

Protección de datos y responsabilidad jurídica ante fallos eléctricos: un análisis civil y público en Panamá

The Protection of Personal Data and Legal Liability in Case of Power Failures: A Civil and Public Analysis in Panama

La protection des données et la responsabilité juridique en cas de pannes électriques : une analyse civile et publique au Panama

Proteção de dados e responsabilidade jurídica em caso de falhas elétricas: uma análise civil e pública no Panamá

Obeth Ricardo Ponte Zárate

Universidad de Panamá, Facultad de Derecho y Ciencias Políticas, Panamá

obeth-r.ponte@up.ac.pa

 <https://orcid.org/0009-0005-7293-4608>

DOI <https://doi.org/10.48204/contacto.v5n2.9573>

Recibido: 10/06/2025

Aceptado: 11/08/2025

RESUMEN

El presente escrito analiza la interdependencia entre la protección de datos personales y la infraestructura energética en Panamá, identificando una desarticulación normativa entre la Ley 81 de 2019 (que exige seguridad de la información) y el marco eléctrico (Ley 6 de 1997), el cual no fue concebido para sostener sistemas digitales. En Panamá, la protección de datos personales, comúnmente asociada a amenazas cibernéticas, revela una vulnerabilidad sistémica fundamental cuando se analiza su interdependencia con la infraestructura energética nacional. La Ley 81 de 2019 impone deberes de seguridad, confidencialidad e integridad, pero su aplicación se torna problemática ante fallas del suministro eléctrico, regulado por un marco (Ley 6 de 1997 y Decreto Ley 10 de 1998) concebido para una era pre-digital, generando una zona gris de responsabilidad: ¿responde el custodio del dato por una falla estructural que escapa a su control? La experiencia comparada evidencia que la seguridad de la información es un archipiélago interconectado con políticas públicas sectoriales, por lo que exigir previsión absoluta al responsable del tratamiento en un entorno energético frágil puede resultar desproporcionado. Así, Panamá enfrenta el desafío de armonizar su régimen de protección de datos con la realidad de su infraestructura, requiriendo un marco coherente que articule responsabilidad civil, responsabilidad pública y derechos fundamentales para salvaguardar la confianza digital, lo que implica que el derecho debe superar una concepción aislada de la seguridad para abordar las interdependencias estructurales del siglo XXI.

Palabras clave: Protección de datos, infraestructura energética, desconexión normativa, responsabilidad, interdependencia

ABSTRACT

This paper examines the interdependence between personal data protection and energy infrastructure in Panama, identifying a normative disconnect between Law 81 of 2019 (which mandates information security requirements) and the electrical framework (Law 6 of 1997), which was not designed to support digital systems. In Panama, personal data protection—commonly associated with cyber threats—reveals a fundamental systemic vulnerability when analyzed in relation to its interdependence with national energy infrastructure. Law 81 of 2019 imposes duties of security, confidentiality, and integrity; however, its application becomes problematic in the face of electrical supply failures regulated by a framework (Law 6 of 1997 and Decree Law 10 of 1998) conceived for a pre-digital era, generating a gray zone of liability: should the data custodian be held responsible for a structural failure beyond their control? Comparative experience demonstrates that information security constitutes an interconnected archipelago with sectoral public policies, thus requiring absolute foresight from data controllers within a fragile energy environment may prove disproportionate. Consequently, Panama faces the challenge of harmonizing its data protection regime with the reality of its infrastructure, necessitating a coherent framework that articulates civil liability, public responsibility, and fundamental rights to safeguard digital trust—implying that the law must transcend an isolated conception of security to address the structural interdependencies of the twenty-first century.

Keywords: Data protection, Energy infrastructure, Normative disconnect, Liability, Interdependence

Introducción

La protección de datos personales en Panamá al menos en el plano normativo ostenta la dignidad de derecho fundamental, cuidadosamente blindado por la Ley 81 de 2019. Sus principios confidencialidad, lealtad, seguridad avanzan con la solemnidad de una procesión jurídica impecable. Todo parece en orden. Todo parece firme. Hasta que se va la luz.

