

Marcos Sólidos	Rezagos Significativos	Giro Restrictivo
Costa Rica y Panamá cuentan con los marcos más robustos: ambos han adoptado leyes de protección de datos personales inspiradas en estándares internacionales y disponen de autoridades especializadas.	**Guatemala y Honduras** presentan vacíos importantes: carecen de leyes integrales de protección de datos y sus intentos de regulación han enfrentado fuertes críticas.	**El Salvador y Nicaragua** ilustran un enfoque autoritario: han promulgado leyes que concentran poder en el Ejecutivo y facilitan censura y vigilancia.

Guatemala: Marco normativo

Guatemala continúa sin una ley integral que regule los ciberdelitos o la seguridad digital. En 2022, el Congreso aprobó el Decreto 39-2022, Ley de Prevención y Protección contra la Ciberdelincuencia, cuyo propósito era tipificar nuevos delitos informáticos.

Decreto 39-2022

Generó amplio rechazo por su redacción ambigua que podía vulnerar la libertad de expresión. Fue archivado en agosto de 2022 antes de su entrada en vigor.

Vacío Normativo

En ausencia de legislación especial, las autoridades recurren a disposiciones generales del Código Penal, insuficientes para abordar fenómenos digitales contemporáneos.

Protección de Datos

No existe ley nacional de protección de datos personales. La tutela depende principalmente de la acción constitucional de hábeas data.

Guatemala continúa sin una ley integral que regule los ciberdelitos o la seguridad digital. En 2022, el Congreso aprobó el **Decreto 39-2022**, Ley de Prevención y Protección contra la Ciberdelincuencia, cuyo propósito era tipificar nuevos delitos informáticos y actualizar disposiciones penales relacionadas con la protección de datos personales y la privacidad digital (Prensa Libre, 2022a). Sin embargo, esta normativa generó un amplio rechazo de especialistas y organizaciones civiles, que advirtieron que su redacción ambigua podía vulnerar la libertad de expresión y facilitar el silenciamiento de críticas dirigidas a funcionarios públicos (Criterio.hn, 2019). Finalmente, antes de su entrada en vigor, el Congreso dejó sin efecto la ley y la archivó en agosto de 2022 (Prensa Libre, 2022b), manteniendo al país sin un marco normativo específico en materia de ciberdelitos. En ausencia de una legislación especial, las autoridades recurren a disposiciones generales del Código Penal, que resultan insuficientes para abordar fenómenos contemporáneos del entorno digital. A ello se suma la inexistencia de una ley nacional de protección de datos personales: la tutela de este derecho depende principalmente de la acción constitucional de **hábeas data** y de principios derivados del derecho a la intimidad. Aunque la **Ley de Acceso a la Información Pública** (Decreto 57-2008) constituye un avance en materia de transparencia, no regula la protección de datos en manos de actores públicos o privados.

La ausencia de un marco robusto coexiste con normas puntuales relacionadas con vigilancia y telecomunicaciones. El cuerpo normativo principal sigue siendo la **Ley General de Telecomunicaciones** (Decreto 94-96), enfocada mayormente en la regulación económica del espectro radioeléctrico. Guatemala no cuenta con obligaciones de retención de datos ni con una ley específica de vigilancia digital, aunque diversas normas permiten la intervención de comunicaciones bajo orden judicial en casos de delincuencia grave, como sucede con la **Ley contra la Delincuencia Organizada**. Asimismo, el Decreto 12-2014 regula el **Control de Telecomunicaciones Móviles en Centros Penitenciarios**, obligando a los operadores a bloquear señales telefónicas en prisiones (ACNUR, 2016). Tras el archivo del Decreto 39-2022, no se han aprobado nuevas leyes de ciberdelitos hasta 2025; persisten iniciativas inconclusas como la **Iniciativa 5928** de reforma a la Ley General de Telecomunicaciones o propuestas de ley de protección de datos personales. El gobierno entrante en 2024 ha expresado interés en actualizar la regulación digital, aunque enfrenta una fuerte resistencia social debido al precedente de una posible "ley mordaza". En este contexto, la **Corte de Constitucionalidad** mantiene un rol clave: si bien no se pronunció directamente sobre el Decreto 39-2022, su jurisprudencia previa muestra una postura firme en defensa de la libertad de expresión y la privacidad, lo que sugiere que cualquier ley penal que limite de manera desproporcionada la crítica pública podría ser declarada inconstitucional. En paralelo, el amparo se ha consolidado como vía para exigir corrección o supresión de datos personales, supliendo parcialmente la ausencia de una ley especializada (Plaza Pública, 2017). En conjunto, la regulación guatemalteca en materia de derechos digitales se encuentra en una fase incipiente y fragmentada, con avances judiciales relevantes pero sin un marco legislativo que otorgue garantías integrales.

Guatemala: Prácticas que atentan contra los derechos digitales

El periodista Sonny Figueroa retrata un escenario donde la libertad de expresión en Guatemala es "a medias". Los grupos poderosos del Ministerio Público han refinado sus estrategias para silenciar voces.

> "Los grupos poderosos utilizan la Ley de Acceso a la Información Pública y el delito de revelación de información reservada para judicializar a periodistas y exfiscales, creando una disyuntiva permanente entre publicar investigaciones de interés público y exponerse a procesos penales."

Judicialización

Uso del artículo 37 sobre revelación de información reservada, punible con 6-8 años de prisión.

Acoso Digital

Campañas coordinadas que publican datos personales de periodistas y estudiantes con calificativos difamatorios

Vigilancia

Contratación de servicios de monitoreo y ataques de saturación contra sitios web tras publicar investigaciones

En una entrevista, el periodista Sonny Figueroa retrata un escenario donde la libertad de expresión en Guatemala es “a medias”. Explica que los grupos poderosos del Ministerio Público han refinado sus estrategias para silenciar voces, utilizando la **Ley de Acceso a la Información Pública** y el delito de revelación de información reservada (artículo 37) –punible con seis a ocho años de prisión– para judicializar a periodistas y exfiscales. Este precepto se ha invocado para dictar órdenes de captura contra exfuncionarios como Juan Francisco Sandoval y, en el propio caso de Figueroa, la Fiscalía abrió un expediente contra él por divulgar imágenes que permitían identificar a una mujer que lo vigilaba. La consecuencia es una disyuntiva permanente entre publicar investigaciones de interés público y exponerse a procesos penales.

Asimismo, relata que tras revelar una operación de desinformación organizada desde la Dirección de Comunicación del Congreso, tanto él como Marvin Del Cid fueron demandados por “violencia psicológica” y recibieron una prohibición judicial de seis meses para entrar al Congreso o mencionar a la funcionaria implicada. Estas tácticas muestran un patrón de criminalización mediante figuras jurídicas imprecisas destinadas a disuadir al periodismo de investigación.

En el plano digital, Figueroa describe campañas de acoso en las que actores anónimos publican datos personales –domicilios, expedientes académicos, números de identificación– de estudiantes y periodistas, acompañándolos de fotografías y calificativos que buscan asociarlos con delitos, al tiempo que etiquetan a instituciones de seguridad. Denuncia que estas operaciones se coordinan con medios de comunicación tradicionales: se emiten clips con afirmaciones difamatorias y luego redes de cuentas anónimas las amplifican, de manera que cuando los afectados interponen querellas por difamación, los tribunales las desestiman alegando libertad de expresión. La divulgación de datos y la difusión concertada de calumnias desdibujan la frontera entre hostigamiento digital y vigilancia estatal, poniendo en riesgo la privacidad y la seguridad de periodistas y activistas.

Por último, Figueroa advierte que aunque aún no se aprueban iniciativas para penalizar las críticas en internet (como el delito de "acoso político"), cada nuevo proyecto legislativo despierta temor de que se use para criminalizar a la ciudadanía y a la prensa. Mientras tanto, las autoridades recurren a medios técnicos: ataques de saturación que dejan fuera de línea sitios web tras publicar investigaciones, denuncias masivas para cerrar cuentas en redes sociales e incluso la contratación de servicios de monitoreo para vigilar lo que se dice de la fiscal general. El periodista subraya que el desafío no es solo legal sino cultural: el plan de protección a periodistas prometido desde 2012 no se ha implementado; el gremio carece de una voz unificada; y la dependencia de financiamiento externo genera autocensura. Figueroa insiste en que callar ante el poder solo fortalece a los censores y que los periodistas deben defender activamente sus derechos y exigir políticas de protección, pues de lo contrario la cultura de intimidación digital seguirá prevaleciendo.

El Salvador: Marco Legal de Ciberdelitos

Desde 2016, El Salvador cuenta con la Ley Especial contra los Delitos Informáticos y Conexos, principal instrumento para perseguir conductas ilícitas cometidas mediante tecnologías de la información.

Ley Especial 2016

Tipifica delitos como acceso indebido, fraude digital, espionaje electrónico, manipulación de datos y suplantación de identidad, con penas de 1 a 12 años.

Reformas 2025

El Decreto 332 amplió definiciones de víctimas, incorporó conceptos de protección de datos y endureció penas por fraude informático con abuso de confianza (10-12 años).

Desde 2016, El Salvador cuenta con la Ley Especial contra los Delitos Informáticos y Conexos, la cual constituye el principal instrumento para perseguir conductas ilícitas cometidas mediante tecnologías de la información (Asamblea Legislativa, 2016). La normativa tipifica un amplio conjunto de delitos —como acceso indebido a sistemas, fraude digital, espionaje electrónico, manipulación de datos, suplantación de identidad y divulgación no autorizada de información personal— con penas que van de uno a doce años de prisión según su gravedad (Asamblea Legislativa, 2016). En 2025, la Asamblea Legislativa aprobó reformas relevantes mediante el Decreto 332, vigente desde el 3 de julio, orientadas a fortalecer la persecución del ciberdelito y la protección de datos (Asamblea Legislativa, 2025).

Entre las reformas de 2025, se amplió la definición de víctimas en delitos informáticos: ahora no solo las personas cuyos datos son afectados, sino también las entidades que los custodian o procesan pueden ser consideradas víctimas en casos como fraude digital (Asamblea Legislativa, 2025a). Asimismo, se incorporaron definiciones de "propietario de los datos", "custodio", "controlador" y "procesador", armonizando la terminología con estándares contemporáneos de protección de datos (Asamblea Legislativa, 2025a; 2025b). Otra modificación relevante fue el endurecimiento de las penas por fraude informático cometido por empleados con acceso legítimo a sistemas, que ahora oscilan entre diez y doce años cuando existe abuso de confianza digital (Asamblea Legislativa, 2025a). Estas medidas buscan reforzar la seguridad de la información tanto en el sector público como en el privado.

El Salvador: Ley de Protección de Datos y Ciberseguridad

En noviembre de 2024, El Salvador aprobó su primera Ley de Protección de Datos Personales, que reconoce derechos como acceso, rectificación, cancelación, oposición y un amplio "derecho al olvido" (Asamblea Legislativa, 2024a).

Agencia de Ciberseguridad (ACE)

Creada y designada directamente por el Ejecutivo, con amplias facultades para supervisar datos y ordenar eliminación de información en línea.

Riesgos Identificados

Organizaciones advierten que la combinación de "derecho al olvido" expansivo y autoridad dependiente del Ejecutivo genera riesgos para la libertad de expresión.

Ley de Ciberseguridad

Establece principios para proteger sistemas informáticos e infraestructuras críticas, otorgando a la ACE rol central en gestión de incidentes.

Preocupación Internacional: Human Rights Watch advierte que estas facultades podrían emplearse para ordenar la remoción de publicaciones críticas bajo aparentes violaciones a la ley de datos, incrementando el riesgo de censura en línea.

La ley crea además la Agencia de Ciberseguridad del Estado (ACE), designada directamente por el Ejecutivo, dotándola de amplias facultades para supervisar el tratamiento de datos y ordenar la eliminación de información en línea (Asamblea Legislativa, 2024a; 2024b). Aunque estas disposiciones buscan fortalecer la protección de datos, organizaciones de derechos humanos advierten que la combinación de un "derecho al olvido" expansivo y una autoridad dependiente del Ejecutivo genera riesgos para la libertad de expresión y el acceso a información de interés público, al permitir la remoción de contenidos considerados "inexactos" o "no pertinentes" bajo criterios discrecionales (Human Rights Watch, 2024; Refworld, 2024).

En este contexto, la ley se convierte en un mecanismo que facilita la censura digital y limita el escrutinio ciudadano, afectando de manera directa los derechos digitales fundamentales, mediante la instrumentalización de un derecho legítimo como es el "derecho al olvido", no podemos pasar por alto que en los últimos años el estado salvadoreño ha sido señalado en múltiples informes por atentar contra la libertad de expresión.

De forma paralela, en noviembre de 2024 El Salvador aprobó la Ley de Ciberseguridad y Seguridad de la Información, orientada a establecer principios y lineamientos para proteger sistemas informáticos e infraestructuras críticas del Estado (Asamblea Legislativa, 2024c). La normativa aplica tanto a instituciones públicas como a entidades privadas vinculadas a infraestructuras esenciales, y otorga a la Agencia de Ciberseguridad del Estado (ACE) un rol central como ente rector en la gestión de incidentes, supervisión de estándares y aplicación de sanciones (Asamblea Legislativa, 2024c; 2024d). Si bien la ley promueve la adopción de marcos internacionales como ISO 27001 para mejorar la resiliencia digital, la concentración de funciones estratégicas —incluidas ciberseguridad, supervisión estatal y protección de datos— en un organismo designado por el Ejecutivo genera preocupación en cuanto a independencia, controles democráticos y posibles usos para vigilancia intrusiva (Human Rights Watch, 2024).

En un contexto de amplia hegemonía institucional del gobierno, esta arquitectura normativa facilita prácticas de monitoreo centralizado y limita garantías procesales, erosionando derechos digitales como la privacidad, la libertad de expresión y la protección frente a injerencias arbitrarias en línea, llevado a la práctica la creación de perfiles de sujetos de interés, nuevamente bajo criterios discrecionales es una preocupación real.

El Salvador: Vigilancia y Marcos Regresivos

El Salvador cuenta desde 2010 con la Ley Especial para la Intervención de las Telecomunicaciones, que autoriza la interceptación de comunicaciones únicamente mediante orden judicial y para delitos graves.

Aunque el artículo 24 de la Constitución exige proporcionalidad y control judicial estricto, investigaciones independientes revelaron el uso del software espía Pegasus contra periodistas y activistas sin autorización judicial.

1. **2010**
   Ley Especial para Intervención de Telecomunicaciones establece requisito de orden judicial.

2. **2022**
   Reforma crea "agentes digitales encubiertos" permitiendo operaciones secretas sin control judicial efectivo.

3. **2024-2025**
   Nuevas leyes de ciberseguridad y datos consolidan facultades en la ACE, generando preocupación por vigilancia centralizada.

Las leyes aprobadas entre 2024 y 2025 consolidan en la Agencia de Ciberseguridad del Estado (ACE) un conjunto amplio de atribuciones en materia de protección de datos y ciberseguridad, pese a que se trata de una entidad designada directamente por el Ejecutivo (Human Rights Watch, 2024; Refworld, 2024). Este diseño normativo, en ausencia de contrapesos institucionales robustos, abre la puerta a un uso instrumental del derecho a la protección de datos para limitar la transparencia, incentivar la autocensura y facilitar prácticas de censura digital de contenido crítico.

El Salvador cuenta desde 2010 con la Ley Especial para la Intervención de las Telecomunicaciones, que autoriza la interceptación de comunicaciones telefónicas y electrónicas únicamente mediante orden judicial y para delitos graves, principio que fue reafirmado en las reformas de 2022 al crear un Centro de Intervención bajo la Fiscalía como único órgano ejecutor (Yahoo Noticias, 2022). Aunque el artículo 24 de la Constitución exige proporcionalidad y control judicial estricto, investigaciones independientes revelaron el uso del software espía Pegasus contra periodistas y activistas sin autorización judicial, evidenciando prácticas de vigilancia fuera del marco legal (Citizen Lab, 2022). La ausencia de una ley general de retención de datos limita la recolección masiva, pero los operadores pueden ser requeridos judicialmente para entregar registros específicos. Con la entrada en vigor de la Ley de Ciberseguridad y el fortalecimiento de la ACE, existe preocupación por la posible consolidación de un aparato de vigilancia digital centralizado que erosione la privacidad y facilite la intervención indebida de comunicaciones. Human Rights Watch advierte que estas facultades también podrían emplearse para ordenar la remoción de publicaciones críticas bajo aparentes violaciones a la ley de datos, incrementando el riesgo de censura en línea (Human Rights Watch, 2024).

Las violaciones a los derechos digitales también se sostienen mediante **marcos normativos regresivos**. En 2022 se aprobó una reforma al Código Procesal Penal que creó la figura de **"agentes digitales encubiertos"**, permitiendo operaciones secretas de acceso a comunicaciones sin control judicial efectivo (Human Rights Watch, 2022). Estas disposiciones permiten infiltración, incautación de datos y monitoreo digital con amplias facultades otorgadas a la Fiscalía, sin mecanismos de escrutinio independiente, contraviniendo estándares interamericanos.

Además de las reformas de 2024 y 2025, El Salvador ha explorado iniciativas como una Ley de Identidad Digital y la modernización de su normativa de comercio electrónico, aunque aún sin propuestas formales (Asamblea Legislativa, 2025c). La adopción simultánea de leyes integrales de ciberseguridad y protección de datos coloca al país a la vanguardia regional (Asamblea Legislativa, 2024c; 2024a). Sin embargo, el diseño centralizado de estas políticas plantea riesgos, especialmente en contextos donde las autoridades buscan ampliar mecanismos de supervisión digital. Experiencias internacionales muestran que arquitecturas tecnológicas fuertemente centralizadas —como las usadas en China para gestionar datos, identidades digitales y sistemas de ciberseguridad— pueden facilitar prácticas de vigilancia, control social y limitación del ejercicio de derechos fundamentales (Creemers, 2022). Si no se establecen salvaguardas, transparencia y controles independientes, marcos similares podrían habilitar en El Salvador un monitoreo estatal ampliado, la identificación masiva de ciudadanos y el uso instrumental de tecnologías digitales para restringir libertades, especialmente en entornos de alta concentración de poder político.

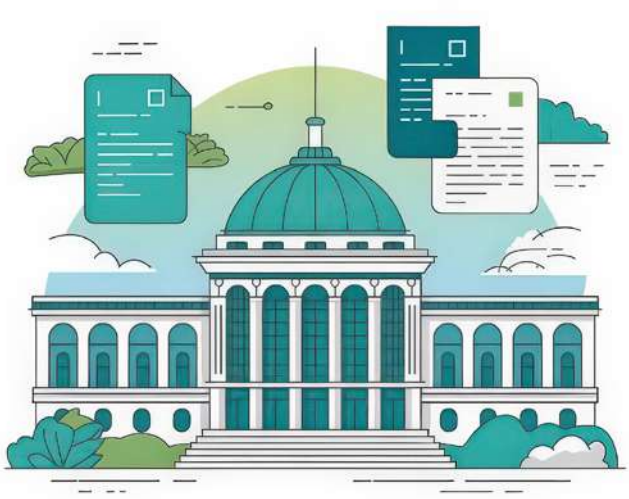
La jurisprudencia salvadoreña reciente en materia de derechos digitales es limitada, dado que la Sala de lo Constitucional —reconfigurada en 2021— no ha conocido casos de alto impacto relacionados con la aplicación de estas nuevas leyes (Refworld, 2024). Esta falta de precedentes deja sin desarrollar criterios sobre transparencia, límites a la intervención estatal o protección frente a órdenes de eliminación de contenido. Observadores internacionales han advertido que una eventual orden de la ACE para suprimir publicaciones periodísticas por supuesta "inexactitud" podría carecer de contrapesos internos efectivos y escalar rápidamente hacia mecanismos regionales o universales de protección de derechos humanos (Human Rights Watch, 2024). En este escenario, los estándares interamericanos adquieren relevancia, especialmente la posición del Relator Especial para la Libertad de Expresión de la OEA, quien ha advertido que el "derecho al olvido" no debe utilizarse para restringir la difusión de información de interés público ni para inhibir el escrutinio democrático (OEA, 2019). La ausencia de control judicial independiente en el ámbito interno aumenta el riesgo de que controversias sobre censura digital, privacidad o acceso a información pública deban resolverse en instancias internacionales, debido a la falta de garantías institucionales suficientes.

Honduras: Ausencia de Marco Integral

Honduras no cuenta, hasta 2025, con una ley integral de ciberdelitos o de ciberseguridad de alcance general. El Código Penal reformado en 2017 incorpora de forma fragmentaria algunas conductas informáticas.

Proyecto de Ley 2018

El Congreso discutió la "Ley Nacional de Ciberseguridad y Medidas de Protección ante Actos de Odio y Discriminación en Internet y Redes Sociales", propuesta altamente polémica.



- **Obligaba a plataformas a retirar "contenido ilegal" en 24 horas**
- **Definiciones ambiguas permitían amplio margen para censura**
- **Duplicaba delitos existentes sin criterios claros**
- **Fue archivada tras aprobación parcial de solo 29 de 96 artículos**

Honduras no cuenta, hasta 2025, con una ley integral de ciberdelitos o de ciberseguridad de alcance general. El Código Penal —reformado en 2017 y vigente desde 2020— incorpora de forma fragmentaria algunas conductas informáticas, como el acceso indebido a sistemas, daños o fraude informático y pornografía infantil en línea, entre otras (Criterio.hn, 2019; Conexihon, 2019). En 2018, el Congreso discutió la “Ley Nacional de Ciberseguridad y Medidas de Protección ante Actos de Odio y Discriminación en Internet y Redes Sociales”, una propuesta altamente polémica que intentaba regular contenidos digitales vinculados a discursos de odio, imponiendo obligaciones a plataformas y medios. Diversos sectores señalaron que el texto era ambiguo y permitía un margen amplio para la censura, pues duplicaba delitos ya existentes —como la difamación— sin criterios claros de aplicación (Artículo 19, 2020; HRW, 2018). Expertos también advirtieron que mezclaba de forma inadecuada temas de seguridad informática con regulación de contenidos, abriendo la posibilidad de estigmatizar la crítica política como expresión de odio (OACNUDH, 2022). La iniciativa terminó archivada tras la aprobación parcial de solo 29 de sus 96 artículos (Criterio.hn, 2019).

