VIGILANCIA DIGITAL EN CUBA

Primer Informe Integral

ENERO 2026

▶ LA DISTOPÍA DEL "BIG BROTHER", UNA REALIDAD EN CUBA

PRISONERS DEFENDERS | Consorcio Justicia

ÍNDICE DE CONTENIDOS

BLOQUE I – INTRODUCCIÓN Y RESUMEN EJECUTIVO

INTRODUCCIÓN

La vigilancia digital en Cuba no constituye un fenómeno aislado ni coyuntural, sino una política estructural de control estatal que ha evolucionado, partiendo del control desde hace décadas de las comunicaciones telefónicas y postales, de forma paralela a la expansión del acceso a Internet y de las tecnologías de la información. En el contexto cubano, la ampliación de la conectividad no ha estado acompañada de garantías democráticas, marcos efectivos de protección de derechos digitales ni mecanismos independientes de control judicial. Por el contrario, el espacio digital ha sido progresivamente incorporado como un nuevo ámbito de supervisión, control y represión política generalizada y sin límites.

Desde la introducción masiva del acceso móvil a Internet, el Estado cubano ha consolidado un modelo de gobernanza digital altamente centralizado, caracterizado por el monopolio estatal de las telecomunicaciones, la ausencia de transparencia normativa y la utilización de disposiciones legales amplias y ambiguas para criminalizar la expresión crítica en entornos digitales. Este modelo combina herramientas tecnológicas, marcos legales restrictivos y prácticas de vigilancia fraudulenta y violatoria del derecho internacional que, en conjunto, permiten un seguimiento, control y represión amplísima del comportamiento ciudadano tanto en el espacio virtual como en el físico.

La vigilancia digital en Cuba debe entenderse, y más aún cuando el lector compruebe el inmenso arsenal de mecanismos de seguimiento, control y represión en torno a ésta, que se deduce con todo detalle de la presente denuncia avalada por cientos de declaraciones, como una política de Estado articulada en múltiples niveles —técnico, jurídico, social, policial y administrativo— cuya finalidad no sólo trasciende de forma extrema la seguridad pública legítima, sino que más bien parece un sistema de sometimiento, un ecosistema de control social de carácter panóptico, siendo análogo a una implementación del "Big Brother" de Orwell en su libro "1984". Su objetivo principal es la neutralización del disenso, la inhibición del debate público y la desarticulación de redes sociales, cívicas y políticas independientes, como forma de sometimiento. En definitiva, el control absoluto de la persona violando sus derechos fundamentales, también en su entorno más personal. Tan absoluto es el control ejercido, que afecta igualmente a los ciudadanos que están fuera del país, siempre que alguien de su familia se encuentre dentro del mismo, o que deseen volver al país de visita, ya que el Estado ejerce el control de los que están fuera por medio de las represalias a los que están dentro, o en cuanto vuelven a su territorio nacional, incluso de visita turística.

El presente informe de denuncia documenta algo sabido popularmente en Cuba, como también se verá más adelante por el temor generalizado que emerge como conclusión no sólo a publicar, sino a hablar por cualesquiera medios de comunicación personal, y denunciado en numerosos casos a lo largo de los años con un nivel de detalle y escrutinio jamás visto hasta la fecha, toda la operativa de este sistema de vigilancia y control, a partir del análisis metódico de cientos de declaraciones y testimonios de primera mano de ciudadanos cubanos, y analiza sus implicaciones a la luz de los estándares internacionales de derechos humanos aplicables al entorno digital.

METODOLOGÍA

Este informe documenta y analiza patrones de vigilancia digital ejercidos contra personas cubanas, tanto dentro como fuera del país, a partir de evidencia empírica obtenida mediante una declaración estructurada como un amplio formulario diseñado a medida, así como de investigación jurídica y análisis de estándares internacionales de derechos humanos aplicables al entorno digital.

El análisis se basa en **200 declaraciones válidas de ciudadanos cubanos de dentro y fuera de Cuba**, recogidas mediante un formulario de declaración entre el 28 de noviembre de 2025 y el 5 de enero de 2026. El instrumento incluyó 47 preguntas sustantivas parametrizables y un número más reducido de preguntas abiertas orientadas a documentar experiencias concretas y aportar contexto cualitativo. Aunque se exponen todos los resultados de las declaraciones abiertamente, se han omitido los datos personales de forma pública por la represión que

sufrirían en caso de ser publicadas sus identidades, pero los contactos de aquellos denunciantes que así lo permitan están a disposición de las autoridades y organismos de protección de derechos que soliciten contacto con éstos.

La muestra de esta denuncia (200 declarantes/denunciantes) es **suficiente para un análisis descriptivo y exploratorio**, permitiendo **identificar patrones recurrentes y su coherencia interna**, así como relaciones consistentes entre variables.

Se utilizó un diseño muestral abierto mediante la técnica de bola de nieve, adecuado para el estudio de una población de difícil acceso, priorizando la identificación de patrones y dinámicas, mediante difusión por enlace directo, mensajería privada y redes de confianza. **Este enfoque resulta especialmente pertinente en contextos autoritarios y de alto riesgo, donde la denuncia pública puede generar represalias y donde los canales de confianza son esenciales para lograr la participación**. Por su naturaleza, los resultados no estiman prevalencias poblacionales, sino que describen patrones reportados por los participantes (n=200), útiles para identificar modalidades de represión y orientar análisis jurídicos y recomendaciones.

Todas las respuestas fueron sometidas a un proceso de validación interna que incluyó revisión de coherencia, comprobaciones de contraste entre preguntas relacionadas, y contacto posterior con los participantes para aclarar o confirmar la información. Los hallazgos fueron complementados con entrevistas cualitativas en profundidad y con un análisis jurídico exhaustivo de la normativa nacional e internacional aplicable.

Todos los testimonios se gestionan bajo estrictos criterios de ética y seguridad. La información se presenta al público de forma anónima y los datos sensibles de identificación se conservan con fines de documentación, comprobación, contraste, y eventual activación de mecanismos internacionales de protección, previa autorización expresa de las personas afectadas.

FICHA TÉCNICA

- **Objeto del informe de denuncia:** Documentación de patrones de vigilancia digital contra personas cubanas, dentro y fuera de Cuba, y su impacto en el ejercicio de derechos fundamentales.
- **Universo de referencia:** Ciudadanos cubanos usuarios de tecnologías digitales.
- **Tamaño muestral:** 200 declaraciones válidas.
- **Instrumento:** Cuestionario estructurado diseñado específicamente para este estudio, con 47 preguntas sustantivas, en muchos casos mediante la elección de opciones amplias y abarcadoras, pero parametrizables, y un número limitado de preguntas abiertas cualitativas.
- **Diseño muestral:** Muestreo abierto, mediante la técnica de "bola de nieve", gracias a la difusión por enlace directo y mensajería privada, invitando a los usuarios a compartir entre sus contactos de confianza.
- **Trabajo de campo:** 28 de noviembre de 2025 – 5 de enero de 2026.
- **Cobertura geográfica:** Ciudadanos cubanos residentes dentro (174) y fuera de Cuba (26).
- **Criterios de inclusión:** Ciudadanos cubanos.
- **Validación y contraste:** Revisión manual de coherencia, contraste interno entre variables, contacto posterior con personas participantes, entrevistas cualitativas adicionales y análisis documental y jurídico.
- **Ética y seguridad:** Anonimato integral en la exposición pública de los resultados, consentimiento informado, datos identificativos sensibles protegidos y compartidos únicamente con organismos internacionales de protección, previo consentimiento expreso de la/s persona/s afectada/s.
- **Análisis e inferencia:** Análisis descriptivo y exploratorio. No se realizan inferencias estadísticas ni estimaciones de representatividad poblacional. Los porcentajes se calculan sobre el denominador válido por cada pregunta.
- **Ponderación:** No se aplican pesos, y cada observación tiene el mismo valor analítico.
- **Enlace a las declaraciones** (se entregan anónimas por defecto, pero los organismos internacionales pueden solicitar los casos sin anonimato, con el consentimiento de las víctimas): https://docs.google.com/spreadsheets/d/1lNr1YUhf6kRivce1xyCdCgmRxIKgVssi

ALGUNOS HALLAZGOS SIGNIFICATIVOS PRELIMINARES

El análisis de las 200 respuestas válidas recogidas para este informe permite identificar una serie de hallazgos empíricos claros y consistentes sobre el funcionamiento de la vigilancia digital en Cuba y sus efectos sobre el ejercicio de derechos fundamentales.

En sentido general, los resultados son abrumadores. Al analizar todas las declaraciones -y las variables de cualesquiera formas de represión física derivada de publicaciones y comunicaciones-, este informe de denuncia documenta que **la casi totalidad de los declarantes/denunciantes, el 98,50% (197 de 200) ha sido o sancionado (penalmente, administrativamente o de facto), o citado o amenazado, o bien él mismo o su familia, en relación con sus publicaciones y/o comunicaciones telefónicas o digitales**. Las modalidades de represión, sin embargo, varían de unos a otros individuos. Cabe destacar que aquellos que nunca han sufrido represalia alguna, ni ellos ni sus familiares, son precisamente los que más elevados niveles de temor muestra en todos y cada uno de los medios de comunicación, mostrando una autocensura absoluta en las llamadas telefónicas, el whatsapp y las redes sociales, y sólo un ligero menor temor (grado 4 de 5) en Telegram, Signal y Videollamadas. Es decir, los que no reciben represión, de entre los 200 declarantes, tienen una autocensura absoluta en prácticamente todos los medios de comunicación, **indicando estos resultados empíricos cuál sería el objetivo de la represión ejercida por el régimen cubano: la completa autocensura del individuo**.

Los datos resultantes muestran de forma abrumadora que la vigilancia digital por parte del Estado en Cuba no opera como una práctica aislada o esporádica, sino como un sistema estructurado, reiterado y articulado con mecanismos de control presencial y sanción institucional. Ejemplo de ello son algunos de los resultados que a continuación se exponen, y otros múltiples que se detallan en los siguientes apartados de este informe de denuncia:

- **La vigilancia digital se manifiesta de manera sistemática y con una amplísima cobertura**. El **88%** de los declarantes/denunciantes manifiestan que **las autoridades cubanas mencionaron o reprocharon sus publicaciones o mensajes digitales** como causa de procesos de citación, detención e interrogatorios. El **76,50%** de los declarantes/denunciantes afirmó que autoridades cubanas mencionaron o reprocharon sus publicaciones o mensajes digitales **en múltiples ocasiones** asociado a citaciones o interrogatorios, mientras que un **11,50%** indicó que esto ocurrió **al menos una vez**. Estos datos confirman la existencia de un monitoreo activo, continuado y generalizado de la actividad en línea, con una capacidad de alcance ampliamente extendida en la población usuaria de servicios digitales. La inversión necesaria para una cobertura semejante conlleva **una ingente cantidad de recursos humanos y económicos del régimen destinados a la vigilancia digital de su población**.
- La vigilancia digital **se asocia de forma consistente con la represión presencial**, en particular mediante **citaciones, interrogatorios, amenazas y detenciones**, según los testimonios recogidos. En respuesta a sus comunicaciones privadas, su navegación en medios digitales y sus publicaciones en redes sociales y otros medios, **el 60% de los declarantes/denunciantes fue citado** formalmente por autoridades, **el 61% fue interrogado** y **el 55% fue incluso detenido**, lo que evidencia la articulación entre vigilancia digital y coerción física.
- **La vigilancia no se limita a contenidos públicos**. Un **46,50% de los declarantes/denunciantes, 93 de 200**, declara que **sus comunicaciones privadas de mensajería fueron intervenidas y mencionadas por las autoridades** en procesos de interrogatorio, amenazas, citaciones y detenciones, **sin su conocimiento ni tutela judicial alguna**. Un **42,50%** de los declarantes/denunciantes, **85 de 200**, reportó que las autoridades llegaron a mencionarles con todo detalle **mensajes privados** intercambiados mediante aplicaciones de mensajería personal. Incluso, un **20% de los declarantes/denunciantes, 40 de 200,** indicó que se utilizaron como ejemplos de reproche sus propios **audios privados** durante interrogatorios. Estos datos evidencian la extensión de la vigilancia a espacios de comunicación que deberían estar estrictamente protegidos también por el derecho a la privacidad.
- El análisis revela también **indicios graves de acceso no autorizado a cuentas y dispositivos**. El **49,50%** de las personas detectó **sesiones abiertas** desde ubicaciones desconocidas, el **46,50%** reportó **cambios de contraseña fraudulentos** no realizados por ellos mismos y el **37%** indicó que **se enviaron mensajes en usurpación de su identidad** desde sus cuentas sin consentimiento. Esta abrumadora cantidad de anomalías y violaciones de acceso denota **un patrón sistemático y coordinado de accesos no autorizados y control de cuentas compatible con una actuación organizada**.
- **La vigilancia digital opera** además **en un entorno de conectividad intervenido y manipulado estructuralmente**. Un indicio consistente para tal afirmación es que sólo un 5% de los declarantes/denunciantes, 10 de 200, afirmó no haber experimentado anomalías en su conexión. El **77,50%** reportó **cortes selectivos de Internet personalizados para ellos** mientras otras personas seguían teniendo

acceso normal, particularmente en contextos de protesta o actividad política. Igualmente, el **63,00%** reportó **bloqueos selectivos de servicios diversos de mensajería y/o páginas web** a las que no se puede acceder en Cuba salvo mediante servicios de VPN.

- **Los efectos de la vigilancia se extienden al espacio físico**. Un **84,50%** de los declarantes/denunciantes afirmó haber observado **vigilancia física posterior a su actividad digital frente a sus viviendas,** incluyendo presencia policial, seguimientos, cámaras frente a su casa, visitas de advertencia, patrullas y otros tipos de seguimiento, lo que confirma la existencia de **un modelo híbrido institucionalizado de control digital-presencial**.
- **Las represalias alcanzan también a los entornos familiares**. El **88,00% de los declarantes/denunciantes reportó represalias por sus comunicaciones y publicaciones contra sus familiares o allegados**, incluyendo detenciones, citaciones, amenazas, pérdida de empleo, problemas en el sistema educativo para alguno/s de su/s familiar/es, vigilancia física y otros tipos de represalias, lo que evidencia **una estrategia estatal de presión indirecta sobre el entorno familiar de los ciudadanos**. Esta diversidad de ataques represivos contra los familiares y allegados incluyeron represalias contra las parejas (40,50%), lo/s hijo/s (34,00%), lo/s hermano/s (29,50%) y otro/s familiar/es y allegado/s (32,50%). **De los 200 declarantes/denunciantes, sólo 24 indicaron que sus familiares no sufrieron represión por las publicaciones de otro familiar.**
- **Los datos confirman el temor generalizado sobre el ejercicio de la libertad de expresión en entornos digitales**. El **55,50%** de los declarantes/denunciantes tomaron medidas limitativas de su propia libertad de expresión por temor a las represalias: **un 24%dejó de publicar sobre política**, **un 21%borró alguna o algunas publicaciones antiguas**, **un 13,50%salió de grupos de WhatsApp/Telegram/otros**, **un 21,50% dejó de comunicarse con ciertas personas**, **un 18,50%usó seudónimos** y **un 19% cerró o cambió sus cuentas** por temor. Los niveles de temor reportados son elevados en todos los canales de comunicación, sin que exista ningún espacio percibido por los cubanos como seguro.