Basta un corte eléctrico, breve pero decisivo, para que esa arquitectura normativa se quede en suspenso. Porque los datos, por etéreos que parezcan, no flotan en el aire: dependen de servidores que respiran energía. Y cuando ese flujo se interrumpe, la ficción de autonomía digital se desvanece. Una base de datos no sufre infartos, es cierto; pero puede corromperse, fragmentarse o quedar expuesta con la misma facilidad con la que una nevera deja de enfriar. No hace falta un ciberataque sofisticado. A veces basta un apagón.

En Panamá, además, los apagones no pertenecen al género de la distopía futurista. Son, más bien, una rutina intermitente. Las fluctuaciones de voltaje compiten en frecuencia con los discursos sobre modernización tecnológica. Y sin embargo, en este discreto divorcio entre derecho y realidad material, la legislación parece asumir que la seguridad digital existe en un vacío técnico. No hay un puente normativo claro entre la estabilidad energética y la protección de datos. Como si los centros de datos funcionaran con convicción jurídica y no con corriente eléctrica.

La omisión no es trivial. En el derecho comparado piénsese en la directiva NIS2 de la Unión Europea o en la lógica estructural del Reglamento General de Protección de Datos de la Unión Europea la seguridad ya no se concibe como un simple atributo del software, sino como una condición vinculada a infraestructuras críticas. Sin energía confiable, no hay disponibilidad. Sin continuidad eléctrica, la confidencialidad se vuelve promesa frágil. Es una antítesis incómoda: proclamamos derechos digitales robustos sobre cimientos energéticos inestables.

Por eso, el problema no puede reducirse a un incidente técnico. Es, ante todo, un dilema jurídico. ¿Quién responde cuando una falla eléctrica deja al descubierto información sensible? Puede un apagón activar responsabilidad civil o incluso administrativa bajo la Ley 81. Cómo se delimita la negligencia en un entorno donde lo fortuito la tormenta, la sobrecarga, el transformador que estalla, forma parte del paisaje cotidiano.

Una lectura dogmática y hermenéutica sugiere que no bastan ajustes marginales. Lo que está en juego es el propio concepto de “seguridad”. Tal vez haya que dejar de entenderla como una propiedad del código y comenzar a asumirla como una cualidad del sistema entero. Seguridad no es solo cifrado ni autenticación multifactor; es continuidad operativa, planificación tecnológica y estabilidad energética. Es, en el fondo, infraestructura.

La protección de datos no puede seguir suspendida en un limbo normativo, desconectada de la realidad física que la sostiene. De lo contrario, persistiremos en una paradoja inquietante: confiar en un derecho que se apaga, literalmente, cada vez que se va la luz.

Materiales y Métodos

Diseño del estudio

La arquitectura metodológica de esta investigación responde a una lógica cualitativa, sustentada principalmente en el análisis dogmático y hermenéutico del derecho. No se trata aquí de contar opiniones ni de medir percepciones como quien pesa granos en una balanza estadística, sino de desentrañar el sentido profundo de las normas, reconstruir sus fundamentos y examinar sus tensiones internas.

El eje central del análisis fue la Ley 81 de 2019, estudiada en diálogo sistemático con la legislación eléctrica vigente y con instrumentos normativos comparados de la Unión Europea, Colombia, México y Argentina. Este contraste no persigue la simple acumulación de referencias extranjeras esa tentación tan académica como decorativa, sino la identificación de convergencias, divergencias y modelos regulatorios subyacentes. Allí donde una norma nacional afirma estabilidad, otra revela flexibilidad; donde una proclama apertura de mercado, otra protege la soberanía energética con celo casi litúrgico. Esa antítesis permite iluminar con mayor nitidez los presupuestos ideológicos y técnicos de cada sistema.

