3.1. Tabla 1. Marco Constitucional sobre Derechos Digitales[38]

Guatemala	Honduras	El Salvador	Nicaragua	Costa Rica
Derecho a la Privacidad Digital[39] y la Inviolabilidad de las Comunicaciones				
Art. 24: inviolabilidad de correspondencia, documentos o libros y se garantiza el secreto de la correspondencia y de las comunicaciones.	**Art. 76:** derecho al honor, la intimidad personal, familiar y a la propia imagen. **Art. 100:** derecho a la inviolabilidad y secreto de las comunicaciones.	**Art. 2:** derecho al honor, a la intimidad personal, familiar y a la propia imagen. **Art. 24:** se prohíbe la interferencia y la intervención de las telecomunicaciones.	**Art. 27: 5)** derecho a la vida privada y familiar. **6)** derecho al respeto de la honra y reputación. **8)** inviolabilidad del domicilio, correspondencia y comunicaciones.	**Art. 24:** derecho a la intimidad, la libertad y el secreto de las comunicaciones. Derecho fundamental de acceso a las telecomunicaciones y las TIC.
Derecho a la Libertad de Expresión en Línea				
Art. 35: derecho a la libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa y sin restricción por ley o disposición alguna.	**Arts. 72-74:** derecho a la libre emisión del pensamiento por cualquier medio de difusión, sin previa censura, libertad de prensa y la no restricción.	**Art. 6:** toda persona puede expresar y difundir libremente sus pensamientos y el ejercicio de este derecho no estará sujeto a previo examen, censura ni caución.	**Art. 30:** derecho a expresar libremente el pensamiento en público/privado, siempre y cuando no trasgreda los principios de seguridad, paz y bienestar.	**Art. 29:** todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura.
Derecho de Acceso a la Información y Petición de la Información				
Arts. 28-31: derecho a dirigir, individual o colectivamente, peticiones a la autoridad y el derecho de acceso a información sobre registros estatales.	Derecho de acceso a la información se deriva de los **Arts. 72-74.** **Art. 182:** garantía del Hábeas Data. **Art. 80:** presentar peticiones a las autoridades.	Derecho de acceso a la información se deriva de los **Arts. 6 y 18.** **Art. 18:** derecho a dirigir peticiones por escrito a las autoridades.	**Art. 60:** derecho a la información, comprende la libertad de buscar, recibir y difundir ideas e información por cualquier medio. **Art. 176:** recurso de Habeas Data, garantía de tutela de datos.	**Arts. 27 y 30:** se garantiza el derecho a la libertad de petición y acceso a la información pública.

[38] Constitución Política de Guatemala, 1985; Constitución de la República de Honduras, 1982; Constitución de la República de El Salvador; Constitución Política de la República de Nicaragua, 1986 y reformas constitucionales de 2025; y Constitución Política de Costa Rica de 1949.

[39] Peri L. (2016). "El derecho a la privacidad digital. Análisis de los marcos legales de Guatemala, Honduras, El Salvador y Nicaragua". *Cuaderno Jurídico y Político, Vol. 2, N. 5.*

