Informe Final sobre Derechos Digitales en Centroamérica: Enfoque en Honduras, Guatemala, El Salvador y Nicaragua

Septiembre 2024

Índice de Contenidos

1. Resumen Ejecutivo 4
1.1. Resultados Principales 4
1.2. Puntos de Acción 4
2. Introducción 5
3. Propósito del Análisis 6
4. Objetivos del Análisis 6
4.1. Objetivo General 6
4.2. Objetivos Específicos 6
5. Hipótesis 7
6. Enfoque Metodológico 7
7. Preguntas y Criterios del Análisis 7
7.1. Preguntas del Análisis 7
8. Situación Democrática y Estado de Derecho 8
9. Marco Normativo Internacional sobre Derechos Digitales 10
9.1. Marco Normativo Universal 10
9.2. Marco Normativo Interamericano y Regional 10
9.3. Marco Normativo Europeo 12
10. Análisis Comparativo de la Legislación Vigente 14
10.1. Tabla 1. Marco Constitucional sobre Derechos Digitales 15
10.2. Tabla 2. Marco Legal Secundario sobre Derechos Digitales 19
11. Evaluación de la Legislación Interna 20
11.1. Estado de Honduras 21
11.1.1. Análisis de la Legislación Hondureña 21
11.1.2. Documentación de Casos y Denuncias 24
11.1.3. Recomendaciones y Reformas Necesarias 27
11.2. Estado de Guatemala 29
11.2.1. Análisis de la Legislación Guatemalteca 29
11.2.2. Documentación de Casos y Denuncias 31
11.2.3. Recomendaciones y Reformas Necesarias 33
11.3. Estado de El Salvador 34
11.3.1. Análisis de la Legislación Salvadoreña 34
11.3.2. Documentación de Casos y Denuncias 36

11.3.3. Recomendaciones y Reformas Necesarias 38
11.4. Estado de Nicaragua 40
11.4.1. Análisis de la Legislación Nicaragüense 40
11.4.2. Documentación de Casos y Denuncias 45
11.4.3. Recomendaciones y Reformas Necesarias 48
12. La Desinformación y Manipulación Digital en los Procesos Electorales 50
12.1. Conceptos Generales 50
12.2. Situación en Guatemala, Honduras El Salvador y Nicaragua 51
12.3. Medidas para Mitigar el Impacto de la Desinformación y Manipulación Digital 54
13. Entrevistas a Expertos en Derechos Digitales 55
13.1. Estado de Honduras 56
13.1.1. Carlos Sierra de la organización CIPRODEH 56
13.1.2. Efrén Godoy de la plataforma OSConectadas 58
13.2. Estado de Nicaragua 60
13.2.1. Experto Legal Anónimo 60
13.3. Estado de Guatemala 62
13.3.1. Alejandro Valverth de la organización LEGIS 62
13.4. Estado de El Salvador 64
13.4.1. Ismelda Villacorta de la organización FESPAD 64
14. Conclusiones 67
15. Sumario de Recomendaciones Generales y Específicas 68
15.1. Tabla 3. Recomendaciones Generales 70
15.2. Tabla 4. Recomendaciones a la Sociedad Civil y otros Actores 71
15.3. Recomendaciones por Estado 73
15.3.1. Tabla 5. Recomendaciones al Estado de Honduras 73
15.3.2. Tabla 6. Recomendaciones al Estado de Guatemala 74
15.3.3. Tabla 7. Recomendaciones al Estado de El Salvador 75
15.3.4. Tabla 8. Recomendaciones al Estado de Nicaragua 76

1. Resumen Ejecutivo

El informe presenta una revisión sobre los derechos digitales en cuatro países de Centroamérica: Honduras, Guatemala, El Salvador y Nicaragua, centrándose en analizar los marcos legislativos actuales que regulan las libertades digitales, en particular la privacidad y la libertad de expresión en el espacio digital. Se examinan tanto los marcos constitucionales como los legales secundarios, destacando sus limitaciones e inconsistencias con los estándares internacionales de derechos humanos. A través de un análisis documental y entrevistas a expertos, el informe explora el uso de la legislación como una herramienta represiva y documenta casos de violaciones contra periodistas, medios de comunicación y la sociedad civil en el entorno digital. Los hallazgos principales revelan importantes brechas en ciberseguridad, protección de datos y el uso indebido de las leyes para restringir las libertades fundamentales. Además, el informe ofrece recomendaciones para reformar las leyes vigentes, alineándolas con los estándares universales y regionales, como los del sistema interamericano y europeo, con el objetivo final de mejorar la protección de los derechos digitales en la región.

1.1. Resultados Principales

El estudio reveló importantes brechas en la protección de la privacidad y la libertad de expresión en línea en todos los países analizados. Aunque algunos de ellos cuentan con marcos legales sobre delitos informáticos y protección de datos, en general, estos son insuficientes y en ocasiones utilizados de manera represiva. Las legislaciones a menudo permiten el monitoreo estatal y la censura, afectando especialmente a periodistas, activistas y medios de comunicación independientes. Asimismo, se identificaron graves deficiencias en la ciberseguridad y la protección de datos personales, lo que aumenta la vulnerabilidad de la ciudadanía.

Los hallazgos confirman que, aunque existen legislaciones que abordan ciertos aspectos de los derechos digitales, estas no son suficientes para proteger de manera efectiva la privacidad y la libertad de expresión. Además, en muchos casos, las leyes vigentes facilitan la censura y el control estatal. Las entrevistas a expertos también reflejan una preocupación por la falta de voluntad política para reformar estas leyes en favor de la protección de derechos fundamentales.

1.2. Puntos de Acción

Se recomiendan varias acciones clave:

1. La creación de leyes nacionales de ciberseguridad y protección de datos personales alineadas con estándares internacionales;
2. La derogación de leyes represivas que vulneran derechos fundamentales, como las leyes que permiten la vigilancia masiva sin control judicial;
3. El reconocimiento del derecho a internet como un derecho humano dentro de las leyes internas; y

4. La promoción de una mayor colaboración entre gobiernos, sociedad civil y organismos internacionales para proteger los derechos digitales en la región.

2. Introducción

Se presenta el informe sobre Derechos Digitales en Honduras, Guatemala, El Salvador y Nicaragua, centrándose en revisar y analizar la legislación actual sobre el ejercicio de las libertades fundamentales en el espacio digital en Guatemala, Honduras, El Salvador y Nicaragua, identificar áreas de mejora en la protección de estos derechos y analizar el uso de la ley como instrumento represivo.

El análisis inicia con la presentación del marco metodológico, siguiendo un enfoque cualitativo y cuantitativo, combinando análisis documental y entrevistas, sin recolección de datos de campo directa. Asimismo, se presenta la situación democrática, el Estado de derecho y el autoritarismo que caracteriza a estos países por sus bajos niveles de democracia y falta de independencia judicial como garantía del Estado de derecho.

Seguidamente, se presenta el marco normativo universal, interamericano y europeo sobre la materia expuesta con el objetivo de tener un mayor entendimiento de cómo son tutelados estos derechos a nivel global, regional y en el continente europeo, este último presentando un desarrollo bastante fuerte, al contar con el Reglamento General de Protección de Datos (RGDP), la nueva Ley de Inteligencia Artificial, el Convenio Europeo sobre Ciberdelincuencia, entre otros.

En este contexto, se realiza un análisis comparativo sobre la legislación vigente. En primer lugar, se presenta el Marco Constitucional sobre derechos digitales, donde se destaca el derecho a la privacidad digital y la inviolabilidad de las comunicaciones, el derecho a la libertad de expresión en línea y el derecho de acceso a la información y la petición de información. En segundo lugar, se expone el Marco Legal Secundario, que aborda la protección de datos personales dentro de la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales de Nicaragua, así como la tipificación de delitos informáticos dentro del Código Penal y otras leyes específicas.

Este marco jurídico permite desarrollar la evaluación de la legislación actual sobre la privacidad digital y la libertad de expresión en línea en Honduras, Guatemala, El Salvador y Nicaragua. El análisis se basa en tres etapas: a) Análisis de la legislación vigente, como la Ley de Telecomunicaciones, la Ley de Acceso a la Información Pública, la Ley de Ciberdelitos, el Código Penal y otras leyes con enfoque represivo; b) Documentación de casos y denuncias sobre la falta de legislación en materia de ciberseguridad y privacidad digital, así como las arbitrariedades ejercidas contra medios de comunicación y periodistas, tanto nacionales como internacionales, en espacios digitales y redes sociales como **Facebook, X** (anterior **Twitter**), **Instagram, YouTub**e y **TikTok**; y c) Recomendaciones sobre reformas a las legislaciones existentes para proteger y promover los derechos a la libertad de expresión en línea y la privacidad digital, incluyendo normativas propuestas por organismos internacionales como la CIDH y organizaciones de la sociedad civil.

Posteriormente, se analiza la desinformación en línea y la manipulación digital en los procesos electorales, abordando conceptos generales, ejemplos de campañas de desinformación en los países en contexto y medidas para mitigar el impacto de las noticias falsas (*fake news*) en estos procesos.

En la etapa de entrevistas se desarrollan una serie de entrevistas a expertos en la materia de derechos digitales de Honduras, Guatemala, El Salvador y Nicaragua con el objetivo de obtener una perspectiva detallada y contextual dichos derechos. La dinámica de las entrevistas se basa principalmente en 5 puntos:

1) Contexto general sobre los derechos digitales;
2) Legislaciones a favor, contrarias o faltantes;
3) La privacidad digital y la libertad de expresión en línea;
4) La desinformación y manipulación digital en los procesos electorales; y
5) Reformas necesarias y recomendaciones.

En definitiva, estos aportes serán esenciales para contextualizar los hallazgos dentro de la realidad sociopolítica de cada país y ofrecer recomendaciones ajustadas a sus particularidades. Este enfoque integral permitirá no solo un diagnóstico preciso de la situación de los derechos digitales en estos países, sino también la elaboración de propuestas concretas para mejorar la protección de estos derechos en el futuro.

3. Propósito del Análisis

El presente informe se centra en analizar el ejercicio de las libertades fundamentales en el espacio digital en Centroamérica, con un enfoque específico en Guatemala, Honduras, El Salvador y Nicaragua. En una era digital creciente, la protección del ejercicio de estos derechos se ha vuelto fundamental para garantizar la privacidad, la libertad de expresión y la seguridad en línea de las y los ciudadanos. Sin embargo, la legislación en estos países varía considerablemente y, en algunos casos, las leyes se han utilizado como herramientas represivas para violar los derechos de la ciudadanía.

4. Objetivos del Análisis

4.1. Objetivo General

Revisar y analizar la legislación actual sobre el ejercicio de las libertades fundamentales en el espacio digital en Guatemala, Honduras, El Salvador y Nicaragua, identificando áreas de mejora en la protección de estos derechos y analizando el uso de la ley como instrumento represivo.

4.2. Objetivos Específicos

1. Realizar un análisis comparativo de la legislación vigente en cada uno de los países.
2. Identificar brechas legales y proponer posibles reformas necesarias.

3. Evaluar el impacto de las leyes actuales en la privacidad y la libertad en línea.
4. Identificar riesgos y vulnerabilidades en la protección del ejercicio de las libertades fundamentales en el espacio digital.
5. Recopilar y documentar casos relevantes de violaciones al ejercicio de las libertades fundamentales en el espacio digital en la región.
6. Realizar entrevistas a expertos legales y activistas para obtener una perspectiva detallada y contextual.
7. Analizar el impacto de la desinformación y la manipulación digital en los procesos electorales.

5. Hipótesis

El informe parte de la hipótesis de que, en los países analizados, las leyes relativas a derechos digitales no sólo son insuficientes para proteger la privacidad y la libertad de expresión, sino que, en muchos casos, se usan para limitar o violar estos derechos fundamentales.

6. Enfoque Metodológico

El análisis seguirá un enfoque cualitativo y cuantitativo, combinando análisis documental y entrevistas, sin recolección de datos de campo directa. Pasos del Proceso:

1. **Revisión Documental:** Compilación y análisis de la legislación vigente, informes y estudios relevantes.
2. **Análisis Comparativo:** Comparación de las leyes entre los cuatro países para identificar similitudes y diferencias.
3. **Entrevistas:** Realización de entrevistas semiestructuradas a expertos, activistas y ciudadanía afectada.
4. **Recopilación de Casos:** Documentación de casos de violaciones al ejercicio de las libertades fundamentales en el espacio digital mediante revisiones de medios y bases de datos.
5. **Análisis de Datos:** Evaluación de los datos recopilados para responder a las preguntas de investigación.
6. **Redacción del Informe:** Elaboración de un informe detallado con hallazgos, análisis y recomendaciones.

7. Preguntas y Criterios del Análisis

7.1. Preguntas del Análisis

1. ¿Cuál es la legislación que regula o restringe el derecho a la libertad de expresión o acceso a la comunicación usando las redes sociales u otras herramientas tecnológicas?

2. ¿Existen en estos países brechas significativas en la protección del ejercicio de libertades fundamentales en el espacio digital?
3. ¿De qué manera las leyes actuales afectan la privacidad y la libertad en línea de las y los ciudadanos?
4. ¿Qué casos de violaciones al ejercicio de las libertades fundamentales en el espacio digital han sido documentados en la región?
5. ¿Cómo se están utilizando las leyes como instrumentos represivos?
6. ¿Qué reformas podrían fortalecer la protección del ejercicio de las libertades fundamentales en el espacio digital?
7. ¿Qué patrones y tendencias se pueden identificar en las violaciones al ejercicio de libertades fundamentales en el espacio digital?
8. ¿Cómo afecta la desinformación digital a los procesos electorales en estos países?
9. ¿Existen ejemplos de campañas de desinformación con fines electorales?
10. ¿Qué medidas pueden implementarse para mitigar el impacto de la desinformación en elecciones?

8. Situación Democrática y Estado de Derecho

Se presenta un panorama bastante crítico para los Estados centroamericanos debido a la falta de regulación en lo que respecta a los derechos digitales, las tendencias de autoritarismo y los obstáculos democráticos que se fundamentan en un control estatal de la información. Asimismo, se evidencia el control de las telecomunicaciones, la represión de la disidencia, denuncias y casos de restricción a la libertad de expresión en línea y las violaciones a la integridad personal de los periodistas y usuarios informáticos.

Estudios evaluativos sobre derechos civiles y políticos, Estado de derecho, democracia y acceso a la información en Guatemala, El Salvador y Honduras, detallan que estos países presentan un nivel parcial de apertura gubernamental y puntuaciones bajas en cuanto a derechos civiles y políticos, democracia y Estado de derecho. [1] Por su parte, Nicaragua presenta una situación muy crítica para su ciudadanía, dado que, se considera un Estado sin garantías a los derechos políticos y civiles, y obtiene una calificación muy baja en el índice de Estado de derecho, democracia y libertad de expresión.

En ese contexto, este tipo de estudios nos permiten tener un entendimiento de la situación actual de los países de la región al evidenciarse una baja evaluación de apertura gubernamental, bajos índices de Estado de derecho y por ende falta de independencia judicial, la garantía de separación de poderes, índices bajos de democracia y derechos humanos y una fuerte debilidad institucional, lo que conlleva a la creación de marcos legales represivos y en contra de derechos fundamentales como la libertad de expresión aplicable en el entorno digital.

[1] Estrada Vargas, E. (2024). "Evaluación de la apertura gubernamental mediante el concepto de gobierno abierto: el caso de Honduras". *Revista Política Austral Vol. 3. N. 1.*

Human Rights Watch organización encargada de monitoreo constante de derechos humanos en la región advierte sobre el autoritarismo en Guatemala, Honduras, El Salvador y Nicaragua.[2] Señalan que los países centroamericanos "se están cayendo como fichas de dominó en el autoritarismo". El presidente de Nicaragua Daniel Ortega ha intensificado su represión contra opositores políticos, periodistas y defensores de derechos humanos. En El Salvador el Poder Judicial ha sufrido un ataque sin precedentes, en donde, se reemplazaron a todos los jueces de la Corte Suprema de Justicia, Fiscal General y Fiscal Adjunto, y se votó a favor de permitir que el presidente Bukele se presentará a su segundo mandato aun cuando la Constitución lo prohíbe a través de un artículo pétreo.

De igual forma, ocurrió en Honduras, donde el expresidente Hernández que hoy guarda prisión por delitos de narcotráfico en una cárcel de Estados Unidos, expulsó a 4 magistrados de la Sala Constitucional de la Corte Suprema de Justicia y posterior a ello los magistrados ilegítimamente impuestos brindaron su interpretación favorable a la reelección presidencial a pesar de estar prohibida por el artículo 41 (pétreo) de la Constitución.[3] Guatemala también presenta intentos de socavar la independencia judicial al destituir al jefe de la Fiscalía Especial que investigaba al exmandatario Giammattei y otros funcionarios de alto nivel, sumado a la injerencia en el proceso electoral de 2023.[4]

Dentro de ese marco, Steven Levitsky un reconocido profesor de la prestigiosa Universidad de Harvard autor de “Cómo Mueren las Democracias” afirma que en Centroamérica y en general en América Latina “los gobiernos elegidos con los mecanismos de la democracia son los que a veces tumban la democracia”.[5] Se trata de Estados débiles resultando complejo implementar políticas públicas en favor de la ciudadanía, controlar la corrupción, mantener la seguridad pública y con ello resulta difícil gobernar. Además, Levitsky resalta que “la democracia se muere a través de gobiernos electos siendo importante poder identificar a los autoritarios potenciales antes de que sean elegidos”.[6]

En definitiva, podemos deducir los desafíos que presenta Guatemala, Honduras, El Salvador y Nicaragua, enfrentándose con democracias desafiadas,[7] la ausencia del Estado de derecho e independencia judicial y la presencia de leyes y normativas contrarias a los derechos fundamentales como la libertad de expresión, privacidad, libertad de prensa, entre otros.

---

[2] Vivanco, M. (2021). “The rule of law is disintegrating in Central America”, *Human Rights Watch*.
[3] Caso Gutiérrez Navas y otros Vs. Honduras. Fondo, Reparaciones y Costas. Sentencia de 29 de noviembre de 2023. En este caso la Corte Interamericana fallo a favor de los 4 magistrados destituidos ilegítimamente por el Congreso Nacional en 2014.
[4] *Ibid., supra* nota 2.
[5] Levitsky, S. & Ziblatt, D. (2018). “How Democracy Dies”. *Penguin Random House UK.*
[6] Roura, A. (2021). “Steven Levitsky: En América Latina son gobiernos elegidos con los mecanismos de la democracia los que a veces tumban la democracia”. *Reportaje de BCC News Mundo*.
[7] Morales Antoniazzi, M. et al. (2024). “América Central. El Derecho ante Democracias Desafiadas”. *Instituto de Estudios Constitucionales del Estado de Querétaro y el Instituto Max Planck de Derecho Público Comparado.*

9. Marco Normativo Internacional sobre Derechos Digitales

El marco normativo universal, interamericano y europeo sobre derechos digitales está compuesto por una serie de tratados, declaraciones, directrices e informes de instituciones jurídicas y organismos internacionales con el propósito de proteger, garantizar y promover los derechos humanos fundamentales en el entorno digital, en otras palabras, se busca la digitalización de los derechos "pasando a los derechos de siempre por el tamiz de las características del mundo digital".[8]

9.1. Marco Normativo Universal

Dentro del **marco universal de protección de derechos humanos** se presenta la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos bajo la protección a la privacidad, la libertad de opinión y de expresión, esenciales en el entorno digital. Asimismo, se dispone de diversas Resoluciones de las Naciones Unidas sobre el derecho en la era digital que fomentan, protegen y disfrutan de los derechos humanos en la internet, con el objetivo de fomentar, proteger y disfrutar de los derechos humanos en internet. Además, de Convención sobre los Derechos del Niño que incluye protecciones para los derechos de los niños en el entorno digital, la privacidad y acceso a la información, entre otras.

Ante este panorama, según Secretaría General de las Naciones Unidas es necesario que los Estados creen una protección eficaz sobre datos personales y la protección del derecho a la privacidad de conformidad con las normas internacionales. A su vez, es necesario que las leyes y prácticas nacionales se basen en los derechos humanos para la protección de la privacidad de datos, incluidos los mecanismos de aplicación de ley, con revisión judicial o autoridades encargadas de su protección independientes y con la total imparcialidad. Además, los Gobiernos están en la obligación de aportar con los recursos para que estos mecanismos funcionen y puedan abordar el uso de datos por parte de empresas privadas o Gobiernos.[9]

Ahondado a ello, el derecho de acceso a la Internet es reconocido por las Naciones Unidas como un derecho fundamental debiendo ser garantizando a través de la conectividad,[10] el acceso a la infraestructura y a los servicios tecnológicos y comunicaciones, de manera económicamente accesible y de una calidad adecuada.

9.2. Marco Normativo Interamericano y Regional

En el **contexto del derecho interamericano**, la protección de los derechos digitales se enmarca en los mecanismos y tratados promovidos por la OEA por medio del Comité Jurídico Interamericano, la Comisión Interamericana de Derechos Humanos (CIDH) a través de la relatoría

[8] Martínez-Villalba J. (2014). "La Cuarta Ola de Derechos Humanos: Los Derechos Digitales". *Revista Latinoamericana de Derechos Humanos, Vol. 25, 1*, p.19.
[9] Departamento de Comunicaciones Globales, (2020). "Roadmap for Digital Cooperation". *Report of the Secretary General of the United Nations.*
[10] Asamblea General de las Naciones Unidas y su Consejo de Derechos Humanos (2016). Promoción, protección y disfrute de los derechos humanos en Internet.

para la Libertad de Expresión y la Corte Interamericana (Corte IDH) por medio de sus casos contenciosos, como ser: *Claude Reyes vs. Chile* y *José Alvear Restrepo "Cajar" vs. Colombia*.[11]

En esa misma línea, la Convención Americana de Derechos Humanos (CADH) garantiza derechos fundamentales en el espacio digitales, dentro de ellos se encuentran, la libertad de expresión (Art. 13) y el derecho a la privacidad (Art. 11). Asimismo, con el objetivo de promover el desarrollo progresivo de estos derechos y la codificación del derecho internacional, la OEA creó la Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública y Principios Actualizados sobre la Privacidad y la Protección de Datos Personales.[12]

Sumado a ello, se presenta la Carta Iberoamericana de Principios y Derechos en Entornos Digitales, aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno de 2023.

Por su parte, la Corte IDH ha destacado de manera consistente la importancia del derecho a la libertad de expresión como piedra angular en la existencia misma de la sociedad, con ello sostiene:

> La libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública. Es también condición *sine qua non* para que los partidos políticos, los sindicatos, las sociedades científicas y culturales, y en general, quien desee influir sobre la colectividad puedan desarrollarse plenamente. Es, en fin, condición para que la comunidad, a la hora de ejercer sus opiniones, esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no está bien informada no es plenamente libre.[13]

Asimismo, el Tribunal Interamericano se ha expresado en el caso *Artavia Murillo y otros vs. Costa Rica*,[14] en relación con la privacidad pudiéndose extender en el entorno digital, de la siguiente forma:

> La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus

[11] Corte IDH. Caso Claude Reyes y otros Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 19 de septiembre de 2006. Serie C No. 151 y Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506.

[12] Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la OEA. Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública y Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano.

[13] Corte IDH. La Colegiación Obligatoria de Periodistas, Opinión Consultiva OC-5/85, 13 de noviembre de 1985, párr. 70.

[14] Corte IDH. Caso Artavia Murillo y otros (Fecundación in Vitro) Vs. Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2012. Serie C No. 257. Párr. 143.

> propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona.

Dentro de ese orden, se menciona que el acceso a la internet constituye una "condición *sine qua non* para el ejercicio efectivo de los derechos humanos hoy en día, incluyendo particularmente los derechos a la libertad de expresión y de opinión", así como, "el pluralismo y la diversidad como condiciones esenciales del proceso de deliberación pública y del ejercicio de la libertad de expresión deben ser preservados en el entorno digital".[15] Con ello, la CIDH reconoce que este derecho está fuertemente ligado a libertad de expresión, por lo que al no asegurar su accesibilidad se estarían negando derechos constitucionales.

Por su parte, el Parlamento Centroamericano (PARLACEN) conformado por Guatemala, Honduras, El Salvador, Nicaragua República Dominica y Panamá presenta una propuesta Ley Marco de Prevención y Protección contra la Ciberdelincuencia en los Países miembros del Sistema de Integración Centroamericano (SICA).[16] El objetivo de la propuesta es el de regular el marco normativo sobre ciberdelitos mediante la creación de figuras delictivas, la adecuación de normas penales y reglas procesales.

Sin embargo, organizaciones hondureñas denuncian que dicha propuesta de ley es similar a la Ley Especial de Ciberdelitos de Nicaragua al proponer la interceptación de las comunicaciones en su espectro electromagnético, así como, de facultar a las autoridades correspondientes el registro u secuestro de medios digitales o electrónicos y un control casi total sobre los operadores del servicio de las telecomunicaciones. Además, de ser inspirada por marcos normativas de países como Rusia y China.[17]

9.3. Marco Normativo Europeo

En el ámbito de la **Unión Europea** (UE, en adelante) se cuenta con una serie de reglamentos, y directrices para la protección y promoción de los derechos digitales en sus diferentes ámbitos con el objetivo de crear un espacio digital seguro que proteja derechos fundamentales de los usuarios de servicios digitales y el establecimiento de una competencia equitativa para el fomento de la innovación, crecimiento y competitividad,[18] dentro de ellas se encuentran:

---

[15] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 15.

[16] Resolución AP/1-359/2024 sobre la Ley Marco de Prevención y Protección contra la Ciberdelincuencia en los Países Miembros del SICA.