El método dogmático se empleó para sistematizar principios, categorías y estructuras jurídicas. Se analizaron conceptos como servicio público, regulación, competencia y sostenibilidad energética, atendiendo a su evolución doctrinal y jurisprudencial. El método hermenéutico, por su parte, permitió interpretar el texto normativo a la luz de su contexto histórico, económico y político, reconociendo que toda ley es hija de su tiempo, aunque aspire a parecer eterna.

No se incluyeron datos empíricos ni encuestas. La exclusión no responde a una omisión metodológica, sino a una decisión deliberada: el propósito del estudio no fue capturar percepciones sociales, sino reconstruir fundamentos jurídicos. En este sentido, la investigación se aproxima más al trabajo de un cartógrafo que al de un encuestador; dibuja mapas conceptuales antes que estadísticas.

La información fue organizada mediante un análisis sistemático de fuentes primarias (normas y documentos oficiales) y secundarias (doctrina especializada), priorizando la coherencia interna del ordenamiento y su articulación comparada. El criterio de selección se basó en relevancia normativa, vigencia jurídica y representatividad de modelos regulatorios.

En suma, este diseño metodológico combina rigor técnico y perspectiva crítica. Porque interpretar el derecho conviene recordarlo no es simplemente describir lo que dice la norma, sino comprender por qué lo dice, a quién beneficia y qué visión del mundo encarna. Y, a veces, lo que calla resulta tan revelador como lo que proclama.

En esta investigación no hubo entrevistas grabadas ni cuestionarios diligenciados con letra temblorosa. Los “participantes” fueron otros: textos jurídicos. Fríos en apariencia, sí, pero decisivos; mudos en tinta, aunque elocuentes en consecuencias. Porque a veces los documentos hablan más alto que las personas: no levantan la voz, pero imponen límites.

El estudio comenzó con un enfoque en las leyes panameñas, incluyendo la Constitución, el Código Civil, la Ley de 1997 y el Decreto Legislativo No 10 de 1998, y particularmente la Ley No.81 sobre protección de datos personales. Este tema aparece en el mundo legal como un movimiento crucial pero de última hora para mantenerse al día con nuestro mundo digital en rápida evolución, a pesar de que las leyes tienden a cambiar más lentamente. Es curioso cómo la tecnología siempre está en movimiento, siempre cambiando, mientras que la ley es como ese amigo que siempre es el mismo, nunca cambia mucho.

A este entramado normativo se sumó la doctrina especializada, con autores como Solove (2021), Bygrave (2019) y Zuboff (2019), cuyas obras permiten comprender que la privacidad no es simplemente un derecho más en el catálogo constitucional, sino un campo de tensión entre autonomía y control, entre dignidad y mercado. Si el siglo XIX discutía la libertad frente al Estado, el XXI debate la libertad frente al algoritmo. Y no siempre sabemos cuál de los dos observa con mayor atención.

La investigación también examinó jurisprudencia regional, ese espacio donde las normas dejan de ser promesas abstractas y se convierten en respuestas concretas ante conflictos reales. Asimismo, se incorporaron estándares técnicos como el NIST 800, que traducen principios jurídicos en prácticas operativas como si el derecho, de pronto, se vistiera de ingeniero, y documentos regulatorios emitidos por la ASEP y la ANTAI, instituciones que materializan la supervisión estatal en sectores estratégicos y en la protección de datos personales.

Así, los verdaderos protagonistas de este estudio no fueron individuos de carne y hueso, sino arquitecturas normativas y conceptuales. Textos que no sienten, pero condicionan; que no dudan, pero delimitan. En su diálogo silencioso a veces armónico, a veces contradictorio se dibuja el mapa contemporáneo de la protección de datos: un territorio donde la intimidad se defiende no con espadas, sino con cláusulas; no con murallas, sino con principios cuidadosamente redactados.

Y tal vez ahí radique la ironía más profunda: en la era de la hiperconectividad, nuestra esfera más íntima depende, en buena medida, de palabras impresas en papel o codificadas en archivos oficiales. Palabras que, bien interpretadas, pueden ser escudo. Mal aplicadas, simple formalidad.