Honduras: Criminalización y Vigilancia

El Nuevo Código Penal mantuvo la criminalización de los delitos contra el honor (arts. 2293231), ampliándolos al entorno digital y agravando las penas cuando la imputación ocurría en línea, especialmente si se dirige a funcionarios públicos.

1

Delitos contra el Honor

ARTICLE 19 sostiene que estas normas vulneran estándares interamericanos, pues el derecho penal suele usarse para intimidar periodistas.

2

Procesos Penales

En el contexto postelectoral 2017-2019 se reportaron procesos contra usuarios de redes por "instigación" o "apología", generando autocensura.

3

Tecnología Circles

Citizen Lab identificó que la Agencia de Inteligencia hondureña fue cliente de tecnología relacionada con NSO Group para interceptar comunicaciones.

Vacíos Normativos: Honduras carece de ley general de protección de datos personales. El Instituto de Acceso a la Información Pública presentó un anteproyecto, pero su discusión legislativa permanece pendiente.

Durante el gobierno de Juan Orlando Hernández, esta agenda regresiva resurgió mediante un nuevo proyecto de Ley de Ciberseguridad y Actos de Odio en Internet. El borrador obligaba a proveedores de Internet y administradores de sitios web a retirar en 24 horas cualquier “contenido ilegal”, so pena de bloqueo del portal completo, sin supervisión judicial previa. La definición de “contenido ilegal” incluía categorías amplias como “incitación al odio o discriminación que lesione la dignidad”, lo que abría espacio para censurar críticas al gobierno (HRW, 2018). Human Rights Watch alertó que la propuesta otorgaba al Estado un instrumento para silenciar voces opositoras y llamó a rechazarla. Aunque el Congreso llegó a aprobarla en primer debate, la iniciativa se congeló ante el rechazo de organizaciones civiles, gremios periodísticos y actores tecnológicos, que la denunciaron como una “ley mordaza digital” (HRW, 2018). No obstante, parte de ese enfoque persistió: el Nuevo Código Penal mantuvo la criminalización de los delitos contra el honor (arts. 229–231), ampliándolos al entorno digital y agravando las penas cuando la imputación ocurría en línea, especialmente si se dirige a funcionarios públicos o instituciones supervisadas (Artículo 19, 2020).

ARTICLE 19 y otras organizaciones han sostenido que estas normas vulneran los estándares interamericanos, pues el derecho penal suele usarse para intimidar periodistas y desalentar denuncias de corrupción.

En el contexto postelectoral de 2017-2019, también se reportaron procesos penales contra usuarios de redes sociales por delitos como "instigación" o "apología", generando un ambiente de autocensura. A ello se suma la existencia de capacidades de vigilancia estatal: Citizen Lab identificó que la Agencia de Inteligencia hondureña fue cliente de la tecnología Circles (relacionada con NSO Group), utilizada para explotar vulnerabilidades telefónicas y potencialmente interceptar comunicaciones móviles (Citizen Lab, 2020). Aunque el gobierno que asumió en 2022 prometió revisar estas prácticas, Honduras sigue enfrentando el reto de eliminar mecanismos de censura y desmantelar la infraestructura de vigilancia heredada. La continuidad de delitos penales aplicados a expresiones digitales y la falta de rendición de cuentas por el espionaje previo mantienen un entorno restrictivo para el ejercicio de derechos digitales (Artículo 19, 2020; OACNUDH, 2022).

Honduras carece igualmente de una ley general de protección de datos personales. Aunque el Instituto de Acceso a la Información Pública presentó un anteproyecto alineado con estándares internacionales, su discusión legislativa permanece pendiente (IAIP, 2022). En ausencia de un marco específico, la privacidad depende de disposiciones constitucionales y tipificaciones penales dispersas, sin una autoridad especializada ni un sistema integral de sanciones. En materia de telecomunicaciones, el Decreto 185-95 regula el sector y establece a CONATEL como autoridad competente, pero no impone obligaciones de retención de datos. La interceptación de comunicaciones está sujeta a autorización judicial conforme al Código Procesal Penal; sin embargo, durante la administración Hernández se denunciaron prácticas de vigilancia política y se aprobó una normativa de escuchas telefónicas cuya supervisión fue cuestionada (Conexihon, 2020). Tras 2022, la derogación de la "Ley de Secretos Oficiales" buscó fortalecer la transparencia estatal, con implicaciones positivas para el escrutinio público sobre adquisiciones de tecnologías de vigilancia.

Honduras tampoco es signataria del Convenio de Budapest sobre ciberdelincuencia, aunque participa en iniciativas regionales como los proyectos del SICA sobre marcos armonizados de ciberdelitos (SICA, 2023). Expertos locales recomiendan desarrollar una estrategia nacional de ciberseguridad y crear un CERT que centralice la respuesta a incidentes, además de modernizar el marco penal y aprobar una ley de protección de datos (IAIP, 2022; SICA, 2023). Pese al interés declarado del gobierno de Xiomara Castro, la agenda digital enfrenta competencia de otras prioridades nacionales en materia de seguridad ciudadana.

Los litigios sobre expresión en línea y privacidad digital siguen siendo limitados. Un caso relevante fue la declaración de inconstitucionalidad parcial de la Ley de Inteligencia y Seguridad en 2020, por vulnerar el derecho a la intimidad; sin embargo, su alcance se centró más en vigilancia política tradicional que en el entorno digital.

En 2023, periodistas presentaron un recurso de amparo contra el Decreto 57-2020, que actualizó delitos contra el honor en redes sociales; su resolución podría establecer un precedente para la protección de la libertad de expresión en línea (La Prensa, 2023). En conjunto, Honduras continúa en un proceso de construcción normativa: las recomendaciones internacionales enfatizan que cualquier nueva legislación digital debe incorporar definiciones claras y salvaguardias robustas para evitar reproducir esquemas de censura similares a los que ya han sido documentados en la región (OACNUDH, 2022; Artículo 19, 2020).

Nicaragua: Ley Especial de Ciberdelitos

Nicaragua promulgó en octubre de 2020 la Ley Especial de Ciberdelitos (Ley 1042), ampliamente conocida por críticos como la "Ley Mordaza". La normativa, cuestionada por su redacción vaga y amplio margen de interpretación, penaliza diversas conductas en línea bajo el argumento de fortalecer la seguridad digital.

Propagación de "Noticias Falsas"

Art. 30 penaliza difusión de información "falsa o tergiversada" que cause alarma, temor o zozobra", con penas hasta 5 años de prisión.

Imputaciones contra el Honor

Art. 28 criminaliza denuncias en línea que afecten la "honra" de terceros, inhibiendo investigaciones de corrupción.

Aplicación extraterritorial

"Permite perseguir a personas fuera del país por presuntos ciberdelitos que afecten a Nicaragua."

Nicaragua promulgó en octubre de 2020 la Ley Especial de Ciberdelitos (Ley 1042), ampliamente conocida por críticos como la "Ley Mordaza". La normativa, cuestionada por su redacción vaga y su amplio margen de interpretación, penaliza diversas conductas en línea bajo el argumento de fortalecer la seguridad digital. Si bien tipifica delitos informáticos tradicionales —como acceso ilícito, espionaje informático, daño o interferencia a sistemas y uso indebido de dispositivos o datos— incorpora figuras altamente controvertidas, entre ellas la "propagación de noticias falsas y/o tergiversadas" (art. 30), las "imputaciones contra el honor o el prestigio" mediante TIC (art. 28) y una amplia definición de "suplantación de identidad informática" (art. 22) (LJR, 2023; Access Now, 2021). Estas categorías ambiguas han permitido criminalizar actividades legítimas, particularmente el trabajo periodístico y la crítica política: la sanción por difundir supuestas "noticias falsas" carece de criterios verificables y ha sido utilizada para procesar a periodistas, opositores y personas que denuncian violaciones a derechos humanos (CIDH, 2020; ONU, 2021).

La ley también penaliza denuncias en línea que supuestamente afecten la “honra” de terceros, inhibiendo investigaciones de corrupción y señalamiento de abusos estatales. Adicionalmente, prohíbe la posesión de herramientas o software que potencialmente podrían utilizarse para delitos, lo que, en la práctica, criminaliza la labor de investigadores en seguridad digital, una actividad ya severamente restringida en el país (Access Now, 2021; Artículo 19, 2021). Las penas previstas oscilan entre 2 y 10 años de prisión, y la ley incorpora una cláusula de aplicación extraterritorial que permite perseguir a personas fuera del país por presuntos ciberdelitos que afecten a Nicaragua (ONU, 2021). Esta disposición ha generado inquietud entre la diáspora y periodistas exiliados, quienes han sido acusados desde el extranjero mediante esta normativa (LJR, 2023).

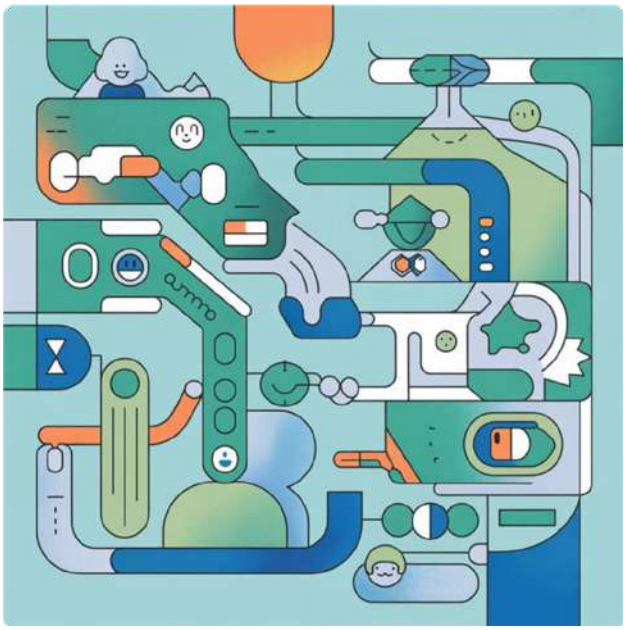
En síntesis, la Ley 1042 proporcionó al gobierno de Ortega una herramienta jurídica para profundizar el control y la persecución de la disidencia digital, complementando la represión offline que se intensificó tras las protestas de 2018 (CIDH, 2020; ONU, 2021). Desde su entrada en vigor, numerosos periodistas, activistas y opositores han sido investigados o procesados bajo cargos de ciberdelitos, generalmente relacionados con expresiones críticas en redes sociales. En septiembre de 2023, la Asamblea Nacional —dominada por el oficialismo— aprobó reformas para endurecer aún más el marco legal. Uno de los cambios más preocupantes fue la legalización explícita de la interceptación de comunicaciones digitales, autorizando a la Policía y órganos de seguridad a interceptar, grabar y reproducir mensajes, correos electrónicos y llamadas con respaldo legal (Confidencial, 2023). Con esta reforma, el régimen formalizó prácticas de vigilancia que ya ejercía de facto, otorgándoles apariencia de legalidad. Las modificaciones también reforzaron la obligación de proveedores de internet y telecomunicaciones de colaborar con las autoridades, consolidando un sistema de control casi total sobre los operadores de servicios (Access Now, 2021; Confidencial, 2023).

Nicaragua: Reformas y Control Digital

En septiembre de 2023, la Asamblea Nacional aprobó reformas para endurecer aún más el marco legal. Uno de los cambios más preocupantes fue la legalización explícita de la interceptación de comunicaciones digitales.

Interceptación Legalizada

Autoriza a la Policía y órganos de seguridad a interceptar, grabar y reproducir mensajes, correos electrónicos y llamadas con respaldo legal. Con esta reforma, el régimen formalizó prácticas de vigilancia que ya ejercía de facto.



Leyes Complementarias

- **Ley de Regulación de Agentes Extranjeros (2020)**
- **Estrategia Nacional de Ciberseguridad 20203 2025**
- **Obligación de proveedores de colaborar con autoridades**

En paralelo, se aprobaron leyes complementarias que consolidan el control estatal del espacio digital y de la sociedad civil. La Ley de Regulación de Agentes Extranjeros (2020) obliga a organizaciones, medios y personas que reciben financiamiento internacional a registrarse como "agentes extranjeros" bajo supervisión gubernamental, lo que ha estrangulado financieramente a medios independientes y ONG (Artículo 19, 2021; ONU, 2021). Ese mismo año, se adoptó por decreto la Estrategia Nacional de Ciberseguridad 2020–2025, cuyo contenido técnico, aunque aparentemente legítimo, se ha utilizado discursivamente para justificar la ampliación del marco jurídico represivo (TELCOR, 2020). En la práctica, el Estado ha integrado estas herramientas en un ecosistema de control que abarca tanto la vigilancia digital como la represión administrativa y financiera.

La infraestructura de telecomunicaciones nicaragüense está fuertemente centralizada bajo el control estatal a través de TELCOR. Aunque no existe transparencia sobre la retención de datos, múltiples informes señalan que las empresas telefónicas —algunas con vínculos directos con el gobierno— cooperan proporcionando metadatos y registros al Estado sin garantías judiciales independientes.

Desde 2018 se ha denunciado la monitorización del tráfico digital y de mensajes, presuntamente con apoyo tecnológico de gobiernos aliados. A falta de una ley específica de interceptación, estas prácticas se han sustentado en la interpretación expansiva de la Ley 1042 y en disposiciones penales complementarias. Si bien la Constitución consagra la inviolabilidad de las comunicaciones privadas (art. 26), la reforma de 2023 institucionaliza un sistema de vigilancia permanente en el que cualquier comunicación electrónica puede ser intervenida y utilizada contra voces críticas (Confidencial, 2023).

Nicaragua: Ausencia de Controles Judiciales

Debido a la falta de independencia judicial, en Nicaragua no existe jurisprudencia que limite la aplicación de la Ley de Ciberdelitos. Los tribunales han aplicado la ley sin controles, emitiendo condenas por publicaciones en redes sociales.

Tribunales Sin Independencia

Aplican la ley sin controles, emitiendo condenas por "noticias falsas" o "incitación al odio".

Condena Internacional

CIDH y ONU señalan que esta legislación viola estándares de libertad de expresión.

Caso Emblemático

Nicaragua se ha convertido en ejemplo regional de cómo las leyes de ciberdelitos pueden suprimir derechos en regímenes autoritarios.

Sin Recursos Internos

La salida de Nicaragua del sistema interamericano limita gravemente las vías de protección.

Debido a la falta de independencia judicial, en Nicaragua no existe jurisprudencia que limite la aplicación de la Ley de Ciberdelitos. Los tribunales han aplicado la ley sin controles, emitiendo condenas por publicaciones en redes sociales calificadas como “noticias falsas” o “incitación al odio”. En el ámbito internacional, la CIDH y la ONU han señalado que esta legislación viola estándares de libertad de expresión por sus definiciones vagas y su potencial para criminalizar la crítica legítima (CIDH, 2020; ONU, 2021). Organizaciones como Access Now y Artículo 19 han documentado sus riesgos y exhortado a su derogación (Access Now, 2021; Artículo 19, 2021). Hasta ahora, el Estado no ha mostrado intención de revisar la norma; en cambio, ha profundizado su aplicación. La ausencia de recursos judiciales internos y la salida de Nicaragua del sistema interamericano limitan gravemente las vías de protección disponibles para la ciudadanía. El país se ha convertido en un caso emblemático regional sobre cómo las legislaciones de ciberdelitos pueden emplearse para suprimir derechos digitales en regímenes autoritarios (Access Now, 2021; CIDH, 2020).

Costa Rica: Marco Pionero de Protección

Costa Rica fue pionera en la región al promulgar la Ley N.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales en 2011, un marco inspirado en modelos europeos que reconoce el derecho a la autodeterminación informativa.

PRODHAB
La ley crea la Agencia de Protección de Datos de los Habitantes, estableciendo principios de consentimiento, finalidad, proporcionalidad y seguridad.

Código Penal
Ley 9048 de 2012 tipificó delitos informáticos. En 2015, la Sala Constitucional declaró inconstitucional el delito de espionaje político.

Convenio de Budapest
Costa Rica es parte desde 2017 y en 2023 ratificó el Segundo Protocolo Adicional sobre cooperación internacional.

Costa Rica fue pionera en la región al promulgar la Ley N.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales en 2011, un marco inspirado en modelos europeos que reconoce el derecho a la autodeterminación informativa (PRODHAB, 2011). La ley establece principios de tratamiento —consentimiento, finalidad, proporcionalidad, seguridad—, crea la Agencia de Protección de Datos de los Habitantes (PRODHAB) y contempla sanciones administrativas para quienes vulneren datos sin autorización. Este marco consolidó los derechos ARCO y fortaleció una cultura sólida de protección de datos. Reglamentos de la SUTEL complementan estas garantías en el sector de telecomunicaciones (SUTEL, 2014; 2016).

Sin embargo, como señala una activista feminista entrevistada, la fortaleza normativa no siempre se traduce en protección efectiva para mujeres, activistas y periodistas. Aunque Costa Rica suele presentarse como un país seguro en términos digitales, en la práctica el entorno virtual se ha vuelto particularmente hostil para mujeres en política, defensoras y comunicadoras, quienes enfrentan violencia digital sistemática —especialmente durante procesos electorales— así como discursos misóginos y campañas de odio altamente organizadas (Entrevista Activista CR, 2025). Esta realidad convive con el robusto marco legal, evidenciando una brecha entre la norma y su aplicación.

En materia penal, el país incorporó los delitos informáticos al Código Penal mediante la Ley 9048 de 2012, que tipificó el acceso indebido, el sabotaje informático y el espionaje digital. Algunos artículos, sin embargo, generaron alarma por su potencial impacto en la libertad de prensa, en particular el artículo 288 sobre "informaciones secretas políticas" y el artículo 196 bis sobre difusión de datos personales, incluso cuando fueran de carácter público. Periodistas y organizaciones advirtieron que estas normas podían inhibir el periodismo de investigación y bloquear filtraciones sobre corrupción (IPLEX, 2014; Colper, 2015). En 2015, la Sala Constitucional declaró inconstitucional el delito de espionaje político y suprimió la penalización sobre la difusión de datos públicos por vulnerar la libertad de expresión y el derecho de acceso a la información (Sala Constitucional, 2015). Este fallo alineó el marco nacional con estándares internacionales y protegió de forma decisiva el ejercicio periodístico.

En términos institucionales, Costa Rica ha desarrollado una Estrategia Nacional de Ciberseguridad 2017–2021 y se encuentra elaborando la estrategia 2023–2027, enfocada en fortalecer capacidades, respuesta a incidentes y cultura digital (MICITT, 2017; 2023). Cuenta con un CERT nacional (CSIRT-CR) para la gestión de incidentes. Sin embargo, según la activista entrevistada, la respuesta estatal a los ciberataques de alto impacto ha sido fragmentaria: se han ofrecido capacitaciones individuales, pero no se ha materializado una modernización integral de la infraestructura ni políticas estables de fortalecimiento institucional (Entrevista Activista CR, 2025). Incluso se ha reducido la virtualidad de algunos trámites, afectando el acceso ciudadano y profundizando problemas burocráticos ya existentes.

Costa Rica también es parte del Convenio de Budapest desde 2017 y, en 2023, ratificó el Segundo Protocolo Adicional, que facilita la cooperación internacional en evidencia digital. La aprobación suscitó debate, especialmente desde sectores que alertaron sobre riesgos a la privacidad y posibles mecanismos de vigilancia transfronteriza (FA, 2023). Aun así, su aprobación compromete al país a armonizar su legislación interna con nuevos estándares procesales.

Costa Rica: Desafíos Actuales

Como señala una activista feminista entrevistada, la fortaleza normativa no siempre se traduce en protección efectiva para mujeres, activistas y periodistas. Aunque Costa Rica suele presentarse como un país seguro en términos digitales, en la práctica el entorno virtual se ha vuelto particularmente hostil.

"Costa Rica mantiene uno de los marcos más avanzados de la región en derechos digitales, pero enfrenta retos crecientes: violencia digital sistémica, polarización incentivada desde el poder político y brechas de acceso entre zonas urbanas y rurales."

Violencia Digital
Mujeres en política y defensoras enfrentan violencia digital sistemática durante procesos electorales.

Discursos de Odio
Discursos antinmigrantes desde cuentas oficiales contribuyen a clima hostil que se traduce en agresiones físicas.

Brecha Digital
Diferencias significativas en acceso y alfabetización digital entre zonas urbanas y rurales.

El análisis de la entrevista realizada a una activista feminista costaricense también muestra que la violencia digital tiene impactos fuera de internet. Discursos estigmatizantes —particularmente antimigrantes— emitidos desde cuentas oficiales y reproducidos en redes contribuyen a un clima hostil que se traduce en marchas, agresiones y estigmatización de personas migrantes en la vida cotidiana (Entrevista Activista CR2025). Esto demuestra que las vulneraciones digitales tienen efectos materiales y profundizan desigualdades. Asimismo, líderes ambientales, defensoras indígenas y periodistas han enfrentado amenazas y acoso, incluidas denuncias administrativas que producen miedo y autocensura, mientras el Estado carece de políticas efectivas para frenar estas violencias.

Costa Rica: Protección de la Privacidad

La protección de la privacidad en comunicaciones ha sido un pilar histórico del sistema costarricense. La Ley 7425 de 1994 exige orden judicial para cualquier interceptación y tipifica como delito la escucha ilegal. Asimismo, obliga a los operadores a custodiar datos de usuarios y entregarlos sólo mediante orden judicial. No existe un régimen de retención obligatoria masiva. Este principio se puso a prueba en 2025 cuando el Ministerio de Hacienda solicitó a las operadoras entregar mensualmente datos completos de millones de usuarios. La solicitud generó rechazo del sector privado y derivó en varios recursos de amparo ante la Sala Constitucional, que admitió al menos uno de ellos, reafirmando el peso jurídico de la protección de datos (Sala IV, 2025; CRHoy, 2025).

Salvaguardas Judiciales

Obliga a los operadores a custodiar datos de usuarios y entregarlos sólo mediante orden judicial. No existe régimen de retención obligatoria masiva.

Caso 2025

El Ministerio de Hacienda solicitó a operadoras entregar mensualmente datos completos de millones de usuarios. La solicitud generó rechazo y derivó en recursos de amparo ante la Sala Constitucional.