[17] Contracorriente (2024). "El SICA promueve una ley de Ciberdelitos en Centroamérica, similar a la de los Ortega-Murillo en Nicaragua". *Contracorriente.red*, ver en: https://contracorriente.red/2024/10/02/el-sica-promueve-una-ley-de-ciberdelitos-en-centroamerica-similar-a-la-de-los-ortega-murillo-en-nicaragua/

[18] Fahey, E. (2022). "The EU as a global digital actor: institutionalising global data protection, trade, and cybersecurity". *Oxford: Hart.*

1. El Reglamento General de Protección de Datos (RGPD);
2. La Declaración Europea sobre Derechos y Principios Digitales;
3. La nueva Ley de Inteligencia Artificial (Ley de IA);
4. El Convenio Europeo sobre Ciberdelincuencia;
5. Ley de Servicios Digitales (Digital Services Act); y
6. Ley de Mercados Digitales (Digital Market Act).

Países como Italia y España destacan por su tutela y promoción de los derechos digitales. Por ejemplo, Italia incluye el derecho a la ciudadanía digital, a la identidad digital, y a la privacidad dentro de su legislación interna. [19] Mientras tanto, España ha aprobado la **Carta de Derechos Digitales**, que busca proteger la identidad, la ciberseguridad, la accesibilidad, y otros derechos relacionados con el entorno digital.[20]

Estonia, un líder mundial en derechos digitales, ha desarrollado una amplia gama de leyes que incluyen la **Ley de Protección de Datos Personales (PDPA)**, la **Ley de Firmas Digitales**, **Ley de Información Pública (PIA)** y la **Ley de Comunicaciones Electrónicas (ECA)**, que permiten un ecosistema digital (*e-government*) avanzado y protegido.[21]

En el año 2000 se presenta la nueva **Ley de Telecomunicaciones** añadiendo el derecho de acceso al servicio de internet disponible universalmente para todos los suscriptores, independientemente de su ubicación geográfica y a un precio uniforme, esto le ha permitido a Estonia desarrollar un ecosistema digital de derechos que hoy en día lo que convierten en un líder en la materia sin limitaciones de acceso y uso del servicio a internet.[22]

El **Reglamento General de Protección de Datos (RGPD)** de la UE, abarca principios relativos al tratamiento de datos personales, tales como: la licitud, lealtad y transparencia, limitación de la finalidad, exactitud, limitación del plazo de conservación, integridad y confidencialidad y minimización de datos. También, contempla los derechos del titular: Acceso, Rectificación, Cancelación y Oposición (ARCO).[23]

En esa misma línea, el reglamento consagra derechos nuevos como el derecho al olvido, donde cualquier persona puede solicitar la supresión de datos; el derecho a la limitación del tratamiento, donde los datos personales puedan ser conservados; derecho a la portabilidad, en la que se puedan

[19] Agenzia per l'Italia Digitale (AGID) (2002). "Guida dei Diritti di Cittadinanza Digitali. D. Lgs. N. 82/2005, Art. 17, comma 1-quinquies".
[20] Gobierno de España. Carta de Derechos Digitales, Plan de Recuperación, Transformación y Resiliencia.
[21] Vassil K. (2016). "Estonian e-Government Ecosystem: Foundation, Applications, Outcomes". *World Development Report.*
[22] Estonia Freedom on the Net (2023). "Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union". *Freedom House.*
[23] Creative Commons (2016). "El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos". *ADC Digital.*

recibir datos personales; derecho a la oposición y marketing directo; y el derecho a toda persona de no ser objeto de una decisión basada únicamente en el tratamiento automatizado.[24]

Adicionalmente, contempla de un mecanismo para la aplicación y cumplimiento (*enforcement*) abordado en 4 aspectos:

a) la autoridad de aplicación y contralor,
b) las sanciones,
c) las acciones y recursos, y
d) la compensación.

Asimismo, el reglamento europeo establece una autoridad para llevar a cabo su aplicación y control, sanciones, acciones y recursos y compensación.[25]

En resumen, el marco normativo universal, interamericano y europeo ofrece una guía clara sobre cómo se deben proteger los derechos fundamentales en el entorno digital. Países como Italia, España y Estonia proporcionan ejemplos útiles para comparar las brechas legales en los países centroamericanos que están en análisis.

10. Análisis Comparativo de la Legislación Vigente

En la región de Centroamérica, la legislación sobre derechos digitales vigente en los países de Guatemala, El Salvador, Honduras y Nicaragua presenta tanto similitudes como diferencias significativas en diversos aspectos del derecho. Estos cuatro países, aunque comparten una historia y cultura común, han desarrollado sus propios marcos legales que reflejan sus contextos políticos, económicos y sociales.[26] El análisis comparativo de la legislación es esencial para entender cómo abordan temas claves como la extensión de los derechos fundamentales en al ámbito digital y cómo se garantiza su acceso y promoción. Asimismo, se examina la situación de los derechos digitales en estos cuatro Estados, abarcando derechos fundamentales como la privacidad, los datos personales la libertad de expresión, el acceso a la información y de petición de información.

Se presenta el marco legal sobre derechos digitales en Guatemala, Honduras, El Salvador y Nicaragua a través de dos cuadros comparativos de la siguiente manera: a) Marco constitucional en donde exponen los derechos fundamentales anteriormente mencionados; y b) Marco legal secundario, que incluyen: las legislaciones sobre datos personales, privacidad y la tipificación de los delitos informáticos y conexos.

A continuación, se expone el Marco Constitucional sobre los derechos fundamentales en el entorno digital:

[24] *Ibid., supra* nota 23.
[25] *Ibid., supra* nota 23.
[26] Urtecho Garcés J. (2021) "¿Existe un *Ius Constitutionale Commune* en Centroamérica?". *Dialnet, e-Archivo.*

10.1. Tabla 1. Marco Constitucional sobre Derechos Digitales[27]

Derechos consagrados	Guatemala	Honduras	El Salvador	Nicaragua
Derecho a la Privacidad Digital[28] y la Inviolabilidad de las Comunicaciones	**Art. 24:** inviolabilidad correspondencia, documentos o libros y se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros de la tecnología moderna.	**Art. 76:** derecho a al honor, la intimidad personal, familiar y a la propia imagen. **Art. 100:** el 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. 26:** **A)** derecho a la vida privada; **B)** la inviolabilidad del domicilio, correspondencia y comunicaciones, y **C)** respeto de la honra y reputación.
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 gubernamental alguna.	**Art. 72:** libre emisión del pensamiento por cualquier medio de difusión, sin previa censura; **Art. 73:** libertad de prensa; y **Art: 74:** no restricción del derecho.	**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 su pensamiento en público o en privado y por cualquier medio.
Derecho de Acceso a la Información y Petición de la Información	**Art. 31:** derecho de conocer archivos, fichas o cualquier otra forma de registros estatales. **Art. 28:** derecho a dirigir, individual o colectivamente, peticiones a la autoridad, la que está obligada a tramitarlas.	Derecho de acceso a la información se deriva de los **Arts. 72, 73 y 74.** **Art. 182:** garantía constitucional de Hábeas Data. **Art. 80:** presentar peticiones a las autoridades por motivos de interés particular o general.	Derecho de acceso a la información no se encuentra explícitamente presente, pero se deriva los **Arts. 6 y 18.** **Art. 18:** derecho a dirigir peticiones por escrito a las autoridades.	**Art. 66:** derecho a la información sin censura; **Art. 67:** derecho de informar, buscar, recibir y difundir información, sin censura; y **Art. 68:** acceso a los medios de comunicación. **Art. 45:** Garantía de Hábeas Data. **Art. 52:** derecho de hacer peticiones, denuncias y críticas, a autoridades del Estado.

Elaboración propia. Julio de 2024.

[27] Constitución Política de Guatemala, 1985; Constitución de la República de Honduras, 1982; Constitución de la República de El Salvador; y Constitución Política de la República de Nicaragua, 1986.
[28] 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.*

En Tabla 1. se presenta el marco constitucional sobre derechos digitales en lo relevante al derecho a la privacidad digital, la libertad de expresión en línea, y de acceso y petición de información. Con ello, se puede observar que todos los Estados cuentan explícitamente o bien implícitamente con el debido respaldo de estos derechos fundamentales dentro de las disposiciones constitucionales. Lo que permite formar la base sobre la cual se desarrollan leyes específicas y regulaciones para proteger y promover los derechos digitales en Guatemala, Honduras, El Salvador y Nicaragua.

No obstante, Guatemala no protege explícitamente el derecho a la privacidad dentro su Carta Magna, por ello, la Corte de Constitucionalidad de Guatemala se expresa en relación a este derecho según el expediente 863-2011 de la siguiente forma:

> Existen otros derechos que por vía de la incorporación autorizada en el artículo 44 de la Carta Magna o de la recepción que también autoriza el artículo 46 del Texto Matriz, también pueden ser objeto de protección, atendiendo, como se dijo, a su carácter de inherentes a la persona humana, aun y cuando no figuren expresamente en este último texto normativo […] aquellos relacionados a la intimidad, al honor y a la privacidad, los cuales, en su conjunto, también garantizan la existencia y goce de otro derecho.[29]

En Honduras, se hace una reforma constitucional en el año 2013 al artículo 182, en donde, se reconoce la garantía constitucional del Hábeas Data, en la que toda persona tiene derecho de acceso a la información en el ámbito público o privado y en caso de que fuere necesario, "actualizarla, rectificarla y/o suprimirla".[30] Asimismo, en 2013 la Asamblea Nacional de Nicaragua aprueba la reforma de la Ley de Amparo, agregándose el recurso de Hábeas Data y se expande su protección en la Ley de Justicia Constitucional Ley N. 983.[31]

Por su parte, El Salvador, no cuenta explícitamente con el derecho de acceso a la información en su marco constitucional, pero es derivado de los artículos 6 y 18 de su Constitución y es ampliado con su Ley de Acceso a la Información Pública.[32] También, la Sala de lo Constitucional de ese Estado (Amparo 142-2012),[33] determina que el derecho a la autodeterminación informativa se considera un derecho fundamental, autónomo, de carácter constitucional y con protección por vía del amparo en sede constitucional.

En noviembre de 2024, se presenta una iniciativa de ley sobre una reforma "parcial" de la Constitución Política de Nicaragua presentada por el Poder Ejecutivo.[34] Según la actual Carta

[29] Sentencia Nº 863-2011 de Corte de la Constitucionalidad de Guatemala, 21 de junio de 2011.
[30] Reforma Constitucional, Decreto N. 237-2012. Sin embargo, el conocimiento de este recurso se enfoca exclusivamente a la Sala de lo Constitucional de la Corte Suprema de Justicia de Honduras, por lo que limita el acceso a la población general al acceso a la interposición de este recurso.
[31] Ley de Justicia Constitucional Ley N. 983, aprobada el 11 de diciembre de 2018.
[32] López J. "Cuestionario: Legislación y Mejores Prácticas sobre Acceso a la Información Pública". *Red Probidad*.
[33] Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador. Amparo 142-2012.
[34] Yader Morazán (2024), ver en: https://www.infobae.com/america/america-latina/2024/11/23/diez-reformas-a-la-constitucion-de-nicaragua-que-ordeno-el-dictador-ortega-para-cumplir-las-ambiciones-de-rosario-murillo/.

Magna bajo sus artículos 191 al 196, se faculta a la Asamblea Nacional (congreso) para reformar parcialmente la Constitución y la misma deberá ser enviada a una comisión especial para su dictaminación en un plazo no mayor de sesenta días, posteriormente debiendo ser discutida en dos legislaturas y requerir el voto favorable del sesenta por ciento de los diputados.[35]

Se desglosan las enmiendas relacionadas con los derechos a la privacidad, libertad de expresión y de acceso y petición de la información de la siguiente manera:

a) **Derecho a la privacidad digital y la inviolabilidad de las comunicaciones** se presenta bajo su nuevo **artículo 24** (5) "toda persona tiene derecho a su vida privada y a la privacidad de su familia", (6) "al respeto de su honra y reputación, (8) "a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo".
b) **Libertad de expresión en línea** se presenta bajo **artículo 27** "los nicaragüenses tienen derecho a expresar libremente su pensamiento en público o en privado, siempre y cuando no trasgreda el derecho de otra persona, de la comunidad y los principios de seguridad, paz y bienestar establecidos en la Constitución".
c) **Derecho de Acceso a la información** bajo **artículo 66** "los y las nicaragüenses tienen derecho a la información veraz. Este derecho comprende la libertad de buscar, recibir y difundir ideas e información por cualquier medio, sin atentar contra los Principios Fundamentales contemplados en esta Constitución", **artículo 67** "el derecho de informar es una responsabilidad social y se ejerce con estricto respeto a los Principios Fundamentales establecidos en la Constitución", y **artículo 68** "el estado vigilará que los medios de comunicación social no sean sometidos a intereses extranjeros ni divulguen noticias falsas que atenten contra los derechos del Pueblo".
d) Se deroga completamente el derecho de **petición de la información** establecido anteriormente en el **artículo 52**.
e) **Recurso Hábeas Data** se presenta bajo **artículo 46 bis y artículo 190** como garantía constitucional "el Recurso de Hábeas Data, como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos [...] de naturaleza pública o privada".

Las enmiendas presentadas ejercen restricciones a los derechos fundamentales y abren paso a la vigilancia e injerencia estatal por parte de los medios de comunicación de Nicaragua otorgando una mayor discrecionalidad sobre el acceso y uso de la información a su ente regulador, lo que

La reforma fue aprobada en su primera legislatura en solamente 3 días debiendo ser aprobada bajo segunda legislatura en enero de 2025, asimismo, según expertos legales nicaragüenses la reforma es de carácter total, dado que, se derogan 38 artículos y se reforman o sustituyen otros 143 artículos de los 198 que tendría la nueva Constitución.

[35] Iniciativa de Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua, 19 de noviembre de 2024. Se reforma completamente los principios, derechos, deberes y garantías de las y los ciudadanos, a su vez, presenta la subordinación de los poderes del Estado al mandato ejecutivo, considerándose como una reforma total, la misma debería ser aprobada por una Asamblea Nacional Constituyente como indica el artículo 193.

conlleva a una mayor censura estatal en detrimento del derecho a la libertad de expresión, la privacidad digital y la inviolabilidad de las comunicaciones.

A continuación, se presenta un cuadro comparativo sobre el marco legal secundario y otras normativas concernientes a la extensión de los derechos fundamentales en el ámbito digital.

10.2. Tabla 2. Marco Legal Secundario sobre Derechos Digitales

Marco Legal	Guatemala	Honduras	El Salvador	Nicaragua
La Protección de Datos Personales	**Ley de Acceso a la Información Pública,** **Art: 30,** Hábeas Data **Art.31:** Consentimiento **Art. 32:** Excepción **Art. 33:** Acceso **Art. 34:** Tratamiento **Art. 35:** Denegación *****Manejo de datos personales sólo en el ámbito de registros públicos o estatales.	**Ley de Transparencia y Acceso a la Información Pública,** **Art. 23:** Se reconoce la garantía de Hábeas Data; **Art: 24:** Sistematización de archivos personales y su acceso; y **Art. 25:** Prohibición de entrega de información de datos personales.	**Ley de Acceso a la Información Pública, Capítulo I,** **Arts. 31-39:** regulan el derecho a la protección de datos personales ***** únicamente recae dentro del contexto gubernamental y entidades públicas.	**Ley de Protección de Datos Personales y su Reglamento**, la ley consta de **9 capítulos**, además de la institucionalización de un Ente para su regulación. **Art. 3, B del Reglamento:** Los derechos del titular: de acceso, rectificación, oposición y cancelación de datos personales (ARCO).
Tipificación del Delito Informático	**Código Penal** **Art. 274 (A-G),** regula los delitos informáticos en donde se prevé la alteración, destrucción, manipulación, de registros o programas informáticos y el uso de información y utilización de programas destructivos.	**Código Penal de 2019** **Art. 398:** acceso no autorizado a sistemas informáticos; **Art. 399:** daños a datos y sistemas informáticos; **Art. 400:** abuso de dispositivos; **Art. 401:** suplantación de identidad.	**Ley contra Delitos Informáticos y Conexos** **Cap. 1:** Delitos contra los sistemas tecnológicos de información; **Cap. 2-3**: Delitos informáticos, relacionados con contenido de datos y contra grupos vulnerables; **Cap. 5** Delito contra el orden económico.	**Ley Especial de Ciberdelitos,** **Art. 1:** la ley tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías.

Elaboración propia. Julio de 2024.

En Tabla 2. Se presenta el marco legal secundario sobre la protección de datos personales en el entorno digital vinculada a la ciberseguridad y la privacidad digital. Asimismo, se presenta la tipificación de los delitos informáticos y conexos dentro de las legislaciones actuales, aunque si bien es cierto algunas se encuentran en desarrollo y por ende se presenta un vacío legal dentro de las mismas.

En cuanto al derecho a la protección de datos personales el único país que cuenta con una legislación adecuada es Nicaragua al contar con la Ley de Protección de Datos Personales y que protege los derechos fundamentales de acceso, rectificación, corrección y oposición, comúnmente conocidos como derechos ARCO, además de contar con un reglamento para lograr su desarrollo y aplicación. En Honduras, la protección de datos personales y de acceso a la información recae en la Ley de Transparencia y de Acceso a la Información Pública aplicable también a entidades no gubernamentales.

En Guatemala su protección recae en el marco constitucional seguido por la opinión emitida por la Corte de Constitucionalidad en relación al derecho de la privacidad en la era digital, según el expediente 863-2011 que menciona que "obtención de datos personales que puedan formar una base de datos, susceptible de transmisión por medios de comunicación masiva o electrónica por medio de la informática debería ser regulado por ley. En Guatemala no existe tal regulación y debe incurrir en situaciones *legibus solutus* [...]" y sobre su tutela judicial se menciona recae en la Ley de Acceso a la Información Pública "a fin de positivar aquellos derechos de corregir, actualizar, rectificar, suprimir o mantener en confidencialidad información o datos que tengan carácter personal".[36]

En El Salvador, su protección recae en los procesos de amparo 934-2007 y 142-2012 que han desarrollado el derecho a la autodeterminación informativa como una manifestación del libre desarrollo de la personalidad y la dignidad, en esa misma capacidad de decidir en los asuntos de su vida privada. Se amplia con una "doble acepción de libertad y control sobre los datos, sin limitación sobre el tipo de datos tratados, desarrollando dos facetas: (i) un material –preventiva–, relacionada con la libertad y la autonomía del individuo con relación a sus datos personales; y (ii) otra instrumental –de protección y reparación–, referida al control que la resguarda y restablece ante restricciones arbitrarias".[37]

De conformidad, Honduras, Guatemala y El Salvador presentan un claro vacío legal sobre la protección de datos personales en el espacio digital para las y los ciudadanos, lo que pone en riesgo la privacidad digital y la libertad de expresión en línea.

Nicaragua por su parte crea en el año 2012 un reglamento a Ley de Datos Personales con el fin de lograr su desarrollo y efectivo cumplimiento. No obstante, no se ha implementado a claridad dicha ley ni se ha formalizado su mandato institucional con la creación de la Dirección de Datos Personales (DIPRODAP).

En cuanto a la tipificación de los delitos informáticos y conexos vemos que Nicaragua y El Salvador cuentan con leyes para la regulación de los sistemas informáticos y las tecnologías de la información, a pesar de las constantes críticas al demostrar que dichas normativas violentan el derecho a la libertad en línea. Guatemala y Honduras recaen en sus Códigos Penales al no contar con normativas específicas de regulación.

11. Evaluación de la Legislación Interna

En este apartado, se procede a la evaluación de la legislación interna sobre la privacidad digital y la libertad de expresión en línea en Honduras, Guatemala, El Salvador y Nicaragua. Este análisis se desarrolla en tres etapas:

[36] COPREDEH (2014). "Resolución 68/167. El Derecho a la Privacidad Digital en la era Digital". *Comisión Presidencial Coordinadora de la Política del Ejecutivo en materia de Derechos Humanos*.
[37] Consortium Legal. "Preguntas y respuestas sobre protección de datos en Centroamérica".

1. **Análisis de la legislación vigente**: Se evalúan las leyes actuales, tales como la Ley de Telecomunicaciones, la Ley de Acceso a la Información Pública, la Ley de Ciberdelitos, el Código Penal, la Ley de Intervención a las Telecomunicaciones, así como leyes con base represiva y las iniciativas de ley presentadas en la última década.
2. **Documentación de casos y denuncias**: Se recogen casos y denuncias sobre la falta de legislación en materia de ciberseguridad y privacidad digital, así como arbitrariedades cometidas contra los medios de comunicación, periodistas nacionales e internacionales, dentro de los espacios digitales y redes sociales como **Facebook, X, Twitter**, **Instagram, YouTube** y **TikTok**.
3. **Recomendaciones**: Se presentan recomendaciones sobre reformas legislativas para proteger y promover los derechos de libertad de expresión en línea y privacidad digital, basadas en propuestas de organismos internacionales como la CIDH, Corte Interamericana, *Freedom House*, y miembros de la sociedad civil.

11.1. Estado de Honduras

11.1.1. Análisis de la Legislación Hondureña

El panorama en Honduras en cuanto a privacidad digital y libertad en línea es crítico. Aunque el país cuenta con algunas leyes en esta materia, muchas de ellas no cumplen con los estándares internacionales de protección de derechos humanos y están orientadas hacia la censura y el control estatal. Además, no se cuenta con una ley integral de protección de datos personales en el entorno digital ni ciberseguridad, dejando a las y los ciudadanos vulnerables a la explotación y uso inadecuado de sus datos.[38]

La **Ley Marco de Telecomunicaciones de Honduras** de 1995 (reformas en 2011 y 2013) creada ante el desarrollo de las Tecnologías de la Información (TIC) da vida al órgano regulador de la ciberseguridad y privacidad digital del Estado, la Comisión Nacional de Telecomunicaciones (CONATEL), encargada de supervisar el sector de las telecomunicaciones en su búsqueda del desarrollo e implementación de las TIC en el país y mantiene el Instituto Hondureño de Ciencia, Tecnología y la Innovación (IHCIETI) para la promoción de las TIC. Asimismo, Honduras cuenta con una Fiscalía Especial de Protección a la Propiedad Industrial y Seguridad Informática (FEPROSI), encargada de realizar investigaciones y formular cargos a quienes se presuman hayan quebrantado la ley penal.[39]

También, mediante el Decreto **PCM-111-2020 sobre el Reglamento de Gobierno Electrónico** se crea la Secretaría de Estado en el Despacho de Transparencia y se le adscribe la Dirección de Gobierno Digital como una de sus dependencias en la que funcionan dos unidades: Unidad de

[38] Honduras y Nicaragua son los países con el mayor riesgo de sufrir un ciberataque a nivel mundial sólo por detrás de Estados como Afganistán, Birmania y Namibia, ver en: https://www.revistaeyn.com/tecnologia-cultura-digital/honduras-y-nicaragua-entre-los-paises-con-mayor-riesgo-en-ciberseguridad-mundial-EA13468963.
[39] Ministerio Público de Honduras. (FE-PROSI) Fiscalía Especial de Propiedad Intelectual y Seguridad Informática.

Simplificación y Gobierno Digital y la Unidad de Innovación Pública teniendo como objetivo la transformación digital del sector público, aunque actualmente no se presenta un acceso a su sitio web oficial.[40] Posterior a ello bajo **Decreto PCM-021-2021**, se establecen los principios que regirán el proceso administrativo digital.[41]

Debe señalarse que el gobierno de la actual presidenta Xiomara Castro promueve normativas sobre un Gobierno Electrónico por medio de la **Dirección de Gobierno Digital** de la Secretaría de Transparencia y **Despacho de Prioridades Presidenciales e Innovación Pública**,[42] sin embargo, no se encuentra mucha información sobre las labores que realizan ni de su financiación.[43] También, cuenta con un plan de acción 2023-2025 de la Alianza de Gobierno Abierto que promueve una Política Nacional de Datos Abiertos, entre otras acciones.[44]

Dentro de ese orden, el Gobierno de Honduras crea la **Dirección General de Información y Prensa** por **Decreto PCM-023-2022** convirtiéndose en un órgano de la Administración Central comenzando a operar en el año 2023 con la finalidad de realizar acciones del Gobierno en materia de información y comunicación y con funciones como la realización de manera permanentes monitoreos y diagnóstico de todos los medios de comunicación convencionales, también, sobre las redes sociales que operan en el país y el monitoreo sobre las noticias referidas a las acciones del Gobierno, expuestas en los medios de comunicación a nivel internacional y nacional, además, de coordinar con las autoridades de CONATEL el inventario de las radioemisoras, televisoras, periódicos impresos y digitales, y todo contenido manejado en redes sociales.[45]

En esa misma línea, el nuevo **Código Penal hondureño** en su título XXII establece los delitos relativos a la seguridad de las redes y los sistemas informáticos, artículo 398 sobre acceso no autorizado a sistemas informáticos, artículo 399 sobre daños a datos y sistemas informáticos, artículo 400 sobre abuso de dispositivos y artículo 401 sobre la suplantación de identidad. Sin embargo, a nivel de denuncia solo se cuenta con una **Unidad de Investigación de Delitos Cibernéticos** en la ciudad de Tegucigalpa las demás postas policiales o unidades de denuncia no cuentan con la capacitación requerida y por ende imposibilita su abordaje. En cuanto a la tipificación del delito de acuerdo con el **Código Procesal Penal** la responsabilidad recae en los fiscales, aunque si los delitos no se encuentran en el Código Penal no se puede avanzar en el proceso judicial.[46]

---

[40] Sitio web de gobierno digital, sin acceso: https://gobiernodigital.gob.hn/.
[41] Decreto PCM-021-2021.
[42] Decreto Ejecutivo Número PCM-044-2020.
[43] Secretaría de Transparencia y Lucha en contra de la Corrupción de Honduras, ver en: https://stlcc.gob.hn/
[44] Open Government Partnership. https://www.opengovpartnership.org/documents/honduras-action-plan-2023-2025/
[45] Contracorriente Honduras (2022), ver en: https://contracorriente.red/2022/10/15/decreto-ejecutivo-abre-polemica-sobre-libertad-de-prensa-en-honduras/.
[46] Espinoza, C. (2022) "Análisis del estado de situación y propuestas sobre gobierno digital en Honduras". *Grupo de Trabajo sobre República Digital,* ver en: https://barracondigital.org/gobierno-digital-en-honduras-aportes-y-propuestas-elaboradas-en-la-mesa-de-transicion-del-gobierno-de-la-presidenta-xiomara-castro.