Toda investigación revela su carácter por las fuentes que elige. En este caso, los materiales no fueron accesorios metodológicos, sino el andamiaje mismo del argumento: tres grandes cuerpos normativos y conceptuales que, como columnas de un templo antiguo, sostienen la arquitectura del análisis.

Tabla 1

Cuerpos normativos y conceptuales

Aspectos normativos	Descripción conceptual
Normativa panameña	El sistema jurídico nacional de Teh está en el centro de todo esto: la Constitución, el Código Civil, la Ley 6 del 97, el Decreto-Ley 10 del 98 y la Ley 81 del 2019 sobre la protección de los datos personales Este conjunto de regulaciones esboza una evolución que no es lineal, sino que zigzaguea. La Constitución proclama principios con vocación de eternidad; el Código Civil traduce responsabilidades en reglas concretas; las leyes sectoriales intentan domesticar realidades técnicas que cambian más rápido de lo que el legislador puede prever. Y la Ley 81 de 2019 aparece como respuesta a una época en la que la información circula con la ligereza del aire, pero deja huellas tan pesadas como el plomo.
Doctrina especializada	El segundo grupo lo integran las reflexiones de Solove (2021), Bygrave (2019) y Zuboff (2019), junto con la literatura civil relativa a la responsabilidad por prestación deficiente de servicios. Aquí el derecho deja de ser únicamente norma y se convierte en pensamiento crítico. Solove desmonta la simplificación de la privacidad como mero “secreto”; Bygrave aporta sistematicidad en el análisis comparado de la protección de datos; Zuboff advierte con una lucidez incómoda sobre el capitalismo de vigilancia y sus asimetrías de poder. Frente a ellos, la dogmática civil recuerda algo elemental y, a la vez, revolucionario: quien presta un servicio debe responder cuando lo hace de manera deficiente. Parece obvio. Y, sin embargo, en el universo digital esa obviedad se diluye como tinta en agua.

Regulación comparada	El tercer bloque incorpora la Directiva NIS2 y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, las normativas mexicanas sobre infraestructura crítica y la jurisprudencia del Consejo de Estado de Colombia. Este enfoque comparado funciona como espejo y contraste. Europa avanza con una vocación regulatoria casi pedagógica; América Latina ensaya soluciones que oscilan entre la innovación y la cautela. La comparación revela tanto convergencias como brechas: mientras algunos sistemas apuestan por una supervisión robusta y sanciones disuasorias, otros aún consolidan sus marcos institucionales. En conjunto, estos materiales no solo proporcionan información; construyen perspectiva. Son piezas de un rompecabezas donde cada norma, cada autor y cada precedente aportan una tonalidad distinta. Y en ese cruce entre lo nacional y lo comparado, entre la teoría y la práctica, entre el ideal y su aplicación imperfecta se perfila la verdadera dimensión del problema: la regulación de la información en una era que produce datos con la misma facilidad con la que antes producía silencio.
----------------------	---

Fuente. Elaboración propia

Se realizó una lectura sistemática de la normativa panameña para identificar límites y omisiones frente a escenarios energéticos. Posteriormente, se confrontó esta lectura con doctrina civil y tecnológica relevante. Finalmente, se elaboró una matriz de tensiones entre deberes de seguridad, imputación de daños y vacíos regulatorios.

Para el análisis de datos, dado que se trata de una investigación cualitativa sin base empírica, el análisis se realizó a partir de herramientas dogmáticas, interpretativas y comparadas. Se utilizó un enfoque hermenéutico para interpretar la norma en contexto, y un análisis de derecho comparado para contrastar el caso panameño con modelos normativos más avanzados.

Resultados

La revisión normativa permitió identificar tres diferencias estructurales entre Panamá y otros marcos jurídicos internacionales en cuanto a la protección de datos frente a riesgos energéticos. Estas diferencias se sintetizan en la siguiente tabla 2.