Los indicadores expuestos más arriba, y más aún con todos los hallazgos que mostramos en capítulos posteriores, demuestran que **la vigilancia digital en Cuba constituye un sistema estructurado de control que combina monitoreo tecnológico, coerción institucional y presión social, generando un efecto disuasorio extremo sobre la participación cívica y el ejercicio de derechos fundamentales.**

BLOQUE II – PERFIL DE LAS VÍCTIMAS Y EL CONTEXTO DE CONTROL DIGITAL EN CUBA

PERFIL DE LOS DECLARANTES/DENUNCIANTES

Las respuestas analizadas permiten trazar un perfil claro de las personas afectadas por prácticas de vigilancia digital documentadas en este informe, así como de los contextos en los que dichas prácticas se producen.

En cuanto al género, el **58% de los declarantes/denunciantes se identifican como hombres** (116 de los 200 declarantes), lo que refleja una ligera mayor participación masculina en la muestra. No obstante, la presencia significativa de mujeres y los resultados, similares para ambos sexos, evidencia que la vigilancia digital no constituye un fenómeno exclusivo de un solo género, sino una práctica transversal que afecta a distintos perfiles de la sociedad cubana.

Dado que la muestra incluía a familiares de presos políticos que querían reportar el caso de sus allegados, respecto a la naturaleza del testimonio el 81,50% de las respuestas corresponden a **experiencias de represión sufridas de manera directa por la propia persona declarante**, mientras que el 18,50% documenta situaciones padecidas por este tipo de allegados cercanos. Por tanto, el informe de denuncia se sustenta mayoritariamente en relatos en primera persona, reforzando el valor probatorio de los patrones identificados y reduciendo el margen de interpretación indirecta, lo que no desacredita los testimonios de los allegados en nombre de las personas que no podían cumplimentar el formulario, muchos de los cuales, es importante mencionarlo, lo rellenaron en diferido desde la prisión y transmitieron los resultados a los familiares encargados de rellenar físicamente la declaración.

Como resultaba relevante medir la represión de los cubanos en el exterior con respecto a sus publicaciones y comunicaciones a través de la represión a sus familiares, la declaración incluyó testimonios de cubanos en el exterior. En relación con la residencia de las víctimas de vigilancia digital, los datos muestran que el **87,00% reside en Cuba** (174 de 200). Solo un **13% de los casos reportados corresponde a personas que residen fuera**

de Cuba (26 de los 200 declarantes), aunque son ciudadanos cubanos vinculados con residentes en la isla, lo que confirma el carácter complementario, aunque significativo, de la **dimensión transnacional del fenómeno represivo**.

La distribución territorial dentro de Cuba de los declarantes revela una **concentración significativa en determinadas provincias**, en particular **La Habana (34,48%)**, seguida de **Artemisa (14,94%)**, **Holguín (10,92%)** y **Santiago de Cuba (8,62%)**, en relación con una mayor densidad poblacional, pero también con el sesgo natural de la muestra por la recolección mediante la técnica de "bola de nieve". La presencia de casos en 15 de las 16 provincias del país, en todo caso, confirma la amplitud de la muestra.

En cuanto a las características de los declarantes, un **51%** (102 de 200) de los declarantes/denunciantes se identifica como **activista o defensor/a con afiliación política**, un 33,50% (67 de los 200 declarantes/denunciantes) son familiares de presos políticos y un **28%** (56 de 200) forma parte de **organizaciones políticas o sociales**. Un **15,00%** (30 de 200) corresponde a **periodistas o comunicadores/as**, lo que asegura una representación notable en la muestra de quienes ejercen funciones informativas o de opinión pública. En la muestra también encontramos una notable representación de ciudadanos sin afiliación ni actividad política o de derechos alguna, un 17,00% (34 declarantes/denunciantes).

Esta distribución de perfiles resulta especialmente relevante desde una perspectiva de derechos humanos, ya que los estándares internacionales reconocen una protección reforzada para personas defensoras de derechos humanos, periodistas, activistas y personas que ejercen su libertad de expresión en asuntos de interés público. **La concentración de casos en estos perfiles de activismo social y político revela el hallazgo de una vigilancia selectiva y no aleatoria, orientada a controlar el disenso**.

En conjunto, esta amalgama de perfiles en la muestra junto a los resultados de represión contra familiares de todos ellos evidencia, además de la amplitud y diversidad de la muestra, que la vigilancia digital en Cuba **opera como una práctica amplia y estructural** con impacto en familias y ciudadanía sin y con afiliación política caso por igual, consolidando un entorno de control que trasciende la actividad individual y alcanza a redes sociales y afectivas completas.

ENTORNO DIGITAL Y CONDICIONES DE CONECTIVIDAD COMO BASE DEL CONTROL ESTATAL

El análisis de las respuestas permite caracterizar el entorno digital en el que los declarantes/denunciantes acceden a Internet y ejercen o intentan ejercer su derecho a la información y a la libertad de expresión en Cuba, así como las condiciones estructurales y técnicas que configuran dicho entorno y lo convierten en un espacio propicio para la vigilancia y el control estatal, en particular mediante **patrones de bloqueo, restricción del acceso y degradación selectiva de la conectividad**.

Desde el punto de vista del derecho internacional de los derechos humanos, **el acceso a Internet ha sido reconocido como un facilitador esencial del ejercicio de la libertad de expresión, de asociación y de participación política**. Diversas resoluciones del Consejo de Derechos Humanos de Naciones Unidas han afirmado que los mismos derechos que las personas tienen fuera de línea deben ser protegidos en línea, en particular la libertad de expresión.[1] Además, el Consejo ha condenado inequívocamente las medidas destinadas a impedir o interrumpir intencionalmente el acceso o la difusión de información en línea —incluidos los cortes, bloqueos y otras interferencias arbitrarias— por ser incompatibles con el derecho internacional.[2] De forma complementaria, el Consejo ha reiterado que la vigilancia y otras injerencias en la vida privada mediante tecnologías digitales deben estar estrictamente sujetas a legalidad, necesidad y proporcionalidad, para evitar injerencias arbitrarias o ilegales.[3]

[1] Consejo de Derechos Humanos, Resolución 20/8, La promoción, protección y disfrute de los derechos humanos en Internet, A/HRC/RES/20/8 (5 de julio de 2012).
[2] Consejo de Derechos Humanos, Resolución 32/13, La promoción, protección y disfrute de los derechos humanos en Internet, A/HRC/RES/32/13 (1 de julio de 2016); y Resolución 57/29, Promoción, protección y disfrute de los derechos humanos en Internet, A/HRC/RES/57/29 (11 de octubre de 2024).
[3] Consejo de Derechos Humanos, Resolución 54/21, El derecho a la privacidad en la era digital, A/HRC/RES/54/21 (12 de octubre de 2023).

ESPACIOS DIGITALES DE EXPRESIÓN Y CIRCULACIÓN DE CONTENIDO CRÍTICO

Las plataformas más utilizadas **para expresar opiniones políticas o compartir contenido crítico** reflejan un ecosistema digital concentrado en un número limitado de servicios ampliamente conocidos y controlables. **Facebook emerge como el espacio central de expresión**, utilizado por el **90,00%** de los declarantes/denunciantes (180 de 200). Le siguen **WhatsApp** en sus distintas modalidades (chats privados, grupos y estados) con un **57,50%** (115 de 200), y **llamadas telefónicas o SMS**, con un **46,00%** (92 de 200).

En otros espacios relevantes **para expresar opiniones políticas o compartir contenido crítico** se incluyen los **medios independientes**, utilizados por el **29,50%** de los declarantes/denunciantes (59 de 200), **Instagram** (**26,50%, 53 de 200**), **correo electrónico** (**20,50%, 41 de 200**), **YouTube** (**19,00%, 38 de 200**), **X/Twitter** (**17,00%, 34 de 200**) y **Telegram** (**17,00%, 34 de 200**). Plataformas como **TikTok** aparecen con una presencia marginal (**7,50%, 15 de 200**).

Esta distribución muestra que la expresión política y el intercambio de información crítica no se concentran en espacios marginales, sino en plataformas de uso cotidiano y masivo, lo que incrementa la exposición de las personas usuarias a mecanismos de control e interferencia en un entorno digital altamente centralizado.

INTERFERENCIAS TÉCNICAS Y ANOMALÍAS EN LA CONECTIVIDAD

Las respuestas evidencian un **patrón extendido de interferencias técnicas en la conectividad**, difícilmente atribuible a fallos aislados. Solo un **5,00%** de los declarantes/denunciantes (10 de 200) afirmó no haber experimentado ninguna anomalía en su conexión.

Entre los problemas reportados con mayor frecuencia se encuentran el **corte total de datos móviles o conectividad específica y afectando únicamente a su línea**, señalado por el **52,00%** de las respuestas (104 de 200), así como los **cortes del entorno cercano mientras otros usuarios de la misma zona mantenían conectividad** (**51,00%, 102 de 200**).

Asimismo, se reportaron **apagones totales de conectividad y/o llamadas en determinadas zonas** (**47,50%, 95 de 200**), **fallos en servicios de mensajería o llamadas durante protestas u otros eventos sensibles** (**49,00%, 98 de 200**) y **reducción extrema e intencionada de la velocidad de navegación (throttling)** (**47,00%, 94 de 200**).

Otras prácticas incluyen el **bloqueo de redes sociales específicas** como Facebook, X o YouTube (**44,50%, 89 de 200**), el **bloqueo permanente de páginas web si no se utiliza una VPN** (**36,00%, 72 de 200**), la imposibilidad de acceso a **páginas de medios independientes u organismos internacionales** (**36,50%, 73 de 200**) y el **bloqueo o imposibilidad de uso de VPN** (**22,50%, 45 de 200**). El bloqueo o limitación del uso de VPN resulta particularmente relevante, al tratarse de una herramienta empleada para eludir censura, acceder a información independiente y proteger la privacidad de las comunicaciones.

En conjunto, estos datos describen un entorno de conectividad **inestable, selectivamente degradado y funcionalmente restrictivo**, que condiciona el acceso a Internet de manera cotidiana y restringe de forma sistemática el ejercicio de derechos fundamentales en el entorno digital. Asimismo estas interferencias técnicas configuran un **patrón consistente de bloqueos y cortes de Internet**, que afecta de manera selectiva y recurrente el acceso a la conectividad.

La recurrencia, selectividad y coincidencia temporal de estas interrupciones con eventos políticos, protestas o fechas simbólicas hacen poco plausible que se trate únicamente de fallos fortuitos y resultan consistentes con un uso instrumental de la infraestructura de telecomunicaciones como herramienta de control.

COINCIDENCIA DE LOS CORTES CON EVENTOS POLÍTICOS Y SOCIALES

Las interferencias en la conectividad presentan una **clara coincidencia temporal con eventos políticos y socialmente sensibles**:

- El **71,00%** de los declarantes/denunciantes (142 de 200) indicó que los cortes o anomalías ocurrieron durante **protestas**;
- El **73,50%** (147 de 200) durante **fechas o momentos simbólicos**, como el 11 de julio, el Día del Trabajo o el Día de los Derechos Humanos.

- Casi la mitad de los declarantes/denunciantes (**50,50%, 101 de 200**) afirmó que las interferencias coincidieron con **publicaciones críticas propias**;
- Un **34,50%** (69 de 200) las asoció a **juicios políticos**;
- Un **27,50%** (55 de 200) a **eventos oficiales del régimen**; mientras
- Solo un **4%** (8 de 200) manifestó no estar seguro de la coincidencia temporal.

La reiterada coincidencia temporal entre cortes de conectividad y eventos políticos o socialmente sensibles refuerza la identificación de un **patrón de bloqueos y cortes de Internet utilizados como mecanismo de control y contención.**

BARRERAS ESTRUCTURALES DE ACCESO A INTERNET

A las interferencias técnicas se suman **limitaciones estructurales y económicas** que afectan de manera sostenida el acceso a Internet. El **80,00%** de los declarantes/denunciantes (160 de 200) considera que la conexión es **demasiado cara para un uso habitual**, mientras que el **69,00%** (138 de 200) reporta **velocidades insuficientes** para acceder a noticias online. La sensación reportada es consistente con una degradación selectiva del tráfico: conectividad funcional para mensajería ligera (p. ej., WhatsApp) pero limitada o nula para navegación web y acceso a contenidos de mayor carga (p. ej., sitios informativos o recursos audiovisuales), lo que sugiere un manejo discriminatorio de la conectividad. **La falta de velocidad, en definitiva, se hace insoportable en muchas ocasiones como para que los cubanos se puedan informar de forma efectiva y cotidiana.**

Asimismo, el **49,50%** (99 de 200) indicó que el acceso a Internet está disponible **solo en horarios limitados**, el **46,00%** (92 de 200) reportó **problemas técnicos recurrentes del proveedor**, y el **46,50%** (93 de 200) percibió un **acceso desigual en comparación con otras zonas urbanas**. Solo un **7%** (14 de 200) afirmó no haber experimentado dificultades para acceder a Internet.

Estas limitaciones no responden únicamente a deficiencias técnicas, sino que se inscriben en **una brecha digital estructural asociada al monopolio estatal del proveedor de servicios de telecomunicaciones**, que condiciona de forma constante el acceso a Internet.

IMPACTO DE LAS LIMITACIONES EN EL EJERCICIO DE DERECHOS

Las consecuencias de estas restricciones son claras. Un **88,50%** de los declarantes/denunciantes (177 de 200) considera que las limitaciones de acceso a Internet **afectan de forma extrema su posibilidad de informarse o participar en debates públicos**, mientras que un **5%** (10 de 200) las considera sólo **parcialmente limitantes**. Solo un **1%** (2 de 200) manifestó que las limitaciones no han tenido impacto en su capacidad de informarse o participar en debates públicos.