En el **Código Penal** en los artículos 229 y 230 se tipifican los delitos de injurias y calumnias con penas de multas y prisión para proteger el honor de las personas incluyendo a los funcionarios públicos, a pesar de constantes recomendaciones para eliminar estas figuras penales incluidas la CIDH. Por ello, se presentan dos iniciativas de ley en 2022 con la finalidad de derogar dichos delitos, pero hasta la fecha no se ha priorizado en su avance.[47]

La CIDH, detalla que en Honduras "persiste el uso del derecho penal para sancionar a periodistas y comunicadores por el ejercicio de su labor informativa", vinculado a la permanencia de los delitos de calumnias e injurias de su Código Penal.[48]

En perspectiva la Corte Interamericana señala que la persecución penal "es la medida más restrictiva a la libertad de expresión, por lo tanto, su uso en una sociedad democrática debe ser excepcional y reservarse para aquellas eventualidades en las cuales sea estrictamente necesaria para proteger los bienes jurídicos fundamentales de los ataques que los dañen o los pongan en peligro, pues lo contrario supondría un uso abusivo del poder punitivo del Estado".[49]

Anteriormente, en el año 2011 (posterior reforma en 2013) se adoptó la **Ley Especial para la Intervención de las Comunicaciones Privadas** comúnmente denominada **Ley de Escuchas** con la finalidad establecer un marco legal de regulación procedimental de la intervención de las comunicaciones como herramienta esencial en la lucha contra la criminalidad.[50]

Dicha ley es aplicada a las y los ciudadanos que sean investigados por la supuesta participación de un delito y consiste en escuchar, captar o grabar las comunicaciones de las personas, intervención de las llamadas telefónicas, mensajes telefónicos y correos electrónicos. La particularidad de la misma es que no se necesita el consentimiento de los intervenidos. Por otro lado, la intervención solo puede ser autorizada por una juez debidamente justificada y el responsable de llevar a cabo las intervenciones es la Unidad de Intervención de las Comunicaciones (UIC). A su vez, los fiscales y jueces que hayan solicitado y autorizado la solicitud tienen libre acceso a los resultados.[51]

En resumidas cuentas, la **Ley de Escuchas** comúnmente llamada de esa manera por la población, permite el acceso y la búsqueda de comunicaciones privadas en diversos ámbitos sin consentimiento del presunto inculpado y deja la información abierta a cargo del órgano jurisdiccional, juez de garantía, el fiscal y persona de la UIC, dejando entrever que dicha ley no es más que una inmunidad a las autoridades estatales de responsabilidad en las investigaciones y no cumple con ser una legislación integral en materia de privacidad.

---

[47] Código Penal de la República de Honduras de 2019.
[48] Comisión Interamericana de Derechos Humanos (2024). Informe Situación de Derechos Humanos en Honduras, pp. 289-333.
[49] Corte IDH, Caso Álvarez Ramos Vs. Venezuela, Excepción Preliminar, Fondo, Reparaciones y 1200 Costas, Sentencia de 30 de agosto de 2019, Serie C No. 380, párr. 119; Caso Baraona Bray Vs. Chile, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 24 de noviembre de 2022, Serie C No. 481, párr. 120.
[50] Ley Especial sobre Intervención de las Comunicaciones Privadas de Honduras. Decreto No. 243-2011.
[51] Rodríguez, A. Paso a paso para una política de ciberseguridad integral en Honduras. *IPANDETEC Centroamérica* y Portal de Cibernética de las Naciones Unidas, ver en: https://cyberpolicyportal.org/es.

Sumado a ello, en el año 2018 se presentó una iniciativa de ley sobre seguridad cibernética a través de la **Ley Nacional de Ciberseguridad y Medidas de Protección ante los Actos de Odio y Discriminación en Internet y Redes Sociales**, dicho proyecto de ley estaba orientado a obligar a las empresas a bloquear o eliminar contenido ilegitimo publicado en las plataformas digitales dentro de las 24 horas de recibir una denuncia pudiéndose ampliar dicho periodo. Asimismo, dicho proyecto de ley establece censura previa, pretendía imponer obligaciones a los administradores de sitios web, regulando el odio en las redes sociales de manera general lo que podría ocasionar confusión. Además, de contener elementos que ya se contemplaban en el Código Penal y Código Procesal Penal como el delito de difamación.[52]

Seguidamente, se han presentado otros proyectos similares a la **Ley de Escuchas** como la **Ley para la Protección de los Usuarios de las Telecomunicaciones** de 2023 en búsqueda de crear una base datos de los usuarios de la telefonía móvil por actores gubernamentales, aunque los marcos reguladores no le otorguen esas funciones. A su vez, con la pretensión de obligar a los operadores móviles la entrega de información sobre las comunicaciones de sus clientes sin orden judicial. Por lo que, se puede deducir que dicho proyecto de ley abre las puertas a la vulneración de derechos fundamentales de privacidad, protección de datos y libertad de expresión aplicables al espacio digital.[53]

En cuanto al derecho de protección de datos personales, en el año 2013 se presentó el proyecto de **Ley de Protección de Datos Personales** promovido por el Instituto de Acceso a la Información Pública pero no tuvo éxito a pesar de que su fin era el de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas de conformidad con los lineamientos de la Unión Europea sobre protección de datos. No obstante, al no contar con dicho marco legal, su regulación recae en la **Ley de Transparencia y Acceso a la Información Pública** en sus artículos 23 al 25 y las disposiciones de la Ley Penal hondureña.[54]

11.1.2. Documentación de Casos y Denuncias

La Comisión Interamericana en su Informe sobre la Situación de Derechos Humanos de 2024 en Honduras señala que el **Decreto PCM-023-2022** creado por la Dirección General de Información y Prensa puede tener efectos negativos para la libertad de expresión debido a sus atribuciones amplias y discrecionales que otorga a la entidad y la falta de claridad de sus objetivos, potencializando un control estatal sobre el contenido difundido por los medios de comunicación. Con ello, "abre la puerta a una aplicación discrecional y abusiva de las facultados otorgadas encaminada al control gubernamental de la información difundida por los medios independientes"

[52] Criterio HN (2019), ver en: https://criterio.hn/ley-de-ciberseguridad-de-honduras-es-ambigua-y-se-enmarca-en-el-odio/.
[53] Criterio HN (2023), ver en: https://criterio.hn/congreso-busca-aprobar-en-tercer-debate-la-ley-de-proteccion-de-los-usuarios-de-las-telecomunicaciones/.
[54] Paz, J. Protección de Datos y Privacidad de la Información en Honduras. *Consortium Legal.*

y convertirse en un medio indirecto de restringir la libertad de expresión incompatible con estándares interamericanos.[55]

En esa misma línea, se señala que el **Código Penal** en lo relacionado a la tipificación de los delitos de injuria y calumnia en los artículos 229 y 230 según C-Libre una organización de la sociedad civil entre 2001 y 2022 se han documentado 50 periodistas querellados por injuria, calumnia y difamación en Honduras con procesos judiciales aun abiertos.[56] Diversos medios internacionales condenaron que dichas reformas no acaban con la criminalización del periodismo.[57] Se prometió derogarlos del Código Penal debido a presiones externas e internas de la sociedad civil, pero hasta la fecha aún se encuentran tipificados.[58]

Por ejemplo, el periodista Carlos Eduardo Ávila fue sentenciado a 4 años de prisión por el delito de calumnias tras una investigación sobre acoso sexual y presuntamente por los delitos de honor que siguen vigentes en el país para criminalizar y amedrentar periodistas.[59]

En cuanto a las arbitrariedades de la **Ley de Escuchas**, en 2015, se reportó un caso en donde se trascendió públicamente una llamada telefónica entre el vicepresidente del Consejo de la Judicatura, Teodoro Bonilla y el magistrado Víctor Lozano, en la conversación se expresan sobre una compañera del Poder Judicial. Sin embargo, Teodoro Bonilla "negó que fuera su voz".[60] De igual forma, se han presentado diversas denuncias sobre espionaje durante el mandato del expresidente Juan Orlando Hernández con el objetivo de realizar intervención a las comunicaciones de los diputados de su propio partido político y al rabino Bar-Levy exintegrante de su defensa ante la Justicia Norteamericana.[61]

Otro ejemplo claro se da en 2016 con la intimidación e intervención a las comunicaciones de la Junta Nominadora encargada de presentar a los perfiles de los magistrados que iban a componer la nueva Corte Suprema de Justicia en Honduras, y denunciaron intervenciones telefónicas y pudieron observar cámaras de seguridad como método de presión externa.[62]

Por su parte, **Facebook** y **Twitter** denunciaron que el expresidente de Honduras había pagado enormes sumas de dinero para la creación de ejércitos de *bots* en las principales redes sociales para beneficiarse de la fama por medio de perfiles de empresas, organizaciones y figuras públicas

---

[55] *Ibid., supra* nota 48.
[56] Criterio HN (2022), ver en: https://criterio.hn/delitos-contra-el-honor-estan-en-vias-de-ser-despenalizados/.
[57] Committee to Protect Journalists, ver en: https://cpj.org/es/2020/06/honduras-adopta-codigo-penal-que-mantiene-los-delitos-contra-el-honor/.
[58] La Prensa (2019), ver en: https://www.laprensa.hn/honduras/congreso-nacional-eliminara-delitos-injuria-calumnia-nuevo-codigo-penal-honduras-GYLP1314332#image-1.
[59] Comité para la Libre Expresión (2022), ver en: https://clibrehonduras.com/2022/05/04/condena-penal-provoca-huida-de-periodista-sentenciado-a-la-carcel/.
[60] Proceso Honduras (2015), ver en: https://proceso.hn/solo-el-estado-escucha-en-honduras/. La Prensa (2015), ver en: https://www.laprensa.hn/honduras/piden-que-se-controle-ley-de-escuchas-HELP899871.
[61] Criterio HN (2023), ver en: https://criterio.hn/ley-sim-violaria-privacidad-de-ciudadanos-y-representaria-futura-misiva-contra-opositores/.
[62] El Heraldo (2016), ver en: https://www.elheraldo.hn/honduras/junta-nominadora-denuncia-intervencion-telefonica-y-vigilancia-con-camaras-ocultas-PFEH917190#image-1.

falsas.[63] **Facebook** informó que en julio de 2019 el expresidente Juan Orlando Hernández había pagado en anuncios a su favor y en 2021 el Diario *The Guardian* publicó que Hernández infló la popularidad de sus poblaciones con "me gusta" falsos por medio de cuentas no auténticas de perfiles de empresas, organizaciones y figuras públicas.[64] Además, de diversas denuncias de empleados públicos que son obligados a crear cuentas falsas para promocionar al gobierno provocándoles un "grave daño psicológico y una fuerte ansiedad".[65]

Entre 2016 y 2018 bajo la investigación de *Citizen Lab* sobre el seguimiento del *spyware Pegasus* de *NSO Group* se encontraron 1,091 direcciones IP (*Internet Protocol*, en inglés) que coincidían con huella digital y 1,014 nombres de dominio de personas hondureñas.[66] También, *Circles* una empresa de vigilancia que explota el sistema mundial móvil para espiar llamadas, mensajes de texto y ubicación de teléfonos apoyo al espionaje en Honduras y se detectaron 252 direcciones IP siendo 25 del gobierno. De igual forma, se identificaron dos sistemas de *Circles* en Honduras, un sistema anónimo, pero con registro son las siglas DNII, pudiendo hacer alusión a la Dirección Nacional de Investigación de Inteligencia.[67]

En cuanto a la compra y uso de software espía el gobierno hondureño comenzó a negociar desde el año 2012 con *Hacking Team* y por medio de la Dirección Nacional de Investigación e Inteligencia se compró el software Galileo a través de la compañía israelí *NICE Systems*, dicho software tuvo un supuesto monto de 355, 000 euros.[68]

Sobre la iniciativa de **Ley de Ciberseguridad y medidas de Protección ante los Actos de Odio y Discriminación en Internet y Redes Sociales** diversos sectores de la sociedad civil denunciaron que genera herramientas para "promover y legalizar censura y el control de la libertad de expresión en cualquier espacio digital, se pretende la creación irregular de órganos para la vigilancia sanciones incluidas en la propuesta, son altamente desproporcionadas y podrían crear un efecto inhibidor a la libertad de expresión, y sobre todo de medios alternativos de comunicación que han recurrido a Internet para difundir sus contenidos".[69]

Adicionalmente, ante la falta de legislación que regule el odio y las *fake news* en redes sociales en Honduras, los medios de comunicación reportan el aumento de los ataques de odio y desinformación a través de las redes sociales como **Facebook**, **Twitter e Instagram**, y señalan que se ha convertido en una conducta normal al grado de motivar a líderes empresariales y

---

[63] Denuncias de Redes sociales, ver en: https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/ https://www.theguardian.com/technology/2021/apr/13/facebook-honduras-juan-orlando-hernandez-fake-engagement.

[64] Diario The Guardian, ver en: https://www.theguardian.com/technology/2021/apr/13/facebook-honduras-juan-orlando-hernandez-fake-engagement.

[65] *Ibid., supra* nota 46.

[66] Citizen Lab, ver en: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[67] Perez de Acha, G. (2016). "Hacking Team Malware para la Vigilancia en América Latina". *Organización Derechos Digitales.*

[68] *Ibid., supra* nota 46.

[69] Artículo 19 (2019), ver en: https://articulo19.org/declaratoria-conjunta-sobre-ley-de-ciberseguridad/.

funcionarios de gobierno.[70] Asimismo, diversos sectores del país en especial los periodistas y funcionarios del gobierno denuncian continuamente ataques de odio y noticias falsas en las redes sociales, dentro de ellos la reconocida periodista Thelma Mejía. Por ello, se hace un llamamiento a "no normalizar la ciber violencia".[71]

En suma, la situación actual de Honduras presenta un panorama bastante crítico, dado que, no cuenta con un equipo nacional de ciberseguridad, una estrategia de ciberseguridad, una ley que regule la protección de datos personales, ciberseguridad y los discursos de odio en las redes sociales, no es signatario de convenios internacionales sobre ciberseguridad y presenta una ausencia de tipificación adecuada dentro de la Ley Penal sobre la materia.

Además, se carece de un centro de respuesta a incidentes, adopción oficial de estándares internacionales, requerimientos de certificaciones para entidades y para profesionales, políticas específicas de ciberseguridad, gobernabilidad y hoja de ruta de ciberseguridad, agencia oficial responsable por la ciberseguridad en el país, estadísticas y mediciones oficiales de ciberseguridad, estandarización en base a mejores prácticas de la industria.[72]

11.1.3. Recomendaciones y Reformas Necesarias

Por ello, en lo concerniente a la legislación vigente y necesaria se recomienda:[73]

1) Declarar el reconocimiento del Derecho a Internet como un derecho humano, e incorporarlo a través de una iniciativa de ley en la Constitución de la República;
2) La redacción y aprobación de una Ley Nacional sobre Ciberseguridad y Ciberdefensa, que cree una Política Nacional sobre Ciberseguridad y Ciberdefensa en correspondencia con la protección de los derechos humanos en el ecosistema digital;
3) La creación una Ley Marco Sobre el Gobierno Digital que abarque todas las relaciones intra-Estado y con los particulares, ya que el actual es un reglamento del Consejo de Ministros;
4) La creación de una Ley de Protección de Datos para regular el uso de Datos personales, tanto de entes privados como públicos, aunque la actual ya ha pasado por 2 de 3 debates en el Congreso, esta no puede ser aprobada debido a que se presenta artículos que podrían facilitar el borrado de datos de personas acusadas de delitos, como el derecho al olvido;
5) La derogación de leyes violatorias de derechos humanos, y que fomentan actuaciones arbitrarias y sombrías de la administración pública, dentro de ellas: la Ley Nacional de Inteligencia, Ley Especial del Consejo Nacional de Defensa y Seguridad y, de la Ley de Creación de la Secretaría de Transparencia;

---

[70] La Prensa (2024), ver en: https://www.laprensa.hn/honduras/honduras-frenar-discurso-odio-redes-sociales-congreso-nacional-EK16856130.
[71] Expediente Público (2024), ver en: https://www.expedientepublico.org/periodistas-bajo-el-asedio-y-campana-de-odio-en-honduras/.
[72] *Ibid., supra* nota 44. Espinoza, C. et al. (2017). "La Brecha Existente en la Ciberseguridad en Honduras". *Innovare Ciencia y Tecnología. &* Observatorio de la Ciberseguridad en América Latina y el Caribe. Análisis de 2020.
[73] *Ibid., supra* notas 46, 54 y 72.

6) Revisión y reforma de varias leyes, en base a estándares de derechos humanos en la materia tales como: la Ley de Escuchas, Ley Marco del Sector de las Comunicaciones y el Reglamento de Gobierno Electrónico;
7) Otros sectores recomiendan formalmente la derogación de la Ley de Escuchas o bien revisar quien opera bajo el mecanismo supervisor, ya que representa un riesgo para la dignidad e integridad humana y las amenazas a la privacidad;[74] y
8) Realizar un control de convencionalidad de la tipificación de delitos cibernéticos en el Código Penal, tomando de referencia el Convenio de Budapest sobre Ciberdelincuencia y otros instrumentos internacionales de la materia.

La Comisión Interamericana recomienda:[75]

9) Revisar la legislación nacional y eliminar figuras penales que puedan restringir el ejercicio del derecho a la libertad de expresión y la labor de periodistas; en particular respecto al delito de injurias y calumnia; y
10) Asegurar que los funcionarios públicos contribuyan, a través de su discurso, a crear un ambiente favorable para la libertad de expresión. Ello implica que (i) reconozcan de manera constante, clara, pública y firme la legitimidad y el valor de la labor periodística; (ii) constaten razonablemente los hechos en los que fundan sus opiniones.

Otros expertos en la materia recomiendan:[76]

11) Crear una agencia nacional dedicada a la seguridad cibernética y altamente capacitada en la materia con el objetivo de proteger los datos personales y la privacidad digital;
12) La creación de un programa nacional de protección de infraestructura crítica;
13) Contar con un plan de respuesta y recuperación de incidentes, centrándose en procedimientos de información, vigilancia activa de las ciber amenazas, inteligencia de amenazas, esfuerzos para su abordaje, una matriz de evaluación y un plan de movilización para responder a incidentes cibernéticos;
14) La creación de un dinámico ecosistema de seguridad cibernética compuesto por la sociedad civil, autoridades gubernamentales y expertos informáticos con el objetivo de prosperar en su aplicación; y
15) Adherirse al Convenio de Budapest sobre ciberdelincuencia, el Llamamiento de Paris para la Confianza y la Seguridad en el Ciberespacio, y seguir los lineamientos de la Unión Europea en la materia por medio del Reglamento General de Protección de Datos (RGPR), Declaración Europea sobre Derechos y Principios Digitales y la nueva Ley de Inteligencia Artificial (Ley de IA) de la UE.

[74] El Pulso (2022), ver en: https://www.elpulso.hn/2022/03/25/solicitan-al-congreso-nacional-derogar-ley-de-intervencion-de-llamadas/.
[75] *Ibid., supra* nota 46.
[76] *Ibid., supra* nota 72.

11.2. Estado de Guatemala

11.2.1. Análisis de la Legislación Guatemalteca

La legislación guatemalteca en relación con el derecho a la privacidad y la libertad de expresión en la era digital presenta avances significativos ante la iniciativa de Ley de Prevención y Protección contra la Ciberdelincuencia, aunque diversos sectores señalan que atenta contra derechos constitucionales como a la libertad de la emisión del pensamiento, así como ataques a medios de comunicación, obstáculos debido a la criminalización en redes sociales y persecución de periodistas y activistas. A pesar de estos desafíos, existen esfuerzos en curso por parte de organizaciones no gubernamentales y algunas entidades gubernamentales para mejorar la protección de datos personales y promover la ciberseguridad.

La Ley de Telecomunicaciones de 1996 figura como el marco legal de las telecomunicaciones en Guatemala y viene acompañada del mandato institucional, la Superintendencia de Telecomunicaciones (SIT) responsable de gestionar el espectro de las telecomunicaciones, pero sin contar con un mandato legal para regular la calidad del servicio ni el desempeño de proveedores de dicho servicio.

En cuanto a la regulación de intervención de las comunicaciones se encuentra en la **Ley Contra la Delincuencia Organizada** y en la **Ley de la Dirección General de la Inteligencia Civil**, donde se establece que se pueden intervenir las comunicaciones en actividades de crimen organizado donde existiese peligro para la vida, integridad física y libertad de las personas. Cabe resaltar, que entre ambos tipos de intervención la información recogida mediante la Ley de Inteligencia sólo tiene carácter preventivo, y no es apta para ser usada como prueba.[77]

Seguido a ello, se han presentado varias iniciativas de ley con el objetivo de respetar y proteger los derechos a la privacidad, libertad de expresión, datos personales en la era digital, tales como: la **Ley Cibercrimen N. 4054**, donde se estipulaban crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información, delitos de Contenido y delitos contra las Telecomunicaciones; **la Ley de Delitos Informáticos N. 4055**, tenía por objeto principal dictar medidas de prevención y sanción de los actos ilícitos de naturaleza informática, cometidos a través de artificios tecnológicos, mensajes de datos, sistemas o datos de información; y la **Ley de Protección de Datos N. 4090**, tenía como objeto garantizar a cualquier persona física o jurídica, sea cual fuere su personalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derechos a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la persona.[78]

[77] 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*.
[78] *Ibid., supra* nota 36.

Cabe mencionar, que ante la falta de legislación específica sobre la protección de datos personales de privacidad digital su protección recae en la **Ley de Acceso a la Información Pública** y las opiniones emitidas por la Corte de Constitucionalidad en el expediente 863-2011.

Sumado a estas iniciativas de ley fallidas, se añade la iniciativa de **Ley contra la Ciberdelincuencia N. 5254** de 2017, en donde, se detallaban las medidas de prevención y penalización de los actos ilegales en el ámbito cibernético que se cometan empleando dispositivos tecnológicos, mensajes de datos, sistemas informáticos o datos. Así como, las medidas de protección contra la explotación en línea, la pornografía y otras formas de abuso sexual con menores.[79]

Además, la Policía Nacional Civil cuenta con un Departamento de Investigación de Ciberdelitos e Información Forense y se cuenta con una Sección de Delitos Cibernéticos del Ministerio Público de Guatemala.[80]

En lo concerniente a la legislación conexa, el **Código Penal**, decreto 17-73, en su artículo 274 incisos A-G, se encuentra tipificado el delito de destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información y programas destructivos.[81]

Ante esa falta de legislación, Guatemala ha recibido una invitación para adherirse al Convenio de Budapest sobre Ciberdelincuencia con estatus de Observador, y en 2021 por medio de Acuerdo Gubernativo N. 200-2021, en coordinación con la Subsecretaría de Estado de Inteligencia Estratégica, la Secretaría Técnica del Consejo de Seguridad Nacional (STCNS) creó el Comité Nacional de Ciberseguridad.[82]

También, en 2018 se crea la Estrategia de Ciberseguridad con el objeto de regular la protección de los sistemas de información digital en los sectores público y privado con el fin de garantizar la continuidad de sus servicios; establecer organismos de coordinación (CSIRT-GT) para implementar la ciberseguridad nacional; y diseñar un plan nacional de protección de infraestructuras críticas para fortalecer los planes de contingencia y recuperación.[83] En 2021, por medio del **Acuerdo Gubernativo N.º 200-2021**, en coordinación con la Subsecretaría de Estado de Inteligencia Estratégica, la Secretaría Técnica del Consejo de Seguridad Nacional (STCNS) creó el Comité Nacional de Ciberseguridad siendo un organismo asesor del Consejo de Seguridad Nacional encargado de lograr las metas de la Estrategia Nacional de Ciberseguridad.[84]

---

[79] Evaluación de País del Ecosistema Digital (DECA) Guatemala (2023). *Digital Frontiers, USAID,* ver en: *https://www.usaid.gov/es/digital-development/guatemala-deca.*

[80] Unidad de Cibercrimen de Guatemala, ver en: https://mingob.gob.gt/unidad-de-cibercrimen-se-fortalece-y-apoya-en-resolucion-de-275-casos/.

[81] Código Penal de Guatemala. Decreto 17-73.

[82] *Ibid., supra* nota 79.

[83] Portal de Política Cibernética, ver en: https://cyberpolicyportal.org/es/states/guatemala.

[84] Comité Nacional de Seguridad Cibernética & Secretaría Técnica Consejo Nacional de Seguridad (STCNS) (2021), ver en: https://stcns.gob.gt/comite-nacional-de-seguridad-cibernetica/.