Jurisprudencia Protectora

La Sala Constitucional ha protegido la crítica en redes sociales, incluyendo fallos que prohíben a autoridades bloquear usuarios en cuentas oficiales.

Costa Rica discute actualmente el Proyecto de Ley 21.187 sobre ciberdelincuencia, orientado a armonizar el Código Penal con estándares internacionales sin repetir las controversias de la Ley 9048 (Asamblea Legislativa, 2019). También se evalúan iniciativas de gobierno digital y seguridad para el sector público. En este contexto, los desafíos democráticos resaltados en la entrevista —como la necesidad de proyectos políticos comprometidos con instituciones sólidas, la urgencia fiscal y la polarización digital— se alinean con las exigencias del entorno digital contemporáneo.

La activista enfatizó que el discurso agresivo desde liderazgos políticos —incluido el presidente Rodrigo Chaves— ha deteriorado la libertad de prensa, dinamizado la presencia de bots y amplificado la polarización, afectando directamente a periodistas, funcionarias y activistas (Entrevista Activista CR2025).

En conjunto, Costa Rica mantiene uno de los marcos más avanzados de la región en derechos digitales, pero enfrenta retos crecientes: violencia digital sistémica, polarización incentivada desde el poder político, tensiones institucionales en la implementación de la identidad digital, brechas de acceso entre zonas urbanas y rurales y desafíos en ciberseguridad. Según la activista entrevistada, avanzar hacia una protección real de derechos digitales exige fortalecer políticas públicas integrales, modernizar la infraestructura, reforzar la alfabetización digital y promover un clima democrático que desincentive la violencia y los discursos de odio en entornos digitales.

Panamá: Modernización Legislativa 2025

Panamá actualizó de manera integral su legislación penal en materia de ciberdelitos con la promulgación de la **Ley 478 de 2025**, publicada el 5 de agosto de ese año, mediante la cual reformó su Código Penal para incorporar nuevos delitos informáticos (Asamblea Nacional de Panamá, 2025a; Ministerio Público de Panamá, 2025). Hasta entonces, el Código Penal contemplaba únicamente figuras básicas como el acceso indebido y el sabotaje informático, insuficientes frente a la evolución del ecosistema digital (Asamblea Nacional de Panamá, 2008; Sucre, 2025).

La Ley 478 llenó ese vacío normativo y tipificó, entre otros, los siguientes delitos:

Acceso ilícito a sistemas informáticos,
penalizando la intrusión no autorizada aun sin causar daño (Asamblea Nacional de Panamá, 2025a).

Manipulación no autorizada de datos o sistemas,
incluyendo conductas como malware, ransomware y sabotaje digital (Ministerio Público de Panamá, 2025).

Suplantación de identidad digital,
relativa al uso indebido de credenciales o datos personales con fines ilícitos (Asamblea Nacional de Panamá, 2025a).

Difusión no autorizada de datos personales,
castigando la divulgación de información sensible sin consentimiento (ANTAI, 2025).

Ataques contra infraestructura crítica,
penalizando interferencias que afecten servicios esenciales (Ministerio Público de Panamá, 2025).

Estas reformas buscan alinear al país con estándares internacionales y cerrar brechas que anteriormente dejaban múltiples conductas impunes (Sucre, 2025; ANTAI, 2024). Las sanciones varían desde penas moderadas hasta sanciones más severas —como 5 a 10 años para sabotajes agravados—. El sector tecnológico y jurídico recibió la reforma de forma positiva por su capacidad para modernizar el marco penal (Sucre, 2025).

Panamá: Protección de Datos y Vigilancia

En materia de privacidad, Panamá adoptó la **Ley 81 de 2019 de Protección de Datos Personales**, vigente desde marzo de 2021 (ANTAI, 2021). Esta normativa reconoce los derechos ARCO, exige consentimiento para el tratamiento de datos y establece principios de seguridad, confidencialidad y finalidad. Su aplicación corresponde a la Autoridad Nacional de Transparencia y Acceso a la Información, que reguló su implementación mediante el Decreto Ejecutivo 285/2021 (ANTAI, 2021). La Ley 478 de 2025 complementa la Ley 81 al tipificar penalmente la divulgación no autorizada de datos personales (Asamblea Nacional de Panamá, 2025a), reforzando la protección frente a filtraciones dolosas.

Régimen de Retención

La Ley 51 de 2009 obliga a operadores e ISP a conservar por seis meses determinados datos de tráfico y suscriptores para investigaciones criminales, con posibilidad de prórroga mediante orden judicial.

Control Judicial

El Código Procesal Penal establece que toda interceptación debe contar con autorización judicial. La Corte Suprema ha intervenido para equilibrar seguridad y privacidad.

Antecedentes de Vigilancia: El caso de los "pinchazos telefónicos" durante el gobierno de Ricardo Martinelli (200932014) reveló una estructura clandestina de interceptación sin orden judicial, incluyendo uso de Pegasus desde 2012.

Panamá cuenta también con un régimen de **retención de datos de telecomunicaciones**. La **Ley 51 de 2009** obliga a operadores e ISP a conservar por seis meses determinados datos de tráfico y suscriptores —como direcciones IP, historial de llamadas y ubicación de celdas móviles— para investigaciones criminales, con posibilidad de prórroga mediante orden judicial (Asamblea Nacional de Panamá, 2009). Asimismo, se exige el registro de usuarios de tarjetas SIM prepago (Autoridad Nacional de los Servicios Públicos, 2015). En materia de intervención de comunicaciones, el Código Procesal Penal establece que toda interceptación debe contar con autorización judicial y es ejecutada por unidades especializadas del Ministerio Público (Ministerio Público de Panamá, 2020). Aunque no se han documentado abusos sistemáticos recientes, organizaciones civiles han cuestionado la falta de transparencia en investigaciones de alto perfil (De León, 2021).

La Corte Suprema de Justicia ha intervenido en diversas ocasiones para equilibrar seguridad y privacidad. En 2015, declaró inconstitucional un artículo de la Ley 51-2009 que permitía el acceso a datos de comunicaciones sin orden judicial (Corte Suprema de Justicia de Panamá, 2015). En 2020 evaluó facultades de vigilancia contenidas en legislación antiterrorista, confirmándolas al considerar adecuados sus límites (Corte Suprema de Justicia de Panamá, 2020). Aunque la Ley 81 no ha sido sometida a control constitucional, sí se han presentado múltiples habeas data ordenando la corrección o eliminación de datos personales manejados incorrectamente por entidades públicas, incluida una sentencia de 2022 que obligó a eliminar antecedentes policiales tras un sobreseimiento (Sala Tercera, 2022).

En materia de derechos digitales, aunque Panamá no experimentó entre 2018 y 2025 una persecución sistemática contra la prensa digital comparable a la de otros países de la región, persisten secuelas de graves episodios de vigilancia estatal. El caso más emblemático es el de los **"pinchazos telefónicos"** ocurridos durante el gobierno de Ricardo Martinelli (2009–2014). Durante los juicios de 2019 y 2021, la Fiscalía presentó pruebas de que operó una estructura clandestina en el Consejo de Seguridad Nacional dedicada a interceptar comunicaciones de opositores, periodistas, empresarios y sindicalistas sin orden judicial (AP News, 2021). Peritajes forenses confirmaron el uso de al menos dos sistemas de espionaje, incluido **Pegasus**, situando a Panamá entre los primeros países donde este software fue utilizado, desde 2012 (AP News, 2021). Aunque Martinelli fue absuelto por falta de evidencia que acreditara su orden directa, el caso reveló vulnerabilidades en la protección de la privacidad y la ausencia de controles institucionales robustos.

En conjunto, Panamá muestra avances significativos en 2025 gracias a la modernización de su legislación penal digital y la consolidación de su régimen de protección de datos personales. Sin embargo, persisten retos en su implementación práctica, la capacitación técnica de fiscales y jueces, y la prevención de la repetición de episodios de vigilancia ilegal que marcaron la década anterior (De León, 2021; ANTAI, 2024).

Vigilancia y criminalización en línea en Centroamérica: uso (y abuso) de marcos de cibercrimen, datos personales y telecomunicaciones.

Los marcos normativos de ciberdelitos, protección de datos personales y telecomunicaciones en Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica y Panamá han sido utilizados —o pueden serlo— para monitorear y criminalizar la actividad en línea. Con especial énfasis en el uso de tipologías penales vagas, competencias de interceptación y regímenes de retención/entrega de datos, así como en la existencia (o ausencia) de salvaguardas judiciales e institucionales.

La región muestra tres patrones: (i) modelos punitivos y de vigilancia con bajos controles (Nicaragua, y en parte El Salvador); (ii) marcos en transición con vacíos y riesgos de proyectos ambiguos (Guatemala, Honduras); y (iii) esquemas con salvaguardas judiciales e institucionales robustas (Costa Rica, Panamá), lo cual se ilustra a continuación:

País	Marco legal clave	Facultades de vigilancia /retención	Uso para criminalizar discurso	Salvaguardas /contrapesos	Nivel de riesgo
Nicaragua	Ley Especial de Ciberdelitos (Ley 1042, 2020) y reformas; Ley de Telecomunicaciones Convergentes; Estrategia Nacional de Ciberseguridad.	Intercepción amplia (mensajes, llamadas, correos) con control estatal; cooperación forzosa de telcor; posible monitoreo sistemático de tráfico.	Delitos por 'noticias falsas' y 'daño al honor' aplicados a críticas; procesos contra periodistas y opositores; extraterritorialidad.	Poder judicial no independiente; escaso control constitucional efectivo.	Alto
El Salvador	Ley de Ciberseguridad y Seguridad de la Información (2024); Ley de Protección de Datos (2024); Ley Especial contra Delitos Informáticos (2016, reformada 2025).	ACE centraliza regulación; posibles órdenes de eliminación de contenidos (derecho al olvido); interceptación con orden; antecedentes de spyware (Pegasus).	Riesgo de remoción de contenidos periodísticos por 'inexactitud' de datos; persecución de fraudes y filtraciones con impacto en prensa.	Medios y sociedad civil activos; control judicial formal, pero regulador no independiente.	Alto
Guatemala	Archivo del Decreto 39-2022 (ciberdelincuencia); marco penal general y ley de telecomunicaciones; sin ley integral de datos.	Intercepción con orden judicial en delitos graves; sin retención general obligatoria conocida.	Intento fallido de 'ley mordaza digital'; hoy riesgo medio por vacíos y herramientas puntuales.	Corte de Constitucionalidad activa; amparo y hábeas data; prensa y OSC vigilantes.	Medio

País	Marco legal clave	Facultades de vigilancia /retención	Uso para criminalizar discurso	Salvaguardas /contrapesos	Nivel de riesgo
Honduras	Proyecto de Ley de Ciberseguridad (2019) detuvo su avance; sin ley de datos ni ciberseguridad integral.	Intercepción con orden judicial; antecedentes de escuchas con bajo control; sin CERT nacional consolidado.	Riesgo por proyectos que regulan 'odio' con ambigüedad; uso de figuras penales comunes para perseguir críticas.	Rechazo social a iniciativas ambiguas; reformas de transparencia desde 2022.	Medio
Costa Rica	Ley 8968 (datos personales, 2011); Código Penal reformado (Ley 9048, 2012) modulado por Sala Constitucional; adhesión a Budapest y 2° Protocolo.	Intercepción solo con orden; rechazo a solicitudes masivas de datos por Hacienda (2025).	La Sala anuló 'secretos políticos' y limitó la criminalización de datos públicos; protección a la prensa.	PRODHAB, Sala Constitucional, cultura de privacidad; cooperación internacional con salvaguardas.	Bajo
Panamá	Ley 81 (datos personales, 2019); Ley 51 (retención de datos telco, 2009); Ley 478 (ciberdelitos, 2025).	Retención obligatoria (6 meses) de ciertos metadatos; acceso con orden judicial; interceptación en delitos graves.	En general focalizado en delitos técnicos; riesgo moderado si retención se usa sin controles.	Control judicial y precedentes sobre acceso; ANTAI supervisa datos personales.	Medio

Vigilancia digital y restricciones a la libertad de expresión en Centroamérica (2018–2025).

Entre 2018 y 2025, el espacio cívico digital en Centroamérica se ha convertido en un terreno clave de disputa entre gobiernos, prensa independiente y sociedad civil. Lejos de ser únicamente un entorno de innovación tecnológica, el ámbito digital ha sido utilizado por distintos regímenes para vigilar, desacreditar y castigar a voces críticas mediante una combinación de espionaje con spyware sofisticado, campañas coordinadas de troles, reformas penales regresivas y procesos judiciales selectivos. En este contexto, periodistas, defensores de derechos humanos y activistas han pasado de ver internet como una herramienta de ampliación de derechos a experimentarlo también como un campo de riesgo, donde cada publicación puede convertirse en un potencial detonante de hostigamiento, criminalización o exilio (Access Now, 2022; Human Rights Watch, 2022; Freedom House, 2023).

Los casos de Guatemala, El Salvador, Nicaragua, Honduras, Costa Rica y Panamá muestran patrones comunes, pero también diferencias importantes en la intensidad y sofisticación de la represión digital. En algunos países se han documentado operaciones de vigilancia con herramientas como Pegasus y Circles dirigidas contra periodistas y opositores, acompañadas de intentos de aprobar o aplicar leyes "mordaza" que penalizan la expresión en línea bajo figuras vagas como "odio", "apología" o "noticias falsas". En otros, aunque persisten marcos legales más garantistas, han emergido prácticas preocupantes de hostigamiento en redes, discursos estigmatizantes desde el poder y uso instrumental de delitos contra el honor para presionar a medios críticos. Este acápite examina comparativamente estos procesos, mostrando cómo la combinación de tecnología, legislación y narrativas oficiales puede erosionar los derechos digitales en la región y reconfigurar los límites de la libertad de expresión en internet (CPJ, 2022; RSF, 2023; Freedom House, 2024).

Guatemala

En Guatemala, la erosión de los derechos digitales se evidenció en casos graves de espionaje y hostigamiento contra la prensa.

En Guatemala, la erosión de los derechos digitales y de la libertad de expresión se evidenció en casos graves de espionaje y hostigamiento contra la prensa. En 2018 se documentó que la Dirección General de Inteligencia Civil (DIGICI) adquirió herramientas de espionaje israelí, entre ellas el software Pegasus de NSO Group y la plataforma Circles, que habrían sido utilizadas para vigilar ilegalmente a periodistas, empresarios y opositores políticos (Citizen Lab, 2018). Estos hechos se produjeron en un contexto de crecientes ataques contra la sociedad civil: organizaciones internacionales registraron más de 900 agresiones contra activistas y periodistas entre 2017 y 2018, atribuibles tanto a actores estatales como no estatales (Citizen Lab, 2018). En 2022, el Congreso aprobó de manera acelerada la Ley de Prevención y Protección contra la Ciberdelincuencia (Decreto 39-2022), que creaba nuevos delitos informáticos; sin embargo, artículos redactados de forma ambigua fueron señalados por expertos y organizaciones como un intento de instalar una "ley mordaza" digital, susceptible de usarse para castigar la crítica en redes sociales (Plaza Pública, 2022). Ante la presión pública, la norma fue archivada pocas semanas después de su aprobación (Plaza Pública, 2022).

Paralelamente, el gobierno intensificó la persecución del periodismo independiente. En 2022, el periodista José Rubén Zamora, director de elPeriódico, fue detenido bajo cargos de lavado de dinero que observadores internacionales han calificado como represalia por sus investigaciones sobre corrupción (The Washington Post, 2022). Entre 2018 y 2025, Guatemala registró un uso combinado de espionaje estatal, procesos judiciales selectivos e intentos legislativos de censura, al tiempo que funcionarios y aliados políticos promovían campañas de troles digitales (netcenters) y hostigamiento en línea contra periodistas y disidentes (Human Rights Watch, 2022; Reporteros Sin Fronteras [RSF], 2023; Freedom House, 2023). Estas prácticas han deteriorado el espacio cívico en línea y forzado a numerosos comunicadores a autocensurarse o exiliarse por razones de seguridad (Freedom House, 2023).

Restricciones 2018-2025: El Salvador

En El Salvador, bajo la presidencia de Nayib Bukele (2019–presente), se consolidó un patrón de espionaje digital, hostigamiento en línea y uso de marcos legales punitivos contra la prensa independiente. Investigaciones técnicas de Citizen Lab, Access Now y Amnistía Internacional revelaron que, entre 2020 y 2021, al menos 35 periodistas y activistas salvadoreños fueron infectados con el spyware Pegasus, en uno de los casos más persistentes de uso de esta herramienta en el mundo (Access Now, 2022). Entre las víctimas hubo miembros de medios como El Faro y Gato Encerrado, cuyos teléfonos fueron reinfectados repetidamente (Access Now, 2022). Aunque el gobierno negó su participación, NSO Group afirmó que solo vende Pegasus a Estados, y los hallazgos técnicos sugieren que el operador de la campaña estaba ubicado dentro del país (El Faro, 2022; Access Now, 2022).

Reformas Penales 2022

La Asamblea aprobó reformas que penalizan con 10-15 años la difusión de mensajes de pandillas, medida denunciada como "censura antipandillas".

Campañas de Troles

El propio Bukele y altos funcionarios calificaron públicamente a periodistas críticos como "mercenarios", incitando a seguidores a lanzar amenazas y campañas de difamación.

Exilio Masivo

Al menos 40 periodistas salvadoreños se exiliaron entre 2020 y 2023 por temor a la cárcel, resultado del entorno hostil de espionaje, acoso y leyes restrictivas.

Al espionaje se sumaron campañas sistemáticas de troles, doxxing y discursos estigmatizantes desde cuentas oficiales. El propio Bukele y altos funcionarios calificaron públicamente a periodistas críticos como "mercenarios" o supuestos aliados de pandillas, incitando a seguidores en redes a lanzar amenazas y campañas de difamación contra ellos (The Washington Post, 2022). En abril de 2022, la Asamblea Legislativa aprobó reformas al Código Penal que penalizan con 10 a 15 años de prisión la difusión de mensajes, comunicados o declaraciones de pandillas en cualquier medio, medida denunciada por el Comité para la Protección de los Periodistas (CPJ) como legislación de "censura antipandillas" que obstaculiza la cobertura informativa del fenómeno criminal (CPJ, 2022). Como resultado de este entorno hostil —espionaje, acoso digital organizado y leyes restrictivas—, al menos 40 periodistas salvadoreños se exiliaron entre 2020 y 2023 por temor a la cárcel (The Washington Post, 2022). El caso salvadoreño muestra cómo un gobierno popular puede combinar vigilancia digital, propaganda en redes y normas penales regresivas para debilitar gravemente los derechos digitales y la libertad de expresión (Access Now, 2022; CPJ, 2022).

Vigilancia Digital y Restricciones 2018-2025:

Nicaragua

En Nicaragua, el régimen de Daniel Ortega y Rosario Murillo desplegó probablemente la ofensiva más sistemática contra la libertad de expresión en Centroamérica, trasladando la represión al ámbito digital tras las protestas de 2018. En octubre de 2020, la Asamblea Nacional aprobó la **Ley Especial de Ciberdelitos**, conocida como "Ley Mordaza" digital, que penaliza la difusión de información considerada "falsa o tergiversada" en medios electrónicos cuando genere "alarma, temor o zozobra" en la población (Freedom House, 2024). Organizaciones como Access Now señalaron que el texto se basa en conceptos vagos que permiten criminalizar la difusión de información y castigar voces críticas bajo la etiqueta de "noticias falsas", trasladando al entorno digital patrones de represión ya presentes en el espacio físico (Pisanu & Rodríguez, 2020). Paralelamente, el gobierno aprobó una Política Nacional de Ciberseguridad que obliga a plataformas y redes sociales a cooperar con las autoridades y otorga amplias facultades de monitoreo de comunicaciones privadas (Freedom House, 2024).

Política de Ciberseguridad

Obliga a plataformas y redes sociales a cooperar con autoridades y otorga amplias facultades de monitoreo de comunicaciones privadas.

100+

Medios Cerrados

Medios digitales independientes forzados al exilio o clausurados desde 2018.

8

Años de Prisión

Sentencia al periodista Víctor Ticay por transmitir en Facebook Live una procesión religiosa.

2018

Inicio Represión

Año que marca el inicio de la ofensiva sistemática contra libertad de expresión digital.

La combinación de leyes punitivas y operaciones encubiertas dio lugar a un ecosistema de control digital que incluye granjas de troles financiadas con recursos públicos, campañas de difamación contra opositores y uso de tecnologías de espionaje con apoyo de aliados externos (Freedom House, 2024). Periodistas y activistas han sufrido amenazas, hackeos, detenciones y condenas por su actividad en línea; un caso emblemático es el del periodista Víctor Ticay, sentenciado en 2023 a ocho años de prisión por transmitir en Facebook Live una procesión religiosa no autorizada (Freedom House, 2024). La mayoría de medios digitales independientes —como Confidencial, 100% Noticias o Despacho 505— se han visto forzados al exilio, y quienes permanecen en el país trabajan de forma anónima o clandestina (Freedom House, 2024; Human Rights Watch, 2022). Entre 2018 y 2025, Nicaragua institucionalizó la vigilancia masiva y la censura en Internet, convirtiéndose en un caso extremo de uso de marcos legales y herramientas digitales para suprimir derechos fundamentales en el entorno virtual (Human Rights Watch, 2022; Freedom House, 2024).

Vigilancia Digital y Restricciones 2018-2025:

Honduras

En Honduras, la libertad de expresión digital se vio amenazada por iniciativas legales regresivas y por la continuidad de mecanismos de vigilancia heredados de gobiernos anteriores. En 2018, durante la administración de Juan Orlando Hernández, el Congreso discutió una **Ley de Ciberseguridad y Medidas de Protección ante Actos de Odio y Discriminación en Internet y Redes Sociales**. El proyecto obligaba a proveedores de Internet y administradores de sitios web a retirar en 24 horas cualquier "contenido ilegal", so pena del bloqueo total de los portales (Human Rights Watch, 2018). La categoría de contenido ilegal incluía nociones ambiguas como la "incitación al odio o discriminación que lesione la dignidad", sin requerir supervisión judicial previa, lo que habría permitido censurar discrecionalmente críticas al gobierno (Human Rights Watch, 2018). Ante las fuertes críticas de sociedad civil, gremios periodísticos y empresas tecnológicas, el proyecto fue finalmente congelado, pero quedó señalado como un intento de "ley mordaza digital" (Human Rights Watch, 2018).