El impacto descrito **muestra** que los bloqueos, restricciones y barreras estructurales de acceso a Internet **tienen un efecto altamente significativo** sobre el ejercicio de derechos fundamentales de acceso a la información y participación pública.

De acuerdo con los estándares internacionales, las restricciones al acceso a Internet solo pueden ser impuestas de manera excepcional, conforme a criterios de legalidad, necesidad y proporcionalidad. **La magnitud y recurrencia de las limitaciones documentadas en este informe violan claramente dichos estándares, configurando una restricción estructural al ejercicio de la libertad de expresión y el derecho a la información.**

PERCEPCIÓN DE RIESGO Y GRADUACIÓN DEL TEMOR SEGÚN EL MEDIO DE COMUNICACIÓN UTILIZADO

Para medir el temor medio a publicar en diferentes medios, solicitamos a todos los declarantes que indicaran el nivel de temor, del 1 al 5, referido al uso de diferentes medios de comunicación y expresión digital. En el análisis de su respuesta, como en el apartado anterior, debemos tener en cuenta que la representatividad de activistas y familiares de presos políticos en la muestra es muy elevado, y que aquellos que cumplimentaron la declaración de denuncia, realizada por medio de la técnica de "bola de nieve", son precisamente del entorno de confianza de los primeros y, para declarar, han tenido que superar un cierto umbral de temor que no es habitual en la población cubana al comunicarse sobre temas de índole política o derechos humanos.

Aún con dicha consideración, tal y como se documentó anteriormente, los niveles promedio de miedo a denunciar o expresarse alcanzan valores elevados en **llamadas telefónicas** (**un promedio de temor del 3,37**

sobre 5), **redes sociales como Facebook** (**un promedio de temor del 3,31 sobre 5**) y **WhatsApp en grupos** (**un promedio de temor del 3,18 sobre 5**), mientras que se mantienen ligeramente inferiores —aunque aún significativos— en **videollamadas (un promedio de temor de 3,07 sobre 5)**, **Telegram** (**un promedio de temor del 2,80 sobre 5**), **WhatsApp uno a uno** (**media 2,80 sobre 5**) y **Signal** (**media 2,56 sobre 5**).

Estos resultados evidencian que el miedo a expresarse **atraviesa todo el ecosistema digital**, variando según la visibilidad, la trazabilidad percibida y el grado de control atribuido a cada medio.

De los 200, **160 expresaron un alto temor en alguno o varios de los canales de comunicación habituales**, siendo el promedio de temor de los 200 declarantes de **3,01 sobre un máximo de 5**.

Este clima de temor generalizado se asocia con prácticas de autocensura y retraimiento digital, que se analizan de manera específica en capítulos posteriores.

En conjunto, los datos muestran que la vigilancia digital en Cuba se apoya en un **entorno digital estructuralmente precario, económicamente restrictivo y técnicamente intervenido**, que condiciona el acceso a Internet y limita el comportamiento y la expresión de las personas incluso antes de que se produzcan actos explícitos de vigilancia o represión. Este entorno constituye el **sustrato sobre el cual operan posteriormente prácticas más directas de control, vigilancia y sanción**, que se analizan en los capítulos siguientes.

Este clima de temor generalizado constituye un elemento central para comprender los niveles de autocensura y retraimiento digital que se documentan en el capítulo siguiente, y confirma el efecto disuasorio buscado por las prácticas de vigilancia descritas.

BLOQUE III – PATRONES DE VIGILANCIA DIGITAL

Las respuestas analizadas evidencian la existencia de prácticas sistemáticas y reiteradas de vigilancia digital ejercidas por autoridades cubanas, que abarcan el **monitoreo de redes sociales, la interceptación de comunicaciones privadas, el acceso no autorizado a cuentas y dispositivos, así como el uso de información digital como insumo directo para citaciones, interrogatorios, detenciones y otras formas de presión.**

Este capítulo documenta hechos concretos, reportados por las propias personas afectadas, que permiten identificar mecanismos operativos de vigilancia digital y su articulación con prácticas represivas presenciales.

A continuación se presentan los patrones documentados, organizados en diez categorías analíticas.

PATRÓN 1: CIBERPATRULLAJE Y MONITOREO SISTEMÁTICO DE REDES

Este patrón se refiere a la observación sistemática de publicaciones, interacciones y contenidos compartidos en redes sociales y plataformas de mensajería, así como a su registro y utilización posterior por autoridades para intimidar, advertir o sancionar a la persona.

La vigilancia de la actividad en redes sociales y plataformas digitales emerge como una práctica ampliamente documentada. Un **76,50%** de los declarantes/denunciantes (153 de 200) afirmó que **autoridades cubanas mencionaron o reprocharon sus publicaciones o mensajes digitales en múltiples ocasiones, de forma explícita o velada, durante citaciones o interrogatorios**. Un **12,00%** (24 de 200) reportó que esto ocurrió **al menos una vez**, mientras que solo un **11,50%** (23 de 200) indicó que nunca le fueron mencionados contenidos digitales en procesos de citación e interrogatorios.

¿Alguna autoridad cubana ha mencionado o reprochado sus publicaciones o mensajes digitales durante citaciones/interrogatorios?		
Respuesta	**Declarantes**	**Porcentaje**
Sí, múltiples veces, explícita o veladamente	**153**	**76,50%**
Sí, al menos una vez, explícita o veladamente	**24**	**12,00%**
No, nunca, ni veladamente	**23**	**11,50%**

En los casos mencionados, además, la información utilizada por las autoridades provino, en una proporción significativa, de contenidos extraídos directamente de redes sociales y plataformas de mensajería. El **57,50%** de los declarantes/denunciantes (115 de 200) señaló que **las autoridades mostraron o mencionaron capturas**

de sus publicaciones, mientras que el **47,00%** (94 de 200) indicó que durante **interrogatorios se les comentó explícitamente que estaban siendo vigiladas en redes sociales**.

Asimismo, las autoridades mencionaron mensajes privados de aplicaciones de mensajería cifrada o semiprivada (como WhatsApp, Telegram o Signal) en el **42,50%** de los casos (85 de 200 declarantes, cifra que consolida las menciones de mensajes en grupos y mensajes en chats privados), mencionando mensajes en grupos privados en el **29,50%** (59 de 200) y mensajes en conversaciones uno-a-uno en el **33,00%** de los casos (66 de 200). Incluso **audios privados** fueron mencionados en el **20,00%** de los casos (40 de 200).

¿Qué tipo de contenido las autoridades mencionaron, mostraron o reprocharon durante citaciones y otros actos represivos?		
Respuesta	**Declarantes**	**Porcentaje**
Capturas de mis publicaciones	**115**	**57,50%**
Mensajes privados en conversaciones uno-a-uno y de grupos de WhatsApp/Telegram/Signal	**85**	**42,50%**
Mensajes privados en conversaciones uno-a-uno de WhatsApp/Telegram/Signal	**66**	**33,00%**
Mensajes en grupos privados	**59**	**29,50%**
Audios privados	**40**	**20,00%**
Comentaron que “le estaban vigilando en redes”	**94**	**47,00%**
Otro	**32**	**16,00%**

Estos datos confirman que la vigilancia estatal no se limita al contenido público, sino que se extiende de manera sistemática a espacios que las personas usuarias perciben como privados o semiprivados. Estos hallazgos permiten identificar un **patrón sistemático de Ciberpatrullaje y monitoreo de redes sociales**, en el que la actividad digital es observada, registrada y utilizada por las autoridades como insumo para acciones represivas.

PATRÓN 2: BLOQUEOS, CORTES DE INTERNET Y DEGRADACIÓN SELECTIVA DE LA CONECTIVIDAD

Este patrón se refiere a la interrupción, restricción o degradación deliberada del acceso a Internet y/o al funcionamiento de aplicaciones y servicios digitales, ya sea de manera generalizada por zonas, o de forma selectiva sobre líneas específicas. Incluye cortes totales, bloqueos de redes sociales o sitios web, fallos inducidos en servicios de mensajería y llamadas, así como la reducción extrema de velocidad (throttling), especialmente en momentos de movilización social o circulación de contenido crítico.

Las respuestas analizadas evidencian un escenario extendido de interferencias técnicas en la conectividad que, por su recurrencia y consistencia, resulta difícil de atribuir a fallas aisladas o al azar. Solo un 5% de los declarantes/denunciantes (10 de 200) afirmó no haber experimentado ninguna anomalía en su conexión, lo que indica que la gran mayoría de participantes ha enfrentado algún tipo de afectación vinculada al acceso o uso de Internet.

El resumen de este patrón represivo se visualiza con los resultados de las declaraciones:

- Sufren **cortes selectivos de Internet el 77,50%** de los declarantes/denunciantes (155 de 200).
- Sufren **bloqueos selectivos de servicios o páginas el 63,00%** de los declarantes/denunciantes (126 de 200).

Entre las prácticas reportadas con mayor frecuencia se encuentran el **corte total de datos móviles o conectividad dirigido a la línea personal** (**52%**, 104 de 200) y los **cortes que afectaron simultáneamente a la línea propia y a otras del entorno inmediato mientras otros usuarios de la misma zona mantenían conectividad** (**51%**, 102 de 200). Este segundo hallazgo resulta especialmente relevante porque sugiere un componente selectivo y discriminatorio: la conectividad no se interrumpe de forma homogénea, sino que puede operar de manera diferenciada sobre determinadas personas o grupos.

Asimismo, se reportaron **apagones totales de conectividad y/o llamadas en determinadas zonas** (**47,50%**, 95 de 200), **fallos en servicios de mensajería o llamadas durante protestas u otros eventos sensibles** (**49%**, 98 de 200) y **reducción extrema e intencionada de la velocidad de navegación (throttling)** (**47%**, 94 de 200). Estas prácticas, en conjunto, describen un entorno de acceso inestable y degradado que afecta no solo la comunicación interpersonal, sino también la posibilidad de informarse, documentar abusos o participar en debates públicos en tiempo real.

A estas interferencias se suman los **bloqueos de plataformas y contenidos**: un 44,50% (89 de 200) reportó **bloqueo de redes sociales específicas** como Facebook, X o YouTube; un 36% (72 de 200) indicó el **bloqueo habitual de páginas web si no se utiliza VPN**; y un 36,50% (73 de 200) señaló **imposibilidad de acceso a páginas de medios independientes u organismos internacionales**. También aparece un elemento adicional de alta gravedad: el **bloqueo o imposibilidad de uso de VPN** (22,50%, 45 de 200), lo que limita deliberadamente una herramienta asociada a la privacidad, la seguridad digital y el acceso a información sin censura.

¿Ha experimentado alguno de estos problemas en su conexión del celular asociados a su actividad digital?		
Respuesta	**Declarantes**	**Porcentaje**
Corte total de datos móviles o conectividad únicamente en mi línea de forma específica	**104**	**52,00%**
Corte total de datos móviles o conectividad en mi línea y otras de mi entorno, mientras otros usuarios, vecinos o ciudadanos de mi zona aún tenían línea o conectividad	**102**	**51,00%**
Reducción extrema de la velocidad de navegación (throttling) intencionada	**94**	**47,00%**
Bloqueo de redes específicas (Facebook, X, YouTube…)	**89**	**44,50%**
Bloqueo habitual de ciertas páginas web si no se usa VPN (“vi-pi-en”)	**72**	**36,00%**
Páginas de medios independientes u organismos no abrían	**73**	**36,50%**
Fallos en WhatsApp/Telegram/Signal o llamadas precisamente durante protestas	**98**	**49,00%**
Apagón total de conectividad y/o llamadas en su zona	**95**	**47,50%**
Bloqueo de VPN (“vi-pi-en”) o imposibilidad de usarla	**45**	**22,50%**
No, no he experimentado ninguna anomalía	**10**	**5,00%**
Cortes selectivos de Internet	**155**	**77,50%**
Bloqueos selectivos de servicios o páginas	**126**	**63,00%**

La dimensión temporal refuerza la identificación de este patrón como mecanismo de control y contención. Un **71%** de los declarantes/denunciantes (142 de 200) reportó que los cortes o anomalías ocurrieron **durante protestas**, y un **73,50%** (147 de 200) indicó que ocurrieron en **fechas o momentos simbólicos** como el 11 de julio, el Día del Trabajo o el Día de los Derechos Humanos. Además, casi la mitad de la muestra (**50,50%**, 101 de 200) afirmó que las interferencias coincidieron con **publicaciones críticas propias**, lo que sugiere que, en un número significativo de casos, estas restricciones no operan únicamente como medidas generales, sino que pueden activarse como respuesta a expresiones concretas.

¿Coincidieron estos cortes con algún evento?		
Respuesta	**Declarantes**	**Porcentaje**
Protestas	**142**	**71,00%**
Juicios políticos	**69**	**34,50%**
Mis publicaciones críticas	**101**	**50,50%**
Eventos oficiales	**55**	**27,50%**
Días y momentos señalados (en torno al 11 de julio, en torno al día del trabajo, en torno al día de los derechos humanos, etc.)	**147**	**73,50%**
No sé, no estoy seguro	**8**	**4,00%**

En su conjunto, los datos permiten concluir que los bloqueos, cortes y degradaciones de conectividad constituyen un patrón consistente de restricción del entorno digital, utilizado en momentos de especial sensibilidad política y, en ocasiones, con rasgos selectivos. Este patrón no solo limita la comunicación y el acceso a información, sino que crea un entorno de incertidumbre y vulnerabilidad técnica que facilita y complementa otras prácticas de vigilancia, intrusión y represión documentadas en los patrones siguientes.

PATRÓN 3: INTERCEPTACIÓN DE COMUNICACIONES, SPYWARE Y ACCESO NO AUTORIZADO A CUENTAS

INTERCEPTACIÓN/MONITOREO DE COMUNICACIONES PRIVADAS

La información reportada permite identificar un patrón consistente de vigilancia de comunicaciones privadas, particularmente mensajes, audios y conversaciones mantenidas en aplicaciones de mensajería y otros canales digitales.

Además de las menciones directas de mensajes privados durante interrogatorios, un número significativo de personas reportó indicadores indirectos de interceptación o monitoreo. Las interferencias dirigidas en la conectividad (como cortes selectivos, bloqueos de aplicaciones o fallos coincidentes con protestas) fueron experimentadas por amplios sectores de la muestra, mientras solo un **4%** (8 de 200) indicó no haber sufrido ninguna anomalía.