11.2.2. Documentación de Casos y Denuncias

En lo concerniente a la iniciativa de **Ley de Prevención y Protección contra la Ciberdelincuencia**, expertos en la materia consideran que afectaba el derecho a la libre emisión del pensamiento, protegidos por la Constitución guatemalteca y en la Ley de Libre Emisión del Pensamiento, así como, pretendía regular delitos que ya se encuentran regulados en la ley mencionada y en el Código Penal. Además, se señala que la tipificación de los delitos relacionados con la Libre Expresión es materia exclusiva de la **Ley de Emisión del Pensamiento**.[85]

Tampoco fue aprobada por varios sectores de la población guatemalteca, entre ellos organizaciones de periodistas y de derechos humanos, visto que se aducía que la ley buscaba la censura de medios de comunicación, limitaba la libertad de expresión y el derecho de libre emisión del pensamiento garantizados por la Constitución y la **Ley de Emisión del Pensamiento**. De esa forma, se archiva dicha iniciativa, al no responder a las necesidades de la población en la regulación de la materia de ciberdelitos y ciberseguridad.[86]

Los activistas de derechos humanos también denunciaron que dicha ley contravenía con sus libertades fundamentales y se mencionaba que con dicho decreto "las filtraciones podrían ser criminalizadas, así como el acceso a ciertas fuentes, en el caso de los periodistas". También, Iduvina Hernández defensora de derechos humanos menciona que las iniciativas de ley que se han presentado buscan el "revestimiento de la legalidad" por medio de prácticas de regímenes dictatoriales, la concentración de poder, la cancelación continuada de derechos de asociación, la acción violenta de las fuerzas del orden en contra de manifestantes y los atentados constantes a la libertad de expresión y prensa son pautas de que se vislumbra una dictadura.[87]

Por ello, se menciona que es necesaria una ley integral que tipifique los delios informáticos, ya que, la ley anterior no abordaba el sabotaje informático, espionaje informático, el robo o hurto de software, manipulación de programas, ciberterrorismo.[88]

De igual forma, se denuncia la violatoria al derecho a la información bajo resolución (01-2024) emitida por la Corte de Constitucionalidad de Guatemala publicada el 19 de junio de 2024 en la que clasifica como información reservada sobre los magistrados y magistradas, resguardándola por siete años.[89]

Sumado a ello, los medios de comunicación han sufrido ataques cibernéticos como fuel caso del diario La Prensa Libre que fue clonado y se "registró el dominio Prensallibre.com (con doble l) en

---

[85] Fernández Bermejo, D. & Martínez Atienza, G. (2020). *Ciberdelitos.* Ediciones Experiencia, p. 7.
[86] Calderón López, S. (2023). "Ley de Prevención y Protección contra la Ciberdelincuencia en Guatemala". *IPANDETEC Centroamérica.*
[87] Plaza Pública (2022), ver en: https://www.plazapublica.com.gt/content/ley-contra-ciberdelincuencia-la-normativa-que-puso-en-riesgo-la-libertad-de-expresion-y-la.
[88] *Ibid., supra* nota 79.
[89] Artículo 19 (2024), ver en: https://articulo19.org/guatemala-corte-de-constitucionalidad-emite-resolucion-violatoria-al-derecho-a-la-informacion/.

el cual se copiaron ilegalmente notas del diario y se insertaron ataques contra críticos y rivales del partido Líder, así como una supuesta encuesta".[90]

En esa misma línea, la Comisión contra la Impunidad de Guatemala (CICIG) en 2019 publicó un informe temático "*Bots, Nets Centers* y Combate contra la Impunidad" debido a la emergencia de cuentas madre y la viralización de mensajes por cuentas falsas de personas reales por medio de *bots*.[91] Igualmente, se señaló que la operación de los *Net Centers* es la viralización falsa de información y discurso de odio fomentando por la vía digital la vulneración de la integridad de las personas. Además, en un informe de 2021 de la OACNUDH se documentaron ataques en redes sociales en contra de movimientos sociales, periodistas y organizaciones campesinas que denunciaban actos de corrupción.[92]

Otra particularidad, se da a la salida de la CICIG, ya que, la información viralizada por los *Net Centers* se comienza a filtrar siendo información confidencial del Ministerio Público de Guatemala. Con ello, diversos periodistas aducen que pudiera tratarse de la "Fundación Contra el Terrorismo (FCT), la cual maneja un alto nivel de interacción con cuentas falsas que filtran esta información, aun cuando esta filtración puede ser considerada una forma de "obstrucción a la justicia".[93]

La Fundación dirigida por Ricardo Méndez la FCT se encargaba de tomar fotos a periodistas y publicarlas a la internet con comentarios estigmatizantes y eran reproducidos masivamente por net centers. Asimismo, se señala la colusión entre funcionarios públicos, la Fundación del señor Méndez y los *Net Centers*, en donde una ex corresponsal de CNN Michelle Mendoza denunció hostigamiento por parte de la Magistrada de la Corte Suprema de Justicia, Vitalina Orellana, debido a que, las fotos que se le tomaron en un evento fueron publicadas masivamente por **Twitter** desde un *Net Center*.[94]

Por su parte, los órganos de justicia por medio de la Sección de Delitos Cibernéticos en 2021 han colaborado con más de 733 casos concernientes al robo de identidad (*phising*), acoso sexual y difamación, entre otros relacionados con la privacidad digital.[95] En 2022, la Policía Nacional Civil bajo su Departamento de Investigación de Ciberdelitos ya reportaba más de 3 mil denuncias por

[90] Derechos Digitales (2015), ver en: https://www.derechosdigitales.org/9605/por-que-medios-y-periodistas-deberian-involucrarse-en-el-debate-de-la-ciberseguridad/.
[91] *Freedom House* et al. (2023), Informe de Hallazgos de la Misión Internacional sobre Libertad de Prensa y de Expresión en Guatemala.
[92] Informe OACNUDH 2021, ver en: https://issuu.com/oacnudhgt/docs/informe_anual_2021_-_web.
[93] Agencia Ocote "Cómo Mutaron Los Netcenters Anti-Justicia Y Derechos Humanos en Guatemala", 30 de noviembre de 2022, ver en: https://www.agenciaocote.com/blog/2022/11/30/mutaron-netcenters-anti-justicia-yderechos-humanos-en-guatemala/.
[94] Prensa Libre "Corresponsal de CNN denuncia hostigamiento de parte de magistrada de la Corte Suprema de Justicia y ella lo niega", 18 de mayo de 2021, ver en: https://www.prensalibre.com/guatemala/justicia/corresponsal-de-cnn-denuncia-hostigamiento-de-parte-de-magistrada-de-la-corte-suprema-de-justicia-y-ella-lo-niega-breaking/.
[95] Ministerio de Gobernación, sitio web: https://mingob.gob.gt/seccion-de-delitos-ciberneticos-incrementa-apoyo-a-mp/.

delitos a través de redes sociales y señalaba también los datos de 2021, en donde se presentaron más de 5 mil denuncias superiores a las 3mil presentadas en 2020.[96]

En suma, el panorama que se presenta de Guatemala es bastante crítico, en primer lugar debido a que la población recibe ataques constantes a través de las redes sociales sin protección alguna; en segundo lugar, el Estado no cuenta con una Ley Integral de Ciberseguridad encargada de proteger la privacidad y la libertad de expresión en el entorno digital, tampoco se observa voluntad política de hacerlo; y en tercer lugar, tampoco se cuenta con una ley de protección de datos personales encargada de garantizar la protección de los mismos y que permita avanzar en otros derechos y legislaciones como en la Unión Europea.

11.2.3. Recomendaciones y Reformas Necesarias

Las recomendaciones al Estado de Guatemala son parecidas a las que se recomendaron a Honduras, dado que ambos presentan un vacío legal dentro de su marco jurídico interno, con ello se presentan una serie de medidas a tomar en consideración, como ser:

1. Declarar el reconocimiento del Derecho a Internet como un derecho humano y su incorporación en su marco legal;
2. La creación de leyes de Ciberseguridad y Ciberdefensa, con ellas la creación de un mandato institucional para su regulación y promoción;
3. La creación de una Ley de Protección de Datos Personales que incluya como base fundamental los derechos ARCO y las normativas fundamentales desarrolladas por la Unión Europea en su Reglamento General de Protección de Datos (RGPR), Declaración Europea sobre Derechos y Principios Digitales y la nueva Ley de Inteligencia Artificial (Ley de IA); y
4. Adherirse al Convenio de Budapest, el Llamamiento de Paris para la confianza y la seguridad en el Ciberespacio.

La Evaluación de País del Ecosistema Digital de Guatemala por medio de la Agencia de Cooperación de Estados Unidos (USAID),[97] brinda parámetros y recomendaciones claras al Estado de Guatemala en materia de derechos fundamentales en el entorno digital, tales como:

5. Progresar en el perfeccionamiento y la implementación de la política y el reglamento de telecomunicaciones, aumentando la transparencia y la independencia del regulador de las telecomunicaciones (SIT), modernizar el marco regulador y llevar un seguimiento de la implementación;
6. Tomar ventaja de las tecnologías digitales para mejorar la prestación de los servicios públicos, aprovechando la Ley Antitramites de 2021 para facilitar los servicios públicos digitales; y

[96] La Prensa Libre, ver en: https://www.prensalibre.com/guatemala/justicia/van-mas-de-3500-denuncias-por-delitos-a-traves-de-redes-sociales-en-guatemala/.
[97] *Ibid., supra* nota 75.

7. Desarrollar una política de ciberseguridad más robusta, capacidad y concienciación, tomando como precedente la Estrategia Nacional de Ciberseguridad de 2018, necesitándose crear grupos de trabajo sobre ciberseguridad compuestos de expertos técnicos y personal relevante del Gobierno de Guatemala e impartir capacitación en ciberseguridad a todo el personal del Gobierno de Guatemala a todos los niveles y en todas las entidades.

Otros miembros de la sociedad civil recomiendan: [98]

8. Detener la estigmatización y el hostigamiento en especial por parte de autoridades y servidores públicos en contra de periodistas a través del uso de redes sociales;
9. Garantizar la correcta implementación de la Ley de Acceso a la Información Pública (Decreto No. 57- 2008) teniendo conciencia de que se afecta el derecho de información de la ciudadanía cuando se restringe el acceso a la información pública; y
10. La garantía de un estándar mínimo, de que las normas relativas al contenido permitido en redes sociales y plataformas de internet se ajusten a los estándares globales en materia de derechos humanos, no solo en lo sustantivo que respecta al contenido permisible y prohibido, sino en lo referido a estándares de transparencia, garantías mínimas de proceso, apelación e información al usuario.[99]

11.3. Estado de El Salvador

11.3.1. Análisis de la Legislación Salvadoreña

La situación de El Salvador a simple vista presenta un mejor panorama respecto a Honduras y Guatemala al contar con una Ley de Ciberdelitos y una ley en desarrollo sobre Protección de Datos Personales, avances significativos en materia de ciberseguridad y un Centro de Respuesta en materia de seguridad informática. Sin embargo, El Salvador presenta una situación de riesgo ante la implementación de medidas de vigilancia y el control de las comunicaciones electrónicas, prácticas estatales sin el debido proceso legal en socavo de la privacidad digital, la encrucijada ante la batalla de la desinformación, los ataques cibernéticos, las denuncias de intimidación y persecución de periodistas y opositores a través de medios digitales.

La **Ley de Telecomunicaciones** establece que la Superintendencia General de Electricidad y Telecomunicaciones (SIGET) es el ente encargado de regular Telecomunicaciones,[100] la normativa que regula las concesiones para radiodifusión sonora y televisiva, telefonía celular, televisión por suscripción y servicios de internet en El Salvador.

En ese contexto, con el objetivo de salvaguardar las telecomunicaciones y asegurar el ciberespacio se crea la **Ley Especial contra Delitos Informáticos y Conexos** vigente desde el año 2016 con el

[98] *Ibid., supra* nota 86.
[99] Díaz Hernández, M. (2020). "Discurso de Odio en América Latina: Tendencias de regulación, rol de los intermediarios y riesgos para la libertad de expresión". *Derechos Digitales América Latina.*
[100] SIGET, sitio web: https://www.siget.gob.sv/marco-institucional/.

objetivo de brindar protección penal a las personas ante el cometimiento de delitos a través de medios informáticos o electrónicos y velar por la prevención y sanción de los delitos relacionados a datos, sistemas o su infraestructura que afecten la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas, presentados en los artículos del 4 al 34 de dicha Ley. Posterior a ello en 2022, se introducen reformas para la incorporación del tratamiento de la evidencia digital en los procesos judiciales.[101]

No obstante, se cuenta con leyes contrarias a la libertad de expresión y privacidad en el entorno digital, dentro de ellas se encuentra la **Ley Especial de Intervención de las Telecomunicaciones** o **Ley de Escuchas Telefónicas** con el fin de agilizar la autorización de escuchas telefónicas y ampliación de los delitos investigados para disminuir la violencia y delincuencia en el país. Cabe mencionar, que con estas reformas se institucionaliza las escuchas telefónicas de los salvadoreños a solicitud del fiscal general y el director del Centro de Intervenciones y deberá ser autorizada por un juez de garantía.[102]

También, en materia de ciberseguridad El Salvador cuenta con una Política de Ciberseguridad con el objetivo de salvaguardar la seguridad, asegurar las directrices, la implementación de métodos de riesgo, proteger los activos de la organización y los usuarios en el ciberespacio, y se le suma el Consejo Nacional de Ciberseguridad, creada por el Ministerio de Justicia y Seguridad Pública en el Acuerdo N. 218 de 2012.[103]

Sumado a ello, se cuenta con la política pública sobre una **Agenda Digital** para los años 2020-2030 sobre transformación digital bajo 4 pilares fundamentales: la identidad digital, la innovación, educación y seguridad, modernización del Estado y la Gobernanza Digital, en este último se contempla aspectos fundamentales como el desarrollo de las leyes habilitantes y la ciberseguridad

En lo relacionado a la protección jurídica de los datos personales su protección jurídica recae en la **Ley de Acceso a la Información Pública** en los artículos 31 al 39, en donde se menciona el derecho a la protección de los datos personales, los deberes de los entes obligados, la prohibición de difusión, la difusión sin consentimiento y lo concerniente a la solicitud de datos. Sin embargo, sólo es aplicable a registros de entidades estatales y entidades gubernamentales. Asimismo, es ampliado en los procesos de amparo 934-2007 y 142-2012, en donde se desarrolla el derecho a la autoderminación informativa vístase como una manifestación del libre desarrollo de la personalidad y la dignidad.

[101] Ley Especial contra Delitos Informáticos y Conexos. Decreto N. 260.
[102] *The San Diego Union Tribune*, ver en: https://www.sandiegouniontribune.com/2022/11/01/el-salvador-reforman-ley-de-intervenciones-telefnicas/.
[103] Política de Ciberseguridad, ver en: https://diario.elmundo.sv/politica/el-salvador-aprueba-y-publica-su-politica-de-ciberseguridad.

Además, se presenta una ley en desarrollo sobre datos personales según la Secretaría de Innovación de la Presidencia de El Salvador y fundamenta su objetivo en garantizar el manejo adecuado de la información y la protección de los derechos de usuarios de servicios digitales.[104]

11.3.2. Documentación de Casos y Denuncias

Es importante mencionar la visión de punitivita y violatoria del actual gobierno del presidente Nayib Bukele, en continuas extensiones del régimen de excepción, sumadas a las restricciones a las libertades de información, expresión y asociación en la que se involucran periodistas y activistas. De igual forma, se ha reformado el Código Penal en su artículo 345 criminalizando la cobertura y las expresiones relacionadas con el pandillerismo en El Salvador, teniendo como resultado el desplazamiento de 9 periodistas por temores a sus trabajos.[105]

Con ello, se presenta un panorama severo y estricto en cuanto al ejercicio de la libertad de expresión en línea dentro de sus múltiples aspectos para la ciudadanía por medio del amedrentamiento público y directo a grupos de periodistas, académicos y activistas, un ejemplo de ello se da el 3 de abril de 2022 donde el presidente llama de "basura" a Juan Martínez Investigador y antropólogo especializado en temas de violencia y pandillas, por el hecho de verter comentarios contrarios a la opinión del presidente Nayib Bukele.[106]

El informe sobre Libertad de Prensa en el Salvador de 2022 generado por la Asociación de Periodistas (APES) y el Centro de Monitoreo de Agresiones, se documentaron que en ese año 12 periodistas se vieron forzados a huir de El Salvador, [107]136 casos de agresiones a periodistas, 147 vulneraciones de derechos a la libertad de expresión, 161 afectaciones y 35 alertas públicas, así como, el desmantelamiento de los canales televisivos Focos TV y Canal 33 dejándolos sin espacio periodístico del formato audiovisual,[108] ataques especialmente contra mujeres periodistas mediante el acoso digital.[109] Además, se denuncia el *hackeo* de cuentas de **WhatsApp** de periodistas y comunicadores,[110] la amenaza por medios digitales por parte de funcionarios públicos, entre muchas otras.

El Informe de Amnistía Internacional de 2023 sobre la represión y regresión en materia de derechos humanos en El Salvador reflejan un constante desprestigio y estigmatización contra voces críticas

[104] Secretaría de Innovación a la Presidencia de El Salvador, ver en: https://www.innovacion.gob.sv/leyes-habilitantes.php.
[105] Artículo 19, ver en: https://articulo19.org/la-libertad-de-expresion-en-centroamerica-y-el-caribe/.
[106] Denuncias de periodistas, ver en: https://x.com/nayibbukele/status/1513591841656127488?s=20&t=RsrSNZAOpyE8IIw_SaHwXw.
[107] APES (2022). Informe sobre Libertad de Prensa 2022. Asociación de Periodistas de El Salvador (APES).
[108] La Prensa Gráfica (2022), ver en: https://www.laprensagrafica.com/elsalvador/Anuncian-cierre-de-programa-de-entrevistas-Republica-de-Canal-33-20210730-0032.html.
[109] El Faro (2024), ver en: https://elfaro.net/es/202207/el_salvador/26294/El-bukelismo-se-ensa%C3%B1a-con-las-mujeres-periodis-tas.htm.
[110] APES (2022), ver en: https://x.com/apeselsalvador/status/1482194683661107200?s=20&t=PSbAFYhcCXtKvw25AkPaMw.

al gobierno por medio de redes sociales,[111] además, de ser documentado por la *visita in loco* de la CIDH,[112] donde se develó la preocupación por los discursos estigmatizantes contra personas defensoras de derechos humanos, periodistas y medios de comunicación independientes, provenientes de altas autoridades estatales.

Otros ejemplos altamente graves vienen de las opiniones que realizan algunos jueces bajo anonimato a los medios de comunicación ante el temor de ser removidos de sus cargos por la Asamblea Legislativa que controla totalmente el presidente y con el precedente de remoción total de la Corte Suprema de Justicia anterior sumado el fiscal general y adjunto de ese país. Dichos expertos legales consideran que las reformas de ley "crean tipos penales tan abiertos que no se sabe cuáles serán los límites", las penas a implementarse son desproporcionadas y se criminaliza la labor informativa, ya que se presta a persecuciones del derecho de la información de la población.[113]

En ese mismo contexto, se han documentado situaciones de censura, violaciones al derecho de acceso a la información, limitaciones a la libertad de expresión por medio de la violencia digital que viven los periodistas, especialmente en el periodo de elecciones, en donde, la APES monitoreó 64 casos de ataques en 2023 e inicios de 2024 en el ámbito digital por medio acoso, difamación, amenazas legales y vigilancia. Asimismo, se señala desigualdad de género, en donde se dirigen ataques directamente relacionados con periodistas y si es dirigida a hombres con contenido transfóbico, homofóbico y misógino, denotando una violencia basada en género.[114]

Ante esta situación, se señala la falta de una garantía de protección legal hacia el grupo de personas LGBTI+ y las mujeres, debido a que bajo la Ley de Delitos Informáticos no existe ninguna protección alguna ni la pretende abordar bajo la perspectiva de género.

En ese mismo reporte, a raíz del régimen de excepción impuesto por el gobierno y el legislativo, se mencionan numerosas denuncias de espionaje y ataques cibernéticos en contra de periodistas y medios de comunicación principales como El Faro, en donde sus trabajadores reciben constantes amenazas, hostigamientos e intimidaciones en espacios digitales y con ello la obligación de la Comisión Interamericana de Derechos Humanos de otorgar medios cautelares a favor de 34 miembros del gremio periodístico y con ello tratar de salvaguardar sus vidas. Por su parte, la organización *Citizen Lab* identificó un software espía denominado *Pegasus* instalado en los teléfonos de 35 periodistas y miembros de la sociedad civil.

---

[111] Informe de Amnistía Internacional sobre la Represión y Regresión en Materia de Derechos Humanos en El Salvador. AMR 29/7423/2023.

[112] CIDH presenta observaciones preliminares de su visita in loco a El Salvador. 27 de diciembre de 2019. Ver en: https://www.oas.org/es/cidh/prensa/comunicados/2019/335.asp.

[113] El Faro, ver en: https://elfaro.net/es/202204/el_salvador/26117/Asamblea-controlada-por-Bukele-aprueba-ley-mordaza-bajo-la-excusa-de-combate-a-pandillas.htm.

[114] Derechos Digitales (2024), ver en: https://www.derechosdigitales.org/23458/las-multiples-caras-de-la-violencia-contra-periodistas-en-el-salvador/.

Otros medios locales como la Revista Factum y Gato Encerrado han sido censurados en conferencias de prensa y han debido bajar investigaciones por orden judicial, aunque diversos sectores mencionan que el ataque es a todo el periodismo salvadoreño, dado que, según El Faro en 2021 aumentaron los ataques de agresiones a periodistas con relación a 2019 y 2020 respectivamente.[115]

En cuanto a la protección de datos personales y la ciberseguridad, Sandra Santos Catedrática de Derecho Constitucional y Procesal Constitucional de la Universidad Centroamericana señala que el Instituto de Acceso a la Información Pública "no cumple con sus atribuciones en defensa de la ciudadanía ni la Sala de lo Constitucional, debido a la falta de independencia e imparcialidad judicial, sumado a la falta de contar con una fecha de una ley de protección de datos personales, aunque en la Agenda 2020-2030 se promete cumplir con la misma" y concluye mencionando que "se presenta un riesgo del uso indebido de la información de las y los ciudadanos por desconocidos y para fines diversos", implicando un "peligro y una puerta abierta a la vulneración de varios derechos".[116]

Otros expertos señalan que el anteproyecto de ley presentado sobre datos personales consta de vacíos legales y de una ambigüedad que no conduce a nada. Por ejemplo, en la redacción del principio de legalidad se presenta una ambigüedad muy clara, el principio de privacidad su interpretación es confusa y el principio de licitud es poco desarrollado. Tampoco se presta atención a las categorías especiales de información, la normativa de rectificación, cancelación y oposición (derechos ARCO) no resulta clara su operatividad ni definición, entre otras aclaraciones.[117]

11.3.3. Recomendaciones y Reformas Necesarias

La Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES),[118] el Centro de Investigación de Estadísticas y el Centro Internacional para la Empresa Privada (CIPE) a través de un estudio exhaustivo de la legislación salvadoreña en materia de privacidad digital y derechos conexos recomiendan al gobierno de El Salvador lo siguiente:

1. Fortalecer la implementación de la Estrategia Nacional de Ciberseguridad y aprobar una Ley de Ciberseguridad bajo una estrategia sólida y efectiva para abordar los desafíos de la ciberseguridad, tales como: contar con equipos de respuesta a incidentes informáticas o equipos de respuesta a emergencias informáticas incluyendo la protección a grupos

[115] Revista Vice, ver en: https://www.vice.com/es/article/jg8b3x/director-de-el-faro-el-periodismo-esta-mas-amenazado-que-nunca-con-bukele.
[116] Revista Factum, ver en: https://www.revistafactum.com/datos-personales/.
[117] Derechos Digitales, ver en: https://www.derechosdigitales.org/15341/ley-de-datos-personales-sin-pausa-pero-sin-prisa-y-de-cara-a-la-sociedad/.
[118] FUSADES (2023). "Camino hacia la Transformación Digital Inclusiva en El Salvador". *Fundación Salvadoreña para el Desarrollo Económico y Social*. Banco Mundial. (2022). "Desarrollo digital", ver en: https://www.bancomundial.org/es/topic/digitaldevelopment/overview. Banco Interamericano de Desarrollo. (2020). "Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe", ver en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgosavances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.

vulnerables mediante la existencia de mecanismos de protección infantil en línea, protección de datos personales, protección de acoso a mujeres en línea, entre otros;

2. Contar con una Ley de Protección de Datos Personales que regule el tratamiento de datos particulares, busque garantizar la seguridad de la intimidad de los usuarios y proporcione la debida seguridad jurídica sobre las restricciones y libertades que se contemplan sobre el uso de la información personal de los usuarios;
3. Se debe garantizar que las personas en el entorno digital tengan la posibilidad de acceder, rectificar, cancelar y oponerse al manejo de sus datos personales por parte de un tercero, también, se deben establecer las condiciones para recolectar información y a determinar expresamente las consecuencias por la infracción de dichos derechos;
4. Se recomienda que la Ley de Datos Personales sirva como fundamento para la adecuada implementación de la firma electrónica certificada, el comercio electrónico, los expedientes electrónicos, la identidad digital, el gobierno electrónico y cualquier otra actividad vinculada a las tecnologías de la comunicación;
5. Retomar las recomendaciones de estándares internacionales de las Naciones Unidas y otros organismos internacionales que establecen medidas sobre la perspectiva de género y aplicarlas al ámbito digital para su protección; y
6. Revisar y reformar el Código Penal y la Ley Especial contra Delitos Informáticos y Conexos con la finalidad de incorporar disposiciones específicas que regulen y tipifiquen el delito de acoso en línea, garantizando la participación de las mujeres en el espacio digital de forma segura.