Proyecto de Ley 2018

Obligaba a proveedores a retirar "contenido ilegal" en 24 horas sin supervisión judicial. Fue congelado tras críticas.

Código Penal 2020

Mantuvo delitos de injuria y calumnia para medios digitales, con penas agravadas cuando se difunden por internet.

Tecnología Circles

Informes revelan que inteligencia hondureña fue cliente de tecnología para explotar vulnerabilidades telefónicas.

Desafío Pendiente: Aunque el gobierno que asumió en 2022 prometió revisar estas prácticas, Honduras sigue enfrentando el reto de desmontar la infraestructura de vigilancia encubierta y reformar la legislación que criminaliza la expresión.

Pese a ello, el **Nuevo Código Penal**, vigente desde 2020, mantuvo y actualizó los delitos de injuria y calumnia para abarcar publicaciones en medios digitales, con penas agravadas cuando las expresiones se difunden por internet o redes sociales (ARTICLE 19, 2020). Estas disposiciones han sido cuestionadas por contravenir estándares interamericanos, ya que las leyes penales de difamación suelen emplearse para intimidar a periodistas y frenar denuncias de corrupción; diversas organizaciones han recomendado que los conflictos de honor se tramiten solo en la vía civil (ARTICLE 19, 2020). Informes técnicos también revelan que la inteligencia hondureña habría sido cliente de la tecnología Circles, vinculada a NSO Group, lo que le permitiría explotar vulnerabilidades de redes móviles e interceptar comunicaciones (Citizen Lab, 2020). Aunque el gobierno que asumió en 2022 prometió revisar estas normas y prácticas, hacia 2025 Honduras sigue enfrentando el reto de desmontar la infraestructura de vigilancia encubierta y reformar la legislación que criminaliza la expresión, en un contexto donde periodistas y activistas se ven obligados a extremar medidas de seguridad digital para protegerse (ARTICLE 19, 2020; OACNUDH, 2022).

Vigilancia Digital y Restricciones 2018-2025:

Costa Rica

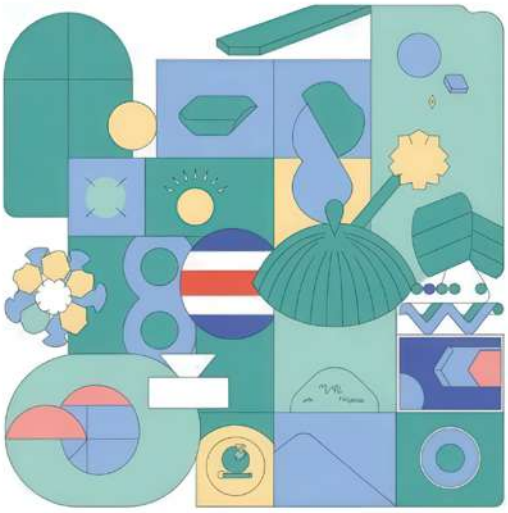
En Costa Rica, país con una larga tradición democrática, también surgieron preocupaciones en torno a la privacidad digital y el clima hacia la prensa, aunque en una escala menor que la de sus vecinos.

Caso UPAD (2020)

La Unidad Presidencial de Análisis de Datos podía acceder a datos confidenciales de instituciones públicas, generando acusaciones de posible espionaje. El decreto fue rápidamente derogado tras investigación fiscal.

Gobierno Chaves (2022-presente)

Se registró aumento en ataques verbales y hostilidad hacia medios críticos. IPLEX documentó incremento de discursos estigmatizantes desde funcionarios públicos contra periodistas.



Uno de los episodios más controvertidos fue la creación de la **Unidad Presidencial de Análisis de Datos (UPAD)** durante el gobierno de Carlos Alvarado. En febrero de 2020 se reveló que, mediante decreto, la UPAD podía acceder a datos confidenciales de distintas instituciones públicas para elaborar análisis estadísticos, lo que generó acusaciones de posible espionaje y uso indebido de información personal (Swissinfo, 2020). La Fiscalía allanó la Casa Presidencial y confiscó dispositivos electrónicos, incluido el teléfono del presidente, para investigar si se violó la privacidad de los ciudadanos (Swissinfo, 2020). Aunque el decreto fue rápidamente derogado y el gobierno negó que se hubiera realizado vigilancia masiva, el caso evidenció los riesgos de estructuras de análisis de datos sin controles suficientes y permanece bajo investigación al cierre de 2025 (Swissinfo, 2020).

A partir de 2022, con la llegada a la presidencia de Rodrigo Chaves, se registró un aumento en los ataques verbales y la hostilidad hacia medios críticos. El Instituto de Prensa y Libertad de Expresión (IPLEX) documentó en 2023 un incremento significativo de discursos estigmatizantes desde funcionarios públicos contra periodistas, lo que se tradujo en campañas de acoso en redes sociales y en restricciones de acceso a información (IPLEX, 2023).

Freedom House ha advertido que estos patrones de hostigamiento digital, algunos vinculados a cuentas cercanas al gobierno, comienzan a erosionar la sólida reputación de Costa Rica en materia de libertad de prensa (Freedom House, 2023). Aunque el país no ha aprobado leyes "mordaza" ni registra periodistas encarcelados, la combinación de agresiones discursivas, acoso en línea y presiones desde el poder ha generado episodios de autocensura y preocupación en el gremio (IPLEX, 2023). Al mismo tiempo, Costa Rica sigue siendo un país de refugio para periodistas exiliados de contextos más represivos, lo que refuerza la necesidad de proteger su ecosistema de derechos digitales y libertad de expresión.

Vigilancia Digital y Restricciones 2018-2025:

Panamá

En Panamá, si bien entre 2018 y 2025 no se observó un ataque sistemático contra la prensa digital comparable al de otros países de la región, persisten las consecuencias de graves escándalos de vigilancia estatal y marcos legales que pueden tener un efecto inhibidor sobre la libertad de expresión.

Caso "Pinchazos" (200C-2014)
Unidad clandestina del Consejo de Seguridad Nacional interceptó sin orden judicial comunicaciones de opositores, sindicalistas, empresarios y periodistas.

Software Pegasus
Peritajes confirmaron uso de al menos dos sistemas de espionaje, incluido Pegasus desde 2012, situando a Panamá entre los primeros países usuarios.

Juicios 201C-2021
Aunque Martinelli fue absuelto por falta de pruebas directas, el caso dejó en evidencia vulnerabilidad de derechos digitales.

Delitos contra el Honor
El Código Penal mantiene tipificación de injuria y calumnia, usados frecuentemente por figuras de poder para demandar a periodistas.

El caso más emblemático es el de los **"pinchazos telefónicos"** durante la presidencia de Ricardo Martinelli (2009–2014). En los juicios celebrados en 2019 y 2021, la Fiscalía presentó pruebas de que una unidad clandestina del Consejo de Seguridad Nacional interceptó sin orden judicial las comunicaciones de decenas de personas —entre ellas opositores, sindicalistas, empresarios y periodistas— utilizando al menos dos sistemas de espionaje, incluido el software Pegasus (AP News, 2021).

Estos hallazgos sitúan a Panamá entre los primeros países donde se empleó Pegasus, desde alrededor de 2012, mucho antes de que su uso se volviera ampliamente conocido (AP News, 2021). Aunque Martinelli fue finalmente absuelto en el segundo juicio por falta de pruebas directas de su orden, el caso dejó en evidencia la vulnerabilidad de los derechos digitales y la falta de rendición de cuentas frente a estas violaciones (AP News, 2021).

En el plano normativo, Panamá conserva un entorno de prensa relativamente libre, pero su Código Penal aún tipifica delitos contra el honor —injuria y calumnia— que son utilizados con frecuencia por figuras de poder para presentar demandas contra periodistas (Índice Chapultepec, 2021). Organizaciones locales han denunciado que estos procesos, junto con medidas como el embargo preventivo de bienes o cuentas de medios de comunicación, generan un efecto intimidante y fomentan la autocensura, especialmente cuando los querellantes son exmandatarios o altos funcionarios (Índice Chapultepec, 2021). Además, se han identificado dificultades persistentes en el acceso a la información pública, intensificadas durante la pandemia de COVID-19, lo que ha limitado la fiscalización periodística de contrataciones y gastos de emergencia (Índice Chapultepec, 2021). Aunque el país no ha adoptado nuevas leyes de censura digital ni se han producido exilios masivos de periodistas, organismos internacionales lo califican como "parcialmente libre" y advierten que la ausencia de censura directa convive con amenazas más sutiles, como la judicialización del ejercicio periodístico y la impunidad en casos de espionaje (Índice Chapultepec, 2021). La experiencia panameña subraya la necesidad de reformar las leyes penales sobre expresión y fortalecer los controles democráticos para prevenir la vigilancia ilícita y asegurar la plena vigencia de los derechos digitales.

Casos Emblemáticos de violaciones a Derechos Digitales en la Región:

En los últimos años defensores de derechos humanos, activistas y periodistas independientes han enfrentado graves represalias por su labor, a esto se suma una tendencia que hemos venido describiendo a lo largo de este informe a continuación destacaremos casos que reflejan las diferentes modalidades en las que no solamente se violan los derechos digitales, sino se instrumentaliza la tecnología y los estándares legales vinculados para ejercer estas violaciones.

Caso Emblemático: Proyecto Torogoz: uso de Pegasus en El Salvador

En El Salvador, el llamado Proyecto Torogoz reveló una de las campañas de espionaje digital más graves de la región. Entre 2020 y 2021, decenas de teléfonos de periodistas y personas defensoras de derechos humanos fueron infectados con el spyware Pegasus, desarrollado por la empresa israelí NSO Group (Citizen Lab, 2022).

> Los análisis técnico-forenses mostraron el uso de exploits de "clic cero" en dispositivos iOS, lo que permitía la infección sin que la persona usuaria realizara acción alguna, y otorgaba control remoto casi total sobre sus teléfonos: acceso a micrófono, cámara, mensajes, ubicación y otros datos sensibles (Citizen Lab, 2022).

Víctimas Identificadas

Trabajadores de medios críticos como El Faro y organizaciones de sociedad civil. El patrón apunta a operación de vigilancia política vinculada al Estado.

Derechos Afectados

Privacidad, libertad de expresión y seguridad personal. Generó fuerte efecto de autocensura entre las personas vigiladas.

Respuesta Estatal

No se ha conocido base legal transparente ni investigaciones estatales eficaces para esclarecer responsabilidades.

El patrón de víctimas —trabajadores de medios críticos como El Faro y organizaciones de sociedad civil—, junto con el hecho de que Pegasus sólo se comercializa con gobiernos, apunta a una operación de vigilancia política muy probablemente vinculada al Estado salvadoreño. Esta campaña afectó directamente derechos como la privacidad, la libertad de expresión y la seguridad personal, generando un fuerte efecto de autocensura entre las personas vigiladas (Access Now & Amnesty International, 2022).

Pese a la gravedad del caso, no se ha conocido una base legal transparente que justifique estas intervenciones, ni investigaciones estatales eficaces para esclarecer responsabilidades. Las revelaciones de Citizen Lab y de organizaciones aliadas motivaron denuncias públicas y llamados urgentes de la comunidad internacional para que se rindan cuentas y se respete la privacidad de periodistas y activistas salvadoreños (Citizen Lab, 2022; Amnesty International, 2022). En la práctica, el uso de un software de uso militar como Pegasus para vigilar a la prensa constituye una forma extrema de agresión digital que socava el periodismo de investigación y deteriora el espacio cívico en línea.

Caso Emblemático: Bloqueo del dominio .com.ni a medios independientes en Nicaragua

En marzo de 2025, el régimen de Daniel Ortega y Rosario Murillo trasladó un paso más la censura al entorno digital al ordenar el bloqueo del dominio de nivel superior .com.ni para varios medios independientes.

Medios Afectados

- **La Prensa**
- **Confidencial**
- **100% Noticias**
- **Otros sitios críticos**

Sitios comerciales con el mismo sufijo continuaron operando normalmente, evidenciando la selectividad de la medida.

Respuesta de Medios: Ante el bloqueo, los medios afectados migraron a dominios alternativos (.com, .org) y reforzaron su presencia en redes sociales; sin embargo, reportaron pérdidas de tráfico y menor visibilidad dentro del país.

Según reportes de prensa, la Universidad Nacional de Ingeniería (UNI) —administradora del registro .ni— recibió órdenes para suspender los dominios .com.ni de al menos cinco medios críticos, entre ellos La Prensa, Confidencial y 100% Noticias, mientras que otros sitios comerciales con el mismo sufijo continuaron operando con normalidad (El País, 2025; Confidencial, 2025). Esta medida selectiva afectó derechos fundamentales como la libertad de expresión, el acceso a la información y la participación política, al impedir a la ciudadanía nicaragüense acceder a las versiones locales de medios clave para el control democrático.

El bloqueo se enmarca en un contexto de legislación represiva —como la Ley Especial de Ciberdelitos y la Ley de Agentes Extranjeros— utilizada para cerrar medios, organizaciones y perseguir voces críticas (Access Now, 2020; Freedom House, 2024). La Relatoría Especial para la Libertad de Expresión de la CIDH calificó la medida como un ejemplo de censura digital estructural y exigió su reversión (CIDH, 2025). Ante el bloqueo, los medios afectados migraron a dominios alternativos (.com, .org) y reforzaron su presencia en redes sociales; sin embargo, reportaron pérdidas de tráfico y una menor visibilidad dentro del país, profundizando el "apagón informativo" que ya venía configurándose con el cierre físico de redacciones y el exilio de periodistas (Confidencial, 2025; RSF, 2025).

Caso Emblemático: Ataques de ransomware Conti contra el gobierno de Costa Rica

En 2022, Costa Rica sufrió una de las mayores crisis de ciberseguridad de su historia cuando el grupo de ciberdelincuencia Conti lanzó un masivo ataque de ransomware contra instituciones públicas.

1

Primer Ataque (Abril 2022)

Comprometió los sistemas del Ministerio de Hacienda, afectando declaración de impuestos y control de aduanas.

2

Segundo Ataque

Atribuido a Conti y posteriormente a Hive, amplió el impacto a cerca de 30 entidades gubernamentales.

3

Consecuencias

Cifraron grandes volúmenes de datos, robaron información sensible y amenazaron con filtrarla. Paralización parcial del comercio exterior durante semanas.

4

Respuesta Nacional

Declaración de emergencia nacional en ciberseguridad, apoyo de países aliados y empresas tecnológicas especializadas.

El primer ataque, en abril de 2022, comprometió los sistemas del Ministerio de Hacienda; un segundo ataque, atribuido a Conti y posteriormente a Hive, amplió el impacto a cerca de 30 entidades, afectando sistemas de declaración de impuestos, control de aduanas y otros servicios esenciales (Wikipedia, 2023; Cyber Law Toolkit, 2023). Los atacantes cifraron grandes volúmenes de datos, robaron información sensible y amenazaron con filtrarla si el Estado no pagaba un rescate, lo que provocó la paralización parcial del comercio exterior y la prestación de servicios públicos durante semanas. Aunque el ataque fue perpetrado por actores criminales y no por un Estado, sus efectos se tradujeron en violaciones indirectas de derechos: limitaciones al acceso a servicios públicos, riesgos para la protección de datos personales y daños económicos significativos para la población (PurpleSec, 2023).

La gravedad del incidente llevó al gobierno costarricense a declarar un estado de emergencia nacional en ciberseguridad, solicitar apoyo de países aliados como Estados Unidos, España e Israel y recurrir a empresas tecnológicas especializadas para contener el ataque y restaurar sistemas (Wikipedia, 2023). El caso impulsó un intenso debate interno sobre la fragilidad de las infraestructuras críticas y la necesidad de fortalecer políticas, capacidades técnicas y marcos legales para la ciberseguridad. Además, mostró cómo, aun sin intención política directa, ataques técnicos de gran escala pueden afectar de manera masiva derechos digitales y servicios esenciales de la ciudadanía, subrayando la importancia de un enfoque de derechos humanos en la gestión de incidentes cibernéticos (Cyber Law Toolkit, 2023; PurpleSec, 2023).

Caso Emblemático: Netcenters contra periodistas y operadores de justicia en Guatemala

En Guatemala, los llamados netcenters se han consolidado como una herramienta clave de ataque digital contra periodistas de investigación y operadores de justicia vinculados a la lucha anticorrupción. Desde al menos 2018, diversas investigaciones han documentado redes de cuentas falsas y bots en X/Twitter y Facebook dedicadas a difamar, hostigar y desacreditar a fiscales, jueces y periodistas que colaboraron con la CICIG o que han investigado al llamado "pacto de corruptos" (Vance Center, 2021; Committee to Protect Journalists [CPJ], 2022). Estas campañas coordinadas difunden mensajes de odio, teorías conspirativas y acusaciones falsas para erosionar la credibilidad de sus víctimas, afectando su reputación, su seguridad y su capacidad de ejercer la libertad de expresión sin temor.

Desde al menos 2018, diversas investigaciones han documentado redes de cuentas falsas y bots en X/Twitter y Facebook dedicadas a difamar, hostigar y desacreditar a fiscales, jueces y periodistas que colaboraron con la CICIG.

Características de los Ataques

- Campañas coordinadas con mensajes de odio
- Teorías conspirativas y acusaciones falsas
- Erosión de credibilidad de las víctimas
- Afectación de reputación y seguridad

Aunque formalmente son operadas por actores no estatales, diversos informes señalan vínculos de estas redes con élites políticas y económicas, así como indicios de financiamiento organizado para sostener su operación (CPJ, 2022; Departamento de Estado de EE. UU., 2022). El hostigamiento digital suele ir acompañado de procesos penales espurios y amenazas offline, lo que eleva el riesgo para las personas atacadas y las empuja al exilio o a la autocensura. La respuesta institucional ha sido limitada o inexistente: en algunos casos, el propio Ministerio Público ha sido parte del problema, al perseguir a las víctimas en lugar de investigar a quienes coordinan estas campañas (CIDH, 2023). Organismos internacionales han señalado que los netcenters forman parte de una estrategia más amplia para garantizar impunidad en casos de corrupción y debilitar el Estado de derecho mediante la intimidación de quienes lo desafían (Vance Center, 2021; CPJ, 2022).

Caso Emblemático: #malqueridas: violencia digital de género contra mujeres periodistas

La campaña #malqueridas se ha convertido en un símbolo de la violencia digital misógina utilizada para silenciar a mujeres periodistas en Centroamérica, con especial énfasis en El Salvador.

> "Entre 2020 y 2022, una serie de ataques coordinados en redes sociales empleó el hashtag #malqueridas para hostigar a comunicadoras con insultos sexistas, alusiones sexuales y amenazas de violencia, incluidas amenazas de violación."

> "Además de mensajes agresivos, se difundieron imágenes manipuladas y contenidos destinados a ridiculizarlas y cuestionar su credibilidad profesional, configurando una forma de violencia de género que se superpone a la censura política."

Esta violencia digital con sesgo de género afecta derechos como la integridad y la seguridad personal, el derecho a vivir libres de violencia, la igualdad y la libertad de expresión. Muchas de las periodistas afectadas ya enfrentaban otros riesgos por su trabajo de investigación o se encontraban en el exilio.

Respuesta Institucional: Pese a las denuncias de organizaciones de libertad de prensa y de derechos de las mujeres, la respuesta estatal ha sido débil: no se han llevado a cabo investigaciones exhaustivas ni sanciones ejemplares contra los agresores.

Como resultado, muchas periodistas se ven obligadas a autocensurarse, abandonar espacios digitales o replegar su presencia pública, lo que empobrece el debate democrático y refuerza la exclusión de las mujeres de los espacios de decisión e incidencia.

Entre 2020 y 2022, una serie de ataques coordinados en redes sociales empleó el hashtag #malqueridas para hostigar a comunicadoras con insultos sexistas, alusiones sexuales y amenazas de violencia, incluidas amenazas de violación (LatAm Journalism Review, 2022). Además de mensajes agresivos, se difundieron imágenes manipuladas y contenidos destinados a ridiculizarlas y cuestionar su credibilidad profesional, configurando una forma de violencia de género que se superpone a la censura política. Muchas de las periodistas afectadas ya enfrentaban otros riesgos por su trabajo de investigación o se encontraban en el exilio debido a persecución en sus países de origen, lo que demuestra que el hostigamiento se extiende más allá de las fronteras físicas (LatAm Journalism Review, 2022).

Caso Emblemático: "Sicarios de la verdad": campaña de difamación y doxxing contra nueve periodistas hondureños (2025)

En el contexto altamente polarizado previo a las elecciones generales de 2025, Honduras registró una de las campañas de difamación y doxxing más agresivas contra la prensa nacional. La madrugada del 31 de julio de 2025 aparecieron en distintos puntos de Tegucigalpa mantas y carteles de gran tamaño con los nombres, fotografías y afiliaciones profesionales de nueve periodistas reconocidos, acompañados del mensaje: "Sicarios de la verdad, armas de desinformación masiva, no quieren que se realicen elecciones" (SIP, 2025a). Los afiches, firmados por un supuesto "Movimiento Popular Hondureño", presentaban a los comunicadores como enemigos del proceso electoral, criminalizando su labor informativa. Entre los señalados figuraban directores de medios, propietarios de canales y líderes gremiales, entre ellos Juan Carlos Sierra —presidente del Colegio de Periodistas de Honduras—, Dagoberto Rodríguez —director de Radio Cadena Voces— y Renato Álvarez —director de Noticieros TN5—, todos ellos figuras ampliamente reconocidas en el ámbito mediático (SIP, 2025a).

Los Hechos

La madrugada del 31 de julio de 2025 aparecieron en Tegucigalpa mantas y carteles de gran tamaño con nombres, fotografías y afiliaciones profesionales de nueve periodistas reconocidos.

El mensaje: "Sicarios de la verdad, armas de desinformación masiva, no quieren que se realicen elecciones".