La reiteración de estas prácticas, combinada con la posterior utilización de contenidos privados durante citaciones, refuerza la hipótesis de que las comunicaciones digitales son objeto de observación, registro y análisis sistemático por parte de las autoridades.

Aunque el instrumento no permite identificar la herramienta específica utilizada en cada caso, la combinación de (i) referencias a contenido privado durante interrogatorios, (ii) interrupciones selectivas de conectividad y (iii) señales de intervención en cuentas y dispositivos descritas por las víctimas resulta **compatible** con un abanico de **prácticas de vigilancia técnica intrusiva, incluyendo interceptación de comunicaciones y eventual uso de software de intrusión (spyware)**. En consecuencia, el hallazgo relevante para este informe no es la identificación de una tecnología concreta, sino **la existencia de indicadores convergentes que apuntan a un patrón de vigilancia sobre comunicaciones privadas y entornos digitales personales, sin garantías de legalidad ni control independiente.**

La información disponible permite identificar un **patrón consistente de vigilancia de comunicaciones privadas**, incompatible con el carácter confidencial de las comunicaciones digitales.

ACCESO NO AUTORIZADO A CUENTAS Y DISPOSITIVOS

Las respuestas documentan prácticas graves de intrusión digital, que incluyen acceso no autorizado a cuentas personales y dispositivos electrónicos.

Un **49,50%** de los declarantes/denunciantes (99 de 200) reportó **haber recibido avisos de sesiones abiertas desde ubicaciones desconocidas**, mientras que un **46,50%** (93 de 200) detectó **intentos o cambios de contraseña no iniciados por la propia persona**. Asimismo, un **37%** (74 de 200) afirmó que **se enviaron mensajes desde sus cuentas sin su autorización**, y un **23,50%** (47 de 200) **detectó aplicaciones desconocidas instaladas en su teléfono sin consentimiento**.

Adicionalmente, un **37,50%** de los declarantes/denunciantes (75 de 200) señaló que **las autoridades les mencionaron directamente sus mensajes privados**, reforzando la presunción de acceso indebido a comunicaciones personales. Solo un **15%** (30 de 200) indicó no haber notado nunca signos de intervención en cuentas o dispositivos.

Estos indicadores describen un **patrón de acceso no autorizado a cuentas y dispositivos**, compatible con prácticas de intrusión digital y vigilancia técnica.

A esta dinámica se suma la **intrusión coercitiva directa por parte de las autoridades**, documentada de manera consistente en las respuestas del cuestionario. En global, **el 65,50% de los declarantes/denunciantes (131 de los 200) fueron obligados a desbloquear sus teléfonos, a entregar sus contraseñas, a permitir la revisión de su contenido o a mostrar sus redes sociales**.

Un **48,00%** de los declarantes/denunciantes (**96 de 200**) reportó que **fueron obligados a desbloquear su teléfono** durante una detención o interrogatorio; un **33,00%** (**66 de 200**) indicó que **se les exigieron contraseñas** de acceso a sus cuentas o dispositivos; y un **37,50%** (**75 de 200**) señaló que las autoridades **revisaron o copiaron fotos, documentos o chats** almacenados en sus teléfonos. Asimismo, un **33,00%** (**66 de 200**) fue obligado a **mostrar sus redes sociales** a agentes estatales.

¿Alguna autoridad cubana exigió acceso a su teléfono o cuentas sin tener mandato o tutela judicial?		
Respuesta	**Declarantes**	**Porcentaje**
Me (o le) solicitaron u obligaron a desbloquear el teléfono	**96**	**48,00%**
Me (o le) pidieron contraseñas	**66**	**33,00%**
Revisaron/copiaron fotos, documentos o chats	**75**	**37,50%**
Me (o le) hicieron mostrar mis redes sociales	**66**	**33,00%**

No, nunca una autoridad me (o le) ha/n pedido acceso, contraseñas o me pidieron mostrar nada	69	34,50%

Estos datos evidencian que la vigilancia digital no se limita a prácticas encubiertas o técnicas, sino que incluye **formas directas de coacción física y psicológica**, mediante las cuales se fuerza el acceso a información privada sin orden judicial ni garantías procesales. Esta modalidad elimina cualquier expectativa razonable de privacidad y convierte al propio dispositivo personal en un instrumento de control estatal.

La exigencia de acceso a teléfonos y cuentas, combinada con la posterior utilización de esa información en interrogatorios o procesos sancionatorios, confirma la existencia de un patrón sistemático de **intrusión digital coercitiva**, que articula vigilancia técnica y presión presencial como parte de una misma estrategia de control.

Aunque el instrumento no permite identificar la herramienta específica utilizada en cada caso, la combinación de (i) referencias a contenido privado durante interrogatorios, (ii) interrupciones selectivas de conectividad y (iii) señales de intervención en cuentas y dispositivos descritas por las víctimas resulta **compatible** con un abanico de **prácticas de vigilancia técnica intrusiva, incluyendo interceptación de comunicaciones y eventual uso de software de intrusión (spyware).** En consecuencia, el hallazgo relevante para este informe no es la identificación de una tecnología concreta, sino la existencia de **indicadores convergentes** que apuntan a un patrón de vigilancia sobre comunicaciones privadas y entornos digitales personales, sin garantías de legalidad ni control independiente.

En suma, el patrón documentado combina **vigilancia de comunicaciones privadas**, **señales de intervención técnica** y, en algunos casos, **exigencias coercitivas de acceso** a dispositivos y cuentas, configurando un esquema de intrusión incompatible con la confidencialidad de las comunicaciones y con estándares mínimos de legalidad, necesidad y proporcionalidad.

PATRÓN 4: CÁMARAS, VIGILANCIA FÍSICA DIGITALIZADA Y CONTROL DEL ESPACIO PÚBLICO

Las respuestas analizadas permiten identificar **un patrón consistente de vigilancia física digitalizada**, reportada con posterioridad a la actividad digital de los declarantes/denunciantes. Esta forma de control evidencia la existencia de un **sistema híbrido**, en el que **la vigilancia en línea no se limita al entorno virtual, sino que se articula y se acompaña de prácticas presenciales** de seguimiento, intimidación y control territorial.

Tras realizar publicaciones, enviar mensajes o participar en intercambios críticos en redes sociales u otros medios digitales, un **60,50%** (**121 de 200**) de los declarantes/denunciantes afirmó haber comprobado **vigilancia física de manera frecuente**, mientras que un **24,00%** (**48 de 200**) indicó haberla experimentado **de forma ocasional**. En conjunto, un **84,50%** (**169 de 200**) reporta **algún grado de vigilancia física posterior a su actividad digital**. Solo un **4,50%** (**9 de 200**) afirmó no haber observado vigilancia física, y un **11%** (**22 de 200**) manifestó no estar seguro.

Después de alguna actividad digital en redes sociales u otros medios digitales, ¿notó vigilancia física?		
Respuesta	**Declarantes**	**Porcentaje**
Sí, frecuentemente	**121**	**60,50%**
Sí, ocasionalmente	**48**	**24,00%**
No estoy seguro	**22**	**11,00%**
No	**9**	**4,50%**

Estos datos permiten afirmar que, para una mayoría abrumadora de los declarantes/denunciantes, la actividad digital **no queda confinada al espacio virtual**, sino que se asocia con respuestas observables en el espacio físico.

MODALIDADES DE VIGILANCIA FÍSICA OBSERVADAS

Las formas de vigilancia física reportadas muestran un **despliegue amplio y diversificado de recursos**, orientado tanto al control directo como a la intimidación psicológica. La modalidad más frecuentemente observada fue la **presencia de personas vigilando frente a sus casas**, reportada por el **68,50%** de los declarantes/denunciantes (**137 de 200**). A ello se suman las **visitas de advertencia por parte de autoridades o agentes**, señaladas por el **60,50%** (**121 de 200**), que constituyen una forma explícita de presión presencial vinculada a la actividad digital previa.

Asimismo, un **53,50%** (**107 de 200**) reportó **seguimientos mediante motos o automóviles**, y un **49,50%** (**99 de 200**) indicó la **presencia recurrente de patrullas frente a su vivienda**. Estas prácticas sugieren un control sistemático del movimiento y del entorno inmediato de las personas vigiladas.

En menor proporción, pero con especial gravedad, un **13,50%** (**27 de 200**) reportó la **instalación o presencia de cámaras frente a la vivienda**, lo que introduce un componente de vigilancia permanente y tecnológicamente mediada del espacio doméstico. Un **11,00%** (**22 de 200**) señaló **otros tipos de vigilancia física**, que incluyen observación encubierta esporádica, conversaciones informales de agentes o advertencias transmitidas vía telefónica o a través de terceros.

¿Qué tipo de vigilancia física observó?		
Respuesta	**Declarantes**	**Porcentaje**
¿Algún tipo de vigilancia física?	**169**	**84,50%**
Patrullas frente a su casa	**99**	**49,50%**
Personas vigilando en la calle	**137**	**68,50%**
Cámaras frente a la vivienda	**27**	**13,50%**
Seguimiento por motos o autos	**107**	**53,50%**
Visitas de advertencia	**121**	**60,50%**
Otro tipo de vigilancia	**22**	**11,00%**

En conjunto, estas modalidades combinan funciones de **control operativo** del movimiento y del entorno inmediato, con un claro **efecto intimidatorio** orientado a disuadir la expresión y la participación cívica.

ARTICULACIÓN ENTRE VIGILANCIA DIGITAL Y CONTROL FÍSICO

La elevada frecuencia con la que estas prácticas ocurren **después de actividades digitales concretas**, unida al uso reiterado de publicaciones, mensajes privados o audios como insumos durante citaciones e interrogatorios —documentado en capítulos anteriores—, permite identificar una **articulación directa entre la vigilancia digital y la vigilancia física**.

La vigilancia física digitalizada opera así como un **mecanismo de refuerzo y materialización del control digital**, trasladando al espacio cotidiano la presión ejercida previamente en línea. Este desplazamiento cumple una doble función: por un lado, **incrementa la capacidad de control estatal** sobre la persona vigilada; por otro, **produce un efecto intimidatorio ampliado**, al hacer visible y tangible la vigilancia ante la comunidad, la familia y el entorno social inmediato.

Los datos recogidos muestran que la vigilancia física digitalizada **no constituye una práctica excepcional**, sino un componente estructural del sistema de control documentado en este informe. Su recurrencia, diversidad de modalidades y clara vinculación temporal con la actividad digital permiten concluir que se trata de una **estrategia deliberada de control híbrido**, cuyas características plantean serias preocupaciones desde la perspectiva de los estándares internacionales sobre privacidad, libertad de expresión y protección contra injerencias arbitrarias.

PATRÓN 5: USO DE NORMAS JURÍDICAS Y SANCIONES ADMINISTRATIVAS PARA CASTIGAR LA EXPRESIÓN DIGITAL

Este patrón se refiere al uso sistemático de marcos normativos ambiguos o discrecionales para sancionar conductas vinculadas a la expresión en Internet, convirtiendo el derecho administrativo y penal en herramientas de control del discurso público.

Los datos recabados muestran que la vigilancia digital no se limita a la observación o intimidación informal, sino que se articula con mecanismos legales punitivos, utilizados de manera selectiva contra personas que expresan opiniones críticas o difunden información considerada sensible por las autoridades.

El número de sancionados penales y administrativos en la muestra llama la atención por la cantidad de declarantes/denunciantes que han sufrido estas sanciones. En particular, **de los 200 declarantes/denunciantes, y debido a sus comunicaciones digitales**:

- A **116** de ellos (el **58%**) les **prohibieron o advirtieron** de no tener relación con ciertas personas.
- A **93** de ellos (el **46,50%**) les **amenazaron directa o veladamente** con acciones punitivas.

- A **77** de ellos (el **38,50%**) les **realizaron una investigación penal** formal.
- A **35** de ellos (el **17,50%**) les iniciaron una **acusación penal formal**.
- A **61** de ellos (el **30,50%**) les **impusieron una medida cautelar** formal o de facto.
- A **47** de ellos (el **23,50%**) les **impusieron una multa administrativa** por sus publicaciones.

¿Ha sido sancionado(a) por publicaciones o mensajes digitales?		
Respuesta	**Declarantes**	**Porcentaje**
Multa administrativa (ej. Decreto Ley 370, Ley Comunicaciones, etc.)	**47**	**23,50%**
Me (o "le") prohibieron o advirtieron de no tener comunicación con ciertas personas	**116**	**58,00%**
Me (o le) realizaron una investigación formal	**77**	**38,50%**
Me (o le) iniciaron una acusación penal formal	**35**	**17,50%**
Me (o le) impusieron una medida cautelar formal o de facto (arbitraria, como la prohibición policial de salir de casa, de la población, no visitar a tales personas, o similar)	**61**	**30,50%**
Me (o le) amenazaron directa o veladamente con acciones punitivas	**93**	**46,50%**
No sufrí (o sufrió) nada de esto, nunca	**32**	**16,00%**

Es un hallazgo sorprendente que **en la muestra de 200 declarantes/denunciantes, sólo 32 de ellos no sufrieron sanciones o amenazas, penales y/o administrativas derivadas de sus comunicaciones digitales**.

Estas sanciones no operan como respuestas aisladas a conductas específicas, sino como parte de un patrón de criminalización progresiva de la expresión, en el que **la publicación de contenidos críticos, el intercambio de información o la participación en debates públicos es reinterpretada como infracción administrativa o delito.**

El carácter problemático de este patrón radica en el uso de figuras jurídicas amplias y ambiguas (como la *"difusión de información contraria al interés social"*, el *"uso indebido de redes de telecomunicaciones"* o la *"propaganda contra el orden constitucional"*) que permiten una aplicación discrecional, sin garantías de legalidad estricta, previsibilidad ni proporcionalidad.

Además, los datos muestran que estas sanciones suelen ir precedidas de **advertencias, amenazas o prohibiciones informales**, lo que refuerza su carácter disuasorio. Un **58%** de los declarantes/denunciantes (**116 de 200**) recibió advertencias o restricciones adicionales por mantener comunicaciones con determinadas personas, y un **46,50%** (**93 de 200**) fue amenazado directa o veladamente con consecuencias más graves si persistía en su actividad digital.

Este patrón evidencia que **el marco normativo cubano** no actúa como garantía de derechos, sino que **actúa como un instrumento de control político**, en el que **el ejercicio de la libertad de expresión se convierte en una conducta de alto riesgo jurídico**. En la práctica, el derecho se emplea como una extensión del aparato de vigilancia digital, reforzando la autocensura y consolidando un entorno de inhibición estructural del debate público.