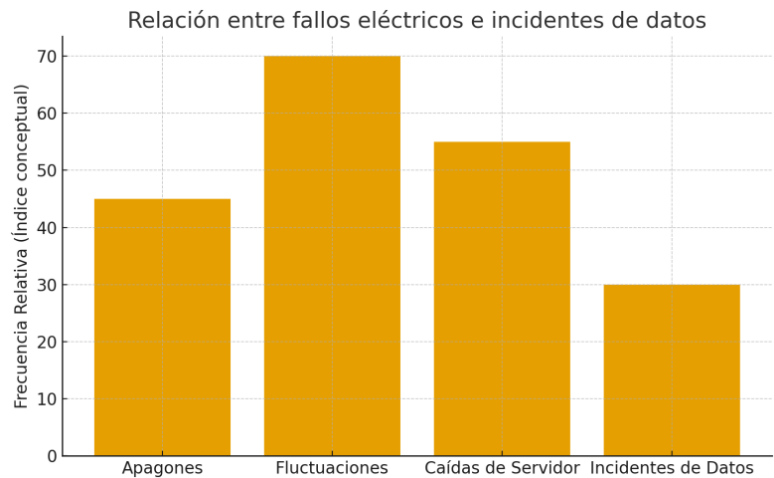
Tabla 2
Tensiones normativas entre energía y protección de datos

Aspecto analizado	Panamá	Unión Europea (NIS2)	Colombia / México / Argentina
Reconocimiento de fallos eléctricos como riesgo digital	No contemplado en la Ley 81 de 2019	Reconocido expresamente como amenaza	Incluido en guías técnicas y fallos judiciales
Requisitos técnicos de respaldo energético	No regulados	Exigidos en sectores críticos	Recomendados en protocolos específicos
Coordinación entre reguladores energéticos y digitales	Inexistente	Coordinación obligatoria entre autoridades	Variable, depende del sector

Fuente. Elaboración propia

La Tabla 2 resume los principales vacíos normativos observados en la legislación panameña respecto a la seguridad de datos ante fallos eléctricos. En comparación con el estándar europeo y algunas experiencias latinoamericanas, el enfoque local resulta aún incipiente.

Figura 1
Nivel de integración entre energía y protección de datos



Fuente. Elaboración propia

La Figura 1 ilustra, de manera sintética pero reveladora, el grado de integración normativa entre el sector energético y la protección de datos personales en distintas regiones. No se trata solo de un contraste visual; es, en cierto modo, un mapa de prioridades jurídicas.

El gráfico evidencia una asimetría clara: mientras algunos ordenamientos han tejido puentes sólidos entre la regulación energética y los estándares de protección de datos integrando obligaciones de ciberseguridad, gestión de riesgos y responsabilidad, otros mantienen ambos ámbitos en compartimentos casi estancos, como si la infraestructura crítica y la información que la sostiene pertenecieran a universos distintos.

En ese panorama comparado, Panamá registra el nivel más bajo de articulación normativa. La conclusión no es meramente estadística; es estructural. La escasa conexión entre la regulación energética y la protección de datos revela una brecha que resulta especialmente delicada en un entorno donde las redes eléctricas dependen de sistemas digitales interconectados, y donde la información fluye con la misma intensidad que la energía que alimenta ciudades enteras. Paradójicamente, cuanto más inteligente se vuelve la infraestructura, más vulnerable puede resultar si el derecho no evoluciona a su mismo ritmo.

La figura, por tanto, no solo describe una posición relativa; sugiere una urgencia. Si en otras regiones la integración normativa actúa como un escudo preventivo, en el caso panameño la fragmentación actual opera como una zona gris que demanda reformas claras, coherentes y técnicamente informadas. No por afán de imitación comparada, sino por necesidad sistémica.

En definitiva, el resultado visualiza algo más profundo que una diferencia regional: expone el desfase entre la complejidad tecnológica del sector energético y la densidad normativa destinada a proteger

los datos que lo atraviesan. Y en esa brecha silenciosa pero significativa se juega buena parte de la resiliencia institucional del país.