Periodistas Señalados

- Juan Carlos Sierra (Presidente Colegio de Periodistas)
- Dagoberto Rodríguez (Director Radio Cadena Voces)
- Renato Álvarez (Director Noticieros TN5)
- Otros directores de medios y líderes gremiales

La Sociedad Interamericana de Prensa condenó la acción como una grave forma de intimidación, advirtiendo que la estigmatización pública de periodistas en un clima electoral tenso puede derivar en agresiones físicas o atentados contra su vida (SIP, 2025b). Además, organizaciones regionales señalaron que estas campañas de odio exacerban la polarización política, erosionan la confianza en la prensa y buscan inducir autocensura justo antes de los comicios (SIP, 2025c). Aunque no se ha identificado de manera oficial a los responsables, el caso evidencia el empleo de tácticas de amenaza colectiva —incluyendo la exhibición pública de datos personales— para amedrentar a voces críticas y deslegitimar el periodismo independiente en momentos clave del ciclo democrático.

Caso Emblemático: Criterio.hn: vigilancia, ataques digitales y presión política contra un medio independiente (2023–2025)

Entre 2023 y 2025, el medio investigativo Criterio.hn y su equipo periodístico enfrentaron una escalada de agresiones que refleja la creciente hostilidad contra la prensa independiente en Honduras.

Amenazas de Muerte

Documentadas por Red Centroamericana de Periodistas y Artículo 19.

Intentos de Hackeo

Ciberataques dirigidos contra reporteros y editores del portal.

Vigilancia

Presuntos episodios de seguimiento físico y digital contra miembros de la redacción.

Campañas de Desprestigio

Difusión coordinada de información falsa para desacreditar al medio.

La Red Centroamericana de Periodistas y Artículo 19 documentaron amenazas de muerte, intentos de hackeo, ciberataques, campañas de desprestigio y presuntos episodios de vigilancia física y digital dirigidos contra reporteros y editores del portal (LatAm Journalism Review, 2024). Las agresiones se intensificaron en paralelo a la publicación de investigaciones sensibles sobre corrupción gubernamental, abusos de poder y posibles violaciones a derechos humanos. Además, miembros de la redacción denunciaron la presencia de vehículos sospechosos, seguimientos y actos de intimidación presuntamente vinculados a cuerpos de seguridad, lo cual generó un clima de riesgo permanente (LatAm Journalism Review, 2024).

La presión no se limitó al ámbito digital. Criterio.hn fue incluido entre los al menos doce medios demandados penalmente por altos funcionarios hondureños en 2025, incluido el jefe de las Fuerzas Armadas, quien presentó querellas por difamación tras la publicación de reportajes sobre presunta corrupción castrense (CPJ, 2025). Estas acciones judiciales se suman a un patrón más amplio de criminalización mediante leyes de difamación penal, usado para intimidar a medios críticos y erosionar la labor periodística. Aunque Criterio.hn continúa operando, sus periodistas trabajan bajo condiciones de vigilancia, hostilidad y autocensura inducida. Organizaciones internacionales como CPJ y Artículo 19 han advertido que este caso no es aislado, sino representativo de un ambiente estructural de violencia y presión política contra la prensa hondureña en el período 2023–2025 (CPJ, 2025; LatAm Journalism Review, 2024).

Caso Emblemático: Acoso y vigilancia digital a periodistas nicaragüenses exiliados ("brazo largo" de la represión) (2021–2024)

Desde 2018, la represión del régimen de Daniel Ortega y Rosario Murillo no se ha limitado al territorio nicaragüense: se ha extendido fuera de las fronteras mediante un patrón de vigilancia, acoso digital y hostigamiento transnacional contra periodistas en el exilio.

Periodistas en el Exilio

Informes de FLED, Voces del Sur y RSF documentan que periodistas desplazados a Costa Rica y Estados Unidos continúan recibiendo:

- Amenazas directas
- Ataques coordinados en redes
- Monitoreo sistemático de programas
- Vigilancia física en países de acogida

Represión Transnacional

Las tácticas forman parte de un mecanismo mediante el cual gobiernos autoritarios intentan silenciar voces críticas más allá de sus fronteras.

Las campañas buscan desacreditar, inducir autocensura y debilitar la continuidad de su labor periodística desde el exterior.

Falta de Protección: A pesar de las denuncias internacionales, no existen aún mecanismos de protección sólidos que frenen estas agresiones. La experiencia nicaragüense muestra cómo el espacio digital se convierte en una extensión de la persecución estatal.

Las tácticas utilizadas forman parte de lo que especialistas denominan "represión transnacional": un mecanismo mediante el cual gobiernos autoritarios intentan silenciar a voces críticas más allá de sus fronteras. Las campañas de insultos, doxxing, amenazas y desinformación contra periodistas exiliados buscan desacreditarlos, inducir autocensura y debilitar la continuidad de su labor periodística desde el exterior (Colectivo DD.HH. Nicaragua, 2024). A pesar de las denuncias internacionales, no existen aún mecanismos de protección sólidos que frenen estas agresiones. La experiencia nicaragüense muestra cómo el espacio digital se convierte en una extensión de la persecución estatal, afectando derechos fundamentales como la libertad de expresión, la privacidad, la integridad personal y la libre circulación.

Caso Emblemático: Ataques DDoS y sabotaje digital contra medios en coyunturas políticas (Guatemala y Costa Rica, 2020–2024)

Entre 2020 y 2024 se registró un aumento significativo de ataques DDoS y sabotajes digitales contra medios centroamericanos, especialmente en momentos de alta tensión política o tras la publicación de investigaciones sensibles.

Guatemala - Prensa Comunitaria

Medios como Prensa Comunitaria han denunciado caídas súbitas de sitios web, eliminación de contenidos y ataques de saturación coordinados tras reportajes sobre corrupción.

Costa Rica - Millones de Intentos

Datos recientes muestran que el país ha recibido miles de millones de intentos de ataques DDoS en un solo año, afectando medios y servicios públicos.

Atribución Compleja

Aunque la atribución suele ser difícil, el patrón evidencia uso creciente de herramientas técnicas para silenciar voces críticas en momentos electorales.

Impunidad Tecnológica

La ausencia de investigaciones concluyentes y la impunidad permiten que estos ataques continúen, debilitando el ecosistema digital.

Caso Emblemático: Hackeo y destrucción de archivos digitales de elPeriódico (Guatemala, 2013–2023)

El diario guatemalteco elPeriódico, uno de los medios más influyentes en investigaciones sobre corrupción, fue blanco de ataques digitales desde al menos 2013.

2013

Ciberataque elimina una década completa de archivo digital (20033 2013), borrando reportajes clave sobre casos de alto impacto político.

2018

Nuevo ataque deja fuera de servicio el sitio web. La SIP condena el incidente como ataque a la libertad de prensa.

2022

Detención de José Rubén Zamora bajo cargos cuestionados internacionalmente. Inicio de asfixia económica y legal.

Mayo 2023

elPeriódico cierra definitivamente tras 27 años de operación. Su legado pasa a ser preservado desde el exilio mediante CAIMA.

La ofensiva estatal se intensificó entre 2022 y 2023, culminando en la detención de su fundador, José Rubén Zamora, bajo cargos ampliamente cuestionados por organizaciones internacionales (RSF, 2024). En mayo de 2023, asfixiado por procesos legales, pérdida de anunciantes y un clima de intimidación, elPeriódico cerró definitivamente tras 27 años de operación. Su legado pasó a ser preservado desde el exilio mediante iniciativas como el Archivo Independiente de Medios de Centroamérica (CAIMA), impulsado por GIJN. La historia de elPeriódico muestra cómo los ciberataques pueden ser el primer paso de un proceso escalado de represión, donde la destrucción digital se combina con estrategias legales y políticas para extinguir medios críticos.

Caso Emblemático: Uso de spyware tipo Hacking Team en Centroamérica (Honduras y Panamá, 2011–2016)

Las filtraciones globales de 2015 sobre Hacking Team revelaron que gobiernos de Honduras y Panamá estaban entre los compradores del software de vigilancia Remote Control System (RCS), una herramienta capaz de tomar control total de dispositivos, monitorear comunicaciones y extraer archivos sin conocimiento del usuario (Derechos Digitales, 2016).

Honduras

Documentos muestran que la Dirección Nacional de Investigación e Inteligencia adquirió RCS en 2014, en un contexto marcado por denuncias de espionaje político y falta de controles judiciales.

Panamá

El software fue comprado directamente en 2011 bajo la administración de Ricardo Martinelli, generando un escándalo que incluyó acusaciones de vigilancia ilegal contra opositores, periodistas y líderes empresariales.

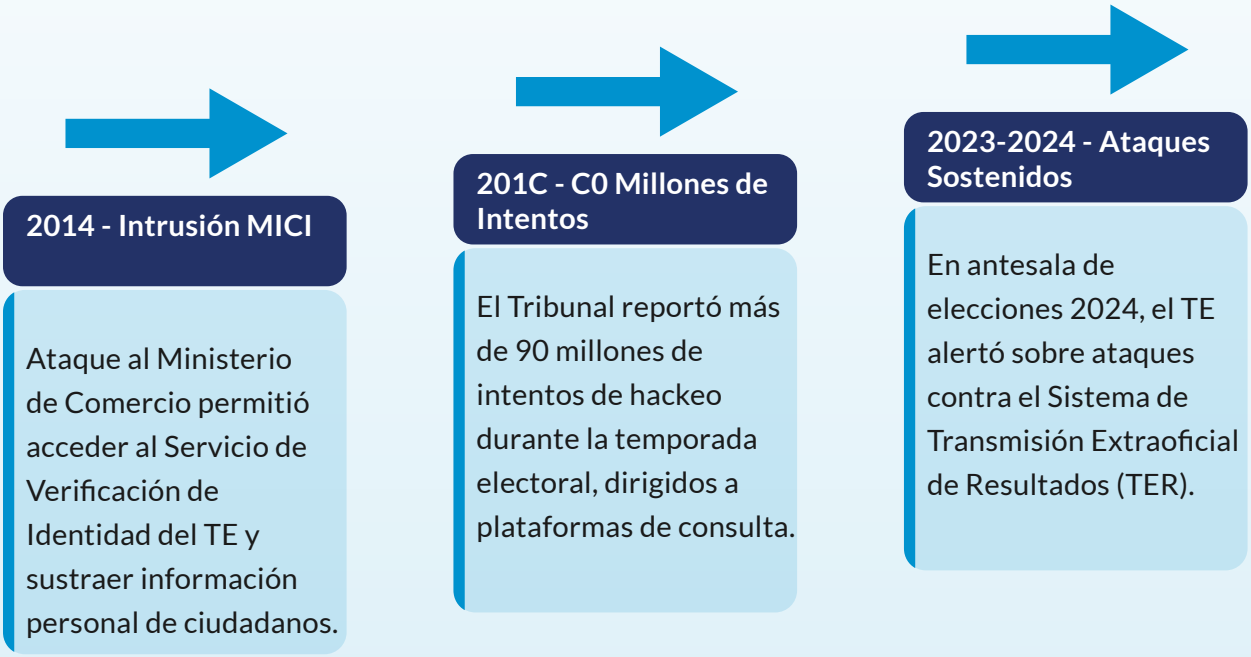
Legado Persistente: La falta de transparencia y ausencia de sanciones en su uso alimentan un ecosistema donde nuevas tecnologías 4como Pegasus o Circles4 pueden adoptarse sin controles efectivos.

En Panamá, el software fue comprado directamente en 2011 bajo la administración de Ricardo Martinelli, generando un escándalo que incluyó acusaciones de vigilancia ilegal contra opositores, periodistas y líderes empresariales (VICE, 2016).

Aunque muchos de estos contratos datan de la década anterior, su impacto perdura, pues marcaron la entrada de Centroamérica en un mercado global de vigilancia intrusiva sin mecanismos democráticos de supervisión. Las herramientas adquiridas permiten vulnerar derechos fundamentales como la privacidad, el debido proceso y la libertad de expresión. Además, la falta de transparencia y ausencia de sanciones en su uso alimentan un ecosistema donde nuevas tecnologías —como Pegasus o Circles— pueden adoptarse sin controles efectivos. Estos casos siguen siendo clave para comprender el actual panorama de espionaje digital en la región.

Caso Emblemático: Ataques e intrusiones al Tribunal Electoral de Panamá (2014–2023)

Desde 2014, el Tribunal Electoral (TE) de Panamá ha sido objeto de una serie de ataques informáticos dirigidos a obtener datos sensibles o a interferir con la infraestructura electoral.



El incidente más significativo ocurrió en 2014, cuando una intrusión al Ministerio de Comercio e Industrias (MICI) permitió a atacantes acceder al Servicio de Verificación de Identidad (SVI) del TE y sustraer información personal de ciudadanos panameños (Crítica, 2014). Aunque el TE aseguró que no se alteraron datos del padrón, la filtración generó preocupación nacional sobre la vulnerabilidad de los sistemas interconectados entre instituciones. Este patrón se repitió en procesos electorales posteriores: en 2019, el Tribunal reportó más de 90 millones de intentos de hackeo durante la temporada electoral, dirigidos a sus plataformas de consulta y verificación ciudadana (La Estrella de Panamá, 2019). Estas agresiones revelan una presión constante sobre el ecosistema electoral panameño, donde actores no identificados buscan tanto información de identidad como posibles vectores para desestabilizar la confianza pública.

En la antesala de las elecciones generales de 2024, el TE volvió a alertar sobre ataques sostenidos contra el Sistema de Transmisión Extraoficial de Resultados (TER) y otros servicios digitales, reiterando que las agresiones tecnológicas contra la institución son “permanentes” y se intensifican en períodos electorales (TVN Noticias, 2023).

Aunque no se han registrado manipulaciones exitosas de resultados, la recurrencia de intentos de intrusión —sumada a la limitada información pública sobre investigaciones o sanciones a responsables— mantiene abiertas las inquietudes sobre la resiliencia del sistema electoral panameño y la protección de los datos de votantes. Como respuesta, el Tribunal ha reforzado progresivamente sus protocolos de ciberseguridad, implementado auditorías y comunicado a la ciudadanía medidas de blindaje tecnológico. No obstante, los episodios reflejan que la infraestructura electoral de Panamá sigue siendo un objetivo atractivo para actores con motivaciones políticas o criminales.

Fuentes APA (2025): Crítica. (2014). Sustracción de datos del TE fue por ataque de 'hackers' al MICI. critica.com.pa.

La Estrella de Panamá. (2019). Tribunal Electoral recibió 90 millones de intentos de hackeo. laestrella.com.pa.

TVN Noticias. (2023). ¿Ataques informáticos al Tribunal Electoral?. tvn-2.com.

Caso Emblemático: Ciberataques y ransomware contra la Caja del Seguro Social (CSS) de Panamá (2017–2023)

La Caja del Seguro Social (CSS), una de las instituciones más grandes y críticas del Estado panameño, ha enfrentado múltiples incidentes de ciberseguridad que han afectado servicios médicos, administrativos y financieros.

WannaCry 2017

Durante la ola global del ransomware WannaCry, la CSS reportó intentos de infección que obligaron a suspender temporalmente sistemas informáticos y activar protocolos de contingencia.

El episodio expuso la fragilidad de infraestructuras hospitalarias dependientes de software desactualizado.

Ataque IFX Networks 2022

El ataque a IFX Networks 4proveedor regional de servicios tecnológicos4 afectó parcialmente sistemas dependientes de la CSS y otras entidades estatales.

Se tradujeron en retrasos administrativos, fallas en plataformas de citas y riesgos para la confidencialidad de datos de asegurados.

Aunque no se confirmó una filtración masiva, la recurrencia de ataques subraya la necesidad de fortalecer la infraestructura de seguridad de la CSS, especialmente considerando su rol en la gestión de historiales médicos y bases de datos laborales.

Fuentes APA (2025): Metro Libre. (2017). CSS activa protocolos ante amenazas de WannaCry. metrolibre.com.

Metro Libre. (2023). Impacto del ataque a IFX Networks en servicios de la CSS. metrolibre.com.

Casos Emblemáticos: Tabla comparativa de casos de agresiones digitales en Centroamérica (2013–2025)

Caso	País / Región	Años	Derechos afectados	Actor responsable	Severidad
1. Proyecto Torogoz – Pegasus	El Salvador	2020–2021 (revelado en 2022)	Privacidad, libertad de expresión, seguridad personal	Estado salvadoreño (probable)	Grave
2. Bloqueo del dominio .com.ni a medios	Nicaragua	2025	Libertad de expresión, acceso a la información	Gobierno de Nicaragua / UNI	Grave
3. Ransomware Conti a instituciones públicas	Costa Rica	2022	Acceso a servicios públicos, protección de datos, propiedad	Grupo criminal Conti / Hive	Grave
4. Netcenters contra periodistas y justicia	Guatemala	2018–2023	Libertad de expresión, seguridad, honor y reputación	Actores políticos y económicos (no estatales, coordinados)	Moderado Grave
5. #malqueridas – violencia digital de género	Centroamérica (énfasis en El Salvador)	2020–2022	Integridad personal, libertad de expresión, no discriminación	Trolls, redes coordinadas (posible tolerancia estatal)	Grave
6. “Sicarios de la verdad” – doxxing a periodistas	Honduras	2025	Libertad de expresión, seguridad personal	Grupo desconocido (“Movimiento Popular Hondureño”)	Grave

Caso	País / Región	Años	Derechos afectados	Actor responsable	Severidad
7. Criterio.hn – vigilancia y criminalización	Honduras	2023–2025	Libertad de expresión, privacidad, seguridad	Actores estatales y paraestatales	Grave
8. Acoso y vigilancia digital transnacional	Nicaragua (origen) - Costa Rica, EE.UU.	2021–2024	Libertad de expresión, privacidad, integridad personal	Estado nicaragüense y redes afines	Grave
9. Ataques DDoS a medios (Prensa Comunitaria, CR medios)	Guatemala / Costa Rica	2020–2024	Libertad de expresión, acceso a información	Actores no identificados (posible motivación política)	Moderado Grave
10. Hackeo histórico y sabotaje a elPeriódico	Guatemala	2013, 2018 (hostigamiento hasta 2023)	Libertad de expresión, acceso a archivos históricos	Autores desconocidos + persecución estatal posterior	Grave
11. Ataques al Tribunal Electoral de Panamá	Panamá	2014–2023	Derecho al voto, protección de datos, integridad electoral	Hackers no identificados (motivación política probable)	Moderado Grave
12. Ciberataques					

Una conversación pendiente: Uso y Regulación de Datos Biométricos en Centroamérica, análisis Comparado.

La recopilación y tratamiento de datos biométricos en Centroamérica presenta un panorama heterogéneo marcado por vacíos normativos, marcos de protección de datos incompletos y creciente utilización de estas tecnologías para fines de seguridad, control migratorio y administración pública. A pesar de que la mayoría de países consideran los datos biométricos como datos sensibles, las legislaciones existentes no ofrecen salvaguardas suficientes frente a los riesgos de vigilancia, uso excesivo, transferencias transfronterizas y discriminación algorítmica (ACCESO, 2024; IPANDETEC, 2023). Debemos de recordar que las regulaciones sobre uso de datos biométricos son intrínsecas a los derechos ARCO, los cuales constituyen conjunto de garantías legales que tienen las personas sobre sus datos personales. El acrónimo ARCO corresponde a las iniciales de cada uno de estos derechos: Acceso, Rectificación, Cancelación y Oposición. Estos derechos permiten a los individuos mantener el control sobre quién y cómo utiliza su información personal.

Costa Rica
Marco más robusto pero insuficiente. Proyecto de repositorio nacional biométrico g e n e r a preocupaciones.

Panamá
Ley 81 clasifica biometría como dato sensible. Sin regulación sectorial específica sobre tecnologías biométricas.

Triángulo Norte
Guatemala, El Salvador y Honduras mantienen acuerdos de cooperación biométrica sin garantías adecuadas.

Nicaragua
Vacíos normativos profundos en contexto de vigilancia estatal intensiva y represión digital.

Riesgos Regionales en Datos Biométricos

A pesar de que la mayoría de los países consideran los datos biométricos como datos sensibles, las legislaciones existentes no ofrecen salvaguardas suficientes frente a los riesgos de vigilancia, uso excesivo, transferencias transfronterizas y discriminación algorítmica.

Vacíos Normativos

Permiten recolección y tratamiento indiscriminado de datos biométricos sin regulación específica.

Cooperación Internacional

Acuerdos de intercambio biométrico sin garantías de proporcionalidad ni protección de derechos.

Reconocimiento Facial

Ausencia de evaluaciones de impacto en tecnologías de reconocimiento facial y vigilancia automatizada.

Vigilancia Estatal

Riesgos especialmente graves en contextos autoritarios donde la biometría puede usarse para persecución política.

Falta de Transparencia

Sobre interoperabilidad entre bases de datos y posibles usos secundarios sin consentimiento.

Poblaciones Vulnerables

Amenazas específicas a pueblos indígenas y grupos marginados sin consulta ni protección especial.

1. Costa Rica: El marco más robusto, pero todavía insuficiente.

Costa Rica cuenta con la **Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales**, la cual prohíbe el tratamiento de datos sensibles sin consentimiento explícito o una base legal específica (Piedra Alegría, 2023; SciELO, 2019). Los datos biométricos se encuentran bajo esta categoría, y su tratamiento debe regirse por principios de proporcionalidad, seguridad y finalidad legítima.

No obstante, la regulación existente es insuficiente frente a los usos modernos de la biometría. Estudios recientes evidencian preocupaciones en torno a:

- El proyecto de repositorio nacional biométrico (Proyecto de Ley 21.321), que plantea una base única de huellas, rostros y firmas.
- La posibilidad de acceso institucional amplio, e incluso comercialización de datos biométricos.
- Riesgos de function creep y ausencia de evaluaciones de impacto.
- Falta de salvaguardas para pueblos indígenas y poblaciones vulnerables bajo estándares de Soberanía de Datos Indígenas (Piedra Alegría, 2023).

2. Guatemala, El Salvador y Honduras (Triángulo Norte): cooperación biométrica sin garantías adecuadas.

Los países del Triángulo Norte mantienen acuerdos de cooperación biométrica orientados a la seguridad y la lucha contra el crimen organizado (Infodefensa, 2023). Sin embargo, la ausencia de leyes integrales de protección de datos genera riesgos significativos.

Guatemala

El **RENAP** recopila huellas dactilares, rasgos faciales y firmas para emitir el DPI, amparado en normativa interna y procedimientos administrativos (RENAP, 2018). Pero **no existe una ley general de protección de datos personales**, lo que deja sin regulación aspectos críticos como:

- Interoperabilidad con otras bases de datos.
- Transferencias internacionales de información biométrica.
- Derechos de oposición, consentimiento o minimización.