PATRÓN 6: REPRESALIAS OFFLINE DERIVADAS DE LA EXPRESIÓN ONLINE

CITACIONES, INTERROGATORIOS Y DETENCIONES VINCULADAS A ACTIVIDAD DIGITAL

La vigilancia digital documentada no opera de forma aislada, sino que se articula con acciones represivas presenciales. Un **61%** de los declarantes/denunciantes afirmó haber sido **interrogado en oficinas de la policía** política, la PNR o el MININT, al igual que un **61%** también reportó **interrogatorios en su vivienda, lugar de trabajo o en la vía pública**. Estas acciones son consistentes con **la articulación entre vigilancia digital y medidas represivas presenciales**, incluidas sanciones administrativas y penales.

Asimismo, un **60%** fue **citado formalmente** por estas autoridades, y un **55%** indicó haber sido **detenido**.

Interrogados, citados, detenidos.

Respuesta[4]	Declarantes	Porcentaje
Yo (o sobre quien reporto) he/ha sido interrogado en mi casa, la vía pública o mi trabajo por la policía política, la PNR o el MININT	**47**	**61%**
Yo (o sobre quien reporto) he/ha sido citado por la policía política, la PNR o el MININT	**46**	**60%**
Yo (o sobre quien reporto) he/ha sido interrogado por la policía política, la PNR o el MININT en sus oficinas	**47**	**61%**
Yo (o sobre quien reporto) he/ha sido detenido por la policía política, la PNR o el MININT	**42**	**55%**

Estas acciones se acompañaron, en muchos casos, de **medidas coercitivas adicionales** y de la apertura o amenaza de **procedimientos administrativos o penales** vinculados al ejercicio de la libertad de expresión en el entorno digital. Tal como se documenta en el **Patrón 5**, el uso del marco normativo sancionador constituye un componente central de esta arquitectura represiva, actuando como refuerzo formal de las citaciones, interrogatorios y detenciones. Como hemos visto en el apartado anterior, el número de sancionados penales y administrativos en la muestra llama la atención por la cantidad de declarantes/denunciantes que han sufrido estas sanciones. En particular, **de los 200 declarantes/denunciantes, y debido a sus comunicaciones digitales**:

- A **116** de ellos (el **58%**) les **prohibieron o advirtieron** de no tener relación con ciertas personas.
- A **93** de ellos (el **46,50%**) les **amenazaron directa o veladamente** con acciones punitivas.
- A **77** de ellos (el **38,50%**) les **realizaron una investigación penal** formal.
- A **35** de ellos (el **17,50%**) les iniciaron una **acusación penal formal**.
- A **61** de ellos (el **30,50%**) les **impusieron una medida cautelar** formal o de facto.
- A **47** de ellos (el **23,50%**) les **impusieron una multa administrativa** por sus publicaciones.

Reiteramos que es un hallazgo sorprendente que en la muestra de 200 declarantes/denunciantes, sólo 32 de ellos no sufrieron sanciones o amenazas, penales y/o administrativas derivadas de sus comunicaciones digitales.

En conjunto, los datos analizados demuestran que la vigilancia digital en Cuba constituye un sistema articulado de observación, intrusión y coerción, que conecta el espacio digital con la represión presencial directa contra las personas vigiladas. Las prácticas documentadas superan ampliamente el umbral de incidentes aislados y permiten identificar patrones consistentes de violación del derecho a la privacidad, a la libertad de expresión y a la protección contra injerencias arbitrarias.

DESPOJO ECONÓMICO Y ABUSO MATERIAL DURANTE DETENCIONES: SUSTRACCIÓN DE SALDO Y BIENES

Las entrevistas cualitativas realizadas para este informe revelan una práctica reiterada y particularmente grave: la sustracción deliberada del saldo telefónico de los dispositivos móviles confiscados por agentes de la Seguridad del Estado o la Policía Nacional Revolucionaria durante detenciones arbitrarias. Diversas personas entrevistadas denunciaron que, tras la ocupación de sus teléfonos móviles, el saldo disponible fue consumido o eliminado sin justificación alguna, sin registro administrativo y sin posterior restitución.

Entre los casos documentados se encuentran los de L.A.P.G., L.R.K.B., M.C.E., M.A.H.L., N.D.M., T.A.S.D. y Y.D.H., quienes reportaron pérdidas que oscilan **entre 1.000 y más de 3.000 pesos en moneda nacional (la mitad del salario mensual cubano medio), extraídos directamente de sus líneas telefónicas mientras se encontraban bajo custodia o después de que sus dispositivos fueran retenidos por las autoridades**. En varios de estos casos, los teléfonos no fueron devueltos o fueron entregados posteriormente sin el saldo original.

De acuerdo con los testimonios recogidos, **esta práctica no constituye un hecho aislado, sino un patrón recurrente en el contexto de detenciones vinculadas a activismo, protestas o ejercicio de la libertad de expresión**. Las víctimas señalan que, además del decomiso de dispositivos, **los agentes aprovechan el control físico del teléfono para apropiarse del saldo disponible**, lo que constituye una forma adicional de castigo y despojo económico, además de un síntoma de corrupción institucional sistémica extrema.

[4] Esta pregunta se incluyó una vez ya había empezado la toma de datos, por lo que los primeros declarantes antes de este cambio no pudieron responderla. El margen de error sobre la muestra de los 200 declarantes, no obstante, es de un máximo de 8,8 puntos porcentuales sobre el valor indicado.

Este tipo de conducta reviste especial gravedad, ya que combina abuso de poder, apropiación indebida de bienes y represalia directa contra personas detenidas, muchas de ellas en situación de vulnerabilidad. Además, refuerza el carácter arbitrario de las detenciones y evidencia una **práctica de saqueo sistemática** e impulsada oficialmente dentro de los operativos policiales.

Más allá del perjuicio económico, significativo en un contexto de precariedad generalizada, estos hechos revelan un patrón de actuación que denota desprecio por la legalidad y ausencia total de controles internos, contribuyendo a un clima de impunidad y temor. **La sustracción de saldo telefónico se suma así a otras formas de violencia institucional documentadas en este informe, y constituye una manifestación adicional del uso de la coerción y el abuso material como herramientas de control político**.

COACCIÓN PARA PROPAGANDA Y CONTROL DEL DISCURSO

Además de castigar o inhibir la expresión crítica, las prácticas documentadas muestran un componente activo de **inducción del discurso**, mediante presiones para publicar contenidos favorables al gobierno o a entidades estatales. Este elemento confirma que el control no es únicamente punitivo: también busca modelar el espacio informativo y disputar la narrativa pública, utilizando la vigilancia y la amenaza como herramientas de direccionamiento comunicativo. Un **45%** de los declarantes/denunciantes reportó haber sido **coaccionada o instigada por las autoridades a publicar contenido favorable al gobierno o a empresas estatales**, lo que evidencia el uso de la vigilancia digital no solo con fines punitivos, sino también como **mecanismo de control del discurso público**.

PATRÓN 7: REPRESALIAS CONTRA FAMILIARES Y ENTORNO CERCANO

Este patrón se refiere a la extensión deliberada de la vigilancia digital y sus efectos represivos hacia el círculo familiar y social de la persona vigilada. Incluye amenazas, citaciones, detenciones, vigilancia física, sanciones laborales u otras medidas coercitivas aplicadas a familiares, como forma de castigo indirecto, presión y disuasión del ejercicio de la libertad de expresión en el entorno digital.

Los datos muestran que las represalias contra familiares constituyen un componente central del sistema de control documentado. Un **66,50%** de los declarantes/denunciantes (**133 de 200**) reportó que **algún familiar fue amenazado**, mientras que un **51,50%** (**103 de 200**) indicó que sus familiares fueron **citados**, y un **32,50%** (**65 de 200**) que fueron **detenidos**. Asimismo, un **50,50%** (**101 de 200**) señaló **vigilancia física contra familiares**, y un **22,50%** (**45 de 200**) reportó **pérdida de empleo** de algún familiar como consecuencia indirecta de la actividad digital de la persona vigilada.

¿Algún familiar de la víctima (usted o el tercero por el que rellena este formulario) ha sufrido represalias por su actividad digital en redes sociales, mensajes o Internet?		
Respuesta	**Declarantes**	**Porcentaje**
Detenciones	**65**	**32,50%**
Citaciones	**103**	**51,50%**
Amenazas	**133**	**66,50%**
Pérdida de empleo	**45**	**22,50%**
Problemas en el sistema educativo para alguno/s de sus familiares	**44**	**22,00%**
Vigilancia física	**101**	**50,50%**
Otra/s represalias/consecuencias	**36**	**18,00%**
No, ningún familiar ha sufrido represalias o consecuencias por mi actividad digital en redes sociales, mensajes o Internet	**24**	**12,00%**

La afectación recae principalmente sobre la familia directa, lo que refuerza la lectura de estas represalias como una estrategia de control social y emocional. **Un 74,50% de los declarantes/denunciantes (149 de 200) tienen familia directa afectada por amenazas, citaciones, detenciones, vigilancia o pérdida del empleo como consecuencia de publicaciones atribuibles sólo a los declarantes/denunciantes**, incluyendo parejas (**40,50%, 81 de 200**), hijos e hijas (**34,00%, 68 de 200**), madres o padres (**26,00%, 52 de 200**) y hermanos/as (**28,50%, 57 de 200**). Esto supone reprimir a los familiares inocentes de los declarantes/denunciantes para detener las publicaciones o comunicaciones de estos últimos.

Si incluimos otros tipos de allegados, **176 de los 200 declarantes/denunciantes (un 88% del total) han sufrido, por sus publicaciones, la afectación de sus familiares o allegados inocentes con amenazas, citaciones, detenciones, vigilancia o pérdida del empleo**. Indudablemente tiene un efecto devastador en la libertad de expresión de los declarantes, como también queda demostrado en este estudio, pero produce una repulsión incontenible comprobar cómo un llamado "estado" actúa así con sus ciudadanos y sus familias.

¿A qué tipo de familiar de la víctima (usted o el tercero por el que rellena este formulario) le ocurrieron estos hechos de la pregunta anterior?		
Respuesta	**Declarantes**	**Porcentaje**
A la familia directa	**149**	**74,50%**
A mi padre/madre	**52**	**26,00%**
A mi pareja	**81**	**40,50%**
A mi/s hijo/s	**68**	**34,00%**
A mi hermano/a	**59**	**29,50%**
A otro/s allegado/s	**65**	**32,50%**
A familiares y allegados	**176**	**88,00%**

Esta clase de actuación represiva del régimen cubano no destila patrón alguno de gobernanza. Por el contrario, presenta todos los patrones característicos de estructuras de naturaleza puramente criminal, como los presentes en las mafias y cárteles criminales.

En su conjunto, estos hallazgos evidencian que el control estatal no se dirige únicamente a la persona que se expresa o comunica en Internet, sino que se proyecta hacia su red afectiva como mecanismo de **intimidación ampliada**. Esta extensión tiene un impacto especialmente disuasorio: incrementa el costo percibido de expresarse, reduce la capacidad de organización social y fragmenta vínculos comunitarios, operando como una forma de coerción indirecta que multiplica el alcance de la vigilancia digital.

Este patrón reviste especial gravedad porque desplaza la sanción desde la conducta individual hacia el **entorno afectivo**, generando una lógica de *"responsabilidad por asociación"* que amplifica el miedo y erosiona el tejido social. La amenaza a familiares funciona como mecanismo de censura indirecta: incrementa el costo percibido de expresarse, reduce la denuncia y debilita redes de solidaridad. En términos de impacto, la vigilancia deja de ser un fenómeno individual y se convierte en una herramienta de **control social extensivo**.

PATRÓN 8: REPRESIÓN Y VIGILANCIA TRANSNACIONAL

En la muestra, la dimensión transnacional se manifiesta principalmente como coerción indirecta mediante familiares dentro de Cuba, más que como acciones directas en el país de residencia, por lo que este patrón se refiere a prácticas de vigilancia, intimidación o coerción vinculadas al ejercicio de la libertad de expresión desde fuera de Cuba (o a la proyección extraterritorial del control) que se materializan principalmente mediante presiones, amenazas y represalias dirigidas contra familiares y vínculos dentro del territorio nacional. Se trata de una modalidad de represión que trasciende fronteras y busca mantener el control sobre el discurso público de la diáspora, utilizando la vulnerabilidad de familiares en Cuba como palanca de presión.

En la muestra analizada, esta dimensión transnacional se manifiesta principalmente como **coerción indirecta**, dirigida a familiares y vínculos dentro de Cuba, más que como acciones directas sobre la persona en el país de residencia. Esta característica es consistente con una estrategia de control extraterritorial basada en el uso del territorio nacional como *"punto de presión"* sobre la diáspora.

133 de los 200 declarantes/denunciantes (el 66,50% del total) reportaron actos represivos contra ellos (dentro de Cuba) o sus familiares (si el declarante/denunciante estaba fuera de Cuba) por publicaciones realizadas por el familiar (fuera el declarante/denunciante o un familiar suyo) que se encontraba fuera de Cuba.

Sobre estos 133, los resultados muestran **indicadores abrumadores de esta dimensión de la represión transnacional**. Un **51,13%** de los declarantes/denunciantes (**68 de 133**) reportó **llamadas o mensajes amenazantes dirigidos a familiares dentro de Cuba**, un **29,32%** (**39 de 133**) recibió **advertencias directas**, y un **15,79%** (**21 de 133**) indicó haber sido informado explícitamente de que debía **cesar su actividad digital** para evitar consecuencias sobre su familia.

Hechos represivos que sufrió el familiar dentro de Cuba (fuera el declarante o un familiar del declarante) como consecuencia de lo que otro familiar/allegado publicaba fuera de Cuba en redes sociales o internet		
Respuesta	**Declarantes**	**Porcentaje**
Llamadas o mensajes amenazantes de las autoridades, chivas o agentes por las publicaciones del familiar fuera de Cuba	**68**	**51,13%**
Advertencias de las autoridades por las publicaciones del familiar fuera de Cuba	**39**	**29,32%**
Campañas de difamación desde cuentas oficialistas por las publicaciones del familiar fuera de Cuba	**3**	**2,26%**
Le dijeron que el familiar fuera de Cuba debía dejar de accionar o expresarse porque tendría consecuencias sobre usted o su familia dentro de Cuba	**21**	**15,79%**
Otro/s hechos represivos o amenazantes por las publicaciones del familiar fuera de Cuba	**2**	**1,50%**

Los otros 2 hechos represivos indicados por los declarantes son, en un caso, **citaciones por parte de la Seguridad del Estado** a sus familiares y, en el otro caso, **la expulsión forzada de la Universidad de una de las hijas de una declarante** por ser forzada a cambiar de carrera a una de grado inferior para la que no tenía vocación, tras las publicaciones de su progenitora, una médico en el exterior. La presión sobre los médicos cubanos en el exterior es terrorífica contra sus familiares en Cuba y, a pesar de que este colectivo apenas tiene representación en esta muestra, ha quedado reflejada esta represión sobre ellos, habitual sobre sus hijos en este colectivo.