Discusión

Lo que esta investigación revela no es un simple descuido técnico, ni una omisión normativa menor. Es algo mucho más estructural: Panamá está levantando su ecosistema digital sobre una base fragmentada, donde los datos circulan sin que nadie asegure, de manera sistemática, la energía que los mantiene vivos.

De esa desconexión emergen tres tensiones profundas. No son meros problemas administrativos. Son fracturas constitucionales en potencia, donde derechos fundamentales quedan a merced de una infraestructura que no fue diseñada para protegerlos.

a) Seguridad digital vs. silencio energético: una promesa sin cimientos

La Ley 81 de 2019, en su artículo 26, establece que los responsables del tratamiento apliquen “medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales”. Pero como advierte Bygrave (2019), los principios generales de protección pierden eficacia cuando no se anclan a condiciones materiales y contextos tecnológicos específicos.

En el caso panameño, esa desconexión es patente: no se exige continuidad eléctrica, no se mencionan protocolos de contingencia ante cortes de energía, ni se contemplan sistemas de respaldo (UPS) como parte del deber de diligencia. Así, la seguridad ese concepto tan invocado se vuelve una promesa sin voltaje.

Zuboff (2019) lo plantea de forma brutal: “la infraestructura es el nuevo lugar donde se juega la soberanía”. Pero en Panamá, esa soberanía sigue sin manual técnico ni obligación energética mínima.

b) ¿Quién responde cuando todo falla?: entre lo civil, lo público y lo invisible

El Código Civil panameño, artículo 1644, establece la obligación de resarcir daños causados por negligencia. A su vez, la Ley 6 de 1997 y el Decreto Ley 10 de 1998 asignan responsabilidades por deficiencias en el servicio eléctrico. Sin embargo, ninguna de estas normas considera expresamente los daños digitales, ni las afectaciones a bases de datos como perjuicios jurídicamente relevantes.

Aquí se produce una tormenta perfecta: la empresa de datos puede alegar que no controla la energía; la eléctrica puede argumentar que no controla la información; el Estado, que no hay norma que le imponga supervisión cruzada. Y el juez ese actor final y solitario queda obligado a improvisar entre lagunas normativas.

Como señala Solove (2021), la protección efectiva de datos no puede depender solo del derecho privado, “porque el riesgo de daño es difuso y la imputación muchas veces fragmentaria”. Hoy, en Panamá, esa fragmentación no solo es doctrinal: es estructural.

c) Privacidad sin voltaje: el derecho fundamental que no se diseñó para sobrevivir un apagón

La Constitución panameña, artículo 42, reconoce el derecho a la privacidad y el respeto de los datos personales. Sin embargo, como bien apunta la doctrina europea bajo el Reglamento General de Protección de Datos (RGPD), la protección efectiva requiere infraestructuras resilientes frente a amenazas físicas, técnicas y organizativas (art. 32 RGPD).

La Directiva NIS2 va más lejos: cataloga los servicios de electricidad como parte de las infraestructuras críticas esenciales para la seguridad digital de la Unión. Es decir, sin electricidad, no hay ciberseguridad.

En América Latina se empieza a recoger esta idea, la jurisprudencia del Consejo de Estado de Colombia ha declarado responsable a una entidad estatal por pérdida de información tras una falla eléctrica no prevista (Sentencia del 3 de octubre de 2019, Exp. 68001-23-15-000-2013-00649-01). México y Argentina, por su parte, han emitido guías técnicas que exigen respaldo eléctrico como componente de la protección de datos en entornos críticos.

En Panamá, en cambio, el derecho a la privacidad sigue pensado como si flotara en el éter, ajeno a la infraestructura que lo sostiene.