El Salvador

La **Ley de Acceso a la Información Pública** regula parcialmente datos personales en entidades estatales, pero **no incluye obligaciones para el sector privado**, que usa biometría en bancos, centros comerciales y sistemas de vigilancia. La expansión gubernamental de tecnologías de reconocimiento facial no está acompañada por un régimen de protección adecuado (ACCESO, 2024).

Honduras

El país ha firmado acuerdos para compartir información biométrica a nivel regional, pero **carece de una ley integral de protección de datos personales** (IPANDETEC, 2023). La ausencia de salvaguardas normativas plantea riesgos de vigilancia estatal sin controles y tratamiento opaco de información sensible.

3. Panamá: avances en protección de datos, pero biometría aún sin regulación sectorial

Panamá cuenta con la Ley 81 de 2019 de Protección de Datos Personales, que clasifica la biometría como dato sensible y exige consentimiento informado. Además, la ANTAI regula su tratamiento y supervisa obligaciones de seguridad.

No obstante:

- No existe una ley especializada sobre tecnologías biométricas.
- El marco actual no aborda riesgos de reconocimiento facial, interoperabilidad ni vigilancia automatizada.
- Las instituciones públicas poseen bases biométricas (p. ej., identificación ciudadana), pero sin regulación sectorial específica, como señala ACCESO (2024).

La reciente **Ley 478 de 2025** moderniza delitos informáticos, pero no regula directamente el uso de biometría (Sucre Levy, 2025).

4. Nicaragua : vacíos normativos profundos.

A pesar de contar con normas generales de privacidad, no existe regulación específica sobre biometría. Este vacío es especialmente grave en un contexto documentado de vigilancia estatal intensiva y represión digital, donde tecnologías biométricas podrían ser utilizadas para persecución política (Access Now, 2025).

Estándar Regional del Sistema de Integración Centroamericano (SICA).

A nivel del Sistema de la Integración Centroamericana (SICA) se ha impulsado un proceso regional de armonización normativa en materia de ciberdelitos. Entre 2023 y 2024, el Parlamento Centroamericano (Parlacen) aprobó la **Ley Marco de Prevención y Protección contra la Ciberdelincuencia**, iniciativa apadrinada por la Dirección de Seguridad Democrática del SICA (Miranda Aburto & Ávila, 2024). Este instrumento pretende servir como modelo para que los congresos nacionales legislen de manera homogénea.

Origen y Contenido

Investigaciones periodísticas señalan que el texto reproduce numerosos elementos de la Ley Especial de Ciberdelitos de Nicaragua, incluyendo su estructura represiva y disposición extraterritorial.

Incorpora mecanismos amplios de cooperación internacional en extradición y persecución penal, otorgando facultades extensas para registro y aseguramiento de medios digitales.

Preocupaciones Principales

- Autorización expresa para interceptación de comunicaciones
- Control estricto sobre proveedores de telecomunicaciones
- Riesgo de "armonizar hacia abajo" garantías de derechos humanos
- Posible uso para restringir libertad de expresión

Estado Actual: Para octubre de 2024, tras su aprobación en Parlacen, la propuesta fue remitida a los congresos de los Estados miembros. Guatemala detuvo su presentación tras cambio de gobierno, mientras Costa Rica y Panamá adoptan postura cautelosa.

Investigaciones periodísticas señalan que el texto de la ley marco reproduce numerosos elementos de la **Ley Especial de Ciberdelitos de Nicaragua**, incluyendo su estructura represiva y disposición extraterritorial, motivo por el cual ha sido descrita como una propuesta "similar a la de los Ortega-Murillo" (Miranda Aburto & Ávila, 2024). Además de la extraterritorialidad, incorpora mecanismos amplios de cooperación internacional en extradición y persecución penal, y otorga facultades extensas para el **registro, secuestro y aseguramiento de medios digitales**, así como un **control estricto sobre proveedores de telecomunicaciones** (Miranda Aburto & Ávila, 2024).

De especial preocupación es la autorización expresa para la **interceptación, grabación y reproducción de comunicaciones** —incluyendo voces, mensajes, correos electrónicos y comunicaciones digitales— basadas en el uso de redes y del espectro radioeléctrico. Esto reproduce casi literalmente las facultades introducidas por Nicaragua en la reforma de su Ley Especial de Ciberdelitos en 2023, que formalizó la vigilancia estatal de comunicaciones privadas (Access Now, 2020/2025).

Según Divergentes, el proyecto comenzó a gestarse en 2019 con la participación de "expertos provenientes de Rusia", según declaraciones de un diputado hondureño que impulsó la iniciativa. El texto ganó tracción durante 2021–2022, cuando Nicaragua ostentó la presidencia pro témpore del SICA (Miranda Aburto & Ávila, 2024). Para octubre de 2024, tras su aprobación en Parlacen, la propuesta fue remitida a los congresos de los Estados miembros. En El Salvador, Honduras, Nicaragua y República Dominicana su socialización estaba avanzada, mientras que Guatemala detuvo su presentación tras un cambio de gobierno (Miranda Aburto & Ávila, 2024). Costa Rica y Panamá han adoptado una postura más cautelosa, considerando que ya avanzan hacia estándares internacionales como el Convenio de Budapest.

Organizaciones como **IPANDETEC** y **Derechos Digitales** han advertido que esta ley marco podría "armonizar hacia abajo" las garantías de derechos humanos, promoviendo marcos penales que puedan ser utilizados para restringir la libertad de expresión bajo el argumento del combate al cibercrimen (Miranda Aburto & Ávila, 2024).

En paralelo, el SICA mantiene otros esfuerzos de integración digital: una **Estrategia Regional de Seguridad Cibernética**, espacios de intercambio entre CSIRTs nacionales y declaraciones del Consejo de Ministros de Seguridad sobre cooperación en delitos transnacionales —fraude bancario, explotación sexual infantil en línea, entre otros—. Sin embargo, ninguno de estos instrumentos tiene el carácter vinculante que alcanzaría la ley marco una vez adoptada por los Estados.

Compatibilidad de la normativa centroamericana con estándares internacionales en entornos digitales y ciberdelincuencia

Los países centroamericanos analizados (Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica y Panamá) presentan niveles muy distintos de alineación con los principales estándares internacionales en materia de derechos digitales y ciberdelincuencia. A continuación, se evalúa la compatibilidad de sus marcos normativos y prácticas con instrumentos clave como el Convenio de Budapest sobre Ciberdelincuencia, la nueva Convención de la ONU contra la Ciberdelincuencia, la Carta Iberoamericana de Principios y Derechos en Entornos Digitales y los estándares interamericanos de derechos humanos aplicables al entorno digital (CIDH, Corte IDH y Relatoría Especial para la Libertad de Expresión). El análisis se centra en vigilancia estatal, interceptación de comunicaciones, legislación penal sobre delitos informáticos, restricciones a la libertad de expresión y criminalización del periodismo, examinando si las normas nacionales respetan los principios de legalidad, necesidad, proporcionalidad y debido proceso, e identificando incompatibilidades o preocupaciones relevantes (CIDH, 2017; SIP, 2024).

País	Convenio Budapest	Convención ONU	Carta Iberoamericana	Evaluación
Costa Rica	7 Ratificado 2017	En proceso	7 Apoyada	Alta Compatibilidad
Panamá	7 Ley 79 / 2013	En proceso	7 Apoyada	Alta Compatibilidad
Guatemala	Pendiente	En proceso	7 Apoyada	Compatibilidad Media
Honduras	Pendiente	En proceso	7 Apoyada	Compatibilidad Media
El Salvador	No adherido	En proceso	7 Apoyada	Baja Compatibilidad
Nicaragua	No adherido	En proceso	7 Apoyada	Baja Compatibilidad

Adopción de instrumentos internacionales de ciberdelincuencia

La adopción del Convenio de Budapest (2001) —considerado el estándar internacional más completo en materia de ciberdelito— es desigual en la región. Solo Costa Rica y Panamá se han adherido plenamente y han adecuado su legislación interna a sus disposiciones. Costa Rica ratificó el Convenio en 2017, impulsando reformas legales y fortaleciendo la cooperación internacional para investigar delitos informáticos (CliffsNotes–UAM, 2025). Panamá hizo lo propio mediante la Ley 79 de 2013, actualizando su Código Penal para tipificar delitos informáticos conforme a definiciones armonizadas, como acceso ilícito, sabotaje informático, fraude informático y pornografía infantil en línea (Prensa Libre, 2024; Facultad de Derecho UP, s. f.). Estas adhesiones han facilitado la convergencia normativa y la asistencia judicial recíproca para la obtención de evidencia digital (CliffsNotes–UAM, 2025).

En contraste, Guatemala, El Salvador, Honduras y Nicaragua no son aún Estados Parte del Convenio de Budapest, lo que refleja rezagos normativos. En Guatemala persiste la ausencia de una ley integral de ciberdelitos, lo que ha impedido cumplir los requisitos técnicos y normativos para la adhesión, de modo que el país sigue "pendiente de aceptar y ratificar" el instrumento por no contar con legislación compatible (Prensa Libre, 2024). De forma similar, El Salvador, Honduras y Nicaragua tampoco han suscrito el Convenio, permaneciendo fuera de este marco común de cooperación en ciberdelincuencia, lo que limita la modernización de sus tipos penales y el acceso a herramientas robustas de cooperación transnacional para perseguir delitos informáticos complejos (IPANDETEC, s. f.).

En paralelo, en 2024 la Asamblea General de la ONU aprobó la nueva Convención contra la Ciberdelincuencia, tras tres años de negociación. El tratado busca reforzar la cooperación internacional, facilitar la asistencia mutua expedita, promover el desarrollo de capacidades y armonizar las medidas legales contra el cibercrimen (Infobae, 2024). Sin embargo, numerosas organizaciones y expertos han advertido que el texto carece de salvaguardas claras en materia de derechos humanos, lo que podría abrir la puerta a usos abusivos por regímenes autoritarios, especialmente dado que fue impulsado por Estados con graves déficits en libertades (Rusia, China, Irán, Nicaragua, entre otros) (Global Voices, 2025).

Las críticas apuntan a definiciones excesivamente amplias de "ciberdelito" que pueden abarcar actividades legítimas de disidencia o periodismo en línea, así como la ausencia de garantías como la doble incriminación o excepciones para delitos de carácter político (Global Voices, 2025).

La Relatoría Especial para la Libertad de Expresión de la CIDH ha recordado que toda norma penal en este ámbito debe respetar estrictamente el principio de legalidad y no criminalizar expresiones amparadas por la libertad de expresión (CIDH, 2017; Criterio Honduras, 2020). De no incorporar salvaguardas robustas, la Convención podría facilitar la persecución transnacional de opositores y periodistas exiliados a solicitud de gobiernos centroamericanos con tendencias represivas (Global Voices, 2025).

Este riesgo es particularmente visible en Nicaragua: bajo la Ley Especial de Ciberdelitos, las críticas al gobierno se califican como "delitos cibernéticos" y se castigan con penas de prisión, incluso cuando se difunden desde el extranjero, sentando las bases para eventuales solicitudes de extradición al amparo de la futura Convención (Amnesty International, 2024; Global Voices, 2025). Aquí se evidencia una tensión frontal entre la vocación garantista de los estándares interamericanos y ciertas disposiciones de la Convención de la ONU tal como está concebida. Por ello, resulta imperativo que, al implementarla, los países centroamericanos introduzcan cláusulas de salvaguarda de derechos fundamentales —por ejemplo, exclusiones para delitos de opinión o políticos y control judicial estricto— tal como recomiendan la CIDH y organizaciones como APC, EFF y redes de sociedad civil (CIDH, 2017; Global Voices, 2025).

Por otra parte, los seis países han apoyado la Carta Iberoamericana de Principios y Derechos en Entornos Digitales (SEGIB, 2023), un marco político no vinculante que recoge compromisos en materia de derechos digitales. Adoptada en la XXVIII Cumbre Iberoamericana (Santo Domingo, 2023), la Carta consagra principios como libertad de expresión, privacidad, protección de datos, acceso a la información, inclusión digital y seguridad en línea, e insiste en que toda restricción a la expresión en internet debe estar fijada por ley, ser necesaria para un fin legítimo y proporcional en una sociedad democrática (SEGIB, 2023). Asimismo, subraya la necesidad de proteger de forma reforzada la privacidad de las comunicaciones y de los datos personales en entornos digitales. En las secciones siguientes se evalúa hasta qué punto las leyes y prácticas de cada país cumplen o vulneran dichos compromisos, a la luz también de los estándares del sistema interamericano.

Vigilancia estatal e interceptación de comunicaciones

Un área crítica es la vigilancia de las comunicaciones y el uso de tecnologías de interceptación por parte del Estado. Los estándares internacionales, especialmente los del sistema interamericano, establecen que la injerencia estatal en la vida privada solo es admisible cuando está claramente autorizada por ley (principio de legalidad), persigue un fin legítimo y resulta necesaria y proporcional en una sociedad democrática, con control judicial previo o mecanismos independientes de supervisión para garantizar el debido proceso (CIDH, 2017).

El Salvador - Pegasus

Al menos 35 dispositivos infectados entre 2020-2021.
No cumple principios de legalidad, necesidad ni proporcionalidad. Sin control judicial previo.

Nicaragua - Sistemático

Vigilancia y control estatal sin controles efectivos. Reforma 2021 amplió facultades de TELCOR. Bloqueo de sitios sin orden judicial.

Panamá - Antecedentes

Caso "Pinchazos" reveló espionaje sin base legal durante gobierno Martinelli. Hoy existe tutela más sólida con orden judicial requerida.

Honduras / Guatemala - Vacíos

Sin ley de protección de datos ni regulación clara de interceptación. Adquisición de tecnologías de espionaje sin marcos legales robustos.

Costa Rica - Garantista

Ley 7425 exige orden judicial para interceptación. Sala Constitucional activa en protección de intimidad y fuentes periodísticas.

En la práctica, varios países centroamericanos han incurrido en prácticas de vigilancia digital opaca y contraria a estos estándares.

En El Salvador, investigaciones técnico-forenses documentaron una campaña masiva de espionaje contra periodistas y miembros de la sociedad civil mediante spyware. Entre 2020 y 2021, al menos 35 dispositivos de reporteros y activistas salvadoreños fueron infectados con el programa Pegasus de NSO Group, vendido exclusivamente a gobiernos y capaz de interceptar comunicaciones, extraer datos y monitorear en tiempo real sin conocimiento del objetivo (Access Now, 2022).

Aunque el gobierno ha negado su participación, el patrón de víctimas —medios críticos y organizaciones de derechos humanos— y la naturaleza de la herramienta apuntan a una operación de vigilancia política (Access Now, 2022). La intervención de comunicaciones privadas de periodistas con Pegasus constituye una violación particularmente grave de la privacidad y la libertad de expresión. Al no existir en El Salvador un marco legal que autorice este tipo de espionaje contra actores de prensa, no se cumplen los principios de legalidad, necesidad ni proporcionalidad, ni el requisito de control judicial previo. La CIDH, su Relatoría Especial y la Oficina del Alto Comisionado de la ONU han expresado "profunda preocupación" y han recordado la obligación estatal de investigar y sancionar el espionaje ilegal (Access Now, 2022; CIDH, 2017).

Nicaragua muestra un patrón aún más sistemático de vigilancia y control estatal de las comunicaciones, estrechamente asociado a la represión política. Desde 2018 se han documentado redes de monitoreo de telecomunicaciones y espionaje político, sin controles efectivos a la interceptación (Amnesty International, 2024). En 2021 se reformó la Ley General de Telecomunicaciones (Ley 200) para ampliar las facultades del ente regulador TELCOR, consolidando su capacidad de bloquear sitios web y vigilar contenidos en tiempo real, mediante decisiones administrativas carentes de transparencia y contrapesos (El País, 2023; Colectivo DD. HH. Nicaragua, s. f.). El bloqueo de dominios de medios críticos, incluidos sitios ".ni", se ejecuta sin orden judicial y en abierta contradicción con la prohibición de censura previa del artículo 13.2 de la Convención Americana (SIP, 2024; SEGIB, 2023). Informes de la SIP señalan, además, que el régimen mantiene vigilancia sobre periodistas, incluso en el exilio, a través de mecanismos de inteligencia y cooperación con otros Estados (SIP, 2024). Este andamiaje vulnera simultáneamente el derecho a la privacidad, la libertad de expresión y la libertad de prensa, en clara incompatibilidad con las obligaciones internacionales y con los principios proclamados en la Carta Iberoamericana (SEGIB, 2023).

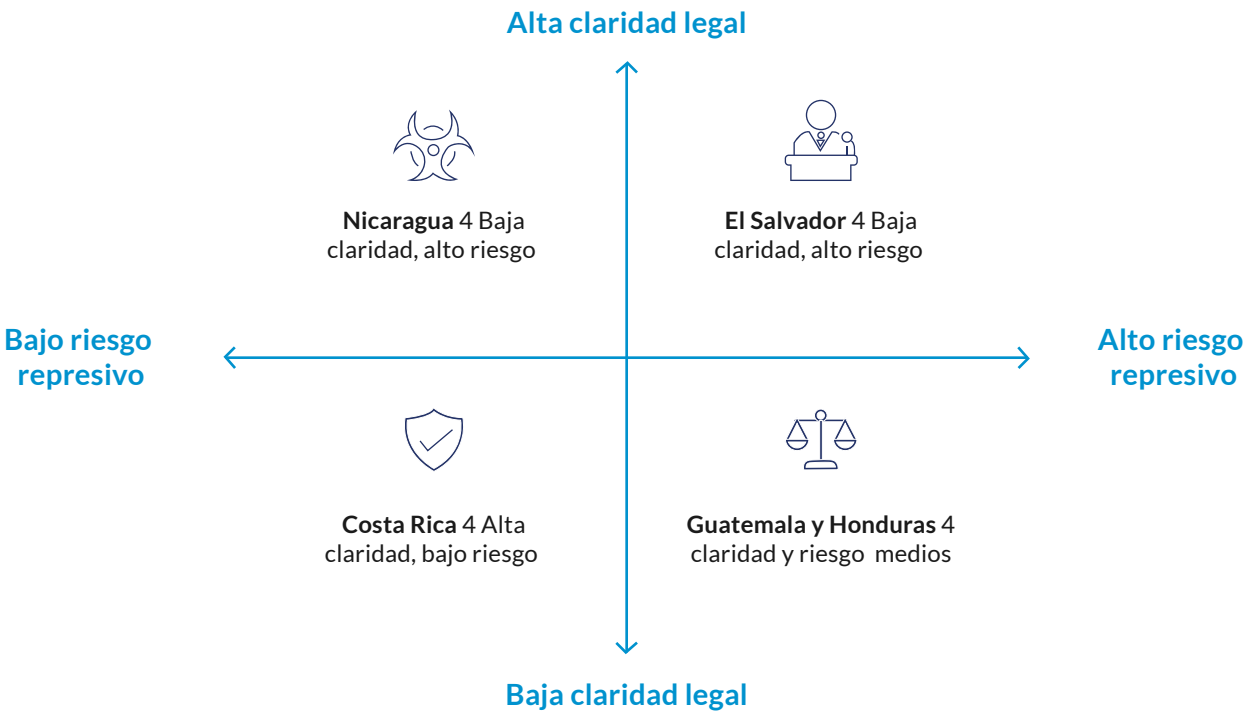
En Panamá, aunque hoy existe una tutela institucional más sólida, persisten antecedentes de vigilancia ilícita de alto nivel. Durante el gobierno de Ricardo Martinelli (2009–2014) se llevó a cabo espionaje telefónico y electrónico contra opositores, periodistas y activistas, mediante software y equipos de interceptación utilizados sin base legal adecuada. El llamado caso "Pinchazos" derivó en procesos penales contra funcionarios del Consejo de Seguridad, pero concluyó con la absolución del expresidente en un fallo polémico, dejando en evidencia lagunas en la regulación y supervisión del uso de tecnologías de interceptación (SIP, 2024). Posteriormente, Panamá ha reforzado la exigencia de orden judicial motivada para intervenir comunicaciones en investigaciones de delitos graves, en línea con su Constitución y Código Procesal Penal; sin embargo, el precedente mostró la necesidad de controles internos más estrictos para evitar abusos.

Honduras y Guatemala presentan riesgos distintos, vinculados principalmente a vacíos normativos. Ninguno de los dos países cuenta con una ley de protección de datos personales ni con una ley de inteligencia que regule de forma clara la interceptación de comunicaciones digitales. En Guatemala, la Corte de Constitucionalidad ya había advertido en 2011 sobre el vacío legal en materia de protección de datos y vigilancia en la era digital, instando a la creación de legislación específica (Plaza Pública, 2017). La ausencia de un marco legal robusto implica que eventuales prácticas de monitoreo digital por parte de organismos de seguridad se desarrollan en un limbo jurídico, incompatible con el principio de legalidad. En Honduras, los intentos de aprobar una Ley de Ciberseguridad incluyeron artículos sobre monitoreo de redes sin garantías suficientes, lo que generó fuertes críticas y frenó la aprobación de la iniciativa (Access Now, 2018; OACNUDH, 2018). Al mismo tiempo, se ha documentado la adquisición de tecnologías de espionaje digital por parte de agencias estatales, generando alarma dado el contexto de graves violaciones de derechos humanos (Access Now, 2018). La CIDH y la OACNUDH han llamado reiteradamente a ambos países a abstenerse de implementar vigilancia masiva o intrusiva sin marcos legales claros y salvaguardas robustas (CIDH, 2017; OACNUDH, 2018).

Costa Rica, por contraste, dispone de un marco relativamente garantista. La Ley 7425 de Intervención de las Comunicaciones y normas posteriores establecen que solo un juez penal puede autorizar la intervención de comunicaciones en casos de delitos graves, bajo estándares estrictos de necesidad y proporcionalidad. La Sala Constitucional ha jugado un papel activo en la protección del derecho a la intimidad y a las fuentes periodísticas, frenando intentos de injerencias indebidas (Téllez, 2025). Además, Costa Rica se convirtió en el primer país de la región en adherirse al Segundo Protocolo Adicional al Convenio de Budapest sobre acceso transfronterizo a evidencia electrónica, lo que exigirá reforzar las salvaguardas de privacidad en la cooperación internacional (CliffsNotes–UAM, 2025). En general, el país se aproxima de forma consistente a los lineamientos de la Carta Iberoamericana en materia de protección de datos y privacidad en entornos digitales (SEGIB, 2023), aunque sigue enfrentando retos de actualización tecnológica de su marco de protección de datos.