3.2. Tabla 2. Marco Legal Secundario sobre Derechos Digitales

Guatemala	Honduras	El Salvador	Nicaragua	Costa Rica
Protección de Datos Personales y Derechos ARCO-POL				
Ley de Acceso a la Información Pública **Art. 1:** derecho a conocer, proteger y actualizar los datos personales. **Art: 30:** garantía de Hábeas Data**.** **Art.31-35:** consentimiento expreso y de excepción, el acceso, tratamiento y denegación expresa de los datos personales. **Art. 46:** autoridad reguladora, PGD. *Manejo de datos sólo en el ámbito de registros y archivos públicos o estatales.	**Ley de Transparencia y Acceso a la Información Pública** **Art. 4:** deber de informar y al acceso a la información pública. **Arts. 8-11:** ente regulador, IAIP. **Art. 23:** garantía de Hábeas Data. **Art: 24:** sistematización de archivos personales y su acceso.	**Ley de Datos Personales** **Art.7:** ente regulador, la Agencia ACE. **Art.7:** derecho a solicitar información. **Arts. 8-14:** derechos del titular, ARCO-POL. **Arts. 56-58:** sanciones administrativas. **Ley de Inteligencia Artificial (IA)** **Arts. 22-23:** protección de datos personales y propiedad intelectual en el desarrollo de la IA.	**Ley de Protección de Datos Personales y Reglamento N.36-2012** **Art. 10:** derecho al olvido digital. **Art. 16:** derecho a solicitar información. **Art. 17:** derechos del titular, ARCO. **Arts. 28-29**: ente regulador y sancionador, DIPRODAP. **Art 46:** sanciones de carácter administrativo.	**Ley de Protección de la Persona frente al tratamiento de sus Datos Personales** **Art. 5:** derecho a la autodeterminación informativa. **Art. 7:** derechos del titular, ARCO. **Arts. 15:** entidad reguladora, PRODHAB. **Art. 28:** sanciones de carácter administrativo.
Tipificación del Delito Informático y Conexos				
Código Penal de 1973 y reformas legislativas, **Delitos Informáticos** **Art. 274 A-C:** destrucción de registros informáticos**,** alteración de programas y reproducción de programas de computación. **Art. 274 D-G:** registros prohibidos, manipulación de Información, el uso no autorizado de información y de programas destructivos.	**Código Penal de 2019,** **Delitos Informáticos** **Arts. 398-399:** acceso no autorizado y daño a sistemas informáticos. **Art. 400:** abuso de dispositivos. **Art. 401:** suplantación de identidad. **Art. 592:** ciberterrorismo o terrorismo electrónico.	**Ley Contra Delitos Informáticos y Conexos** Marco penal que tipifica, previene y sanciona delitos cometidos mediante sistemas digitales, como la estafa y fraude informático, así como el espionaje y el uso indebido de datos.	**Ley Especial de Ciberdelitos y reforma de 2024** Marco penal para la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las TIC con alcance en redes sociales y su aplicación extraterritorial. **Código Penal:** tipifica expresamente los ciberdelitos.	**Código Penal, Sección de Delitos Informáticos y reformas Leyes N.8148, 9048 y 9135** Marco penal contra el cibercrimen, tipifica delitos como el fraude digital y acceso indebido. Delitos complejos como el espionaje, programa maligno, phishing y grooming.

Nota 1: Elaboración propia. Septiembre de 2025.

Nota 2: PGD, se entiende como Procurador de los Derechos Humanos. IAIP, se entiende como Instituto de Acceso a la Información Pública.

5.1. Tabla 4. Marco Legal Represivo sobre las Telecomunicaciones, TIC y Datos Personales

País	Disposiciones represivas	Impacto en Derechos Digitales
Leyes de Telecomunicaciones de El Salvador y Nicaragua, Acuerdo Normativo N. 001-2021 de Nicaragua, Ley de Intervención de las Telecomunicaciones (LEIT) y Ley de Datos Personales de El Salvador		
Nicaragua **Ley Convergentes y Normativa de TELCOR**	**Art. 5 (12): definición de contenido:** toda información generada bajo cualquier modo o forma de expresión por medios digitales. **Art. 27: revocación de licencias** por varias causas tales como no prestar con eficiencia y regularidad los servicios. **Art. 110: obligación de suministrar "toda información"** que sea requerida por TELCOR incluyendo aquella estadística y georreferenciada. **Arts.111-113: supervisión y fiscalización** por parte de TELCOR con la capacidad de inspeccionar instalaciones y acceder a cualquier registro cuando sea necesario. **Arts. 139-158:** se **imponen multas, restricciones de funcionamiento y confiscacione**s por incumplimiento de la ley **Art. 154: facultad de TELCOR** de emitir "cualquier" normativa. **Art. 3 de la Normativa de TELCOR:** obliga a operadores a guardar y **suministrar "todos" los datos personales** de usuarios.	**-Amplia y vaga definición de contenido** genera riesgo de censura por parte de TELCOR y autocensura por parte de la ciudadanía ante el temor de represión. **-Limitación de operación de proveedores** de internet, medios digitales, creadores de contenido por la posibilidad de interrupción de acceso, monitoreo y censura. **-Exposición masiva de datos personales** sin control judicial y vigilancia de comunicaciones, lo que vulnera el derecho a la privacidad, inviolabilidad de las comunicaciones y la ley 787 de datos personales.
El Salvador, **Ley de Telecom., LEIT, y Datos Personales**	**Art. 30, A de la ley de Telecom.:** obliga a los operadores a **conservar y entregar toda información requerida por la Fiscalía** relativa a datos personales tales como la identidad y foto personal. **Art. 35, A de la ley de Telecom.: sanciones** con multas de 500 a 1,000 salarios mínimos por incumplimiento. **Art. 5 de la LEIT: delitos informáticos y conexos** sujetos a la aplicación de la ley. **Art. 7 de la LEIT: Fiscalía, autoridad para solicitar la intervención** de las comunicaciones. **Art. 50 de la Ley de Datos: ACE, ente regulador y sancionador** sujeto al presidente de la República. **Art. 10 de la Ley de Datos: principio de exactitud** puede dar cabida la censura y a sanciones a medios de comunicación.	- Ante la obligación de almacenar datos personales genera el **riesgo de vigilancia y vulneración de la privacidad.** -Frente a la regulación del sector de las TIC se posibilita el **abuso de poder y restricciones a la libertad de expresión**. -Se **centraliza la toma de decisiones** y concentra la autoridad. **-Agiliza la intervención**, menos margen de análisis, autorización judicial exprés.