Estos datos demuestran un patrón de control en el que la vigilancia no se limita al monitoreo de contenidos, sino que se traduce en **acciones de presión sobre familiares "inocentes" en Cuba (que no publican en contra del régimen) orientadas a silenciar o condicionar la expresión de quienes están fuera de Cuba**, manteniendo un efecto disuasorio sostenido mediante amenazas sobre terceros. En términos operativos, la represión transnacional funciona como una prolongación del sistema represivo interno: **el Estado evita el costo de actuar directamente sobre la persona fuera del territorio, pero traslada el impacto hacia su familia o entorno en Cuba, generando una forma de censura indirecta altamente eficaz**.

En conjunto, los hallazgos documentan que la vigilancia digital y sus efectos represivos operan más allá de las fronteras estatales, reforzando un ecosistema de control que afecta tanto a residentes en Cuba como a la diáspora, y que amplía el alcance de la coerción mediante la instrumentalización de vínculos familiares y afectivos.

PATRÓN 9: BRECHA DIGITAL ESTRUCTURAL Y MONOPOLIO ESTATAL COMO MECANISMOS DE CONTROL

Este patrón se refiere al uso estructural de las condiciones de acceso a Internet (económicas, técnicas y administrativas) como herramienta indirecta de control social, limitando el ejercicio efectivo de derechos digitales mediante restricciones de acceso, conectividad deficiente y dependencia de un proveedor estatal único.

Los datos del estudio evidencian que el acceso a Internet en Cuba no se configura como un servicio garantizado, sino como un recurso escaso, costoso y técnicamente inestable, cuya disponibilidad depende de decisiones estatales centralizadas. Un **80,00%** de los declarantes/denunciantes (**160 de 200**) considera que el acceso a Internet es **demasiado costoso** para un uso regular, mientras que un **69,00%** (**138 de 200**) reportó **velocidades insuficientes** para informarse o acceder a contenidos audiovisuales.

Adicionalmente, un **49,50%** (**99 de 200**) indicó que el acceso a Internet está disponible solo en horarios limitados, un **46,00%** (**92 de 200**) señaló problemas técnicos recurrentes del proveedor, y un **46,50%** (**93 de 200**) percibió desigualdades de acceso según la zona de residencia. Solo un **7%** de los declarantes/denunciantes (14 de los 200) afirmó no haber experimentado dificultades relevantes de conectividad.

¿Ha enfrentado dificultades sostenidas para acceder a Internet por motivos económicos, limitaciones técnicas o falta de disponibilidad?		
Respuesta	**Declarantes**	**Porcentaje**
Conexión demasiado cara para el uso habitual	**160**	**80,00%**
Velocidad insuficiente para acceder a noticias o videos	**138**	**69,00%**
Internet solo disponible en horarios limitados	**99**	**49,50%**
Problemas técnicos recurrentes del proveedor	**92**	**46,00%**
Acceso desigual comparado con otras zonas urbanas	**93**	**46,50%**
No, no he experimentado dificultad alguna para acceder a Internet	**14**	**7,00%**

Estas limitaciones no pueden interpretarse como fallas técnicas aisladas. Se inscriben en un contexto de **monopolio estatal absoluto de las telecomunicaciones**, ausencia de competencia y falta de mecanismos independientes de regulación o supervisión. Este modelo permite que el control de la infraestructura se convierta en un instrumento de regulación política del acceso a la información.

El impacto de esta brecha digital es directo sobre el ejercicio de derechos fundamentales. Un **88,50%** de los declarantes/denunciantes (**177 de 200**) considera que estas limitaciones afectan de forma muy significativa su capacidad de informarse o participar en debates públicos. Este dato confirma que el control estructural de la conectividad funciona como una forma indirecta, pero altamente eficaz, de censura.

La combinación de altos costos, baja calidad del servicio, restricciones técnicas y bloqueos selectivos crea un entorno en el que el acceso a la información depende de factores económicos y políticos, y no del ejercicio libre de derechos. En este sentido, **la brecha digital en Cuba no es un fenómeno accidental, sino un componente funcional del sistema de control, que refuerza la vigilancia digital y limita estructuralmente el pluralismo informativo.**

PATRÓN 10: AUTOCENSURA Y RETRAIMIENTO DIGITAL POR MIEDO

Las respuestas analizadas evidencian que las prácticas de vigilancia digital documentadas en los capítulos anteriores **sobre vigilancia digital directa, vigilancia física digitalizada y represalias asociadas** producen un efecto inhibidor **directo sobre el ejercicio de la libertad de expresión y de información en el entorno digital**. Este efecto se manifiesta en decisiones individuales de autocensura y retraimiento, adoptadas **por temor o prudencia**, y no como resultado de una libre elección.

CAMBIOS DELIBERADOS EN EL COMPORTAMIENTO DIGITAL

A pesar de que la muestra contiene un gran número de familias de presos políticos y activistas de derechos humanos, los más resilientes a la represión, una proporción significativa de los declarantes/denunciantes, **el 55,50%** (111 de 200) **reportó haber modificado su comportamiento digital** como respuesta a la vigilancia y a las represalias asociadas. En concreto, un **24%** de los declarantes/denunciantes (**48 de 200**) afirmó que **dejó de publicar contenidos políticos** por temor. De forma complementaria, un **21%** (**42 de 200**) indicó que **borró publicaciones antiguas** con el mismo propósito, lo que implica una revisión retrospectiva autocensurada de la propia expresión como mecanismo de autoprotección.

Asimismo, un **13,50%** (**27 de 200**) señaló haber **abandonado grupos de WhatsApp, Telegram u otras plataformas** por temor, mientras que un **21,50%** (**43 de 200**) afirmó haber **dejado de comunicarse con determinadas personas** para reducir su exposición. Estas decisiones evidencian una **reducción deliberada de la interacción social y política** en espacios digitales.

Otras estrategias de autocensura incluyen el **uso de seudónimos**, reportado por el **18,50%** de los declarantes/denunciantes (**37 de 200**), y el **cierre o cambio de cuentas** en redes sociales o servicios de mensajería, señalado por el **19,00%** (**38 de 200**). Estas prácticas reflejan intentos de **despersonalizar o fragmentar la identidad digital** como forma de evasión frente a la vigilancia.

¿Ha cambiado su comportamiento digital por temor a represalias?		
Respuesta	**Declarantes**	**Porcentaje**
Dejé de publicar sobre política por temor/prudencia	**48**	**24,00%**
Borré alguna o algunas publicaciones antiguas por temor/prudencia	**42**	**21,00%**
Salí de grupos de WhatsApp/Telegram/otros por temor/prudencia	**27**	**13,50%**
Dejé de comunicarme con ciertas personas por temor/prudencia	**43**	**21,50%**
Usé seudónimo por temor/prudencia	**37**	**18,50%**
Cerré o cambié cuentas por temor/prudencia	**38**	**19,00%**
No, nunca cambié mi comportamiento en redes, mensajería o internet por temor alguno	**89**	**44,50%**

En conjunto, estos datos muestran que una parte sustantiva de la muestra adopta **múltiples estrategias de autocensura**, que afectan tanto a la producción de contenido como a las relaciones y dinámicas de participación en línea.

Estas prácticas no constituyen respuestas aisladas, sino estrategias recurrentes de autoprotección frente a un entorno percibido como hostil y vigilado.

PERSISTENCIA DEL EFECTO INHIBIDOR

A pesar de que la muestra contiene un gran número de familias de presos políticos y activistas de derechos humanos, los más resilientes a la represión, una proporción significativa de los declarantes/denunciantes, **el 55,50%** (111 de 200) **reportó haber modificado su comportamiento digital** como respuesta a la vigilancia y a las represalias asociadas. Por tanto, aunque un **44,50%** de los declarantes/denunciantes (**89 de 200**) indicó que no ha cambiado su comportamiento digital **a pesar del temor**, este dato no desvirtúa la existencia del efecto inhibidor, sino que debe interpretarse a la luz del contexto de la muestra, y nos da un indicativo claro de que la autocensura entre los no activistas de derechos humanos es aún más generalizada.

La coexistencia de vigilancia activa, interferencias técnicas, citaciones, interrogatorios y vigilancia física genera un entorno en el que **la autocensura es estructural**.

El hecho de que una proporción significativa de personas mayoritariamente activistas no afines al régimen, aun así, modifique su comportamiento (incluyendo la supresión de contenido, la reducción de vínculos comunicativos y el ocultamiento de identidad) constata un **impacto real y medible en el ejercicio colectivo de la libertad de expresión**, incluso entre quienes deciden continuar expresándose.

TEMOR DIFERENCIADO SEGÚN EL MEDIO DE COMUNICACIÓN

Este retraimiento se ve reforzado por un **clima generalizado de temor**, que varía según el medio utilizado para abordar temas políticos.

Para medir el temor medio a publicar en diferentes medios, solicitamos a todos los declarantes que indicaran el nivel de temor, del 1 al 5, referido al uso de diferentes medios de comunicación y expresión digital. En el análisis de su respuesta, como en el apartado anterior, debemos tener en cuenta que la representatividad de activistas y familiares de presos políticos en la muestra es muy elevado, y que aquellos que cumplimentaron la declaración de denuncia, realizada por medio de la técnica de "bola de nieve", son precisamente del entorno de confianza de los primeros y, para declarar, han tenido que superar un cierto umbral de temor que no es habitual en la población cubana al comunicarse sobre temas de índole política o derechos humanos.

Aún con dicha consideración, tal y como se documentó anteriormente, los niveles promedio de miedo a denunciar o expresarse alcanzan valores elevados en **llamadas telefónicas** (**un promedio de temor del 3,37 sobre 5**), **redes sociales como Facebook** (**un promedio de temor del 3,31 sobre 5**) y **WhatsApp en grupos** (**un promedio de temor del 3,18 sobre 5**), mientras que se mantienen ligeramente inferiores —aunque aún significativos— en **videollamadas (un promedio de temor de 3,07 sobre 5)**, **Telegram** (**un promedio de temor del 2,80 sobre 5**), **WhatsApp uno a uno** (**media 2,80 sobre 5**) y **Signal** (**media 2,56 sobre 5**).

De los 200, **160 expresaron un alto temor en alguno o varios de los canales de comunicación habituales**, siendo el promedio de temor de los 200 declarantes de **3,01 sobre un máximo de 5**.

Temor o miedo para publicar y/o comunicarse en los diferentes medios	
Medio/canal	**Grado de temor promedio (del 1 al 5) entre los declarantes**
Llamadas telefónicas	**3,37**
Facebook/redes sociales	**3,31**
Whatsapp en grupos	**3,19**
Videollamadas	**3,07**
WhatsApp uno a uno	**2,8**
Telegram	**2,8**
Signal	**2,56**

Estas diferencias de temor entre los diferentes medios y canales no indican espacios seguros, sino **grados variables de percepción de riesgo**, que influyen en la selección del canal, el contenido compartido y la decisión de expresarse o guardar silencio. La variación en los niveles de temor, por tanto, se correlaciona con la percepción de visibilidad, trazabilidad y control estatal asociada a cada medio.

La autocensura y el retraimiento digital documentados en este informe son consistentes con **un efecto inhibidor (chilling effect) derivado de la vigilancia y las represalias**, incluso cuando no se materializan sanciones formales en todos los casos.

Los datos muestran que la vigilancia digital en Cuba **cumple una función disuasoria estructural**, orientada a reducir la circulación de información crítica y a fragmentar las redes de comunicación y solidaridad, afectando no solo a las personas directamente vigiladas, sino al ecosistema digital en su conjunto.

SÍNTESIS DE LOS PATRONES IDENTIFICADOS Y SU RELEVANCIA ESTRUCTURAL

El análisis desarrollado en este bloque permite afirmar, con base empírica suficiente, que la vigilancia digital en Cuba no constituye una suma de prácticas aisladas o reactivas, sino un **sistema estructurado, coherente y multidimensional de control estatal**, que articula mecanismos técnicos, jurídicos, policiales y sociales con un objetivo común: **regular, disuadir y sancionar el ejercicio de la libertad de expresión y la participación cívica en el entorno digital**.

Los diez patrones identificados revelan una arquitectura de vigilancia que opera de forma escalonada y complementaria. El monitoreo constante de redes sociales y comunicaciones privadas (Patrón 1), los bloqueos y cortes selectivos de conectividad (Patrón 2) y la interceptación de comunicaciones y acceso no autorizado a dispositivos (Patrón 3) configuran una **fase de observación y control digital permanente**. Esta fase se ve reforzada por mecanismos físicos y presenciales (vigilancia territorial, citaciones, interrogatorios y detenciones) que materializan en el plano cotidiano la información obtenida digitalmente (Patrones 4 y 6).

A su vez, el uso del aparato normativo como herramienta punitiva (Patrón 5) demuestra que la vigilancia no opera al margen del derecho, sino que se apoya en un entramado legal diseñado o aplicado de forma ambigua para legitimar la represión. Las sanciones administrativas, procesos penales y advertencias formales funcionan como instrumentos disciplinarios, reforzando el carácter disuasorio del sistema.

El alcance del control se amplía deliberadamente mediante represalias contra familiares (Patrón 7) y prácticas de represión transnacional (Patrón 8), lo que evidencia que la vigilancia digital no se agota en la persona que emite el contenido, sino que se proyecta hacia su entorno afectivo y social, generando un efecto multiplicador del temor. Paralelamente, el control estructural del acceso a Internet (mediante el monopolio estatal, los altos costos y la degradación del servicio) opera como una forma silenciosa pero eficaz de censura previa (Patrón 9).

Como resultado de este entramado, el último patrón identificado, la autocensura y el retraimiento digital, (Patrón 10) no aparece como un fenómeno espontáneo, sino como la **consecuencia lógica y previsible de un ecosistema de vigilancia integral**. El miedo, la reducción del discurso público, la fragmentación de las redes sociales y el abandono de espacios digitales de participación constituyen indicadores claros del impacto real y sostenido de estas prácticas sobre el ejercicio de derechos fundamentales.