Otras recomendaciones relacionadas al ámbito social e implementación de políticas públicas contemplan las siguientes:

7. Capacitar a las personas activamente en el entorno digital sobre políticas y marcos regulatorios en el país, con el objetivo de conocer derechos y obligaciones que están regulados, y sepan como exigir derechos en caso de ser vulnerados;
8. La articulación de entidades en el ecosistema digital y la sensibilización de dichas instituciones que brindan formación sobre la necesidad de incluir en los temas que imparten la importancia de la ciberseguridad y la protección de datos personales;
9. Promover la alfabetización digital especialmente relacionada a personas vulnerables como las mujeres, niñas y niños, personas de las zonas rurales y grupos LGBTI+, procurando disminuir la actual brecha digital que persiste; e
10. Implementar la Agenda Digital El Salvador 2020-2030 y dotarla de recursos financieros técnicos necesarios para digitalizar los servicios gubernamentales para actualizar, rediseñar e integrar las plataformas digitales públicas existentes.

11.4. Estado de Nicaragua

11.4.1. Análisis de la Legislación Nicaragüense

El marco legislativo en Nicaragua en relación con la privacidad digital y la libertad de expresión en línea refleja un ambiente restrictivo y represivo. Las leyes aprobadas en los últimos años han facilitado una mayor capacidad para la vigilancia y el control de la información por parte del gobierno, al tiempo que han restringido severamente el espacio para la expresión libre y la disidencia.

En 1995 fue promulgada la **Ley General de Telecomunicaciones y Servicios Postales, Ley N. 200,** la cual establece un marco general institucional y jurídico que permite la regulación del sector de las telecomunicaciones en Nicaragua y faculta al Instituto Nicaragüense de Telecomunicaciones y Correos **(**TELCOR) como ente autónomo bajo la Rectoría de la Presidencia de la República y con sucesivas reformas.[119] Asimismo, el Estado cuenta con la **Ley del Digesto Jurídico Nicaragüense de la Materia de Telecomunicaciones y Servicios Postales** con el objetivo de ordenar el marco normativo vigente del país para fortalecer la seguridad jurídica.

En 2020, bajo **Acuerdo Administrativo 004-2020** en reforma del acuerdo previo creado en 2013,[120] y TELCOR decide ampliar el control sobre las empresas encargadas de ofrecer servicios de telecomunicaciones en el país. Se decide obligar a las empresas privadas a informar sobre nombramientos de gerentes de asuntos regulatorios y/o interconexión y acceso, gerentes jurídicos, responsables de la instalación, operación y mantenimiento de las redes y equipos correspondientes. Su inobservancia conlleva a sanciones administrativas o penales según las **leyes N. 735 y 200**. Además, se establece el estricto cumplimiento de los artículos 65 y 66 de la **Ley N. 735** (mencionada en el párrafo siguiente).

En dicho Acuerdo se presenta un régimen de espionaje y de intervención de las telecomunicaciones al citar el artículo 65 de la **Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados, Ley N. 735** que obliga a los prestadores de servicios a informar toda actividad en el espectro electromagnético y radioelectrónico. También, se cita el Art. 66 y se advierte a los operadores de servicios de telecomunicaciones que deben cumplir y facilitar a las autoridades la intervención de las comunicaciones y guardar absoluta reserva, y su inobservancia deberá ser sancionada conforme al Código Penal.[121]

En noviembre de 2024 se aprueba la **Ley N. 1223, Ley General de Telecomunicaciones Convergentes** sustituyendo a la **Ley General de Telecomunicaciones y Correos Postales, Ley 200**. Dicha normativa compuesta por 158 artículos establece su entrada en vigor en un plazo de 12

[119] TELCOR Sitio Web: https://telcor.gob.ni/institucional/marco-legal/.
[120] Diego Silva (2020), ver en: https://www.despacho505.com/nacionales/2581-regimen-amplia-control-sobre-operadores-de-telecom/. Acuerdo Administrativo 004-2020, ver en: http://legislacion.asamblea.gob.ni/gacetas/2020/5/g88.pdf.
[121] *Ibid., supra* nota 120.

meses a partir de su publicación en el Diario Oficial La Gaceta, por lo que la actual Ley 200 permanece en vigencia.[122]

Según el preámbulo de la ley su objetivo radica en el desarrollo del sector de las telecomunicaciones bajo un "marco sólido, actualizado, flexible, previsible, prospectivo y dinámico" así como, la de mejorar "la seguridad jurídica promoviendo la inversión, investigación, innovación y emprendimiento en el sector ampliado de las TIC".

La normativa se presenta como innovadora y moderna al incluir en sus **artículos 1, 2, 40, 89 y 115** el derecho a la portabilidad numérica, el acceso universal a las telecomunicaciones y el fomento de la inversión extranjera, entre otras disposiciones. No obstante, presenta un marco normativo represivo e inconstitucional, ya que, atenta gravemente contra derechos fundamentales como a la libertad de expresión en línea y a la privacidad e inviolabilidad de las comunicaciones protegidos por la Constitución actual, así como, de contravenir con la **Ley 787** sobre datos personales al exponer y manipular la información de las y los usuarios de medios digitales.

En su **artículo 110** sobre la obligación de suministrar información al ente regulador TELCOR se establece que: "los Operadores de Servicios Públicos de Telecomunicaciones y Proveedores de Servicios de Comunicaciones Audiovisuales, están obligados a suministrar toda la información que le sea requerida, incluyendo información estadística y georreferenciada generada de su participación en el mercado, en forma periódica o como resultado de requerimientos específicos de TELCOR, en el ejercicio de sus facultades y atribuciones regulatorias. Para tal efecto, la información requerida deberá ser proporcionada, de forma detallada, exacta, veraz, oportuna y comprobable".

En otras palabras, al estipularse "suministrar toda la información que le sea requerida, incluyendo información estadística y georreferenciada", en observancia con el **artículo 5 (20) (21)** donde establece la definición de información estadística como un "conjunto de datos que describen o expresan características sobre un elemento, fenómeno u objeto de estudio […]" y la información georreferenciada expresada como "esta información permite establecer la ubicación espacial de un elemento geográfico en particular en un momento determinado". Se podría construir un perfil individualizado sobre las preferencias de las y los usuarios en línea, sus interacciones en los medios digitales y el monitoreo en tiempo real de su ubicación.

Expertos legales nicaragüenses señalan que la ley facilita el monitoreo de las comunicaciones digitales sin órdenes judiciales específicas, permite la supervisión de actividades en línea y la

[122] Ley General de Telecomunicaciones Convergentes, Ley N. 1223 aprobada el 31 de octubre de 2024. A su vez, se derogan otra serie de normativas y decretos ejecutivos incluida la **Ley N. 210**, Ley de Incorporación de Particulares en la Operación y Ampliación de los Servicios Públicos de Telecomunicaciones y la **Ley N. 670**, Ley de Prórroga a las Licencias de las Empresas, Personas Naturales o Jurídicas que Operan Radio, Televisión y Tele Cable. Con la derogación de estas leyes TELCOR estaría en la facultad de solicitar nuevamente licencias de operación a todos los medios de telecomunicaciones de Nicaragua.

creación de perfiles de las y los usuarios, así como, requerir a las y los proveedores recopilar y almacenar datos personales con el objetivo de contar con información de identificación personal, metadatos de comunicaciones, el historial de navegación y uso de aplicaciones móviles. Además, se podrían establecer mecanismos para limitar o controlar el acceso a contenidos en los medios digitales.[123]

Ahondado a ello, bajo el **artículo 154** se faculta al ente regulador TELCOR para emitir nuevas normativas con el objetivo de garantizar el cumplimiento de las disposiciones de la ley sin la necesidad de ser aprobadas por la Asamblea Nacional de Nicaragua y establece bajo el **artículo 140 (21)** como infracciones graves su incumplimiento. También, bajo su **artículo 143** establece disposiciones sobre multas que van desde el 1.5 % y 2.5% de los ingresos brutos de las compañías.

En esa misma línea represiva, en el año 2020 se crea **Ley Especial de Ciberdelitos** llamada "**Ley Mordaza**" o "**Ley Bozal**" con el objeto de prevenir, investigar, perseguir y sancionar los delitos cometidos "por medio de las tecnologías de la información y la comunicación, en perjuicio de personas naturales o jurídicas". En su artículo 28 se prescribe de dos a cuatro años de prisión por el uso de tecnologías de la información para calumniar el honor o el prestigio de una persona o bien divulgar los secretos de la misma. El artículo 29 castiga a quien utilice las tecnologías de la información para quienes "inciten, instiguen, provoquen o promuevan la comisión de delitos, ensalce el crimen o enaltezca a su autor o partícipes o se lo adjudique", y con ello la imposición de penas de tres a cinco años de prisión. Ambas disposiciones se redactan de una manera amplia para permitir la supresión del derecho a la libertad de expresión en línea.[124]

En su **artículo 30** se establece que "las publicaciones que perjudiquen el honor, el prestigio o reputación de una persona supondrán una pena de entre uno a tres años de prisión. Así como, de una multa de entre 150 y 300 días de salario". Advirtiendo además que "si la publicación o difusión de la información falsa y/o tergiversada incita al odio o la violencia, pone en peligro la estabilidad económica, el orden público, la salud pública o la seguridad soberana se impondrá una pena de entre 3 a 5 años de prisión y una multa de entre 500 a 800 días de salario". Esta ley es aplicable tanto a los usuarios de redes sociales como a los medios de comunicación, y podría ser usada como una herramienta para castigar la disidencia y control el flujo de información en la red.[125]

Sumado a ello, en el marco de regulación de dicha ley, TELCOR emite el **Acuerdo Administrativo 001-2021** sobre una normativa que obliga a los operadores la preservación de datos generados de los servicios de las telecomunicaciones con el fin de establecer los lineamientos y parámetros que rigen los datos e información generados en el marco de servicios de telecomunicaciones. Teniendo como objetivos principales: "rastrear e identificar el origen y

[123] Alexa Zamora (2024). "Ley de Telecomunicaciones Convergentes y su Impacto en el Ejercicio de los Derechos Humanos" *Fundación por la Libertad de Expresión y Democracia*, ver en: https://fled.ong/ley-de-telecomunicaciones-convergentes-en-nicaragua-un-paso-hacia-el-control-o-la-innovacion/
[124] Ley Especial de Ciberdelitos, Ley N. 1042.
[125] *Ibid., supra* nota 124.

destino de las comunicaciones; identificar la fecha, hora y duración de las comunicaciones; e identificar el tipo de comunicación, el equipo utilizado y la localización del mismo".[126]

El **Código Penal** por su parte tipifica en su Título IV los delitos contra el honor incluidas la calumnia y la injuria en los artículos 202 y 203,[127] con penas de doscientos a trescientos días la multa. Si bien en estas disposiciones no se especifica su aplicación en el espació digital, se considera que la ventana queda abierta para que suceda.

La **Ley de Seguridad Soberana de 2015**, **Ley N. 919**, [128] en su artículo 8 califica a los ciberataques como amenazas a la "seguridad soberana" si alteran o afectan los sistemas de comunicación nacional. En el artículo 3 sobre la finalidad de la ley sobre "el libre disfrute de las libertades públicas, la justicia, la convivencia pacífica, la paz y el desarrollo integral de la persona, como uno de los objetivos primarios del sistema democrático". No se enmarca en su marco constitucional según el Centro Nicaragüense de Derechos Humanos (CENIDH), dado que, "desnaturaliza las funciones que encomienda la Constitución al Ejército de Nicaragua atribuyéndoselas la Secretaría que estará a cargo de la implementación de las acciones de esta Ley que da pie también al espionaje por motivaciones políticas y que representa un duro golpe para los derechos humanos y la democracia en el país".[129]

No obstante, en su artículo 13 se menciona que "ninguna institución parte del Sistema Nacional de Seguridad Soberana podrá ejercer actividades ejercer actividades de espionaje político, realizar actividades que impliquen el uso de la fuerza o intimidación, obtener información de datos sensibles de las personas, revelar o divulgar información, interceptar e intervenir comunicaciones telefónicas e intervenir electrónicas sistemas de transmisión de información sin autorización".

Dentro de ese orden, entre 2020 y 2022 se han aprobado varias leyes y decretos configurando un paquete de leyes represivas, dentro de ellas se encuentran:

1. **Ley de Regulación Agentes Extranjeros, Ley N. 1040** de 2020 llamada "**Ley Putin**" y su normativa correspondiente, segunda legislatura sobre la enmienda constitucional que permite la cadena perpetua por delitos de odio en Nicaragua;
2. **Ley de Reforma y Adición al Código Penal Ley N. 779**;
3. **Ley de defensa de los Derechos del Pueblo a la Independencia, la Soberanía y Autodeterminación para la Paz**;
4. **Ley 1055** conocida como "**Ley de soberanía**" que descalifica a las personas con opinión diferente como "traidores a la patria"; y

[126] Ver normativa: https://telcor.gob.ni/institucional/marco-legal/ y *Arias Law*. https://ariaslaw.com/newsroom/news.
[127] Código Penal, Ley N. 641, aprobada el 13 de noviembre de 2007, ver en: https://www.poderjudicial.gob.ni/spenal/leyes.asp.
[128] Ley de Seguridad Soberana de la República de Nicaragua, Ley N. 919, aprobada el 02 de diciembre de 2015.
[129] Cabe mencionar que en 2018 el gobierno de Nicaragua ordenó la cancelación de la personalidad jurídica del CENIDH, ver en: https://www.amnesty.org/es/latest/press-release/2018/12/nicaragua-attack-on-cenidh-is-a-blow-for-human-rights/ .CENIDH (2016), "CENIDH presenta recurso por inconstitucionalidad contra la Ley de Seguridad Soberana", ver en: https://www.cenidh.org/noticias/871/.

5. La adición a la **Ley N. 1060 de reforma procesal penal** para ampliar de 48 horas hasta 90 días el plazo de detención.[130]

Sobre la **Ley de Regulación de Agentes Extranjeros** bajo artículo 9 de la ley explica que los "agentes extranjeros" deben informar al gobierno con anticipación sobre el origen de los fondos que recibirán y cómo se utilizarán dichos fondos. De conformidad, dichos "agentes extranjeros" tienen prohibido recibir donaciones anónimas y el gobierno tendrá la autoridad de evaluar y determinar si la información es adecuada o no o si bien una entidad no cumple con lo estipulado por la ley pudiéndose imponer multas por actividades relacionadas a su financiación, la imposición de multar y la cancelación de la personalidad jurídica.[131]

Además de eso, la **Ley de Telecomunicaciones Convergentes** presentada con el objeto de "normar, regular, planificar, supervisar, fiscalizar y desarrollar el sector de telecomunicaciones", es señalada como "**Ley de Espionaje**" al ordenar a los operados de servicios de comunicaciones el suministro de toda información requerida al ente regulador TELCOR.[132]

Previo a la aprobación de dicha normativa, la Fundación por la libertad de Expresión y Democracia (FLED) señalaba que la ley tenía por objeto el control de manera más estricta las comunicaciones teniendo un impacto perjudicial para las libertades personales, asimismo, incluyendo aspectos de regulación relacionados a la telefonía, internet, televisión y radio. En concordancia, resaltan que la "vendría a facilitar la persecución de la ciudadanía al obligar a los diferentes entes que prestan servicios a dar información del contenido que visualizan y al mismo tiempo controlará los demás aspectos necesarios para que las empresas gocen de las libertades de producción y emisión de contenido".[133]

En cuanto a la legislación en protección de los Datos Personales, **la Ley N. 787 de Protección de Datos Personales** en su artículo 1 menciona que tiene por objeto la "protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa", sumada a la **Ley de Acceso a la Información Pública**, **Ley N. 621** con el objeto de normar, garantizar y promover el ejercicio de la información pública. También, se cuenta con una **Ley de Protección de los Derechos de las Personas Consumidoras y Usuarias** que establece que las personas proveedoras están obligadas a proteger la información que reciben de las personas consumidoras y usuarias.[134]

---

[130] Colectivo de Derechos Humanos Nicaragua Nunca+ (2023). "Informe Ataques a la Libertad de Expresión en Nicaragua", ver en: https://colectivodhnicaragua.org/un-ano-despues-de-la-ley-mordaza-mas-opresion-contra-la-libertad-de-expresion-en-nicaragua/.
[131] Ley de Regulación de Agentes Extranjeros Ley, 1040**,** aprobada el 15 de octubre de 2020.
[132] La Prensa (2024), ver en: https://www.laprensani.com/2024/03/13/politica/3291263-nueva-ley-de-telecomunicaciones-obliga-a-proveedores-a-dar-informacion-que-le-sea-requerida.
[133] Onda Local, ver en: https://ondalocalni.com/noticias/2666-ley-telecomunicaciones-convergentes-nicaragua-riesgos-control-comunicaciones/.
[134] Cajina, R. (2019). Estudio Centroamericano de Protección de Datos, Nicaragua. *IPANDETEC.*

Además, en el artículo 3 inciso F de la **Ley N. 787**, se extiende esta protección a los datos informáticos, siendo aquellos datos que, tratados por medios electrónicos automatizados, y se establece la obligación de informar previamente a los titulares de dichos datos la finalidad con la que serán utilizados. Asimismo, el artículo 6 menciona que el titular de los datos debe brindar su consentimiento si mismo o por medio de su representante legal. en su artículo 24 se contempla la excepcionalidad del uso de datos personales los cuales pueden ser colectados y tratados para fines administrativos siendo guardados por 5 años, también con fines de seguridad y defensa nacional o seguridad pública por parte de los órganos de inteligencia del Estado.

En cuanto a su implementación mediante artículo 28 de dicha ley se crea la Dirección de Protección de Datos Personales (DIPRODAP) adscrita al Ministerio de la Hacienda y Crédito Público con el objetivo del "control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada". Sin embargo, sigue sin cumplirse el mandato de creación de dicha institución.[135]

En 2020 se crea la Estrategia Nacional de Ciberseguridad que controla las redes sociales y persigue los crímenes provenientes de "gobiernos hostiles y grupos terroristas",[136] y se firma un acuerdo sobre el uso de las tecnologías de la información con Rusia, con el objetivo de "prevenir, detectar e investigar" su uso incorrecto.[137]

11.4.2. Documentación de Casos y Denuncias

En términos generales se expone la documentación de casos y denuncias a través de investigaciones realizadas por la organización *Freedom House* encargada de promover la defensa política en torno a cuestiones de democracia, libertad política y derechos humanos, con ello se presenta su reporte de Libertad en la Red que engloba todos los medios de comunicación locales e internacionales en su estudio, así mismo, se exponen organizaciones en defensa de los derechos humanos como el Centro Nicaragüense de Derechos Humanos (CENIDH).

De conformidad, se expone el reporte de **Libertad en la Red de 2022** realizado por *Freedom House*, en donde se presenta un panorama bastante complejo y represivo ante la creación de la **Ley Especial de Delitos Cibernéticos de 2020** con el objetivo de encarcelar a disidentes por su discurso en línea, la autocensura de los usuarios que optan por el anonimato cuando se expresan en línea y los constantes ataques por piratería, son algunos de los aspectos generales que se exponen. Seguidamente, se detalla que después del año 2018 se han tomado medidas para socavar los derechos humanos por medio de detenciones extrajudiciales, desapariciones y torturas, arrestos, detenciones arbitrarias y denuncias de vigilancia y monitoreo.[138]

---

[135] Morales Angulo, C. (2020). "¿Quién Defiende tus Datos? Nicaragua 2020", *IPANDETEC.*

[136] El Comercio (2020), ver en: https://www.elcomercio.com/actualidad/mundo/nicaragua-decreto-control-redes-sociales.html.

[137] *Swissinfo.ch* (2022), ver en: https://www.swissinfo.ch/spa/nicaragua-y-rusia-firman-acuerdo-sobre-el-uso-de-las-tic/48078854.

[138] *Freedom House* (2022), "Reporte de Libertad en la Red de Nicaragua", ver en: https://freedomhouse.org/country/nicaragua/freedom-net/2022#footnote5_fy92jm9.

En ese mismo reporte, se analiza el control del mercado de los servicios de telefonía fija y móvil por parte del Presidente Ortega y su esposa que poseen alrededor de un 30 por ciento de las acciones de Inversiones Nicaragüenses de Telecomunicaciones en operación con COOTEL junto con la empresa china Xinwei Telecom, asimismo, se resalta que el organismo proveedor de telecomunicaciones TELCOR no respeta los principios de neutralidad e independencia y responde a políticas gubernamentales, por ejemplo, se presenta una falta de nombramientos en examinación y aprobación por la Asamblea Nacional, falta de transparencia en los datos que no se actualizan desde 2011 y el **Acuerdo Administrativo 004-2020** creado con la facultad de ampliar el control sobre los operadores de telecomunicaciones.[139]

En cuanto a dicha ley no se ha informado de ninguna evidencia de que el gobierno o bien los proveedores de servicios bloqueen o filtren contenidos, si bien la **Ley de Ciberdelitos** permite a TELCOR y al Ministerio de Relaciones Exteriores bloquear los sitios web considerados peligrosos, el gobierno no parece tener la capacidad para implementar y hacer cumplir dicho bloqueo. A pesar de las denuncias constantes del CENIDH, que exponen que la ley "no sólo reprime la libertad de expresión y de prensa. También implica espionaje y control absoluto de las redes sociales, plataformas digitales y perfiles en línea. Está dirigida contra activistas políticos, defensores de derechos humanos y toda la población en general que se atreva a oponerse a las políticas gubernamentales".[140]

No obstante, en cuanto a las limitaciones del contenido en el espacio digital, el gobierno nicaragüense ha utilizado las leyes de derechos de autor y la Ley de Derechos de Autor del Milenio Digital de Estados Unidos para lograr la eliminación de contenido producido por medios de comunicación independientes.[141] Por ejemplo, en marzo de 2020 dos cuentas de **YouTube** del canal de noticias independientes 100% Noticias fueron cerradas después de que un medio oficialista presentara quejas por el uso de fotografías y videos.[142]

En ese complejo panorama, Nicaragua carece de organismos independientes que velen por la supervisión de los procesos de restricción de contenidos, las autoridades gubernamentales no actúan con la debida transparencia cuando se trata sobre la eliminación de contenidos en línea. Conforme a la **Ley de Ciberdelitos**, las decisiones de bloquear los sitios web deben ser tomadas por el ente TELCOR y el Ministerio de Relaciones Exteriores dominados por la presidencia Ortega-Murillo.[143]

---

[139] *Ibid., supra* notas 120 y 138. Octavio Enríquez (2022), "La red de negocios privados de la familia Ortega Murillo: 22 empresas a costa del Estado", *Confidencial*, ver en: https://confidencial.digital/politica/la-red-de-negocios-privados-de-la-familia-ortega-murillo-22-empresas-a-costa-del-estado/.

[140] Confidencial (2021), ver en: https://confidencial.digital/english/ortegas-gag-law-takes-effect-in-nicaragua/.

[141] *Access Now* (2023), ver en: https://www.accessnow.org/dmca-takedown-demands-censor-activists/ y https://www.accessnow.org/la-denuncia-por-copyright-como-metodo-de-censura-en-linea-en-nicaragua/.

[142] Comité para la Protección de Periodistas (2020), ver en: https://cpj.org/es/2020/05/youtube-censura-a-medios-independientes-nicaraguen/.

[143] Reporte de Access Now, ver en: https://www.accessnow.org/wp-content/uploads/2018/10/UPR-Nicaragua-digital-human-rights.pdf.

En lo relacionado a la autocensura, debido al clima represivo estatal y la presión extralegal por parte de las fuerzas del régimen, los periodistas y usuarios comunes han seguido expresando su discurso político en línea por medio de plataformas anónimas y encriptadas en lugar de censurarse a totalidad.[144] Se ha dejado de usar firmas, y se han implementado diversas prácticas para protegerse de la represión. Por ejemplo, a través de cuentas anónimas para seguir expresándose y el uso de funciones como "amigos cercanos" en la red social **Instagram** para emitir sus publicaciones.[145]

El régimen también organiza actividades falsas en redes sociales para servir a intereses políticos. Por ejemplo, en una iniciativa llamada Proyecto Digital más de 100 empleados de varias instituciones públicas trabajan desde el edificio de Correos de Nicaragua para producir contenido y publicarlo en múltiples redes sociales incluidas **TikTok, Instagram, Facebook y Twitter**, y se enmarcan en un mandato de crear y difundir noticias e información falsas para brindar un panorama favorable al régimen de Ortega por medio de la difamación de críticos, incitando a la policía al arresto de los mismos y causando ansiedad a la población.[146] Además, durante las masivas protestas de 2018 se emplearon miles de *bots* a favor del gobierno procedentes de Venezuela. [147]

Por su parte, la organización Meta en 2021 informó haber eliminado "una de las operaciones de *trolls* intergubernamentales más grande que habían desbaratado hasta el momento" con una red de más de 1,400 activos (362 cuentas de **Instagram**, 896 cuentas de **Facebook**, 132 páginas de **Facebook** y 24 grupos de **Facebook**) operados por el gobierno y el gobernante Frente Sandinista de Liberación Nacional (FSLN).[148] En enero de 2022 fueron hackeadas cuentas de redes sociales pertenecientes a cuatro medios online independientes el periódico digital Confidencial denunció el hackeo de una cuenta de **WhatsApp** que utilizaba como envió de alertas y recibir denuncias de lectores,[149] asimismo, los usuarios de otros medios como artículo 66, la cuenta de **Twitter** de 100% Noticias y BacanalNica recibieron hackeos.[150]

La censura extrema y represiva ha incluso llegado a los medios de información católicos, en 2022 TELCOR obligó a las empresas de servicio de cable sacar de su programación al Canal Católico

---

[144] Confidencial (2021), ver en: https://confidencial.digital/politica/el-ano-yanomas-en-que-enfrentamos-la-censura-y-resistimos-la-autocensura-en-las-redes-sociales/.

[145] Divergentes (2021), ver en: https://latamjournalismreview.org/es/news/fuentes-anonimas-represion-instala-autocensura-sin-precedentes-en-nicaragua/.