Nota: Elaboración propia. Septiembre de 2025.

5.2. Tabla 5. Marco Legal Represivo sobre Ciberdelitos

País	Disposiciones represivas	Impacto en derechos digitales
Ley de Ciberdelitos de Nicaragua y Ley Contra Delitos Informáticos de El Salvador		
Nicaragua	**Arts. 1:** persecución y sanción de **delitos cometidos en las TIC, redes sociales y aplicaciones móviles** (*apps*). **Art. 2:** ampliación de **sujetos responsables**, y su aplicación y **alcance es extraterritorial**. **Art. 8:** delito por **interferir o alterar sistemas informáticos**, si son del Estado y servicios públicos van con sanciones de hasta 15 años de prisión **Art. 9:** delito de **alteración, daño a la integridad y disponibilidad de datos**. Sanciones de hasta 15 años de prisión. **Arts. 10, 12 y 15:** delitos por **daños a sistemas informáticos, fraude informático y hurto por medios informáticos.** Sanciones con prisión de hasta 7 años. **Art. 30:** delito de **propagación de "noticias falsas"** a través de las TIC, redes sociales y *apps*, difusión de información falsa que perjudique el honor e información que incite al odio con penas de prisión de hasta 10 años.	-Aumento del **poder estatal en la vigilancia y la obtención de datos e información personal** sin garantías procesales ni controles independientes, conlleva un riesgo para la privacidad y la protección de datos personales. -**Autocensura masiva** de las y los ciudadanos y medios de comunicación debido a la severidad de las penas. -Ampliación del **efecto extraterritorial de la ley** para perseguir a disidentes en el exterior. -**Criminalización de la denuncia, investigación periodística y opiniones ajenas** al gobierno mediante figuras como "noticias falsas" con grave afectación a la libertad de expresión en línea. -**Riesgos a la libertad de prensa y de expresión** mediante la criminalización de actividades en internet, redes sociales y *apps*.
El Salvador	**Arts. 10-12:** se tipifican delitos de **estafa, fraude y espionaje informático**. Se incrementan las sanciones con prisión por hasta 12 años. **Art. 22:** delito de **suplantación de identidad**. Sanción con prisión de hasta 10 años **Art. 23:** delito de **obtención y divulgación de información no autorizada** por medio de las TIC y datos en sistemas informáticos. Sanción con prisión de hasta 12 años si pone en peligro la seguridad del Estado. **Art. 24:** delito del **uso indebido de datos personales** o sensibles. Sanción con prisión de hasta 6 años. **Art. 25:** delito de **obtención y transferencia de información "confidencial".** Sanción con prisión de hasta 8 años. *Las reformas de 2022 y 2025 endurecen sanciones de 10- 12 años de prisión por cometer delitos informáticos.	-**Riesgos a la privacidad digital y la protección de datos personales** por el uso indebido de la información, de los datos y sistemas informáticos. -**Tipificación de manera amplia e imprecisa**, penalizando a usuarios de las TIC por obtener o transferir información "confidencial", lo que permite diversas interpretaciones jurídicas. -**Ambigüedad jurídica** genera autocensura, riesgo periodístico y de libertad de expresión. Por ejemplo, mediante persecución a periodistas por denuncias de corrupción, gastos públicos, y violaciones de derechos humanos, como lo ocurrido con Ruth López.