Pero cuando un apagón permite accesos indebidos, genera pérdida irreversible de información, o daña irreversiblemente bases de datos sensibles, ya no estamos ante una falla técnica. Estamos ante una violación estructural de un derecho fundamental que, en la práctica, depende de una infraestructura que no fue diseñada para garantizarlo.

Tres tensiones. Tres fisuras. Y una misma conclusión: La protección de datos ya no puede pensarse solo desde lo digital. Debe pensarse desde lo energético, lo físico, lo material. El derecho a la privacidad no habita únicamente en los códigos legales o binarios. También habita y a veces muere en los circuitos, transformadores y baterías que olvidamos legislar.

Conclusiones

El análisis revela una verdad tan sencilla como alarmante: Panamá aún no ha conectado los cables entre el derecho digital y la realidad energética que lo sostiene. Y mientras eso no ocurra, la protección de datos seguirá siendo un castillo normativo construido sobre cimientos inestables.

La Ley 81 de 2019, pese a su vocación moderna, no contempla los escenarios energéticos que pueden vulnerar la privacidad en segundos. Por su parte, la legislación eléctrica forjada en un paradigma anterior al gobierno electrónico, la nube y la inteligencia artificial, no reconoce el daño digital como categoría jurídica ni como riesgo operativo.

Este vacío no es teórico. Tiene consecuencias muy concretas: a) La responsabilidad se diluye: nadie sabe quién responde cuando un corte eléctrico expone información sensible; b) Las víctimas quedan sin mecanismos claros: no pueden exigir resarcimiento sin atravesar un laberinto judicial; c) Las empresas carecen de reglas técnicas precisas: no saben cuánto invertir, ni en qué condiciones, para prevenir lo que la ley no nombra; y d) el Estado, sin un rol articulador claro, observa desde la barrera un conflicto que, paradójicamente, él mismo ha permitido que se fragmente.

Frente a este panorama, no basta con buenas intenciones regulatorias. Se requieren acciones normativas contundentes y urgentes. Este estudio propone cinco:

Algunas recomendaciones para reconectar el derecho: a) Crear protocolos oficiales que integren energía y protección de datos, especialmente para sectores estratégicos como salud, justicia, finanzas y administración pública; b) Modificar la Ley 6 de 1997 para incluir expresamente el daño digital como consecuencia indemnizable del mal servicio eléctrico; c) Establecer un régimen de responsabilidad solidaria cuando los daños resulten de omisiones concurrentes entre el operador eléctrico y el responsable del tratamiento de datos; d) Incorporar estándares mínimos de respaldo energético (UPS, baterías, generadores) obligatorios en entidades públicas y empresas que procesen datos sensibles; y e) Reconocer explícitamente que la privacidad depende de infraestructuras críticas robustas, y que su protección requiere coordinación multisectorial y visión sistémica.

Porque si el país continúa tratando los fallos eléctricos como simples inconvenientes técnicos, cuando en realidad comprometen derechos fundamentales, entonces seguirá operando en la peligrosa ficción de que los datos se protegen con leyes... cuando lo que en verdad necesitan, muchas veces, es que no se corte la luz.

Referencias bibliográficas

- Bygrave, L. A. (2019). *Data Protection Law: Approaches and Challenges*. Oxford University Press. Disponible en: <https://global.oup.com/academic/product/data-protection-law-9780199675555>
- NIST (2020). *Framework for Improving Critical Infrastructure Cybersecurity*, versión 1.1. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press. <https://www.hup.harvard.edu/books/9780674035072>
- Unión Europea (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (NIS 2). <https://eur-lex.europa.eu/legalcontent/ES/TXT/?uri=CELEX%3A32022L2555>

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *PublicAffairs*. <https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395700/>

Conflicto de interés

El autor de este trabajo declara no tener conflicto de interés.

Información adicional

La correspondencia y las solicitudes de materiales sobre este escrito deben dirigirse al autor al correo electrónico proporcionado.

Las impresiones y la información sobre permisos están disponibles en el siguiente enlace:

https://revistas.up.ac.pa/index.php/contacto/acceso_reuso