Legislación penal en materia de ciberdelitos

Todos los países analizados enfrentan el reto de actualizar sus legislaciones penales para tipificar adecuadamente los delitos informáticos sin convertirlas en herramientas de represión. El principio de legalidad exige que las conductas ilícitas se describan con claridad y precisión, evitando fórmulas vagas que permitan criminalizar actividades lícitas o discrecionales. Asimismo, las penas deben ser proporcionales a la gravedad del hecho y la persecución de ciberdelitos no puede servir de excusa para restringir de manera injustificada libertades fundamentales como la libertad de expresión o de asociación (CIDH, 2017).



En Nicaragua, la Ley Especial de Ciberdelitos (Ley 1042), aprobada en 2020, es uno de los ejemplos más extremos de instrumentalización del derecho penal digital. Aunque incorpora delitos informáticos clásicos (acceso ilícito, fraude, sabotaje), introduce figuras de contenido abierto orientadas a silenciar la disidencia en línea. Entre ellas destaca la criminalización de la difusión de "información falsa o tergiversada" que cause "alarma, temor o zozobra" en la población, sancionada con penas de hasta cinco años de prisión, ampliadas posteriormente mediante reformas que agravan las condenas cuando se considera que se afecta la "seguridad del Estado" (Amnesty International, 2024; SIP, 2024). La redacción imprecisa de conceptos como "noticia falsa" o "zozobra" vulnera el principio de legalidad y se aparta abiertamente de la doctrina interamericana, que prohíbe las restricciones genéricas a la difusión de información supuestamente falsa (CIDH, 2017).

En la práctica, esta ley se ha utilizado para procesar periodistas, opositores y ciudadanos por publicaciones en redes sociales, confirmando su carácter de ley mordaza y su incompatibilidad con la Carta Iberoamericana, que exige que las limitaciones al discurso sean excepcionales, claras y estrictamente necesarias (SEGIB, 2023).

En El Salvador, la evolución ha sido menos abrupta pero igualmente preocupante. La Ley Especial contra los Delitos Informáticos y Conexos de 2016 nació como un instrumento centrado en conductas típicamente técnicas (acceso indebido, sabotaje, fraude digital), relativamente alineado con buenas prácticas. Sin embargo, en el contexto del régimen de excepción y la política de "mano dura" contra las pandillas, se aprobaron reformas al Código Penal que prohíben a medios y personas difundir mensajes o comunicaciones originadas de maras, bajo amenaza de penas de 10 a 15 años de prisión (Human Rights Watch, 2024). Esta modificación ha sido duramente criticada por su efecto inhibidor sobre el periodismo, pues puede castigar la mera cobertura informativa sobre el fenómeno de las pandillas, incluso cuando tiene un propósito crítico o de investigación. Posteriormente, nuevas reformas ampliaron la criminalización a la publicación de documentos oficiales o información "clasificada" del Estado en plataformas digitales, con penas de hasta 12 años de prisión, bajo el argumento de proteger la seguridad y los datos personales (Human Rights Watch, 2024). Organizaciones especializadas han señalado que estas figuras penales pueden utilizarse para perseguir filtraciones sobre corrupción o abusos estatales, contraviniendo el estándar interamericano que protege la divulgación de información de interés público y exige tolerancia reforzada de los funcionarios frente al escrutinio (CIDH, 2017). El Salvador se aleja así de los principios de necesidad y proporcionalidad, al recurrir al derecho penal para sancionar conductas que podrían abordarse mediante mecanismos menos gravosos.

Guatemala, por su parte, no cuenta aún con una ley especial de ciberdelitos vigente, por lo que los delitos informáticos se procesan mediante figuras tradicionales del Código Penal. No obstante, en 2022 el Congreso aprobó el Decreto 39-2022, Ley de Prevención y Protección contra la Ciberdelincuencia, que generó una fuerte reacción social y fue archivado antes de entrar en vigor. La norma contenía disposiciones ampliamente consideradas inconstitucionales: penalizaba el acceso a "datos personales o información confidencial" sin autorización en términos tan abiertos que podían criminalizar filtraciones periodísticas legítimas y obstaculizar el acceso a información de interés público (Plaza Pública, 2022). Además, contemplaba delitos de "acoso" y "difusión de contenido falso" redactados de manera vaga, con el riesgo de castigar críticas a funcionarios y expresiones protegidas por el artículo 35 de la Constitución, que declara no punible la crítica a servidores públicos (Plaza Pública, 2022).

Este intento fallido mostró la tensión entre la necesidad de tipificar ciberdelitos y la tentación de generar mecanismos penales para controlar el discurso digital. Cualquier futura legislación guatemalteca en la materia deberá ajustarse a los estándares interamericanos, evitando tipos penales ambiguos y garantizando que el periodismo y la protesta legítima queden protegidos.

En Honduras, el Nuevo Código Penal (Decreto 130-2017), vigente desde 2020, introduce algunos tipos vinculados a delitos informáticos, pero arrastra graves problemas desde la perspectiva de derechos humanos. El Código mantiene como delitos penales la injuria y la calumnia, incluyendo cuando los hechos se cometen a través de medios electrónicos o redes sociales, con penas que pueden llegar a un año de prisión y multas elevadas en casos de difusión "con publicidad" (Criterio Honduras, 2020). La CIDH y diversos organismos han advertido reiteradamente que la penalización de la difamación, especialmente cuando se aplica a críticas a funcionarios, es incompatible con la Convención Americana, recomendando su despenalización o, al menos, su traslado al ámbito civil (CIDH, 2017). Además, el Código hondureño tipifica figuras amplias como "asociación terrorista" o "reuniones ilícitas" con definiciones imprecisas que pueden abarcar manifestaciones y protestas, lo que crea un riesgo significativo de criminalización de la movilización social (Criterio Honduras, 2020). A ello se suma el intento de aprobar una Ley de Ciberseguridad en 2018 que, de haberse concretado, habría obligado a intermediarios y plataformas a retirar contenido supuestamente "de odio" o "falso" en 24 horas, bajo amenaza de bloqueos y sanciones, delegando funciones censuras en actores privados y sin control judicial adecuado (Access Now, 2018). Aunque el proyecto fue frenado, la iniciativa revela una tendencia regulatoria contraria a los principios de mínima intervención penal y de responsabilidad limitada de intermediarios.

Costa Rica ofrece, en este campo, un caso relativamente más alineado con los estándares internacionales. Desde la aprobación de la Ley 9048 y reformas posteriores, el país tipificó delitos informáticos como sabotaje, acceso no autorizado, fraude informático, difusión de pornografía infantil o violación de datos personales, adaptando posteriormente estas figuras para armonizarlas con el Convenio de Budapest (CliffsNotes–UAM, 2025). A diferencia de otros países, Costa Rica no ha creado delitos específicos para penalizar "noticias falsas" ni ha recurrido al derecho penal para castigar la crítica a funcionarios en entornos digitales. Los delitos de difamación dejaron de aplicarse a asuntos de interés público tras la implementación de la sentencia de la Corte Interamericana en el caso Herrera Ulloa vs. Costa Rica, lo que sitúa al país en línea con la doctrina regional sobre libertad de expresión (CIDH, 2017). Las penas previstas para ciberdelitos se consideran, en general, moderadas y proporcionales a la gravedad de las conductas (CliffsNotes–UAM, 2025). El desafío principal para Costa Rica radica en actualizar su legislación de protección de datos y reforzar políticas públicas frente a fenómenos como desinformación o ciberacoso sin ceder a soluciones punitivas excesivas (Observacom, 2023).

Restricciones a la libertad de expresión y criminalización del periodismo digital

Un eje central para evaluar la compatibilidad normativa es la forma en que los Estados gestionan las restricciones a la libertad de expresión en entornos digitales y su impacto sobre el periodismo. La doctrina interamericana y la Carta Iberoamericana son claras: la regla general es la libertad y toda limitación debe ser excepcional, estar prevista por una ley precisa, perseguir fines legítimos y ser necesaria y proporcional en una sociedad democrática (CIDH, 2017; SEGIB, 2023). Además, se prohíbe la censura previa, se condena la criminalización de la crítica a funcionarios y se rechazan sanciones tan desproporcionadas que produzcan autocensura generalizada.

Nicaragua

Caso más extremo. Ley de Ciberdelitos permite desmantelar prensa independiente y criminalizar expresión digital disidente.

El Salvador

Deterioro acelerado. Reformas penales sobre pandillas y clasificación generan clima de miedo. Discurso estigmatizante desde autoridades.

Panamá

Relativamente favorable. Sin normas claramente mordaza hasta 2025. Riesgos por uso abusivo de figuras penales de honor.

Guatemala

Mecanismos indirectos. Judicialización de periodistas usando tipos penales ajenos al ámbito digital. Lawfare contra medios críticos.

Costa Rica

Contexto favorable. Jurisprudencia protectora de crítica en redes. Sin leyes mordaza ni criminalización sistemática del periodismo.

Honduras

Código restrictivo. Delitos penales de difamación más intentos de legislación punitiva. Alto riesgo por violencia contra periodistas.

Nicaragua constituye el caso más extremo de la región. La combinación de la Ley de Ciberdelitos con otras normas (como la Ley de Agentes Extranjeros o la legislación sobre "traición a la patria") ha permitido desmantelar casi por completo el ecosistema de prensa independiente y criminalizar la expresión digital disidente. La SIP ha señalado que el régimen utilizó estas leyes para justificar confiscaciones, cierres de medios, encarcelamiento y destierro de periodistas, así como persecución de familiares y apropiación de bienes, configurando un escenario de apagón informativo (SIP, 2024). La Ley 1042 ha sido aplicada para castigar publicaciones en redes sociales, opiniones críticas y denuncias de abusos, sin que medie un escrutinio judicial independiente ni un test de proporcionalidad. Los procedimientos penales se desarrollan a menudo a puerta cerrada, con graves violaciones al debido proceso, en abierta contradicción con las obligaciones internacionales de Nicaragua bajo la Convención Americana (Amnesty International, 2024; CIDH, 2017). En la práctica, el entorno digital se ha convertido en una extensión del aparato represivo.

En El Salvador, aunque persiste un mayor pluralismo mediático formal, se observa un deterioro acelerado. Las reformas penales relacionadas con la cobertura de pandillas, sumadas a la criminalización potencial de la difusión de información clasificada, generan un clima de miedo entre periodistas y medios digitales. Las organizaciones de libertad de expresión han documentado un discurso estigmatizante recurrente por parte de las máximas autoridades, que califican a la prensa crítica de "enemiga" o "mercenaria", incentivando campañas de acoso digital y descrédito (Human Rights Watch, 2024; SIP, 2024). En este contexto, casos como el de El Faro —objeto de espionaje con Pegasus, auditorías fiscales abusivas y ataques sistemáticos desde el poder— ilustran cómo se combinan herramientas legales, técnicas y comunicacionales para presionar a medios de investigación (Access Now, 2022). Aunque no se han clausurado formalmente grandes medios, la amenaza de sanciones penales y la hostilidad constante promueven la autocensura y erosionan el debate público, en tensión con los estándares interamericanos y con los principios de la Carta Iberoamericana.

Guatemala ha recurrido con frecuencia a mecanismos indirectos para acallar voces críticas, como la judicialización de periodistas y la utilización de tipos penales ajenos al ámbito digital —por ejemplo, lavado de dinero o obstrucción a la justicia— para perseguir a comunicadores incómodos. El encarcelamiento del periodista José Rubén Zamora y el cierre de elPeriódico han sido interpretados ampliamente como represalias por su labor investigativa, lo que constituye un uso abusivo del sistema penal para silenciar a la prensa (Plaza Pública, 2022; SIP, 2024). Aunque no existe una ley de ciberdelitos vigente, este patrón de lawfare se inserta en un ecosistema digital marcado por campañas de difamación en redes, hostigamiento en línea y exilio forzado de periodistas, que la CIDH ha identificado como parte de una regresión autoritaria (CIDH, 2017).

La tentativa de aprobar el Decreto 39-2022 refuerza la preocupación de que futuras normas en materia digital puedan replicar disposiciones mordaza si no se formulan con enfoque garantista.

En Honduras, la combinación de un Código Penal restrictivo, intentos de legislación de ciberseguridad con enfoque punitivo y altos niveles de violencia contra periodistas configura un entorno de alto riesgo. La permanencia de delitos penales de difamación, sumada a procesos judiciales impulsados por altos funcionarios contra propietarios de medios y reporteros críticos, produce un efecto inhibidor sobre la expresión en redes y plataformas digitales (Criterio Honduras, 2020; SIP, 2024). Además, propuestas de leyes que pretendían responsabilizar a intermediarios por contenidos de usuarios generaron temor entre administradores de páginas y medios digitales, que optaron por moderar o retirar contenidos preventivamente (Access Now, 2018). Aunque algunos de estos proyectos no prosperaron, las señales regulatorias han sido claramente restrictivas y se mantienen como amenaza latente.

Costa Rica y Panamá presentan contextos relativamente más favorables, aunque no exentos de desafíos. En Costa Rica, la jurisprudencia de la Sala Constitucional ha protegido la crítica en redes sociales, incluyendo fallos que prohíben a autoridades bloquear usuarios en cuentas oficiales, al considerar que estas se han convertido en foros públicos de interacción democrática (Téllez, 2025). No se han promulgado leyes específicas que limiten la expresión digital ni se reportan patrones de criminalización sistemática del periodismo por vía penal. Panamá, por su parte, ha debatido proyectos de ley para regular el "hostigamiento en redes sociales" y otros fenómenos digitales, pero hasta 2025 no ha aprobado normas de carácter claramente mordaza. Sin embargo, persisten riesgos asociados al uso abusivo de figuras penales de honor y a demandas civiles millonarias que pueden generar autocensura, lo que la SIP ha identificado como una forma más sutil de presión sobre la prensa (SIP, 2024). Ambos países deben vigilar que futuras reformas en materia de ciberseguridad o combate a la desinformación no se conviertan en instrumentos de restricción indebida del discurso protegido.

Este análisis comparado muestra brechas significativas de compatibilidad entre la normativa centroamericana y los estándares internacionales en materia de derechos digitales y ciberdelincuencia. Países como Nicaragua y El Salvador, y en menor medida Honduras, presentan desviaciones alarmantes, producto de leyes y prácticas que instauran vigilancia intrusiva, penalizan en exceso la expresión en línea y facilitan la criminalización del periodismo, vulnerando los principios de legalidad, necesidad, proporcionalidad y debido proceso (Amnesty International, 2024; CIDH, 2017; SIP, 2024).

Guatemala evitó, por presión social, la entrada en vigor de una ley de ciberdelincuencia problemática, pero continúa utilizando el sistema penal con fines de intimidación y aún no ha construido un marco digital garantista. Costa Rica y Panamá, en cambio, exhiben marcos más acordes con el Convenio de Budapest, la Carta Iberoamericana y los lineamientos interamericanos, aunque se enfrentan a desafíos de actualización tecnológica, fortalecimiento de la protección de datos y prevención de abusos tanto estatales como privados en el entorno digital (CliffsNotes–UAM, 2025; SEGIB, 2023).

En síntesis, la región presenta un panorama heterogéneo: mientras algunas naciones avanzan hacia una política penal contra el cibercrimen compatible con los derechos humanos, otras han optado por regular el espacio digital como un ámbito de control político. Para cerrar estas brechas, es indispensable que los Estados centroamericanos revisen y adecúen sus leyes y prácticas a los estándares globales e interamericanos. Ello implica, entre otras medidas: derogar o reformar normas penales incompatibles con la libertad de expresión (leyes de "fake news", difamación criminal contra funcionarios, tipos amplios de "terrorismo" o "desorden"); establecer marcos legales claros para la vigilancia digital, con control judicial estricto y supervisión independiente; adherirse al Convenio de Budapest y aprovechar los mecanismos de cooperación internacional, incorporando a la vez salvaguardas robustas en la implementación de la nueva Convención de la ONU; garantizar la proporcionalidad de las sanciones por ciberdelitos; y reforzar la independencia judicial para que el debido proceso prevalezca incluso en casos políticamente sensibles (CIDH, 2017; Global Voices, 2025).

Solo mediante estas reformas será posible que la normativa centroamericana en entornos digitales resulte plenamente compatible con los estándares internacionales, permitiendo un equilibrio adecuado entre la seguridad informática y la protección de los derechos humanos en el ciberespacio, conforme a las exigencias de una sociedad democrática en la era digital.

Conclusiones Generales

El análisis comparativo del marco normativo y las prácticas digitales en Centroamérica revela un panorama heterogéneo y preocupantes brechas respecto de los estándares internacionales de derechos humanos. Mientras países como Nicaragua y El Salvador –y en menor medida Honduras– han adoptado enfoques punitivos con vigilancia intrusiva y criminalización del periodismo, otras naciones como Costa Rica y Panamá exhiben marcos más garantistas y acordes con instrumentos globales como el Convenio de Budapest y la Carta Iberoamericana. En general, Costa Rica y Panamá cuentan con las regulaciones más sólidas (leyes de protección de datos inspiradas en estándares internacionales, autoridades independientes y control judicial efectivo), Guatemala y Honduras presentan rezagos normativos sin leyes integrales de datos ni ciberdelitos, y El Salvador y Nicaragua ilustran un giro autoritario: leyes de ciberseguridad que concentran poder en el Ejecutivo, habilitan amplia vigilancia y facilitan la censura y persecución del disenso.

Tendencias Regionales

- Vigilancia estatal sin controles adecuados en varios países
- Criminalización del periodismo mediante figuras penales vagas
- Marcos normativos usados para silenciar disidencia
- Brecha significativa entre países garantistas y autoritarios

Riesgos Emergentes

- Expansión de tecnologías de reconocimiento facial
- Centralización de datos biométricos sin salvaguardas
- Ley Marco del SICA podría "armonizar hacia abajo"
- Violencia digital de género sistemática

Desafíos Estructurales

El análisis comparativo del marco normativo y las prácticas digitales en Centroamérica revela un panorama heterogéneo y preocupantes brechas respecto de los estándares internacionales de derechos humanos. Mientras países como Nicaragua y El Salvador –y en menor medida Honduras han adoptado enfoques punitivos con vigilancia intrusiva y criminalización del periodismo, otras naciones como Costa Rica y Panamá exhiben marcos más garantistas y acordes con instrumentos globales como el Convenio de Budapest y la Carta Iberoamericana. En general, Costa Rica y Panamá cuentan con las regulaciones más sólidas (leyes de protección de datos inspiradas en estándares internacionales, autoridades independientes y control judicial efectivo), Guatemala y Honduras presentan rezagos normativos sin leyes integrales de datos ni ciberdelitos, y El Salvador y Nicaragua ilustran un giro autoritario: leyes de ciberseguridad que concentran poder en el Ejecutivo, habilitan amplia vigilancia y facilitan la censura y persecución del disenso.

Independencia Judicial

Necesidad de fortalecer la independencia del poder judicial para garantizar controles efectivos sobre vigilancia y censura.

Protección de Datos

Urgencia de aprobar leyes integrales de protección de datos en países que carecen de ellas (Guatemala, Honduras, Nicaragua).

Sociedad Civil

Fortalecimiento de organizaciones civiles y medios independientes como contrapeso al poder estatal.

Cooperación Internacional

Necesidad de presión internacional sostenida y condicionalidad en cooperación técnica y financiera.

Alfabetización Digital

Inversión en educación digital y autoprotección para periodistas, activistas y ciudadanía en general.

Vigilancia estatal: Varios gobiernos centroamericanos han extendido las capacidades de vigilancia digital sin los debidos contrapesos. En Nicaragua, por ejemplo, la ley de ciberdelitos de 2020 otorgó facultades de interceptación de comunicaciones amplias y opacas, con cooperación forzosa de empresas telefónicas, posibilitando un monitoreo masivo del tráfico en línea. De forma similar, El Salvador ha centralizado la ciber-vigilancia en una nueva agencia (ACE) bajo control del Ejecutivo, lo que plantea riesgos para la privacidad pese a requerir orden judicial formal. En contraste, Costa Rica dispone de un marco garantista –toda interceptación requiere orden judicial y existe supervisión constitucional–, y Panamá mantiene controles legales (p. ej., límite de 6 meses para retención de metadatos y acceso solo con autorización judicial). No obstante, incluso en estas democracias ha habido controversias, como intentos gubernamentales de obtener datos masivos de usuarios móviles que fueron rechazados por violar la legalidad. En resumen, el principio de proporcionalidad y el debido proceso no están garantizados de manera uniforme: países como Nicaragua y (recientemente) El Salvador incurren en vigilancia opaca contraria a estándares interamericanos, mientras Costa Rica y Panamá han logrado mejores equilibrios con controles institucionales y judiciales.

Criminalización del periodismo: Se observa un preocupante uso de figuras penales para silenciar a la prensa y voces críticas en el entorno digital. Nicaragua representa el caso más extremo: la Ley Especial de Ciberdelitos (Ley 1042/2020) introdujo delitos ambiguos como "propagación de noticias falsas" o hacer imputaciones contra el "honor" que penalizan la crítica en línea, y efectivamente se han utilizado para procesar a periodistas independientes y opositores. En El Salvador, si bien persiste oficialmente pluralismo mediático, las reformas recientes –como la tipificación de "publicación o difusión de noticias falsas" en 2023 y las nuevas leyes de ciberseguridad y datos de 2024– han aumentado el riesgo de censura al permitir a la autoridad ordenar la eliminación de contenido en línea con el pretexto de proteger datos personales o la "verdad". Honduras mantuvo delitos de calumnias e injurias criminales en su nuevo Código Penal (2020) y promovió sin éxito una Ley de "ciberseguridad" orientada a regular el "odio" en redes sociales; tales figuras vagas podrían estigmatizar la crítica legítima como delito. En Guatemala, aunque en 2022 la sociedad civil logró archivar un proyecto de "ley mordaza digital" antes de su entrada en vigor, subsiste la judicialización del periodismo por vías indirectas: se han usado delitos comunes (como revelación de información "reservada" o violencia psicológica) para acosar a reporteros que investigan corrupción. Estas tácticas represivas generan autocensura y vulneran la libertad de expresión en línea, en contravención a los principios democráticos interamericanos.