[146] 100% Noticias (2021), ver en: https://100noticias.com.ni/nacionales/106265-rosario-murillo-trolls-redes-sociales-telcor/ y Divergentes (2021), ver en: https://www.divergentes.com/asi-operan-las-turbas-virtuales-del-regimen-que-provocan-zozobra-desde-instituciones-publicas/.

[147] Overture (2018), ver en: https://www.overtureglobal.io/story/nicaraguas-online-civil-war.

[148] Reporte de Meta sobre Actividad No Auténtica (2021), ver en: https://about.fb.com/wp-content/uploads/2021/11/October-2021-CIB-Report-Updated-Nov-5.pdf.

[149] Confidencial (2022), ver en: https://nicaraguainvestiga.com/politica/71610-confidencial-denuncia-hackeo-a-su-numero-de-whatsapp/.

[150] 100% Noticias (2022), ver en: https://100noticias.com.ni/nacionales/112424-whatsapp-medios-comunicacion-nicaragua-hackeados/ y Expediente Público (2022), ver en: https://www.expedientepublico.org/la-verdad-del-regimen-zanahoria-a-propagandistas-y-palo-a-independientes/.

propiedad de la Conferencia Episcopal de Nicaragua, posterior a ellos la señal reapareció bajo el nombre de Nicarao TV, donde se transmite propaganda gubernamental.[151]

En cuanto a la penalización de las personas por sus actividades en línea, se han dictado numerosas sentencias de prisión de varios años por las actividades en línea a raíz de las leyes creadas en especial la **Ley de Delitos Cibernéticos**. Por ejemplo, hasta enero de 2022 había 10 personas acusadas en virtud de Ley de Ciberdelitos, siendo la primera para Donald Margarito Alvarenga y fue sentenciado a 12 años de prisión por presuntamente incitar al "odio y la violencia", socavar la integridad nacional y difundir noticias falsas a través de publicaciones en **Facebook** y mensajes de **WhatsApp**. Asimismo, en febrero de 2022 el periodista Miguel Mendoza Urbina fue condenado a nueve años de prisión tras ser declarado culpable de conspiración para menoscabar la integridad nacional y difundir noticias falsas.[152]

En mayo de 2023, la policía arrestó a la periodista de Televisión Hazel Zamora, del canal de televisión Canal 10, y la acusó de difundir "noticias falsas". También en mayo, las autoridades acusaron a Víctor Ticay, del Canal 10, de traición y de difundir "noticias falsas". Ticay, que fue arrestado originalmente después de publicar imágenes de una celebración de Pascua en **Facebook** en abril, fue condenado en junio y recibió una sentencia de ocho años de prisión en agosto. En julio, el gobierno impidió que el periodista exiliado Marcos Medina viajara a Nicaragua.[153]

Adicionalmente, se denuncia que el régimen de Ortega-Murillo busca "disfrazar" la **Ley de Telecomunicaciones Convergentes** o **Ley 1223** para promover el desarrollo de las comunicaciones y facilitar las inversiones en el campo, pero lo cierto es que se enmarca a ser una Ley de Espionaje como lo señala el analista José Ulloa de la organización de temas de comunicaciones Voces del Sur. Ulloa resalta que se busca "legalizar el espionaje de las comunicaciones de los nicaragüenses", explicando su artículo 1 sobre la finalidad de la ley, al resaltar el término "fiscalizar" pudiendo ser visto como espionaje, así como, el artículo 110 que ordena a los operadores de servicios públicos de telecomunicaciones a suministrar información que sea requerida al ente regulador TELCOR.[154]

11.4.3. Recomendaciones y Reformas Necesarias

Amnistía Internacional recomienda al gobierno de Nicaragua en lo concerniente a la libertad de expresión, privacidad e integrad personal aplicable al entorno digital lo siguiente: [155]

---

[151] *Swissinfo.ch* (2022), ver en: https://www.swissinfo.ch/spa/la-censura-en-nicaragua-alcanza-a-medios-cat%c3%b3licos-denuncia-voces-del-sur/47665146.

[152] Confidencial (2022), ver en: https://confidencial.digital/nacion/doce-anos-de-carcel-por-opinar-en-facebook-y-mensajes-de-whatsapp/ y CPJ (2022), ver en: https://cpj.org/es/2022/02/condenan-al-periodista-nicaraguense-miguel-mendoza-por-los-delitos-de-difundir-noticias-falsas-y-conspirar-contra-la-integridad-nacional/.

[153] *Freedom House* (2024), "Libertad en el Mundo, Nicaragua", ver en, https://freedomhouse.org/country/nicaragua/freedom-world/2024.

[154] Artículo 66 (2024), ver en: https://www.articulo66.com/2024/03/12/nueva-ley-telecomunicaciones-telcor-voces-del-sur/.

[155] Amnistía Internacional (2023). "Un grito por la Justicia, 5 años de Opresión y Resistencia en Nicaragua", ver en: https://www.amnesty.org/es/documents/amr43/6679/2023/es/.

1. Dar marcha atrás a las normas legales que violan derechos humanos reconocidos en el derecho internacional, en particular derogar o reformar la Ley de Regulación de Agentes Extranjeros, la Ley Especial de Ciberdelitos y la Ley de defensa de los derechos del pueblo a la independencia, la soberanía y autoderminación para la paz para ajustar el sistema legal nicaragüense a las normas y estándares del derecho internacional de los derechos humanos;
2. Detener la criminalización injusta, estigmatización y hostigamiento de personas defensoras de los derechos humanos, periodistas y aquellas que actúan, o son percibidas, como críticas del gobierno;
3. Devolver la personalidad jurídica a las organizaciones de derechos humanos, periodismo y de otras materias que han sido afectadas, así como gestionar la pronta devolución de sus patrimonios; y
4. Abrirse al escrutinio internacional, lo cual incluye asegurar la permanencia de Nicaragua en el Sistema Interamericana de Derechos Humanos y garantizar la adecuada cooperación estatal con los órganos del sistema, incluyendo el cumplimiento irrestricto de sus órdenes de protección.

El Parlamento Europeo en su Resolución B9-0273 de 2023 sobre la situación de Nicaragua y las recomendaciones del Grupo de Expertos en Derechos Humanos sobre Nicaragua de las Naciones Unidas,[156] solicita lo siguiente:

5. El régimen nicaragüense debe poner fin a su política de aislamiento de la comunidad internacional y que permita el retorno de las organizaciones internacionales al país, en particular la CIDH y la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, con el fin de supervisar la situación de los derechos humanos; y
6. Las instituciones nicaragüenses deben abstenerse de cometer graves violaciones y abusos a los derechos humanos de las y los ciudadanos, asimismo, deben ofrecer acceso a la justicia y reparaciones plenas a las víctimas.

La CIDH bajo su Relatoría sobre Libertad de Expresión en su informe anual de 2023,[157] recomienda a los Estados en lo referente a la libertad de expresión en línea lo siguiente:

7. Evitar marcos regulatorios a los intermediarios de internet por el contenido de usuarios que circula en sus plataformas, lo que puede incentivar la dinámica de la "censura privada";
8. Evitar la creación de leyes generales y/o ambiguas con el fin de combatir la desinformación en internet, como así el uso de prohibiciones penales para castigar la difusión de "falsedades" o "información no objetiva"; e

[156] Resolución del Parlamento Europeo sobre la situación en Nicaragua (2023/2743(RSP)), ver en: https://www.europarl.europa.eu/doceo/document/B-9-2023-0273_ES.html y Resolución aprobada por el Consejo de Derechos Humanos el 31 de marzo de 2022 sobre Nicaragua A/HRC/RES/49/3.
[157] CIDH (2023). "Informe Anual de la Relatoría Especial para la Libertad de Expresión de 2023".

9. Involucrarse en los diálogos multilaterales con el objetivo de construir consensos en clave y conforme a estándares del derecho internacional de los derechos humanos, especialmente en materia de moderación de contenidos en línea y la gobernanza de internet.

Otras recomendaciones contemplan:[158]

10. Derogar el marco jurídico represor, abstenerse de instrumentalizar el derecho penal y administrativo para perseguir el ejercicio legítimo de la libre expresión, proteger y garantizar la libertad en independencia de la prensa y de los periodistas, tanto en línea como fuera de ella;
11. Restablecer la personería jurídica de medios de prensa, proteger y asegurar su funcionamiento, reapertura, independencia, así como el pluralismo y diversidad de estos;
12. Establecer un sistema nacional de registro de casos de violaciones a los derechos humanos de la población para monitorear, investigar, documentar y reparar las violaciones a derechos humanos en el entorno físico como digital; y
13. Garantizar el acceso libre al servicio de internet y a los contenidos que circulan en esta bajo condiciones de neutralidad, privacidad, y garantías de no persecución o monitoreo en línea.
14. Ante la escalada represiva se recomienda a la población civil medidas de seguridad digital para tratar de minimizar los riesgos a su privacidad y protección en línea

12. La Desinformación y Manipulación Digital en los Procesos Electorales

En este apartado se procede al análisis de la manipulación digital en los procesos electorales y las consecuencias de la desinformación o *fake news* dentro de dichos procesos. Se divide en tres partes: a) conceptos generales sobre manipulación digital y desinformación; b) ejemplos de campañas de desinformación en Guatemala, Honduras, El Salvador y Nicaragua; y c) medidas para mitigar el impacto de la desinformación digital en los procesos electorales.

12.1. Conceptos Generales

La **manipulación de información** es un "conjunto de tácticas que implican la recopilación y difusión de información para influir o perturbar la toma de decisiones democrática" pudiendo apropiarse de los canales de información comúnmente tradicionales, la prensa escrita o la radio. Sin embargo, en este análisis nos enfocamos en los aspectos digitales de la información, es decir a través del uso de las redes sociales (**Facebook, Instagram, X, TikTok, YouTube**, etc.) y otros medios digitales de información.[159]

Como **actores amenazantes** podemos encontrar: a) los partidos políticos y las campañas, con el objetivo de desacreditar a la oposición y apoyo a su agenda de política; b) los gobiernos extranjeros y nacionales, vístase como herramienta de gobernar y la geopolítica, así como de influir en las

[158] IPANDETEC (2024). "Recomendaciones para Nicaragua sobre Derechos Humanos en Entornos Digitales".
[159] Arnaudo, D. et al. (2021). "Combatiendo la manipulación de información: Un manual para las elecciones y posterior a ellas". *Instituto Republicano Internacional, National Democratic Institute y Stanford Internet Observatory*, pp. 5-7, ver en: https://www.iri.org/wp-content/uploads/2021/12/infomanip_playbook_spanish_final-1.pdf.

actitudes públicas y reprimir la participación política; c) los medios de comunicación no independientes y actores comerciales, influyen en las actitudes del público dependiendo de sus patrocinadores; y d) grupos extremistas, encargados de promover su agenda a través del odio y polarización política.[160]

La **desinformación en línea** puede entenderse como la creación, distribución y ampliación de "información falsa, inexacta o engañosa". Se pueden observar 2 ejemplos dentro de la desinformación aplicada en contextos digitales: a) la propaganda, implica la desinformación robada o verdades a medias para influir en las personas, comúnmente utilizada por los gobiernos en Centroamérica y b) el discurso de odio, bajo el uso del "lenguaje discriminatorio" haciendo referencia a la "identidad, incluida la religión, etnia, nacionalidad, capacidad, género u orientación sexual de una persona". En el contexto electoral se presenta con el objetivo de manipular la información polarizando el discurso político y suprimiendo la participación política de un grupo en específico.[161]

Algunas de las **tácticas digitales** que se usan son: la tecnología generada por medio de la Inteligencia Artificial, el contenido visual manipulado, la propaganda computacional, las cuentas falsas o *sock puppet*, la manipulación de motores de búsqueda, sitios webs falsos, la censura, el *trolling* (intimidación o acoso para provocar una reacción emocional), la publicidad o *microtargeting*, las operaciones de pirateo y fuga, entre otras.[162]

12.2. Situación en Guatemala, Honduras El Salvador y Nicaragua

En el apartado anterior sobre la evaluación de legislación actual en los Estados en análisis pudimos observar que los mismos cuentan con un vacío legal en cuanto a la protección de datos personales en el ámbito digital, la desinformación en línea y la manipulación digital, salvo El Salvador y Nicaragua que cuentan con legislaciones contra Delitos Informáticos o Ciberdelitos, aunque como se analizó anteriormente su finalidad es la censura y el control de la información con tácticas represivas o bien como respuesta punitivista.[163]

Ante ese panorama, se presentan algunos ejemplos de cómo la manipulación digital y la desinformación o *fake news* afecta a los procesos electorales y se traslada al electorado para injerir en la toma de decisión final.

En **Guatemala**, la Misión de Observación Electoral de Guatemala (MOE-Gt) con la participación de 7 organizaciones de la sociedad civil y más de 1,400 observadores a través de su Informe de Interacción en Redes Sociales de septiembre de 2023, brindaron información sobre una serie de ataques y desinformación en línea. Por ejemplo, un ataque al Movimiento Semilla por medio de un **TikTok** en vivo y varias cuentas de dicha aplicación, haciendo burla de una actitud que había

[160] *Ibid., supra* nota 159.
[161] *Ibid., supra* nota 159.
[162] *Ibid., supra* nota 159.
[163] Sobrado González, L. (2024). "La desinformación en los procesos electorales: ¿respuesta punitivista o empoderamiento ciudadano?". *Archivos Jurídicos de la UNAM.*

tomado dicho partido político para defenderse ante la fiscalía y un ataque a Bernardo Arévalo presidente electo de Guatemala con información falsa sobre su vida privada y familiar. Asimismo, varios políticos como Miguel Martínez, Consuelo Porras y el expresidente Giammattei sufrieron ataques a su integridad personal por la desinformación digital.[164]

El MOE-Gt en su Séptimo Informe sobre la Situación Electoral en Guatemala registró 114 hechos de violencia electoral y 151 de conflictividad electoral en 2023 cuando se desarrollaban las elecciones en Guatemala, los registros incluyen ataques por medio de redes sociales Dentro de ese informe se documentó ataques a la candidata Sandra Torres por medio de **TikTok** donde se señala en un video que cuenta con vínculos con la mara 18 y de estar relacionada con motines en centros de detención preventiva y bajo en la aplicación **X**, se le acusa de corrupción y malversación de fondos públicos.[165]

También, a Eleonora Castillo subregidora de ciudadanía se le acusó de tener una plaza en la Municipalidad de Mixco por medio de una campaña en las redes sociales, asimismo, las personas que atendieron al paro el 24 de julio de 2023 se les amenazó de muerte por medio de la cuenta de Armando de León excandidato a diputado del partido Valor. Además, el elegido presidente de Guatemala cuando corría por la presidencia sufrió ataques de desinformación a través de **TikTok** y **X**, mencionado que "atacará la iglesia y las creencias guatemaltecas", "están en contra de la iglesia" y "son proaborto".[166]

En ese orden, se detalla que los ataques y campañas de desinformación en las redes sociales aumentaron especialmente en contra de Bernardo Arévalo con el objetivo de deslegitimar su candidatura y el intento de socavar la democracia por sus opositores.[167]

En **Honduras**, el reconocido Centro Carter quien actúa como observador en procesos electorales a nivel internacional, llevó a cabo una investigación sobre las redes sociales durante el proceso electoral en Honduras en 2021 con enfoque en las elecciones primarias de marzo 2021 y las elecciones generales de noviembre de 2021. Dentro de esa investigación, se analizó la infracción de las normas sobre el uso de propaganda electoral en campaña, la intoxicación del debate político mediante desinformación, y el uso de redes de *bots* para la distorsión artificial del debate político.[168]

---

[164] Informe de interacción en redes sociales (MOE-Gt) (2023), ver en: https://moe.gt/publicaciones-desinformacion-y-medios-de-comunicacion-rrss-informe-26/.
[165] Séptimo informe | Misión de Observación Electoral de Guatemala (2023), ver en: https://moe.gt/septimo-informe-mision-de-observacion-electoral-de-guatemala/.
[166] *Ibid., supra* nota 164.
[167] Gamarro, U. (2023). "Elecciones Generales Guatemala 2023", La Prensa Libre, ver en: https://www.prensalibre.com/guatemala/elecciones-generales-guatemala-2023/ataques-y-campanas-de-desinformacion-aumentaron-en-redes-sociales-especialmente-contra-bernardo-arevalo-dice-moe-gt/.
[168] El Centro Carter (2021). "Análisis de las redes de bots que han operado en Honduras en las elecciones primarias y generales de 2021", ver en: https://www.cartercenter.org/resources/pdfs/news/peace_publications/democracy/honduras-botnets-analysis-sp-022322.pdf.

En su informe se detectó el uso de redes de *bots* por los tres principales partidos en campaña: Libertad y Refundación (LIBRE), el Partido Nacional de Honduras (PNH) y el Partido Liberal de Honduras (PLH). La empresa de ciberseguridad NISOS denunció la existencia de 317 cuentas que durante 8 días buscaban transmitir información falsa para disuadir a los hondureños de votar por Xiomara Castro y animarlos a la abstención. También, al candidato del PLH, Yani Rosenthal se diseminó información sobre riesgos de corrupción y lavado de dinero, en ese entonces **Twitter** suspendió esas cuentas a inicios de noviembre de 2021.[169]

Las etiquetas que se usaban en las redes sociales durante la campaña electoral eran las siguientes: #sevan y #novolverán utilizados por el Partido Libre y Nacional; #depuremoselcongreso, #sivasconyanisosnarco, #fuerajoh, #jodidosporyani, usadas sobre todo por el Partido Libre; y el candidato Yani Rosenthal sufrió desacreditaciones y apoyo por medio de **Twitter** bajo etiquetas de #ibu y #con1500lempiras ya que promovían un Ingreso Básico Universal (IBU) de 1,500 lempiras.[170]

También, en ese mismo informe se documentó una serie de contenidos falsos y engañosos en la campaña electoral de 2021, pudiéndose detectar que los artículos con informaciones falsas o *fake news* aparecían esporádicamente, sin seguir un esquema de publicación congruente que caracteriza a los medios profesionales, se compartían noticias anónimas sin firma, los dominios de internet bajo los que operan estaban ocultos con un supuesto país de procedencia de El Salvador y todas las publicaciones estaban alojadas bajo la misma dirección IPv4 y su línea editorial presentaba un sesgo acentuado en contra de los candidatos del Partido Nacional y Liberal pero mostraban uno favorable al Partido Libre.[171]

En esa misma línea, se analizó el incremento artificial de la base de seguidores, donde se pudo observar que la presidenta electa Xiomara Castro un mes antes de la contienda electoral incrementó en un 65% sus seguidores en **Twitter** en la cual se calcula que el 32% de los perfiles son *bots*, 16% perfiles que podrían no ser reales, el 12% ha sido creado durante la campaña electoral y un 9,4% de las cuentas fueron borradas o suspendidas por **Twitter**.[172]

Además, medios de comunicación locales detallaron que dentro del proceso electoral de 2021 se realizaron campañas engañosas con el objetivo de brindar falsas acusaciones en contra de los candidatos a la presidencia y se mencionaban "alianzas secretas entre los políticos" con la finalidad de deslegitimizar sus candidaturas, se analizaron contenidos de odio repleto de desinformación y difamaciones para intentar posicionar la opinión pública hacía una ideología.[173]

En **El Salvador**, se presenta un panorama muy distinto de Guatemala y Honduras, debido a que en las elecciones de 2023 el Partido Nuevas Ideas bajo el mandato del presidente Nayib Bukele

[169] *Ibid., supra* nota 168.
[170] *Ibid., supra* nota 168.
[171] *Ibid., supra* nota 168.
[172] *Ibid., supra* nota 168.
[173] Barahona, J. (2021). "Investigación expone campaña de desinformación en elecciones 2021*". El Tiempo*, ver en: https://tiempo.hn/investigacion-desinformacion-elecciones-honduras-2021/.

presentaba un apoyo muy fuerte por parte de la población salvadoreña, así como, un grupo opositor muy debilitado con muy poco apoyo de la ciudadanía, sumado a la popularidad creciente del mandatario Bukele.

Sin embargo, en la campaña electoral de 2019 en El Salvador bajo un reportaje de *France 24* se documentó que bajo las redes sociales se le dio favoritismo al mandatario Bukele. Se detalla que "esquematizó de mejor forma lo que quería plantear, nos mostró de mejor manera y de una forma futurista lo que él quería para nuestro país". A su vez, se le acusa de una campaña de ver la información política a través del entretenimiento y la manipulación de las redes a través de robots. Además, se deja ver al candidato y mandatario Bukele como un animador, dado que, busca entretener a la población con la desinformación y cuestionando a sus adversarios.[174]

En **Nicaragua**, se presenta con leyes represivas y punitivas expuestas en el análisis anterior, sumado al control de los medios de comunicación, la presión por el control de las redes sociales, el clima general de miedo y terror que restringe la libertad de expresión.[175] Ante ese panorama, se estudian algunos casos, en donde, el gobierno de Nicaragua ha ejercido el uso indebido en las redes sociales mediante las aplicaciones de Meta en especial **Facebook e Instagram**.

En octubre de 2021 Meta realizó un informe del Comportamiento Inauténtico Coordinado en Nicaragua, en donde Meta eliminó unas 937 cuentas falsas en **Facebook** y 363 en **Instagram**. Además, eliminó 140 páginas y 24 grupos, todas pertenecientes a una red que buscaba manipular a la opinión pública de cara a las elecciones. El informe detalla que desde 2018 y 2019 el discurso en las redes sociales se basó en desacreditar a miembros de la oposición y enfocarse en publicar y amplificar artificialmente elogios al gobierno nicaragüense y al partido oficialista el Frente Sandinista de Liberación Nacional (FSLN).[176]

12.3. Medidas para Mitigar el Impacto de la Desinformación y Manipulación Digital

La organización *Freedom House* brinda una serie de medidas a las empresas de comunicaciones y redes sociales,[177] así como, a los gobiernos en el marco de elecciones libres y justas en 2024 aplicadas al ámbito digital, que incluyen las siguientes:

a) Los gobiernos democráticos, la sociedad civil y las empresas tecnológicas deben defenderse de los daños de la inteligencia artificial durante los períodos electorales;
b) Los partidos políticos, los comités y las campañas deberían abstenerse de tergiversar intencionalmente a los candidatos en la publicidad que presenta imágenes generadas o manipuladas por la Inteligencia Artificial;

[174] Regidor, C. (2019). "El Salvador: el uso de redes sociales que le dio favoritismo a Bukele en su campaña presidencial", *France 24*, ver en: https://www.france24.com/es/20190203-salvador-presidenciales-redes-bukele-campana.
[175] *Ibid., supra* nota 153.
[176] Meta (2021), "Informe de Comportamiento Inauténtico Coordinado – Octubre 2021", ver en: https://about.fb.com/ltam/news/2021/11/informe-de-comportamiento-inautentico-coordinado-octubre-2021/.
[177] *Freedom House* (2023). "Freedom on The Net 2023, The Repressive Power of Artificial Intelligence", pp. 30-35, ver en: https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.

c) Las empresas tecnológicas deberían aumentar los esfuerzos para defender la integridad electoral;
d) Apoyar la accesibilidad de la tecnología de elusión y resistirse a las órdenes gubernamentales de cerrar la conectividad a Internet o prohibir los servicios digitales durante un período electoral;
e) Trabajar en estrecha colaboración con investigadores independientes que puedan estudiar los efectos que sus servicios tienen sobre la integridad de la información y la libertad de expresión; y
f) Las empresas deberían invertir en personal dedicado a trabajar en cuestiones de derechos humanos, incluidos especialistas regionales y nacionales, para comprender mejor el impacto local de sus productos.

La organización IDEA encargada de promover la democracia nivel mundial,[178] brinda una serie de recomendaciones que los gobiernos deben seguir para asegurar el efectivo uso de la información de los medios de comunicación incluidas las redes sociales en los procesos electorales, siguiendo estándares internacionales, dentro de ellas se encuentran:

g) Los organismos electorales deben proveer los recursos necesarios para mitigar y desacreditar las actividades de desinformación electoral, así como promover la alfabetización mediática;
h) Garantizar de forma proactiva que los sistemas algorítmicos de recomendación no impidan el acceso a información electoral precisa o a una pluralidad de opiniones dentro del espectro democrático;
i) Incluir algoritmos de aprendizaje automático (*machine learning*) para frenar la viralidad de la desinformación electoral;
j) Garantizar que la publicidad política esté claramente identificada, que el uso de datos personales sensibles para direccionar anuncios políticos esté prohibido; y
k) Difundir la información financiera relativa al pago de anuncios en línea y establecer una estricta política corporativa que limite la publicidad política de acuerdo con las regulaciones vigentes en cada país con respecto al financiamiento político.

13. Entrevistas a Expertos en Derechos Digitales

En esta sección se desarrollan una serie de entrevistas a expertos en la materia de derechos digitales de Honduras, Guatemala, El Salvador y Nicaragua con el objetivo de obtener una perspectiva detallada y contextual dichos derechos. La dinámica de las entrevistas se basa principalmente en 5 preguntas:

1) ¿Cuál es el contexto general sobre los derechos digitales en su país?
2) ¿Cuáles son las legislaciones a favor, represivas y faltantes?

[178] IDEA (2024). "Proteger las elecciones democráticas mediante el resguardo de la integridad de la información", pp. 4-6, ver en: https://www.idea.int/publications/catalogue/protecting-democratic-elections-through-safeguarding-information-integrity?lang=es.

3) ¿Qué se sabe sobre la privacidad digital y la libertad de expresión en línea?
4) ¿Existe desinformación y manipulación digital en los procesos electorales?
5) ¿Qué reformas son necesarias para garantizar los derechos digitales?