En su conjunto, los hallazgos de este bloque permiten concluir que la vigilancia digital en Cuba funciona como una **política pública de control social**, caracterizada por su sistematicidad, su alcance transversal y su capacidad para articular mecanismos tecnológicos, legales y coercitivos. Lejos de responder a criterios

excepcionales de seguridad, las prácticas documentadas configuran un modelo de gobernanza digital orientado a restringir el pluralismo, neutralizar la disidencia y moldear el comportamiento ciudadano mediante el miedo.

DEL ANÁLISIS EMPÍRICO AL ANÁLISIS JURÍDICO

Los patrones descritos en este bloque no pueden entenderse únicamente como fenómenos sociales o tecnológicos. Su alcance, recurrencia y coherencia interna obligan a examinarlos a la luz del **derecho internacional de los derechos humanos**, que establece límites claros al uso de tecnologías de vigilancia, a la restricción de la libertad de expresión y al ejercicio del poder punitivo del Estado.

El bloque siguiente aborda precisamente esta dimensión normativa. A partir de los hechos documentados, se realizará un **análisis transversal y jurídico** que permitirá:

- Evaluar la compatibilidad de los patrones identificados con los estándares internacionales aplicables en materia de privacidad, libertad de expresión, debido proceso y protección contra injerencias arbitrarias.
- Analizar el incumplimiento de obligaciones internacionales asumidas por el Estado cubano, a la luz de tratados, resoluciones y jurisprudencia relevante.
- Identificar cómo la vigilancia digital documentada configura violaciones estructurales y no meros excesos individuales.

De este modo, el **Bloque IV** no solo contextualiza jurídicamente los hallazgos, sino que permite establecer con claridad el carácter ilícito, desproporcionado y sistemático del modelo de vigilancia digital descrito en este informe.

BLOQUE IV – ANÁLISIS TRANSVERSAL Y JURÍDICO

El presente bloque tiene por objeto realizar un análisis jurídico integral de los patrones de vigilancia digital identificados en los apartados anteriores, a la luz del derecho internacional de los derechos humanos y de los estándares desarrollados por los sistemas universal y regional de protección.

A diferencia del bloque precedente —centrado en la exposición empírica de los hechos y en la sistematización de las prácticas documentadas—, este apartado aborda el **significado jurídico de dichos hallazgos**, evaluando en qué medida las prácticas descritas constituyen violaciones a obligaciones internacionales asumidas por el Estado cubano y cómo se configuran como un sistema estructural de restricción de derechos fundamentales en el entorno digital.

El análisis se construye a partir de un enfoque **transversal**, que no examina los hechos de manera aislada, sino como parte de un **entramado coherente de control, vigilancia y represión**, en el que interactúan herramientas tecnológicas, normas jurídicas, prácticas administrativas y acciones policiales. Este enfoque permite identificar no solo vulneraciones puntuales, sino **patrones reiterados de actuación estatal**, dotados de coherencia interna y efectos acumulativos sobre el ejercicio de los derechos humanos.

Para ello, se utiliza como herramienta principal una **matriz de doble entrada**, que cruza:

- Los **diez patrones de vigilancia digital identificados** en el Bloque III;
- Los **derechos humanos afectados**, conforme al derecho internacional; y
- Los **estándares normativos aplicables**, derivados de tratados, observaciones generales, resoluciones y doctrina especializada de los sistemas internacional y regional de derechos humanos.

Esta metodología permite visualizar de forma sistemática cómo cada práctica documentada (desde el Ciberpatrullaje y la interceptación de comunicaciones, hasta las represalias contra familiares o la autocensura inducida) se vincula con obligaciones jurídicas concretas del Estado, y cómo su aplicación reiterada configura un **modelo de control incompatible con los principios de legalidad, necesidad, proporcionalidad y finalidad legítima** exigidos por el derecho internacional.

El análisis se fundamenta, entre otros instrumentos, en:

- La **Declaración Universal de Derechos Humanos** y el **Pacto Internacional de Derechos Civiles y Políticos (PIDCP)**;

- Las **Observaciones Generales del Comité de Derechos Humanos**, en particular las relativas a libertad de expresión, privacidad y reunión pacífica;
- Las **resoluciones del Consejo de Derechos Humanos de la ONU** sobre derechos humanos en Internet y vigilancia digital;
- Los informes del **Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión**;
- Los estándares desarrollados por la **Comisión Interamericana de Derechos Humanos (CIDH)** y su Relatoría Especial para la Libertad de Expresión; entre ellos la **Declaración Americana de los Derechos y Deberes del Hombre (DADH)**, utilizada por la CIDH para el seguimiento de Cuba en virtud de su mandato y de la Carta de la OEA.
- Y otros instrumentos relevantes en materia de privacidad, protección de datos, libertad de expresión y garantías frente a la vigilancia estatal.

Nota sobre el uso del PIDCP en este informe: Cuba firmó el **Pacto Internacional de Derechos Civiles y Políticos (PIDCP)** en 2008, pero no lo ha ratificado. No obstante, el PIDCP se cita en este informe **como estándar universal y guía interpretativa** de referencia para evaluar restricciones y prácticas estatales que afectan derechos como la privacidad, la libertad de expresión, reunión y asociación en el entorno digital. Su análisis se **complementa** con la **Declaración Universal de Derechos Humanos (DUDH)** y, en el plano regional, con los **instrumentos interamericanos aplicables** —en particular, la **Declaración Americana de los Derechos y Deberes del Hombre**, utilizada por la CIDH en el seguimiento de la situación de Cuba—, además de otros estándares internacionales relevantes.

Sistema interamericano (nota de aplicabilidad): en el ámbito regional, este informe emplea como instrumento de referencia primaria la **Declaración Americana de los Derechos y Deberes del Hombre (DADH)**, utilizada por la **CIDH** para el seguimiento de Cuba en virtud de su mandato y de la Carta de la OEA. La **Convención Americana sobre Derechos Humanos (CADH)** se cita adicionalmente como **estándar regional consolidado** y parámetro interpretativo comparado, sin perjuicio de la aplicabilidad principal de la DADH en el caso cubano.[5]

Con toda esta perspectiva, el Bloque IV no se limita a describir infracciones formales, sino que demuestra cómo la vigilancia digital en Cuba opera como un **sistema estructural de control social**, que afecta de manera acumulativa a:

- La libertad de expresión;
- El derecho a la privacidad;
- La libertad de asociación y reunión;
- El derecho a la participación política;
- La vida privada y familiar; y
- El acceso a la información.

Asimismo, el análisis pone de relieve que muchas de las prácticas documentadas no pueden justificarse bajo los criterios de legalidad, necesidad o proporcionalidad exigidos por el derecho internacional, y que, por el contrario, responden a una lógica de **prevención del disenso y disuasión del ejercicio de derechos**, incompatible con los estándares democráticos mínimos.

En las secciones siguientes se presenta, en primer lugar, la **matriz de análisis jurídico**, que sintetiza de manera sistemática la relación entre patrones de vigilancia, derechos vulnerados y normas internacionales aplicables. Posteriormente, se desarrolla un **análisis jurídico sustantivo por patrón**, en el que se examina con mayor detalle el alcance de las violaciones identificadas y su relevancia a la luz del derecho internacional de los derechos humanos.

MATRIZ DE PATRONES DE VIGILANCIA DIGITAL Y DERECHOS AFECTADOS

Con el fin de sistematizar los hallazgos empíricos expuestos en el Bloque III y evaluar su compatibilidad con el derecho internacional de los derechos humanos, el presente informe de denuncia incorpora una **matriz de**

[5] https://www.oas.org/en/iachr/reports/pdfs/Cuba2020-en.pdf

análisis transversal que permite vincular de manera estructurada los patrones de vigilancia digital documentados con los derechos fundamentales afectados y los estándares normativos aplicables.

Esta matriz cumple una doble función. Por un lado, organiza de forma sintética los **diez patrones de vigilancia identificados**, facilitando su lectura comparada y evidenciando la recurrencia de determinadas prácticas. Por otro, permite establecer con claridad la **relación directa entre los hechos documentados y las obligaciones internacionales del Estado**, conforme a los tratados, observaciones generales y resoluciones adoptadas en el marco del sistema universal y del sistema interamericano de derechos humanos.

El enfoque adoptado parte del principio de que las vulneraciones analizadas no constituyen incidentes aislados, sino manifestaciones de un **sistema estructural de control digital**, en el que convergen mecanismos tecnológicos, normas jurídicas ambiguas, prácticas administrativas discrecionales y acciones coercitivas directas. La matriz permite así visualizar cómo cada patrón afecta simultáneamente múltiples derechos —como la libertad de expresión, la privacidad, la libertad personal, la participación política o la vida familiar— y cómo su aplicación reiterada configura un entorno incompatible con los estándares internacionales de legalidad, necesidad, proporcionalidad y finalidad legítima.

A partir de esta herramienta, el informe de denuncia desarrolla posteriormente un análisis jurídico detallado por patrón, examinando el alcance de las violaciones identificadas y su contradicción con el marco normativo internacional vigente, con el objetivo de aportar una base sólida para la incidencia internacional, la rendición de cuentas y la adopción de medidas de protección adecuadas.

Matriz de patrones de vigilancia digital, derechos afectados y hallazgos empíricos relevantes

Patrón	Descripción	Derechos afectados	Hallazgos relevantes del informe de denuncia	Interpretación del patrón y vínculo con derechos humanos
1: Ciberpatrullaje y monitoreo sistemático de redes	Monitoreo de perfiles, publicaciones y grupos; uso de capturas como "prueba"; hostigamiento en línea.	Libertad de expresión (art. 19 PIDCP / art. 13 CADH) / art. IV DADH.[6] Derecho a la privacidad (art. 17 PIDCP / art. 11 CADH / art. V DADH).[7] Derecho a no ser objeto de injerencias arbitrarias en la vida privada, comunicaciones y correspondencia.	88% reportó que autoridades mencionaron o reprocharon sus publicaciones. 57,50% afirmó que se usaron capturas de sus redes. 47,00% recibió comentarios explícitos de que era vigilado en redes. 42,50% reportó mención de mensajes privados.	El Ciberpatrullaje constituye una injerencia en la vida privada y en las comunicaciones (art. 17 PIDCP / art. 11 CADH) y, cuando se emplea como insumo para advertencias, citaciones, intimidación o sanción, opera como una forma de censura indirecta sobre la libertad de expresión (art. 19 PIDCP / art. 13 CADH / art. IV DADH). Derecho a la privacidad y vida privada/familiar (art. 17 PIDCP / art. 11 CADH / art. V DADH). Inviolabilidad de correspondencia/comunicaciones (art. X DADH). Al realizarse sin una base legal clara, sin control judicial independiente y con rasgos masivos o no individualizados, la práctica no supera los estándares de legalidad, necesidad y proporcionalidad exigidos por el derecho internacional y genera un efecto inhibidor estructural que desalienta el debate público y la

[6] Abreviaturas: PIDCP = Pacto Internacional de Derechos Civiles y Políticos; DADH = Declaración Americana de los Derechos y Deberes del Hombre; CADH = Convención Americana sobre Derechos Humanos.
[7] Se cita la CADH como "estándar regional de referencia"

				participación cívica en entornos digitales.[8]
2: Bloqueos, cortes de internet y degradación selectiva de la conectividad	Apagones, cortes selectivos, bloqueo de redes y VPN.	Libertad de expresión (art. 19 PIDCP / art. 13 CADH / art. IV DADH). Derecho de reunión pacífica (art. 21 PIDCP / art. XXI DADH). Libertad de asociación (art. 22 PIDCP / art. XXII DADH). Derecho a la participación política (art. 25 PIDCP / art. XX DADH).	52% sufrió cortes selectivos de datos. 49% fallos durante protestas o eventos políticos. 47% reducción deliberada de velocidad (throttling). 44,50% bloqueo de redes sociales. 22,50% bloqueo o imposibilidad de usar VPN	La interrupción deliberada del acceso a Internet constituye una forma de censura técnica que restringe el ejercicio colectivo de derechos fundamentales y opera como un mecanismo de control social, especialmente durante contextos de movilización o expresión crítica.
3: Interceptación de comunicaciones, spyware y acceso no autorizado a cuentas	Lectura de mensajes, accesos no autorizados, vigilancia masiva.	Derecho a la privacidad y a la inviolabilidad de las comunicaciones (art. 17 PIDCP / art. 11 CADH). Derecho a la privacidad y vida privada/familiar (art. V DADH) e inviolabilidad de correspondencia/comunicaciones (art. X DADH), además de garantías judiciales y debido proceso (art. 14 PIDCP, arts. XVIII y XXVI DADH) cuando la información obtenida se usa como "prueba" sin control independiente. Libertad de expresión (art. 19 PIDCP), por su efecto inhibidor.	49,50% detectó accesos desde ubicaciones desconocidas. 46,50% cambios de contraseña no realizados por la persona. 37,00% mensajes enviados desde su cuenta sin permiso. 37,50% autoridades citaron mensajes privados.	La vigilancia de comunicaciones privadas y el acceso no autorizado a dispositivos constituyen una forma de injerencia grave y arbitraria, incompatible con los estándares internacionales que protegen la confidencialidad de las comunicaciones y la vida privada.[9]
4: Cámaras, vigilancia física digitalizada y control del espacio público	Cámaras, seguimientos, patrullaje tras actividad digital.	Derecho a la privacidad (art. 17 PIDCP / art. V DADH), e inviolabilidad del domicilio (art. IX DADH). Libertad de circulación y movimiento (art. 12 PIDCP / art. VIII DADH). Libertad de reunión pacífica (art. 21 PIDCP / art. XXI DADH).	84,50% percibió vigilancia física tras actividad digital. 68,50% presencia de agentes en la calle. 53,50%	La traslación del control digital al espacio físico revela un modelo híbrido de vigilancia que vincula la actividad en línea con control presencial, generando un entorno de intimidación permanente contrario a los estándares democráticos.

[8] Este estándar ha sido reafirmado en el plano universal por la Asamblea General de la ONU para el contexto digital, al advertir sobre el riesgo de injerencias arbitrarias o ilegales en la privacidad mediante vigilancia e interceptación de comunicaciones." (AGNU, Res. 73/179, "The right to privacy in the digital age" (2018), A/RES/73/179).