Normativa de ciberdelitos: La región muestra diferencias marcadas en sus leyes penales informáticas. Costa Rica incorporó tempranamente los delitos informáticos en su Código Penal (Ley 9048 de 2012) de forma relativamente acorde con estándares internacionales y con revisión de su Sala Constitucional para evitar excesos. Panamá modernizó integralmente su legislación penal con la Ley 478 de 2025, tipificando delitos como acceso ilícito, sabotaje informático, suplantación de identidad digital o difusión no autorizada de datos personales, cerrando vacíos previos. Ambos países buscan alinearse con las definiciones del Convenio de Budapest. En cambio, Guatemala sigue sin una ley específica: su polémico Decreto 39-2022 fue anulado antes de implementarse por vulnerar la libertad de expresión. El Salvador endureció figuras delictivas vinculadas a tecnologías en reformas recientes (2023–2025), y Honduras mantiene un marco difuso sin una ley integral de ciberdelitos. En síntesis, en varios países la falta de claridad legal deja vacíos para perseguir delitos informáticos reales, mientras otros han promulgado normas excesivamente amplias que confunden ciberdelitos con expresión digital protegida.

Protección de datos personales: Costa Rica (Ley 8968) y Panamá (Ley 81) cuentan con leyes robustas y autoridades independientes. En El Salvador, la nueva Ley de Protección de Datos (2024) depende de la agencia de ciberseguridad ACE, lo que genera preocupaciones de independencia. Guatemala y Honduras carecen de una ley integral, limitándose al hábeas data y normas fragmentarias, lo que deja desprotegidos a los ciudadanos frente a abusos estatales y privados. La región requiere urgentemente marcos armonizados que sigan estándares como la Convención 108+ o el RGPD.

Uso de tecnologías de espionaje: La región ha experimentado graves casos de espionaje estatal digital. El Salvador fue escenario de infección masiva con Pegasus (al menos 35 periodistas entre 2020–2021). Panamá enfrentó los “pinchazos” bajo Martinelli, con uso confirmado de sistemas de interceptación. Honduras adquirió spyware como Hacking Team, y Nicaragua centraliza infraestructura y censura digital de forma totalizante. La ausencia de regulaciones y supervisión democrática facilita abusos.

Jurisprudencia: Costa Rica destaca por una Sala Constitucional activa en la defensa de derechos digitales. Panamá ha tenido fallos protectores importantes. Guatemala ha emitido amparos en temas de privacidad y expresión. En contraste, El Salvador y Nicaragua carecen de independencia judicial, lo que impide frenar abusos.

Compatibilidad internacional: Solo Costa Rica y Panamá han adherido al Convenio de Budapest. La nueva Convención ONU de ciberdelincuencia (2024) preocupa por su falta de salvaguardas y riesgo de persecución transnacional y abuso. La región ha respaldado la Carta Iberoamericana de Derechos Digitales, pero su implementación real es desigual.

Recomendaciones: Sociedad Civil y Medios

1

Monitoreo y Denuncia

Fortalecer observatorios y redes locales de vigilancia ciudadana sobre derechos digitales. Documentar sistemáticamente casos de censura, vigilancia y persecución digital.

2

Litigio Estratégico

Emprender acciones legales para desafiar normas y prácticas que vulneren derechos. Promover acciones de inconstitucionalidad y recurrir al sistema interamericano.

3

Educación Digital

Impulsar campañas de formación en seguridad digital y privacidad dirigidas a periodistas, defensoras de derechos humanos y ciudadanía activa.

4

Incidencia Regional

Profundizar articulación transfronteriza entre ONGs, colectivos técnicos y gremios periodísticos para presentar frente común ante iniciativas regresivas.

5

Empoderamiento Ciudadano

Promover que la ciudadanía se involucre en defensa de derechos digitales mediante campañas de sensibilización y participación en procesos legislativos.

Recomendaciones: Comunidad Internacional

1 **Condicionalidad y Diplomacia**
Organismos multilaterales deben condicionar cooperación en seguridad y desarrollo al respeto de derechos digitales. Señalar públicamente a gobiernos que usen leyes de ciberdelitos para silenciar disidencia.

2 **Asistencia Técnica**
Brindar asistencia independiente para reforma legal e institucional. Apoyar redacción de leyes modelo de ciberdelitos que tipifiquen conductas ilícitas sin menoscabar libre expresión.

3 **Protección a Periodistas**
Ofrecer refugio y apoyo a periodistas centroamericanos en riesgo. Reforzar programas de protección internacional con visados humanitarios y fondos de reubicación.

4 **Implementación Convención ONU**
Acompañar implementación nacional de la Convención contra Ciberdelincuencia incorporando salvaguardas. Exceptuar delitos contra honor y protesta pacífica.

5 **Agenda Regional Positiva**
Apoyar desarrollo de estrategia regional de derechos digitales. Promover Carta Centroamericana de Derechos Digitales de carácter declarativo.

Recomendaciones: Gobiernos Democráticos

Reforma Legal Garantista
Revisar y reformar leyes nacionales para alinearlas con estándares internacionales. Derogar disposiciones penales vagas y desproporcionadas. Aprobar leyes integrales de protección de datos.

Control Judicial de Vigilancia
Establecer marcos normativos claros que regulen interceptación y vigilancia digital con controles democráticos robustos. Toda intrusión debe estar autorizada por juez independiente.

Independencia Judicial
Garantizar que jueces y fiscales actúen con independencia. Designación transparente y meritocrática de magistrados. Capacitación especializada en derechos digitales.

Adhesión a Estándares
Ratificar Convenio de Budapest sobre ciberdelincuencia. Implementar Convención ONU con salvaguardas explícitas. Adoptar Carta Iberoamericana como guía interna.

Cooperación Regional
Coaligarse dentro del SICA para bloquear iniciativas represivas. Construir estándares compartidos que privilegien seguridad con derechos.

Protección de Periodistas
Implementar mecanismos nacionales de protección que incorporen componente digital. Garantizar que ninguna agencia estatal hostigue o espíe a comunicadores.

Llamado a la Acción

"El compromiso de los gobiernos con estas recomendaciones determinará si Centroamérica logra cerrar la brecha entre sus marcos legales y los estándares internacionales. Solo a través de reformas legales profundas, instituciones fortalecidas e independientes y una colaboración regional basada en derechos humanos, la región podrá garantizar que la seguridad informática no sirva de excusa para conculcar libertades."

Sociedad Civil

Monitorear, denunciar, litigar y educar. Fortalecer redes regionales y exigir rendición de cuentas.

Comunidad Internacional

Condicionar cooperación, brindar asistencia técnica y proteger a periodistas en riesgo.

Gobiernos

Reformar leyes, fortalecer controles judiciales y adherir a estándares internacionales.

Referencias Bibliográficas

Access Now. (2020, 30 de septiembre). Ley Especial de Ciberdelitos en Nicaragua: la opresión se traslada al mundo en línea. Recuperado de https://www.accessnow.org/ley-especial-de-ciberdelitos-en-nicaragua-opresion-en-linea/

Access Now; Amnesty International. (2022). Informe técnico sobre Proyecto Torogoz / Pegasus en El Salvador (2020–2021). Recuperado de https://www.accessnow.org

Amnesty International. (2024). Nicaragua: análisis sobre la Ley Especial de Ciberdelitos y prácticas de represión. Recuperado de https://www.amnesty.org

AP News. (2021). Panamanian "pinchazos" case: peritajes confirman uso de sistemas de espionaje (incluido Pegasus). Recuperado de https://apnews.com

Artículo 19. (2020). Observaciones sobre proyectos de ley de ciberseguridad y libertad de expresión en Honduras / Centroamérica. Recuperado de https://www.article19.org

Asamblea Legislativa de Costa Rica. (2011). Ley N.º 8968: Protección de la persona frente al tratamiento de sus datos personales. San José: Asamblea Legislativa. Recuperado de https://www.prodhab.go.cr

Asamblea Legislativa de Costa Rica. (2012). Ley N.º 9048: Reforma al Código Penal en materia de delitos informáticos. San José: Asamblea Legislativa. Recuperado de https://globalfreedomofexpression.columbia.edu/es/cases/demanda-de-inconstitucionalidad-de-los-articulos-que-penalizan-el-tratamiento-de-datos-personales-y-tipifican-el-espionaje-en-costa-rica/

Asamblea Legislativa de Costa Rica. (2019). Proyecto de Ley 21.187: Ley para combatir la ciberdelincuencia. Recuperado de https://d1qqtien6gys07.cloudfront.net/wp-content/uploads/2021/03/21187.pdf

Asamblea Legislativa de El Salvador. (2016). Ley Especial contra los Delitos Informáticos y Conexos. San Salvador: Asamblea Legislativa. Recuperado de https://www.lexology.com/library/detail.aspx?g=a1188143-72f2-47a2-9c1d-df5098a8ecee

Asamblea Legislativa de El Salvador. (2024, noviembre). Ley de Ciberseguridad y Seguridad de la Información. San Salvador: Asamblea Legislativa. Recuperado de https://www.lexology.com/library/detail.aspx?g=2d00bc2b-a646-4f23-bd68-956d2d5b1afa

Asamblea Legislativa de El Salvador. (2024). Ley de Protección de Datos Personales. San Salvador: Asamblea Legislativa. Recuperado de https://www.lexology.com/library/detail.aspx?g=2d00bc2b-a646-4f23-bd68-956d2d5b1afa

Asamblea Legislativa de El Salvador / Diario Oficial. (2025, 19 de junio). Decreto 332: Reformas a la Ley Especial contra los Delitos Informáticos y Conexos (vigente 3 jul. 2025). San Salvador: Diario Oficial / Asamblea Legislativa. Recuperado de https://www.lexology.com/library/detail.aspx?g=a1188143-72f2-47a2-9c1d-df5098a8ecee

Asamblea Nacional de Nicaragua. (2020). Ley No. 1042: Ley Especial de Ciberdelitos. Managua: Asamblea Nacional. Recuperado de https://www.asamblea.gob.ni

Asamblea Nacional de Nicaragua. (2020). Ley de Regulación de Agentes Extranjeros. Managua: Asamblea Nacional. Recuperado de https://www.confidencial.com.ni

Asamblea Nacional de Panamá. (2009). Ley No. 51 de 23 de septiembre de 2009: Normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y otras disposiciones. Ciudad de Panamá: Asamblea Nacional. Recuperado de https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf

Asamblea Nacional de Panamá. (2013). Ley 79 de 2013: Aprueba el Convenio sobre la Ciberdelincuencia (Convenio de Budapest). Ciudad de Panamá: Asamblea Nacional.

Asamblea Nacional de Panamá. (2019). Ley 81 de 2019: Ley de Protección de Datos Personales. Ciudad de Panamá: Asamblea Nacional. Recuperado de https://fmm.com.pa/es/la-proteccion-de-datos-personales-en-panama/

Asamblea Nacional de Panamá / ANTAI. (2021). Decreto Ejecutivo 285/2021: Reglamento de la Ley 81/2019 de Protección de Datos Personales. Ciudad de Panamá: ANTAI. Recuperado de https://antai.gob.pa/reglamentan-ley-81-de-proteccion-de-datos-personales/

Asamblea Nacional de Panamá. (2025). Ley 478 de 2025: Reforma del Código Penal para delitos digitales. Ciudad de Panamá: Asamblea Nacional. Recuperado de https://www.asamblea.gob.pa y https://www.sucre.net/ley-478-2025-delitos-digitales-panama/

Ciudad de Guatemala — Congreso de la República de Guatemala. (2017). Iniciativa 5928: Proyecto de reforma a la Ley General de Telecomunicaciones [Documento legislativo]. Recuperado de https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/de7d7-5928.pdf

Colectivo DD.HH. Nicaragua. (2024). Documentación sobre acoso transnacional contra periodistas nicaragüenses en el exilio. Recuperado de https://www.colectivoddhh.org

Confidencial. (2023, 15 de septiembre). Reformas a la Ley de Ciberdelitos en Nicaragua. Recuperado de https://www.confidencial.com.ni

Convention on Cybercrime (Budapest Convention). (2001). Consejo de Europa. Recuperado de https://www.coe.int/en/web/cybercrime/the-budapest-convention

Criterio.hn. . (2019). Ley de ciberseguridad de Honduras es ambigua y se enmarca en el odio. Recuperado de https://criterio.hn/ley-de-ciberseguridad-de-honduras-es-ambigua-y-se-enmarca-en-el-odio/

CRHoy. (2025). ¿Los operadores telcos de Costa Rica deben entregar los datos de sus usuarios móviles? Recursos de amparo y cobertura sobre solicitud de datos masivos por parte del Ministerio de Hacienda. Recuperado de https://www.crhoy.com y https://www.telesemana.-com/blog/2025/05/06/los-operadores-telcos-de-costa-rica-deben-entregar-los-datos-de-sus-usuarios-moviles/

Cyber Law Toolkit. (2023). Costa Rica and Conti: International law aspects of ransomware. Recuperado de https://cyberlawtoolkit.org

DERECHOSDIGITALES (IPANDETEC). (s. f.). Minuta / aportes sobre protección de datos y proyectos. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/minuta_ipandetec.pdf

Divergentes (Miranda Aburto, W., & Ávila, J.). (2024, 2 de octubre). El SICA promueve una ley de Ciberdelitos en Centroamérica. Recuperado de https://www.divergentes.com/sica-ciberdelitos-centroamerica/

El Faro. (2022). Cobertura sobre infecciones con Pegasus en periodistas salvadoreños y análisis técnico. Recuperado de https://elfaro.net

Freedom House. (2023–2024). Informes sobre espacios cívicos digitales y violencia en línea en Centroamérica. Recuperado de https://freedomhouse.org

Global Freedom of Expression (Columbia). (s. f.). Demanda de inconstitucionalidad de los artículos que penalizan el tratamiento de datos personales y tipifican el espionaje en Costa Rica. Recuperado de https://globalfreedomofexpression.columbia.edu/es/cases/demanda-de-inconstitucionalidad-de-los-articulos-que-penalizan-el-tratamiento-de-datos-personales-y-tipifican-el-espionaje-en-costa-rica/

Global Voices. (2025). Análisis crítico sobre la Convención de la ONU contra la Ciberdelincuencia y sus riesgos para derechos humanos. Recuperado de https://globalvoices.org

Hacking Team leaks / VICE. (2016). Filtraciones sobre ventas de RCS y adquisiciones por gobiernos centroamericanos (Honduras, Panamá). Recuperado de https://www.vice.com

Human Rights Watch. (2022; 2024). Informes sobre vigilancia y marcos legales regresivos en El Salvador, Nicaragua y la región. Recuperado de https://www.hrw.org

IAIP (Instituto de Acceso a la Información Pública, Honduras). (2021). Anteproyecto de Ley de Protección de Datos Personales (documento de trabajo). Recuperado de https://www.iaip.gob.hn y cobertura en https://criterio.hn/ley-de-ciberseguridad-de-honduras-es-ambigua-y-se-enmarca-en-el-odio/

Índice Chapultepec. (2021). Informes sobre litigios contra periodistas y uso de delitos contra el honor en Panamá. Recuperado de https://chapultepec.juridicas.unam.mx

Infobae. (2024). Noticia sobre aprobación en la ONU de la nueva Convención contra la Ciberdelincuencia (2024). Recuperado de https://www.infobae.com

Infodefensa. (2023). Reportes sobre cooperación biométrica en el Triángulo Norte. Recuperado de https://www.infodefensa.com

IPANDETEC. (2023–2024). Informes y alertas sobre biometría, protección de datos y debates legislativos en la región. Recuperado de https://ipandetec.org

IPLEX (Instituto de Prensa y Libertad de Expresión, Costa Rica). (2014; 2023). Informes sobre libertad de prensa y amenazas digitales en Costa Rica. Recuperado de https://iplex.cr

La Estrella de Panamá. (2019). Cobertura sobre intentos de hackeo al Tribunal Electoral y advertencias sobre intrusiones. Recuperado de https://www.laestrella.com.pa

LatAm Journalism Review (LJR). (2022; 2023; 2024). Reportes sobre #malqueridas, agresiones a periodistas y menciones al uso extraterritorial de Ley 1042 (Nicaragua). Recuperado de https://latamjournalismreview.org

MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones, Costa Rica). (2017). Estrategia Nacional de Ciberseguridad 2017–2021 (borrador). San José: MICITT. Recuperado de https://www.micitt.go.cr/sites/default/files/transparencia/-consulta-publica/Estrategia%20Nacional%20de%20Ciberseguridad-Borrador-Consulta%20pu%CC%81blica.pdf

MICITT (Ministerio de Ciencia, Tecnología y Telecomunicaciones, Costa Rica). (2023). Estrategia Nacional de Ciberseguridad 2023–2027. Recuperado de https://www.micitt.go.cr

Ministerio Público de Panamá. (2020). Procedimientos y unidades especializadas para interceptación judicial (documentación institucional). Recuperado de https://www.mp.gob.pa

Ministerio Público de Panamá / Asamblea Nacional de Panamá. (2025). Ley 478 de 2025: Reforma del Código Penal (delitos informáticos). Recuperado de https://www.asamblea.gob.pa y https://www.mp.gob.pa

Observacom. (2023). Análisis sobre desinformación, ciberacoso y marcos regulatorios con enfoque de libertades. Recuperado de https://observacom.org

OACNUDH (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos). (2018; 2021; 2022). Observaciones sobre proyectos de ley y prácticas de vigilancia en la región. Recuperado de https://www.ohchr.org

OEA / Relatoría Especial para la Libertad de Expresión. (2019). Opinión sobre el derecho al olvido y límites frente al interés público. Recuperado de https://www.oas.org/es/cidh/expresion/

Organización de Estados Americanos / CIDH. (2017; 2020; 2023; 2025). Informes y pronunciamientos sobre libertad de expresión, vigilancia y bloqueo de dominios (.com.ni). Recuperado de https://www.oas.org/es/cidh

Plaza Pública. (2017; 2022). Protección de datos y hábeas data; cobertura sobre el archivo del Decreto 39-2022 (Guatemala). Recuperado de https://www.plazapublica.com.gt/content/proteccion-de-datos-y-habeas-data-tercera-parte y https://www.plazapublica.com.gt

Prensa Libre. (2022, 1 de septiembre). Congreso oficializa que se archiva el Decreto 39-2022 que contenía la Ley contra la ciberdelincuencia. Ciudad de Guatemala: Prensa Libre. Recuperado de https://www.prensalibre.com/guatemala/politica/congreso-oficializa-que-se-archiva-el-decreto-39-2022-que-contenia-la-ley-contra-la-ciberdelincuencia-breaking/

PurpleSec. (2023). Informe sobre el ataque Conti en Costa Rica (2022). Recuperado de https://www.purplesec.us

Pillku / Movimiento por la Libertad de Expresión. (s. f.). Nueva ley de delitos informáticos amenaza la libertad de expresión (Costa Rica). Recuperado de https://pillku.org/costa-rica-nueva-ley-de-delitos-informaticos-amena

Refworld. (s. f.). Recursos y reportes sobre legislación y derechos humanos. Recuperado de https://www.refworld.org

RENAP (Registro Nacional de las Personas, Guatemala). (2018). Procedimientos y uso de biometría para el DPI (documentación institucional). Recuperado de https://www.renap.gob.gt

Reporteros Sin Fronteras (RSF). (2023; 2024; 2025). Informes regionales sobre ataques a la prensa y bloqueo de dominios (Nicaragua). Recuperado de https://rsf.org

SICA / Parlacen. (2023–2024). Proyecto de Ley Marco de Prevención y Protección contra la Ciberdelincuencia (Parlacen/SICA). Recuperado de https://www.sica.int y https://www.parlacen.int

SIP (Sociedad Interamericana de Prensa). (2024; 2025). Comunicados sobre intimidación a la prensa regional y campañas de doxxing. Recuperado de https://www.sipiapa.org

Sucre Levy, D. (2025, 25 de agosto). Ley 478 de 2025: Panamá fortalece su Código Penal con nuevos delitos digitales. Recuperado de https://www.sucre.net/ley-478-2025-delitos-digitales-panama/

Swissinfo. (2020). Investigación sobre UPAD (Unidad Presidencial de Análisis de Datos) en Costa Rica y allanamientos. Recuperado de https://www.swissinfo.ch

Téllez, N. (2025, 6 de mayo). ¿Los operadores telcos de Costa Rica deben entregar los datos de sus usuarios móviles? TeleSemana.com. . Recuperado de https://www.telesemana.com/blog/2025/05/06/los-operadores-telcos-de-costa-rica-deben-entregar-los-datos-de-sus-usuarios-moviles/

TELCOR (Nicaragua). (2020). Estrategia Nacional de Ciberseguridad 2020–2025 (decreto). Recuperado de https://www.telcor.gob.ni

The Washington Post. (2022). Cobertura sobre detenciones y exilios de periodistas (Guatemala; El Periódico). Recuperado de https://www.washingtonpost.com

TVN Noticias (Panamá). (2023). Alertas sobre ataques sostenidos contra el Sistema de Transmisión Extraoficial de Resultados (TER). Recuperado de https://www.tvn-2.com

Vance Center; GIJN; colectivos de prensa. (2021–2024). Investigaciones sobre netcenters, financiamiento y campañas coordinadas de difamación (Guatemala y región). Recuperado de https://www.vancecenter.org y https://gijn.org

Vice / VICE News. (2016). Filtraciones Hacking Team y compras gubernamentales de RCS. Recuperado de https://www.vice.com

Wikipedia. (2023). Conti (grupo criminal): cronología del ataque a Costa Rica (uso referencial). Recuperado de https://es.wikipedia.org/wiki/Conti_(grupo_criminal)

Yahoo Noticias. (2022). El Salvador: reforman ley de intervenciones telefónicas. Recuperado de https://es-us.noticias.yahoo.com/salvador-reforman-ley-intervenciones-telef%C3%B3nicas-034726388.html

Informe Regional Derechos Digitales y Ciberdelincuencia en Centroamérica

Análisis comparado

2018-2025

FLED

https://fled.ong/

https://www.facebook.com/fledONG

@FLED_ong

Autor: Alexa Zamora.