Se entrevistó a:

- Abogado Carlos Sierra del Centro de Promoción e Investigación de Derechos Humanos (CIPRODEH) de Honduras;
- Ingeniero Efrén Godoy de la Plataforma de Organizaciones de la Sociedad Civil, OSConectadas de Honduras;
- Abogado Alejandro Valverth, la Asociación para el Desarrollo Legislativo y la Democracia (LEGIS) de Guatemala;
- Experto Legal Anónimo de Nicaragua; e
- Ismelda Villacorta, en representación del equipo de Fundación de Estudios para la Aplicación del Derecho (FESPAD) de El Salvador.

13.1. Estado de Honduras

13.1.1. Carlos Sierra de la organización CIPRODEH[179]

Carlos Sierra de CIPRODEH expone la **situación de Honduras** como un Estado "sin regulaciones" y con un "vacío legal" sobre la materia de derechos digitales en el país. Comienza analizando el marco normativo primario la Ley de Telecomunicaciones donde se regula el espectro radial y la otorgación de frecuencias de televisión y radio, y con impacto directo en los medios de comunicación y redes sociales. Además, detalla que en Honduras se presenta un "emporio empresarial" que controla al país, un "emporio de internet", concesiones a compañías telefónicas que dominan el mercado de internet.

También, menciona un ejemplo "en la pandemia del Covid-19 el margen de cobertura de internet era muy bajo y la ley favorece a las compañías de telecomunicaciones, por ende, hubo mucha exclusión de acceso a la internet durante ese tiempo".

En ese mismo orden, **sobre la legislación actual** en materia de derechos digitales, menciona que en Honduras la Ley de Acceso a la Información Pública es más usada para "el tema de auditorías, veedurías y portales de transparencia de las instituciones públicas" y por ende no protege verdaderamente los datos personales de las y los ciudadanos, dejándolos "desprotegidos" ante ataques cibernéticos. En esa línea, menciona que ante última iniciativa de una Ley de Ciberseguridad hasta la fecha "no se tiene nada concreto ni existen propuestas sobre la mesa", solamente "se menciona un apartado sobre ataques cibernéticos en la Estrategia Nacional contra el Crimen Organizado de Honduras en colaboración con las Naciones Unidas".

[179] Entrevista realizada el día 15 de agosto de 2024 a las 10 am por medio de la plataforma *Google Meet* a Carlos Sierra quien es el Coordinador y Soporte Técnico del Programa de Seguridad Ciudadana en el Centro de Promoción e Investigación de Derechos Humanos en Honduras (CIPRODEH).

Sobre la **privacidad digital y liberad de expresión en línea** se refiere al Código Penal de 2019 menciona que los delitos de injuria y el honor aún forman parte de dicha normativa y también menciona en especial atención a la tipificación del delito de terrorismo y asociación para delinquir dentro de ámbito penal, dado que, "no es clara su normativa" y pareciera "perseguir intereses particulares o políticos".

En cuanto a la **desinformación digital en los procesos electorales**, menciona "la hegemonía de los medios de comunicación, las corporaciones que controlan prácticamente todo el mercado nacional" así como, una fuerte "debilidad institucional que tiene el país, con canales de difusión concentrados, no confiables, no amplias y no accesibles", y se denota "su debilidad en los procesos electorales". Además, menciona "que dichos medios generan encuestas a boca de urna y anticipan los procesos electorales generando mucha desinformación por medio de las redes sociales y hacienda una labor que no les compete".

En esa línea, añade que "en Honduras en Consejo Nacional Electoral puede tardarse hasta 1 o 2 semanas en brindar el total de los resultados de las elecciones, lo que genera mucha especulación en las redes, y los medios de comunicación toman ventaja de ello".

Sobre las **reformas necesarias y recomendaciones** brinda las siguientes:

9.2. La progresividad de los derechos humanos y sus avances de ellos en el ámbito digital y de las comunicaciones;
9.3. Actualización de la norma primaria, la Ley de Telecomunicaciones, en donde, deben abrirse el "espectro electro radial", ya que "el acceso a la internet es bajo, controlado y la calidad del mismo no es buena";
9.4. El Estado debe brindar mayor cobertura de internet y de electricidad bajo la presencia estatal. Por ejemplo, en la Mosquitia y Roatán el fluido eléctrico es controlado por empresas privadas;
9.5. Mayor presencia estatal en todos los departamentos del país para garantizar la efectividad del acceso a las telecomunicaciones;
9.6. Regular el Código Penal sobre los delitos al honor e injuria y pasarlos al ámbito civil;
9.7. Inversión por parte del gobierno en educación digital y la importancia de la alfabetización digital e informática en las escuelas de todo el país;
9.8. Revisar la Ley de Acceso a la Información Pública para brindar mayor protección a las y los ciudadanos; y
9.9. Minimizar el riesgo de la exclusión que puede generar el avance digital en Honduras.

13.1.2. Efrén Godoy de la plataforma OSConectadas[180]

Efrén Godoy se presenta como Ingeniero en Sistemas conocedor sobre los derechos digitales en Honduras a través de sus años de experiencia en el sector de las telecomunicaciones. En esta entrevista desarrolla puntualmente las 5 preguntas.

Sobre el **contexto general** de la materia, expone que "en Honduras los derechos digitales son muy poco conocidos, la gente no sabe mucho de ello y poco se habla, a pesar de ser un tema de gran relevancia en la actualidad, también, es un tema poco desarrollado con pocas leyes y sin voluntad de los gobiernos por mejorar la situación". No obstante, menciona que "en Honduras existe un acceso del 80% a la internet y ha ido en aumento al pasar de los años, especialmente el internet móvil, casi todos cuentan con acceso a la internet, el costo de los megabytes ha bajado, aunque aún existe mucha desigualdad en las zonas rurales en cuanto a su acceso".

En su introducción menciona un caso de Guatemala que menciona también Alejandro Valverth sobre los menores de edad de un centro educativo en Guatemala que distorsionaron unas fotos normales de sus compañeras transformándolas en "fotos desnudas" y exponiéndolas a las redes sociales. Esto como "un ejemplo de los riesgos de la falta de regulación en la materia en Centroamérica y que pudiera ocurrir en Honduras".

En cuanto a las **leyes actuales**, comienza detallando "en Honduras hacen falta instrumentos y mecanismos para proteger los datos personales de las personas en el espacio digital, son inexistentes, solo han existido intentos como la Ley de Redes Sociales, pero no se logró su aprobación". Asimismo, detalla que la Ley de Intervención de las Comunicaciones guiada por una unidad de la DPI de la Policía Nacional "es un arma que tienen los políticos en el país para invadir las llamadas telefónicas de las personas aduciendo que se trata de actos criminales cuando puede no ser así, esto debido a la corrupción tan grande de Honduras".

Sumado a ello, "se presenta la Ley de Lavado de Activos que puede interferir en la privacidad de las personas y pudiera ser también en el espacio digital".

Asimismo, menciona que el Código Penal de Honduras "es insuficiente tan solo presenta algunos delitos cibernéticos, se necesita una ley específica o bien ampliar esos delitos dentro de ese Código".

En su tercer punto sobre la **privacidad digital y la libertad de expresión en línea**, expone que en Honduras se presenta una situación de libertad en las redes sociales y de las y los ciudadanos de publicar y hacer uso de la información. Sin embargo, menciona que cuando trabajo en el Pulso un diario digital "identifique ciertos patrones del gobierno anterior de Juan Orlando cuando publicábamos información contraria al gobierno, nos invadían la página para tratar de hackearla y lo lograban, solamente cuando se publicaba algo contrario a ellos". Con ello deja entrever que "en

[180] Entrevista realizada el día 23 de agosto a las 10 am por medio de plataforma *Google Meet* al colaborador e Ingeniero en Sistemas Efrén Godoy de la Plataforma OSConectadas que agrupa diversas organizaciones de la sociedad civil en defensa de marcos regulatorios, políticas de gobierno y otros que son de interés para la población hondureña.

Honduras existe libertad en los medios solamente cuando no comentas nada de partidos políticos y no atacas al gobierno".

En esa línea, menciona los "ataques constantes del secretario del Congreso Nacional a la privacidad digital y libertad de expresión de los hondureños a través de campañas de desprestigio de los medios de comunicación".

Además, se presentan riesgos a través de las redes sociales que no son controlados por el Estado por la falta de regulaciones menciona que "**You Tube, Facebook, Amazon, Alibaba, X** y otras aplicaciones pueden tener acceso a nuestros datos personales y generar algoritmos dependiendo de nuestros gustos sin regulación por parte de nuestro gobierno, dejándonos sin protección a nuestra privacidad digital", Asimismo, "las cookies representan una amenaza, ya que almacenan nuestra información y generan patrones de búsqueda y el control de nuestros datos personales".

Sobre la **desinformación digital en los procesos electorales** en Honduras "presenta muchas *fake news* e intentos de desprestigio por parte de los medios de comunicación, representando solo interés de partidos políticos con falta de imparcialidad, veracidad y neutralidad". A su vez, "se crean perfiles falsos que buscan atacar a los partidos políticos, generando una división en la sociedad entre la izquierda y la derecha", esto debido "la falta de medios imparciales en la carrera del periodismo, que deberían ser neutrales sin trastocar la veracidad de la información". También, menciona que "los *Call Centers* en Honduras generan opiniones parciales a través de la empresa privada y se denota que su función es orientada a generar división en la sociedad".

En definitiva, menciona como último punto las **reformas necesarias**, dentro de las cuales se encuentran:

1. Impulsar el tema de los derechos digitales en especial la privacidad digital y los datos personales dentro de todos los sectores del país;
2. Generar espacios de análisis sobre la materia como fomento de la investigación que conlleve a su desarrollo;
3. Abrir espacios de *lobbying* dentro de todos los sectores de la sociedad en conjunto con el gobierno y con ello permitir la creación del marco jurídico faltante;
4. Revisar el último anteproyecto de ley sobre las redes sociales y ver si se acopla a la realidad actual;
5. La creación de un gobierno digital y electrónico; y
6. La educación digital dentro de los centros educativos y universitarios.

13.2. Estado de Nicaragua

13.2.1. Experto Legal Anónimo[181]

El ejercicio de esta entrevista se realizó bajo el anonimato de por medio de una aplicación de mensajería no tan común en el país. Con ello se evidencia un claro ejemplo de la falta de libertad de expresión en línea en Nicaragua, sumado al temor de las y los ciudadanos de utilizar medios tradicionales de mensajería como **WhatsApp, Instagram** o **X**.

El experto legal brinda un panorama de la **situación de Nicaragua** bastante crítico al brindar detalles sobre las leyes represivas creadas después de 2020 como la Ley de Ciberdelitos y la Ley de Soberanía que promueven la censura ciudadana a través de las redes sociales y medios de comunicación. También, detalla que existe dentro de las garantías constitucionales el recurso de Hábeas Data, la Ley de Acceso a la Información Pública y la Ley de Datos Personales con la finalidad de garantizar el derecho de protección de datos personales, acceso a la información y la protección de la privacidad, sin embargo, resalta que dichas normativas en la práctica no son empleadas para salvaguardar la integrad personal del ciudadano en el espacio digital.

Además, es fundamental destacar la ausencia de un marco legal adecuado en Nicaragua que regule el acceso a internet, lo cual resulta en una restricción significativa de este derecho en la práctica. Esta carencia normativa facilita la imposición de censura estatal, especialmente mediante la aplicación de leyes represivas. En particular, la Ley de Ciberdelitos se ha convertido en un instrumento de control estatal, utilizado para perseguir judicialmente a cualquier crítico del gobierno, vinculándolos con otras normativas penales. Esta situación genera un entorno donde la libertad de expresión en el ámbito digital se ve gravemente comprometida, afectando el ejercicio pleno de derechos fundamentales. No obstante, se resalta que en Nicaragua la cobertura de internet se ha incrementado grandemente y se cuenta con una red de banda ancha bastante accesible y funcional, así como una infraestructura de las telecomunicaciones en constante crecimiento y acceso a la internet en espacios públicos.

Sobre la Ley de Telecomunicaciones y Servicios Postales, se menciona que el ente regulador TELCOR presenta afines políticos, empresas ligadas a las telecomunicaciones rinden cuentas al gobierno o bien son partes de ellos, a pesar de que Tigo y Claro son operadores internacionales.

Por ejemplo, menciona que "se habla de 39 antenas telefónicas que no pertenecen a Tigo y Claro pudiendo ser de espías de la administración del gobierno para monitorear las redes sociales y las comunicaciones de todas las personas en Nicaragua".[182]

En cuanto a la **privacidad digital y libertad de expresión en línea**, menciona que "en las redes sociales existe mucha autocensura debido al temor que se vive dentro de la población por las

[181] Entrevista realizada el día 17 de agosto a las 8 am por medio de una aplicación móvil.
[182] *Deutsche Welle*, "Nicaragua: Detectan 39 falsas antenas que espían celulares," *DW.com*, publicado el 18 de octubre de 2022, ver en: https://www.dw.com/es/nicaragua-detectan-39-falsas-antenas-que-esp%C3%ADan-celulares/a-63468522

acciones represivas del gobierno" y "se deja a un lado cualquier espacio de disidencia en el país con nulos espacios cívicos, medios de comunicación independientes y más de 3 mil organizaciones sin fines de lucro cerradas". Durante la entrevista, se mencionó que habían sido cerradas más de 5,000 organizaciones sin fines de lucro desde 2018. Asimismo, el 19 de agosto de 2024, el gobierno clausuró 1,500 adicionales mediante un único decreto.[183]

El entorno de las redes sociales se torna bastante complejo cuando se presenta la desinformación en línea o *fake news,* ya que, no se cuenta con medios de comunicación independientes, se circulan en las redes numerosas páginas falsas de información mediante blogs, enlaces de internet y esos mismos se circulan por todo el territorio a pesar de tener certeza de su veracidad.

En esa misma línea, el experto legal recurre a la obra de Ray Bradbury, *Fahrenheit 451*, para ilustrar la situación en Nicaragua en relación con las noticias falsas. En la novela, Bradbury describe una sociedad donde la manipulación de la información y la censura mantienen a la población en un estado de ignorancia y conformismo. El experto señala que, al igual que en *Fahrenheit 451*, en Nicaragua "todo lo que aparece en los medios de comunicación es tomado como verdad; si se inventa una invasión marciana, la población se prepara para ella". Esto refleja cómo, debido al acceso limitado a fuentes de información verídicas y la falta de educación digital, la sociedad nicaragüense se vuelve vulnerable a la manipulación y la desinformación, preparando a la gente para realidades fabricadas.

De igual forma, detalla que en Nicaragua "no existe la educación digital y muchas personas desconocen sobre las nuevas tecnologías como la inteligencia artificial, es muy limitado su conocimiento se conoce poco sobre el tema y por ende las personas utilizan los mismos motores de búsqueda comunes controlados por el gobierno".

En cuanto a la **desinformación en línea dentro de los procesos electorales**, denota que la misma "se presenta bajo un ambiente de desconfianza que conlleva al abstencionismo y la pérdida de confianza de las y los ciudadanos del proceso electoral". Asimismo, menciona que "la desinformación digital es un arma poderosa que los políticos usan para controlar la información y generan incertidumbre".

Ante todo, ese panorama represivo, hostil y en socavo de la democracia a través de las redes sociales, medios de comunicación brinda una **serie de medidas** que deberían de tomarse para garantizar la privacidad digital y la libertad de expresión en línea, tales como:

1. Se deben reformar la legislación existente sobre ciberdelitos, debido a que, la misma atenta contra la libertad de expresión en línea, se crea un ambiente hostil, se cierra el espacio cívico y se socava la democracia;
2. Se debe derogar la Ley de Soberanía, la misma atenta contra la integridad personal al existir el delito de terrorismo, expandiéndose al ciberterrorismo;

[183] *Deutsche Welle*, "Gobierno de Nicaragua ilegaliza otras 1500 ONG," *DW.com*, publicado el 19 de agosto de 2024, ver en: https://www.dw.com/es/gobierno-de-nicaragua-ilegaliza-otras-1500-ong/a-69985718.

3. La Ley de Datos Personales debe actualizarse y entrar en funcionalidad en protección del usuario/ciudadano sobre sus datos personales y su ciberseguridad sin afectar la libertad de expresión; y
4. Establecer el derecho de acceso a la internet dentro del marco jurídico nicaragüense, así como darle paso a la alfabetización digital en todo el país.

13.3. Estado de Guatemala

13.3.1. Alejandro Valverth de la organización LEGIS[184]

Sobre el **contexto general sobre derechos digitales en Guatemala** Alejandro menciona que, en primer lugar "es importante mencionar que el Sistema Judicial de Guatemala se encuentra cooptado por lo que se impide un verdadero acceso a la justicia y su progreso". En segundo lugar, "no se encuentra debidamente reglamentando, en otras palabras, no existen legislaciones que traten específicamente la materia, tampoco existen normas que castiguen a las personas que cometan ciberdelitos", solo se encuentra presente una oficina encargada de delitos informáticos dentro de la Policía Nacional. En tercer lugar, menciona que en si el desarrollo de esta temática ha sido solo a través de políticas públicas.

En esa introducción, menciona la falta de protección a los datos personales y la **privacidad digital** por medio de las redes sociales y uso en los espacios escolares, brindando un ejemplo, en donde, "una serie de menores de edad de un instituto educativo distorsionaron las fotos de sus compañeras con la inteligencia artificial con fines pornográficos y las publicaron en las redes sociales causando un gran revuelo en el país y la concientización de que necesitamos una normativa legal para proteger a los más vulnerables".

En cuanto a **normativa legal**, detalla que no existe legislación sobre privacidad digital y libertad de expresión en línea, pero brinda una serie de iniciativas de ley que se han presentado desde el año 2009 tales como: a) Ley 4054 sobre Cibercrimen; b) Ley 5254 sobre Ciberdelincuencia, que involucraba la ciberseguridad y la tipificación del acceso ilícito a las redes de telecomunicación; c) Ley contra la Ciberdelincuencia bajo Decreto 39-2022, menciona que "los artículos 9 y 19 sobre acceso ilícito a datos con información protegida y acoso por medios cibernéticos respectivamente, contravenía con el Art. 35 de la Constitución sobre libertad de expresión y la Ley sobre la Libre Emisión del Pensamiento". Además, denota que "la prensa independiente interpretó dichos enunciados en contra de su labor diaria de fiscalizar y documentar a los funcionarios públicos".

Asimismo, menciona d) la Ley sobre Ciberseguridad 6347, "recientemente anunciada como proyecto de ley dentro del Congreso de Guatemala, y se encuentra desde marzo de 2024 en comisión pendiente de su dictamen favorable", a su vez, "se crean tipos penales dentro de su título 2 como la tipificación del acceso ilícito a las redes y la integridad del sistema informático, sumado

[184] Entrevista realizada el día 22 de agosto a las 10 am por medio de WhatsApp al Miembro del Equipo Consultor de Asociación para el Desarrollo Legislativo y la Democracia (LEGIS) de Guatemala.

a la eliminación de las figuras precedentes de los artículos 9 y 19 del precedente proyecto de ley que causaron controversia".

Sobre la **privacidad digital y la libertad de expresión en línea**, comienza presentando la protección de los datos personales en el espacio digital, menciona la Ley de Acceso a la Información Pública, aunque denota que "dicha ley es muy vaga su ámbito de aplicación al ciudadano guatemalteco es más orientada a los funcionarios públicos y por ende no contempla la protección a las personas", señala un proceso de amparo de la Corte de Constitucionalidad que también "es muy vaga su protección".

De esa forma deja entrever que "en Guatemala se cuenta tan sólo con la Ley Constitucional como base legal para la protección de estos derechos fundamentales en su esfera digital y la Ley de Libre Emisión del Pensamiento que pudiera ser aplicada en lo digital".

En esa misma línea, presenta la **desinformación dentro de los procesos electorales** bajo 4 puntos:

a) "En Guatemala existe un monopolio de la televisión pública y se ve reflejado en las elecciones;
b) La ley electoral se logra reformas para dar mayor pluralidad informativa, pero sigue siendo insuficiente;
c) Las redes sociales juegan un papel fundamental en el país; y
d) Se presentan una serie de *fake news* debido a la falta de legislación en la materia y el control de las telecomunicaciones".

Brinda un ejemplo: "se filtró un audio del presidente actual Bernardo Arévalo cuando despedía a la ministra de Comunicaciones de su cargo, por faltar con la planificación del presupuesto asignado y con ejercer una serie de pagos. En dicho audio se le destituye y se publica la grabación de audio, la ministra desmiente de ser ella quien graba y emite dicha grabación. Por ello, se especula que haya sido el Ministerio Público quien se encuentra cooptado y favor de las autoridades anteriores a través de las llamadas diligencias de ante funciones para poder hacer control de las llamadas telefónicas y ejercer miedo a la población".

Adicionalmente, el presidente Arevalo ha sido objeto de diversos ataques en su campaña electoral "es un comunista", "Guatemala será como Venezuela", "se espera lo peor en el país", etc.

Para cerrar menciona **recomendaciones** orientadas a la necesidad de "crear una legislación enfocada en la protección de los derechos fundamentales de las personas en la esfera digital que incluya tipos penales para la defensa de ellas", ya que, "actualmente el marco legal sobre la materia es insuficiente y los judiciales y los policías no logran realizar una persecución justa". También, "que incluya la protección contra las nuevas tecnologías como la inteligencia artificial y el phishing que se sufre cada día en Guatemala".

Asimismo, concluye expresando que "los periodistas se encargan de desmentir la **información en línea y la manipulación digital** pero no existe la libertad de expresión plena, aunque tampoco

podemos decir que Guatemala es como Nicaragua, aun no se llega a ese punto". Con ello menciona que es necesario "mejorar las libertades especialmente al gremio periodístico y frenar los crímenes de persecución a periodistas que traten de desmentir la información falsa, siendo supuestamente orquestado por el secretario del Ministerio Público".

13.4. Estado de El Salvador

13.4.1. Ismelda Villacorta de la organización FESPAD[185]

Ismelda Villacorta comienza presentándose como parte del equipo de FESPAD de El Salvador en su lucha por apoyar a la democracia y la institucionalidad del país a través del monitoreo constante de la situación política y los contactos directos con organizaciones de la sociedad civil, periodistas y medios de comunicación.

Sobre el **contexto general sobre los derechos digitales** en El Salvador, Ismelda menciona que "han ido en avance por parte del gobierno, notable uso de las tecnologías de la información y comunicación como herramienta principal para transmitir la información", sin embargo, menciona "la Asociación de Periodistas (APES) en su informe de 2023 documentaron 300 vulneraciones a medios de comunicación, en donde, se violentaron sus derechos humanos dentro del espacio digital y con un incremento del 66% respecto del 2022".

También, "se dieron 173 vulneraciones de derechos humanos durante el periodo de las elecciones presidenciales antes y después de febrero de 2024, la mayoría por **Facebook**", y resalta que "estas plataformas se usan para promover discursos estigmatizantes y de odio hacía los periodistas por parte de funcionarios del Estado".

Adicionalmente, señala que "se ha restringido el espacio cívico, la libertad de expresión en línea, claros ejemplos de ellos son los ataques que FESPAD y otras organizaciones de la sociedad han recibido por hacer críticas al gobierno actual, con intentos de hackear los correos electrónicos y el sitio web de las organizaciones", así como, los riesgos de la vigilancia que se dieron en 2022 con la plataforma espía Pegasus por parte de funcionarios del gobierno".

Ismelda menciona que El Salvador cuenta con una Procuraduría de Derechos Humanos "pero que no hay un avance en temas de derechos humanos".

En cuanto a la **normativa regulatoria sobre la materia** menciona "la falta de un marco regulatorio sobre datos personales y brinda el ejemplo del robo de 5.1 millones de datos de los salvadoreños que se vendían por 250 dólares", con ello "se refleja una necesidad primordial de crear una ley que nos amparé a todos los salvadoreños y no nos dejé en la desprotección total de nuestros datos personales".

[185] Entrevista realizada el día 11 de septiembre a las 11 am por medio de *Google Meet* a la Directora de Fortalecimiento a la Institucionalidad del Estado, Transparencia y Anticorrupción de la Fundación de Estudios para la Aplicación del Derecho (FESPAD).

Ismelda menciona varias leyes y normativas que de acuerdo con ella promueven los derechos digitales en el ámbito de acceso a la información, comercio electrónico, firma electrónica, simplificación de datos dentro de la administración pública mediante el uso de las nuevas tecnologías informáticas, el desarrollo científico y tecnológico, la protección del consumidor por medios electrónicos, entre otras.

De ese modo, las nombra de la siguiente manera:

- Ley de Acceso a la Información Pública de 2011, según Ismelda "con un poco o nada de apertura de datos públicos, su acceso es muy restringido";
- Agenda Digital 2030, contiene aspectos importantes sobre la ciberseguridad;
- Ley de Protección al Consumidor de 2005 y posterior reforma en 2018 con el objetivo de brindar protección por medios electrónicos;
- Ley de Desarrollo Científico y Tecnológico de 2013, con el objetivo de mejorar la productividad nacional;
- Ley Especial contra Delitos Informáticos y Conexos de 2022, brinda protección a las personas contra los denominados delitos informáticos, sin embargo, Ismelda detalla que "el tratamiento de la evidencia digital en procesos judiciales, no se sabe a ciencia cierta si hay capacidad de procesar esa documentación y como los jueces valoran dicha prueba digital".
- Ley de Firma Electrónica de 2018, que viene a dar validez legal a la firma simple o certificada;
- Ley de Procedimientos Administrativos, con el objetivo de lograr la transformación digital y mejorar los servicios públicos por medio de la simplificación regulatoria;
- Ley de Regulación de Teletrabajo de 2020, con el fin de regular el teletrabajo a causa de la pandemia del COVID;
- Ley de Comercio Electrónico de 2021, con el objeto de regular medios digitales y la emisión de facturas electrónicas;
- Ley de Títulos Valores Electrónicos de 2022;
- Ley Bitcoin de 2021; y
- Ley de Emisión de Activos Digitales de 2023.

Seguidamente, sobre la **privacidad digital y la libertad de expresión** en línea detalla que "existe un retroceso muy fuerte sobre la democracia y los contrapesos dentro del sistema democrático de El Salvador, por ello se puede observar el retroceso de la libertad de expresión en línea, ya que, actualmente el presidente controla todo". En otras palabras "Bukele contra la Asamblea Legislativa, el fiscal general y adjunto y el sistema judicial, por lo que cualquier intento de disidencia se ve fuertemente amedrentado". Además, añade "El Salvador actualmente vive un régimen de excepción donde se violan las garantías fundamentales y sin respeto a los derechos humanos".

Por ejemplo, "el derecho de asociación se ha visto fuertemente restringido al pensarse que cualquier intento de agrupar personas sean pertenecientes a maras o pandillas y no es así". También, "existe una fuerte reducción del espacio cívico en medios digitales y se reciben constantes ataques comúnmente procedentes de la aplicación **X**.

Sumado a ello, Ismelda expresa que "existe un fuerte ataque a la disidencia por medio de los *trollers* que son controlados por funcionarios del gobierno a periodistas disidentes y defensores de derechos humanos", sin embargo, no menciona nombres de funcionarios públicos involucrados o periodistas afectados.

Sobre la **desinformación digital dentro de los procesos electorales** señala que "dentro de la campaña política anterior a febrero de 2024, se exponían por medio de las redes sociales, televisión, prensa escrita y radio a funcionarios que supuestamente tenían tratos con pandillas o grupos criminales sin tener veracidad de la información", sumado a ellos "ataques de campañas desleales con mucha desinformación digital, en donde se presentaban personas tatuadas haciendo alusión a pandillas con el objetivo de que las personas no votaran por dichos políticos".

Además, según la Universidad Centroamericana (UCA), el 80% de las personas se informaron por medio de **Facebook** durante la campaña electoral. Ismelda señala que "en **Facebook** existía mucha desinformación y ataques en contra de los opositores de Bukele".

Para finalizar menciona una **serie de recomendaciones** que según su criterio son fundamentales para avanzar en la protección de privacidad digital, la mejora de las tecnologías actuales y el progreso de los derechos fundamentales en el espacio digital, dentro de ellas se encuentran:

- Aprobación de una Ley de Datos Personales apegada a los estándares internacionales;
- Mayor regulación por parte del Tribunal Superior Electoral en cuanto a la desinformación dentro de los procesos electorales y especial atención a las campañas anticipadas, donde se denota una complacencia por parte de dicho ente;
- Una mayor verificación de la información de la prensa, ya que se publica mucha *fake news* sin la correcta evidencia digital dentro de los procesos de publicación de la información;
- Alfabetización digital a la población salvadoreña, especialmente a grupos vulnerables, dentro de esa educación digital se debe incluir los riesgos de las plataformas digitales, entre otros; y
- Se debe abordar la violencia de género dentro del progreso de estos derechos, Ismelda aclara que "actualmente las mujeres se ven muy perjudicadas por las *fake news* y la desprotección de sus datos personales a una mayor escala que los hombres".

En definitiva, Ismelda brinda un panorama de El Salvador que ella denomina "es bastante delicado podría decir la situación de El Salvador presenta un retroceso, si bien es cierto no es como Nicaragua, la situación no deja de ser similar, al no contar con garantías hacía nuestros derechos

por el régimen de excepción vigente, el control total por parte del presidente, los ataques a la disidencia, y los retrocesos democráticos que ha tenido el país en la última década".

14. Conclusiones

La investigación ha permitido analizar la legislación actual sobre el ejercicio de las libertades y garantías fundamentales en el espacio digital en Guatemala, Honduras, El Salvador y Nicaragua, identificando áreas de mejora en la protección de estos derechos y analizando el uso de la ley como instrumento represivo. De igual forma, abordando la desinformación en línea y la manipulación digital dentro de los procesos electorales, además, de contar con la opinión de expertos en la materia con el objetivo de tener una perspectiva más detallada y dinámica.

En los cuatro países, el marco legal para la protección de los derechos digitales es fragmentado y, en muchos casos, inadecuado para abordar los desafíos contemporáneos. Aunque existen algunas leyes que regulan aspectos como la ciberseguridad, de acceso a la información y la protección de datos, estas a menudo son insuficientes, mal implementadas o usadas de manera represiva. El desarrollo legal no ha avanzado al mismo ritmo que las tecnologías digitales, lo que deja a las y los ciudadanos vulnerables ante abusos y violaciones de derechos.

Se identificaron múltiples brechas legales en todos los países estudiados. Las más notables incluyen la falta de leyes robustas de protección de datos personales, ciberseguridad y privacidad digital salvo Nicaragua, aunque sus leyes son con una finalidad represiva, asimismo se evidencia la ausencia de regulaciones claras sobre el uso de la inteligencia artificial y las nuevas tecnologías informáticas.

También, la investigación muestra que las leyes relacionadas con la intervención de las comunicaciones y ciberdelincuencia son a menudo son utilizadas como herramientas para restringir la libertad de expresión y controlar la disidencia en línea. En particular, se han documentado casos donde la legislación es empleada para justificar la vigilancia estatal, el bloqueo de sitios web, y el acoso a periodistas y activistas, especialmente en contextos de crisis política o social.

El impacto de las leyes actuales en la privacidad y libertad en línea varía, pero es predominantemente negativo en contextos donde las leyes son utilizadas para controlar la disidencia y restringir la libertad de expresión. En Nicaragua, por ejemplo, se han documentado casos de vigilancia estatal y restricciones a la prensa digital, mientras que, en El Salvador, el aumento de la censura en línea y el acoso a periodistas se ha intensificado bajo el gobierno actual. En Guatemala y Honduras, la preocupación se centra en la vulnerabilidad a la vigilancia ilegal y el acceso no autorizado a los datos personales.

Se documentaron varios casos relevantes de violaciones a los derechos digitales en la región. Estos incluyen el bloqueo de sitios web opositores en Nicaragua, la vigilancia y acoso digital a activistas en El Salvador, la criminalización del discurso crítico en línea en Guatemala, y las denuncias de intervenciones ilegales en comunicaciones privadas en Honduras. Estos casos subrayan el uso de

la ley como un instrumento represivo y la necesidad urgente de reformas para proteger los derechos digitales.

Las entrevistas con expertos legales y activistas confirmaron las preocupaciones planteadas en la investigación, destacando que el marco legal actual es insuficiente para proteger adecuadamente los derechos digitales y que existe una tendencia preocupante hacia el uso de las leyes con fines represivos. También se señaló la necesidad de fortalecer la educación digital, ampliar el marco jurídico, el acceso a la internet, la concientización sobre los derechos en el espacio digital entre la población, entre otros.

Adicionalmente, el análisis del impacto de la desinformación y la manipulación digital en los procesos electorales reveló que estos fenómenos están contribuyendo a la erosión de la democracia en la región. En todos los países estudiados, se observó la proliferación de noticias falsas o *fake news* y campañas de desinformación, a menudo fomentadas por actores políticos, que buscan manipular la opinión pública y deslegitimar a los oponentes. Esto subraya la necesidad de implementar medidas efectivas para combatir la desinformación sin comprometer la libertad de expresión.

En definitiva, aunque hay avances en la legislación sobre derechos digitales en Guatemala, Honduras, El Salvador y Nicaragua, existen graves deficiencias y brechas legales que permiten la violación de estos derechos. La legislación vigente, en algunos casos, es utilizada como un instrumento represivo y punitivo, y se requiere una reforma integral para garantizar la protección de las libertades fundamentales en el espacio digital. Además, se necesita un enfoque más proactivo para abordar los desafíos emergentes como la desinformación y la manipulación digital, con la colaboración de la sociedad civil, los gobiernos y la comunidad internacional.

15. Sumario de Recomendaciones Generales y Específicas

Para abordar de manera integral los desafíos que plantea el entorno digital actual en los países en análisis, se han elaborado una serie de recomendaciones fundamentales. Estas recomendaciones se centran en:

1. Reformar o derogar según el contexto el marco jurídico actual represivo que restringe la libertad de expresión en línea;
2. La creación de nuevas leyes sobre datos personales, ciberseguridad y la promoción de los derechos fundamentales en el ámbito digital;
3. Se recomiendan procesos electorales limpios, libres y democráticos por medio del uso de las redes sociales, internet y la inteligencia artificial; y
4. La promoción de un gobierno abierto y electrónico, ecosistemas digitales y la alfabetización digital.

Se procede a realizar recomendaciones generales, especificas por Estado y una serie de medidas que las organizaciones de la sociedad civil, activistas y partidos políticos deben seguir con el objetivo de promover los derechos digitales en la región.

La siguiente tabla resume las recomendaciones clave que deberían considerarse para garantizar un entorno digital seguro, inclusivo y respetuoso con los derechos fundamentales:

15.1. Tabla 3. Recomendaciones Generales

N.º	Recomendaciones Generales
	Recomendaciones de ámbito legal
1	El reconocimiento del Derecho a Internet como un derecho humano fundamental dentro de las leyes internas al considerar este derecho como una condición *sine qua non* para el ejercicio de los derechos en el espacio digital;
2	La creación de una Ley sobre Ciberseguridad con el objetivo de proteger la actividad que realizan las personas en el mundo digital y proteger a las y los ciudadanos ante las amenazas y riesgos cibernéticos;
3	La creación de una Ley de Datos Personales que tenga como finalidad acceder, rectificar, cancelar y oponerse al manejo de sus datos personales por parte de un tercero, en concordancia con estándares internacionales y europeos;
4	La derogación y revisión de leyes arbitrarias a la libertad de expresión en línea por medio del control de las telecomunicaciones y las redes de la información;
5	Evitar la creación de leyes generales y/o ambiguas con el fin de combatir la desinformación en internet, como así el uso de prohibiciones penales para castigar la difusión de información de supuesta falsedad;
	Recomendaciones sobre procesos electorales democráticos
6	Garantizar de forma proactiva que los sistemas algorítmicos de recomendación no impidan el acceso a información electoral precisa o a una pluralidad de opiniones dentro del espectro democrática;
7	Los organismos electorales deben proveer los recursos necesarios para mitigar y desacreditar las actividades de desinformación electoral, así como promover la alfabetización mediática;
8	Incluir algoritmos de aprendizaje automático (*machine learning)* para frenar la viralidad de la desinformación electoral;
	Otras recomendaciones
9	Crear ecosistemas digitales para la promoción de los derechos fundamentales en el espacio digital, siguiendo el ejemplo de países como Estonia;
10	Promover la alfabetización digital especialmente relacionada a personas vulnerables como las mujeres, niñas y niños y personas de zonas rurales; y
11	Adherirse a los Convenios Internacionales sobre Ciberdelincuencia, el Llamamiento de Paris para la Confianza y Seguridad en el Ciberespacio, y seguir los lineamientos de la Unión Europea en materia de protección de datos personales, la Declaración Europea sobre Derechos y Principios Digitales y la nueva Ley de Inteligencia Artificial de la UE (Ley IA).

Nota 1: Tabla 3. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 50 y 51 para profundizar en las recomendaciones sobre procesos electorales democráticos.

15.2. Tabla 4. Recomendaciones a la Sociedad Civil y otros Actores

N.º	Recomendaciones a la Sociedad Civil y otros Actores
	Recomendaciones de ámbito legal
1	**Ejemplo 1:** **Estonia** ha implementado el derecho universal de acceso al servicio de internet y el seguimiento de las normativas de la UE en materia de derechos digitales, lo que ha permitido desarrollar un ecosistema digital y gubernamental (*e-government*) avanzado con fuerte protección de la privacidad y los derechos en línea. **Acciones:** Abogar por la neutralidad de la red y el acceso equitativo a Internet, especialmente en zonas rurales o marginalizadas; y proponer proyectos comunitarios para establecer puntos de acceso a Internet y colaborar con empresas tecnológicas para ampliar la conectividad.
2	**Ejemplo 2:** **Italia** ha integrado el derecho a la ciudadanía digital, identidad digital y ciberseguridad a su legislación. **Acciones:** Proponer una Ley Nacional de Ciberseguridad que incluya garantías explícitas para proteger los derechos a la privacidad, la libertad de expresión y el debido proceso en investigaciones relacionadas con delitos cibernéticos; y organizar campañas para exigir la derogación de leyes que vulneren la privacidad o la libertad de expresión en el entorno digital.
3	**Ejemplo 3:** La **UE** ha desarrollado el **Reglamento General de Datos Personales (RGPD)** que establece normas estrictas sobre cómo las empresas pueden recopilar, almacenar y utilizar los datos personales, con el objetivo de proteger a las y los ciudadanos de la explotación o el mal uso de su información. **Acciones:** La sociedad civil debe impulsar la creación de una Ley Integral de Protección de Datos Personales que contemple los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), siguiendo el modelo RGPD de la Unión Europea; y organizar audiencias públicas, mesas redondas y debates con diputados del Congreso Nacional para presentar dichas propuestas legislativas.
4	**Ejemplo 4:** La **CIDH** en su Relatoría para la Libertad de Expresión dentro de sus Informes Anuales recomienda que el ejercicio de la libertad de expresión y otros derechos fundamentales debe ser preservados en el entorno digital. **Acción:** Iniciar litigios estratégicos ante tribunales nacionales e internacionales para demostrar que las leyes vigentes son contrarias a los derechos a la libertad de expresión y a la vida privada protegidos por la Convención Americana sobre Derechos Humanos.
5	**Ejemplo 5:** La **Ley de Servicios Digitales de la UE (Arts. 26 y 30),** regula de manera directa y detallada la difusión de desinformación en periodos electorales a través de obligaciones de transparencia, auditoría de algoritmos y mecanismos para eliminar contenido falso. **Acción:** La sociedad civil y los partidos políticos deben ejercer presión para implementar leyes que regulen la publicidad política y exijan transparencia en las

	plataformas digitales durante los procesos electorales, así como, la rendición de cuentas. Se debe tomar como ejemplo esta normativa europea.
	Colaboración con actores estratégicos
6	**Ejemplo 6:** Organizaciones como *Freedom House*, *Electronic Frontier Foundation* (EFF), *Access Now, InternetLab,* Derechos Digitales, *Privacy International*, Amnistía Internacional y *Human Rights Watch*, promueven los derechos digitales a nivel Latinoamericano, regional y universal. **Acción 1:** Establecer alianzas con estas organizaciones para recibir asistencia técnica, compartir buenas prácticas y ganar mayor visibilidad en la lucha por la protección de datos, privacidad y otros derechos en el entorno digital en Centroamérica. **Acción 2:** A partir de esas alianzas, se deben crear mesas de trabajo que incluyan actores gubernamentales, empresas tecnológicas y organizaciones civiles para desarrollar políticas sobre derechos digitales.
	Monitoreo de casos de violaciones de derechos humanos
7	**Ejemplo 7:** Organizaciones Fundación Acceso promovían el monitoreo de la seguridad digital en Centroamérica, sin embargo, ya no continúan operando.[186] **Acción:** Crear y continuar con el uso plataformas de denuncia y monitoreo similares que permitan a los ciudadanos reportar abusos relacionados con la protección de datos, como filtraciones de información, *hackeos*, y usos indebidos por parte de empresas o el gobierno.
8	**Ejemplo 8:** La organización Derechos Digitales promueve la creación de observatorios ciudadanos para el monitoreo de casos de violaciones de derechos a la privacidad en línea y el uso de *spywares* y *malwares* en Centroamérica. **Acciones:** Crear y unirse a observatorios ciudadanos que monitoreen el uso de tecnologías de vigilancia por parte del Estado; y exigir transparencia sobre los contratos de adquisición de software espía y otros mecanismos de control digital.
	Educación sobre Derechos Digitales
9	**Ejemplo 9:** En España, diversas organizaciones como Fundación Atresmedia y UNICEF han colaborado con escuelas y medios de comunicación para crear conciencia sobre los reglamentos de la UE y la Carta de Derechos Digitales.[187] **Acción:** Organizar seminarios, charlas y campañas en medios sociales para educar a las y los ciudadanos sobre los riesgos de la exposición de sus datos personales y la necesidad de contar con una legislación robusta.

Nota 1: Tabla 3. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 10-13 para profundizar en los marcos regulatorios europeos e interamericanos.

[186] Fundación Acceso, ejemplo 8, ver en: https://www.acceso.or.cr/publicaciones/
[187] Fundación Atremisa y UNICEF, ver ejemplo 9 de España : https://fundacion.atresmedia.com/actualidad/fundacion-atresmedia-unicef-espana-lanzan-campana-menores-edad-derechos-digitales-que-derechos-infancia-hagan-realidad-entorno-digital_202404246628e38bc0b95c0001135a98.html

15.3. Recomendaciones por Estado

15.3.1. Tabla 5. Recomendaciones al Estado de Honduras

N.º	Recomendaciones al Estado de Honduras
	Recomendaciones de ámbito legal
1	Declarar el reconocimiento del Derecho a Internet como un derecho humano, e incorporarlo a través de una iniciativa de ley en la Constitución de la República;
2	Redactar y aprobar una Ley Nacional sobre Ciberseguridad y Ciberdefensa, que cree una Política Nacional sobre Ciberseguridad y Ciberdefensa en correspondencia con la protección de los derechos humanos en el ecosistema digital;
3	Crear una Ley Marco sobre el Gobierno Digital que abarque todas las relaciones intra-Estado y con los particulares;
4	Crear una Ley de Protección de Datos Personales para regular el uso de dichos datos tanto entes privados como públicos;
5	Revisar y reformar leyes, en base a estándares de derechos humanos en la materia tales como: la Ley de Escuchas, Ley Marco del Sector de las Comunicaciones y el Reglamento de Gobierno Electrónico;
6	Reformar el Código Penal de 2019, en especial sobre los delitos al honor e injuria y pasarlos al ámbito civil;
8	Actualizar la norma primaria, la Ley de Telecomunicaciones, en donde, deben abrirse el espectro electro radial y mejorarse la calidad y cobertura de internet;
7	Realizar un control de convencionalidad de la tipificación de delitos cibernéticos en el Código Penal, tomando de referencia el Convenio de Budapest sobre Ciberdelincuencia y otros instrumentos internacionales de la materia;
	Otras recomendaciones
9	El Estado debe brindar mayor cobertura de internet y de electricidad bajo la presencia estatal y una mayor presencia estatal en todos los departamentos del país para garantizar la efectividad del acceso a las telecomunicaciones; e
10	Inversión por parte del gobierno en educación digital y la importancia de la alfabetización digital e informática en las escuelas de todo el país.

Nota 1: Tabla 4. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 24 y 25 y la sección de entrevistas para profundizar en las recomendaciones.

15.3.2. Tabla 6. Recomendaciones al Estado de Guatemala

N.º	Recomendaciones al Estado de Guatemala
	Recomendaciones de ámbito legal y reglamentario
1	La creación de una Ley de Protección de Datos Personales que incluya como base fundamental los derechos ARCO y las normativas fundamentales desarrolladas por la Unión Europea en su Reglamento General de Protección de Datos (RGPR), Declaración Europea sobre Derechos y Principios Digitales y la nueva Ley de Inteligencia Artificial (Ley de IA);
2	Progresar en el perfeccionamiento y la implementación de la política y el reglamento de telecomunicaciones y su entidad reguladora;
3	Aprovechar las tecnologías digitales para mejorar la prestación de los servicios públicos, tomando ventaja de la Ley Antitramites de 2021 para facilitar los servicios públicos digitales;
4	Crear una Ley de Ciberseguridad con el fin de proteger a las y los ciudadanos ante amenazas y riesgos cibernéticos;
5	Garantizar la correcta implementación de la Ley de Acceso a la Información Pública, teniendo conciencia de que se afecta el derecho de información de la ciudadanía;
6	Desarrollar una política de ciberseguridad más robusta, capacidad y concienciación, así como, crear grupos de trabajo sobre ciberseguridad compuestos de expertos técnicos y personal relevante del Gobierno de Guatemala e impartir capacitación en ciberseguridad a todo el personal del Gobierno de Guatemala a todos los niveles y en todas las entidades;
	Otras recomendaciones
8	La garantía de un estándar mínimo, de que las normas relativas al contenido permitido en redes sociales y plataformas de internet se ajusten a los estándares globales en materia de derechos humanos, no solo en lo sustantivo que respecta al contenido permisible y prohibido, sino en lo referido a estándares de transparencia, garantías mínimas de proceso, apelación e información al usuario; y
9	Detener la estigmatización y el hostigamiento en especial por parte de autoridades y servidores públicos en contra de periodistas a través del uso de redes sociales y con ello mejorar sus libertades y derechos.

Nota 1: Tabla 5. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 30 y 31 y la sección de entrevistas para profundizar en las recomendaciones.

15.3.3. Tabla 7. Recomendaciones al Estado de El Salvador

N.º	Recomendaciones al Estado de El Salvador
	Recomendaciones de ámbito legal
1	Aprobar una Ley de Ciberseguridad bajo una estrategia sólida y efectiva para abordar los desafíos de la ciberseguridad;
2	Contar una Ley de Protección de Datos Personales que regule el tratamiento de datos particulares, busque garantizar la seguridad de la intimidad de los usuarios y proporcione la debida seguridad jurídica sobre las restricciones y libertades que se contemplan sobre el uso de la información personal de los usuarios;
3	Revisar y reformar el Código Penal y la Ley Especial contra Delitos Informáticos y Conexos con la finalidad de incorporar disposiciones específicas que regulen y tipifiquen el delito de acoso en línea, garantizando la participación de las mujeres en el espacio digital de forma segura;
	Recomendaciones de sobre educación y capacitación digital
4	Capacitar a las personas activamente en el entorno digital sobre políticas y marcos regulatorios en el país, con el objetivo de conocer derechos y obligaciones que están regulados, y sepan como exigir derechos en caso de ser vulnerados;
5	La articulación de entidades en el ecosistema digital y la sensibilización de dichas instituciones que brindan formación sobre la necesidad de incluir en los temas que imparten la importancia de la ciberseguridad la protección de datos personales y la alfabetización relacionada con derechos digitales;
6	Promover la alfabetización digital especialmente relacionada a personas vulnerables como las mujeres, niñas y niños, personas de las zonas rurales, grupos LGBTI+, procurando disminuir la actual brecha digital que persiste;
	Otras recomendaciones
7	Retomar las recomendaciones de estándares internacionales de las Naciones Unidas y otros organismos internacionales que establecen medidas sobre la perspectiva de género y aplicarlas al ámbito digital para su protección;
8	Implementar la Agenda Digital El Salvador 2030 y dotarla de recursos financieros técnicos necesarios para digitalizar los servicios gubernamentales para actualizar, rediseñar e integrar las plataformas digitales públicas existentes; y
9	Mayor regulación por parte del Tribunal Superior Electoral en cuanto a la desinformación dentro de los procesos electorales y especial atención a las campañas anticipadas.

Nota 1: Tabla 6. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 35 y 36 y la sección de entrevistas para profundizar en las recomendaciones.

15.3.4. Tabla 8. Recomendaciones al Estado de Nicaragua

N.º	Recomendaciones al Estado de Nicaragua
	Recomendaciones de ámbito legal
1	Derogar el marco jurídico represor, abstenerse de instrumentalizar el derecho penal y administrativo para perseguir el ejercicio legítimo de la libre expresión, proteger y garantizar la libertad en independencia de la prensa y de los periodistas, tanto en línea como fuera de ella;
2	Reformar la legislación existente sobre ciberdelitos, dado que, la misma atenta contra la libertad de expresión en línea, se crea un ambiente hostil, se cierra el espacio cívico y se socava la democracia;
3	Derogar la Ley de Soberanía, la misma atenta contra la integridad personal al existir el delito de terrorismo, expandiéndose al ciberterrorismo;
4	La Ley de Datos Personales debe actualizarse y entrar en funcionalidad en protección del usuario/ciudadano sobre sus datos personales y su ciberseguridad sin afectar la libertad de expresión en línea;
5	Evitar marcos regulatorios a los intermediarios de internet por el contenido de usuarios que circula en sus plataformas, lo que puede incentivar la dinámica de autocensura;
6	Establecer el derecho de acceso a la internet dentro del marco jurídico nicaragüense, así como, darle paso a la alfabetización digital en todo el país y promover el acceso universal a internet para garantizar el disfrute universal y efectivo del derecho a la libertad de expresión por este medio;
7	Garantizar el acceso libre al servicio de internet y a los contenidos que circulan en esta bajo condiciones de neutralidad, privacidad, y garantías de no persecución o monitoreo en línea;
8	Evitar la creación de leyes generales y/o ambiguas con el fin de combatir la desinformación en internet, como así el uso de prohibiciones penales para castigar la difusión de supuesta información falsa o *fake news*; e
	Otras recomendaciones
9	Involucrarse en los diálogos multilaterales con el objetivo de construir consensos en clave y conforme a principios y estándares del derecho internacional de los derechos humanos, especialmente en materia de moderación de contenidos en línea y gobernanza de internet.
10	Ante la escalada represiva de normativas inconstitucionales y contrarias a los estándares interamericanos se recomienda a la población civil de Nicaragua mayores medidas de seguridad digital para minimizar los riesgos a su privacidad y protección en línea, como por ejemplo el uso de una red privada virtual (VPN).

Nota 1: Tabla 7. Elaborada a partir de la investigación realizada y entrevistas a expertos en derechos digitales.
Nota 2: ver páginas 44, 45 y 46 y la sección de entrevistas para profundizar en las recomendaciones.