[9] En la misma línea, la Asamblea General de la ONU ha reiterado —como estándar universal— que la privacidad debe ser protegida también 'en la era digital' y que las injerencias mediante vigilancia e interceptación solo son compatibles con el derecho internacional bajo criterios estrictos de legalidad, necesidad y proporcionalidad, con salvaguardas efectivas." (AGNU, Res. 73/179, "The right to privacy in the digital age" (2018), A/RES/73/179).

		Libertad de expresión (art. 19 PIDCP).	seguimiento en motos o autos. 49,50% patrullas frente a su vivienda. 13,50% cámaras cerca del domicilio.	
5: Uso de normas jurídicas y sanciones administrativas para castigar la expresión digital	Multas, procesos penales, uso de normas administrativas.	Libertad de expresión (art. 19 PIDCP / art. 13 CADH / art. IV DADH). Principio de legalidad y previsibilidad (art. 15 PIDCP). garantías de legalidad/debido proceso y recurso (art. 14 PIDCP / arts. XVIII y XXVI DADH).	23,50% recibió multas (incl. Decreto 370). 38,50% fue objeto de investigaciones. 17,50% enfrentó procesos penales.	El uso de normas amplias y ambiguas para sancionar la expresión digital demuestra una instrumentalización del derecho como mecanismo de control político, incompatible con el principio de legalidad y con la protección internacional de la libertad de expresión.
6: Represalias OFFLINE derivadas de la expresión ONLINE	Detenciones, citaciones, amenazas, despidos.	Libertad de expresión (art. 19 PIDCP / art. IV DADH). Libertad personal (art. 9 PIDCP / art. XXV DADH). Garantías judiciales y debido proceso (art. 14 PIDCP / art. XXVI DADH). Derechos económicos y sociales (trabajo, educación).	61,04% interrogado. 58,44% detenido. 60,50% recibió advertencias. 46,50% amenazas directas.	Este patrón evidencia la conversión de la vigilancia digital en represión física directa, materializando el control estatal mediante detenciones, amenazas y sanciones que exceden cualquier finalidad legítima.
7: Represalias contra familiares y entorno cercano	Presión, amenazas y sanciones indirectas.	Derecho a la vida privada y familiar (art. 17 PIDCP / art. 11 CADH / art. V DADH) y, cuando medie vigilancia/hostigamiento domiciliario, inviolabilidad del hogar (art. IX DADH). Libertad de expresión y asociación (art. 19 y 22 PIDCP). Protección contra represalias indirectas.	66,50% reportó amenazas a familiares. 51,50% citaciones a familiares. 32,50% detenciones de familiares. 22,50% pérdida de empleo de familiares.	La extensión de las represalias a familiares constituye una forma de castigo colectivo e intimidación indirecta, orientada a disuadir el ejercicio de derechos mediante la instrumentalización del entorno afectivo.
8: Represión y vigilancia transnacional	Presión a personas fuera del país mediante la represión a familiares dentro de Cuba (sobre 133 de 200)	Libertad de expresión (art. 19 PIDCP / art. IV DADH). Derecho a la vida privada y familiar (art. 17 PIDCP / art. V DADH). Libertad de circulación y movimiento (art. 12 PIDCP / art. VIII DADH).	51,13% recibió amenazas dirigidas a familiares en Cuba. 29,32% advertencias directas desde el exterior. 15,79% condicionado a cesar actividad digital.	La proyección extraterritorial de la vigilancia mediante amenazas a familiares demuestra que el control estatal trasciende las fronteras físicas, configurando una forma de represión transnacional contraria al derecho internacional.
9: Brecha digital estructural y monopolio estatal como mecanismos de control	Monopolio estatal, precios altos, acceso desigual.	Principio de igualdad y no discriminación ante la Ley (art. 26 PIDCP / art. II DADH). Libertad de expresión/difusión por cualquier medio (art. IV DADH). Derecho de acceso a la información (art. 19 PIDCP).	80% considera Internet demasiado caro. 69% velocidad insuficiente. 49,50% acceso	El control estatal de la infraestructura digital convierte la conectividad en un instrumento de regulación política, afectando de forma estructural el acceso a la información y el ejercicio efectivo de derechos.

		Derechos económicos y sociales (educación, trabajo, participación).	limitado por horarios.	
10: Autocensura y retraimiento digital por miedo	Silenciamiento por miedo o autoprotección.	Libertad de expresión (art. 19 PIDCP / art. IV DADH). Libertad de reunión y asociación (arts. 21 y 22 PIDCP / art. XXI DADH). Derecho a la participación política (art. 25 PIDCP / art. XX DADH).	24% dejó de publicar. 21% borró contenidos. 19% cerró o cambió cuentas. Altos niveles de miedo en llamadas (3,37/5) y redes sociales (3,31/5).	La autocensura observada constituye el efecto acumulado de la vigilancia sistemática y las represalias, configurando un "efecto inhibidor" que restringe de facto el ejercicio de la libertad de expresión en ausencia de censura formal directa.

LECTURA ANALÍTICA DE LA MATRIZ

PATRÓN 1: CIBERPATRULLAJE Y MONITOREO SISTEMÁTICO DE REDES

La información analizada evidencia un patrón sostenido de vigilancia activa sobre la expresión digital, mediante el monitoreo sistemático de publicaciones, interacciones y mensajes en redes sociales y plataformas de mensajería. Este patrón revela una práctica estatal orientada a observar, registrar y utilizar el discurso digital como insumo para acciones de intimidación, advertencia o sanción, afectando directamente la libertad de expresión y la expectativa legítima de privacidad en entornos digitales.

La reiteración de menciones a publicaciones durante interrogatorios, el uso de capturas de pantalla y la referencia expresa a mensajes privados demuestran que el Ciberpatrullaje no es incidental, sino organizado, sistemático y dirigido. La vigilancia no se limita a contenidos públicos, sino que se extiende a espacios semiprivados y privados, generando un entorno de supervisión constante.

CONCLUSIÓN JURÍDICA DEL PATRÓN

Este patrón configura una forma de censura indirecta incompatible con el **artículo 19 del PIDCP** y con la Observación General Nº 34 del Comité de Derechos Humanos. El monitoreo sistemático del discurso digital, sin base legal clara ni control judicial, vulnera el principio de legalidad y produce un efecto inhibidor estructural sobre la libertad de expresión, en términos también del **artículo IV de la DADH**; y, cuando se extiende a mensajes o entornos no plenamente públicos, compromete además la protección de la **vida privada y familiar (art. V)** y la **inviolabilidad de la correspondencia (art. X)** de la DADH.

PATRÓN 2: BLOQUEOS, CORTES DE INTERNET Y DEGRADACIÓN SELECTIVA DE LA CONECTIVIDAD

Los datos confirman que las interrupciones del servicio, los bloqueos selectivos y la degradación deliberada de la conectividad constituyen un mecanismo recurrente de control social. Estas prácticas se activan de forma coincidente con protestas, eventos políticos o difusión de contenido crítico, operando como una forma de censura indirecta y control preventivo de la información.

La naturaleza selectiva de los cortes, su coincidencia temporal con momentos de movilización social y la restricción del uso de VPN evidencian que no se trata de fallas técnicas, sino de medidas deliberadas orientadas a limitar la circulación de información y la capacidad de organización social.

CONCLUSIÓN JURÍDICA DEL PATRÓN

Los bloqueos y cortes de Internet vulneran directamente los **artículos 19 y 21 del PIDCP** y contravienen las resoluciones del Consejo de Derechos Humanos que prohíben expresamente la interrupción del acceso a Internet como medida de control. Su carácter generalizado y preventivo los hace incompatibles con los

principios de necesidad y proporcionalidad, y opera asimismo como restricción ilegítima del **derecho a la libertad de expresión y difusión por cualquier medio (art. IV DADH)**, con impacto directo sobre la **reunión pacífica (art. XXI DADH)** y sobre la **participación en el gobierno y en los asuntos públicos (art. XX DADH)** cuando se emplea para neutralizar protestas, organización social o deliberación pública.

PATRÓN 3: INTERCEPTACIÓN DE COMUNICACIONES, SPYWARE Y ACCESO NO AUTORIZADO A CUENTAS

La evidencia recogida muestra indicios consistentes de interceptación de comunicaciones privadas, acceso no autorizado a cuentas y dispositivos, y uso de información privada durante interrogatorios. La exigencia directa de contraseñas, la revisión de contenidos personales y la detección de accesos desde ubicaciones desconocidas revelan prácticas de intrusión sistemática.

Este patrón sugiere la existencia de mecanismos técnicos de vigilancia digital que operan sin control judicial, sin notificación y sin garantías procesales. La reiteración de estos hechos descarta que se trate de incidentes aislados.

CONCLUSIÓN JURÍDICA DEL PATRÓN

Estas prácticas constituyen una violación directa del **artículo 17 del PIDCP** y de los principios internacionales sobre vigilancia de las comunicaciones. La ausencia de legalidad, control judicial y proporcionalidad permite calificar este patrón como una forma de vigilancia arbitraria e ilegítima, incompatible con el derecho a la privacidad y con el debido proceso; en clave interamericana, ello se traduce también en afectaciones a la **vida privada y familiar (art. V DADH)** y a la **inviolabilidad y circulación/transmisión de la correspondencia (art. X DADH)**, agravadas por la falta de **garantías contra detenciones arbitrarias (art. XXV DADH)** y de un **proceso regular (art. XXVI DADH)** cuando la intrusión se usa como insumo coercitivo o sancionatorio.

PATRÓN 4: VIGILANCIA FÍSICA DIGITALIZADA Y CONTROL DEL ESPACIO PÚBLICO

La información analizada demuestra que la vigilancia digital se traduce de forma directa en vigilancia física: seguimientos, presencia policial reiterada, visitas de advertencia y control territorial posterior a la actividad en línea. Este patrón evidencia una articulación operativa entre el monitoreo digital y la coerción presencial.

La vigilancia física no aparece como un fenómeno independiente, sino como una extensión del control digital, orientada a reforzar el efecto intimidatorio y a hacer visible el poder de vigilancia estatal en la vida cotidiana.

CONCLUSIÓN JURÍDICA DEL PATRÓN

La vigilancia física vinculada a la actividad digital vulnera el derecho a la privacidad, la libertad de circulación y la libertad de expresión. Su carácter reiterado y selectivo configura una restricción indirecta e ilegítima de derechos fundamentales, incompatible con los estándares internacionales sobre vigilancia y reunión pacífica; y, en el sistema interamericano, compromete igualmente la **protección de la vida privada (art. V DADH)**, la **libertad de residencia y tránsito (art. VIII DADH)** y el núcleo de la **libertad de investigación, opinión, expresión y difusión (art. IV DADH)**, con efectos disuasorios sobre la **reunión pacífica (art. XXI DADH)** cuando la vigilancia territorial se despliega para desmovilizar o intimidar.

PATRÓN 5: USO DE NORMAS JURÍDICAS Y SANCIONES ADMINISTRATIVAS PARA CASTIGAR LA EXPRESIÓN DIGITAL

El análisis demuestra que el marco normativo cubano es utilizado como instrumento de represión del discurso digital. Multas, investigaciones y procesos penales se activan en respuesta a publicaciones, mensajes o contenidos críticos, mediante normas vagas y de aplicación discrecional.

El uso del **Decreto-Ley 370** y otras figuras administrativas y penales convierte la legalidad en una herramienta de control, no de protección de derechos, generando inseguridad jurídica y autocensura.

CONCLUSIÓN JURÍDICA DEL PATRÓN

La aplicación de normas ambiguas para sancionar expresión digital vulnera los principios de legalidad, previsibilidad y proporcionalidad, contraviniendo el **artículo 19 del PIDCP**. Este patrón constituye una forma de censura legalizada incompatible con un sistema democrático; y, desde la perspectiva interamericana, entra igualmente en tensión con la **libertad de investigación, opinión, expresión y difusión por cualquier medio (art. IV DADH)**, al tiempo que la discrecionalidad sancionatoria sin garantías suficientes erosiona el **derecho a**

proceso regular (art. XXVI DADH) cuando se instrumentaliza el derecho interno para castigar discurso protegido.

PATRÓN 6: REPRESALIAS OFFLINE DERIVADAS DE LA EXPRESIÓN ONLINE

Las citaciones, interrogatorios, detenciones y amenazas documentadas muestran que la vigilancia digital se materializa en represalias físicas directas. La expresión en línea se convierte en un detonante de consecuencias personales, laborales y sociales.

Esta conexión directa entre expresión digital y castigo presencial evidencia que, en los casos documentados, la vigilancia opera con un efecto disciplinador, más allá de una mera finalidad informativa.

CONCLUSIÓN JURÍDICA DEL PATRÓN

Las represalias presenciales constituyen violaciones autónomas de los derechos a la libertad personal, a la integridad y a la libertad de expresión. Además, refuerzan el efecto inhibidor del sistema de vigilancia, contraviniendo los estándares internacionales sobre protección frente a represalias; y, conforme a la DADH, comprometen el **derecho a la vida, la libertad y la seguridad e integridad de la persona (art. I)**, la **protección contra la detención arbitraria (art. XXV)**, el **derecho a proceso regular (art. XXVI)** y la **libertad de investigación, opinión, expresión y difusión (art. IV)**, especialmente cuando las represalias se activan como castigo por discurso o interacción digital.

PATRÓN 7: REPRESALIAS CONTRA FAMILIARES Y ENTORNO CERCANO

El informe de denuncia evidencia una extensión deliberada de la represión hacia familiares de personas vigiladas, mediante amenazas, citaciones, detenciones o sanciones laborales. Este patrón amplía el impacto de la vigilancia más allá del individuo y transforma el entorno familiar en un espacio de coerción.

La utilización de familiares como mecanismo de presión refuerza el control social y genera un efecto intimidatorio de alto impacto emocional.

CONCLUSIÓN JURÍDICA DEL PATRÓN

Las represalias contra familiares violan el derecho a la vida privada y familiar y constituyen una forma agravada de coerción indirecta, prohibida por el derecho internacional. Este patrón refuerza el carácter estructural del sistema represivo; y, en el plano interamericano, se proyecta de forma directa sobre la **protección frente a ataques abusivos a la honra, reputación y vida privada y familiar (art. V DADH)**, al instrumentalizar vínculos familiares como mecanismo de intimidación y silenciamiento.

PATRÓN 8: REPRESIÓN Y VIGILANCIA TRANSNACIONAL

La evidencia recopilada sugiere que la vigilancia y/o sus efectos represivos se proyectan más allá del territorio nacional mediante amenazas dirigidas a familiares en Cuba, con el fin de silenciar a personas que se expresan desde el exterior. Esta práctica amplía el alcance del control estatal y afecta a la diáspora.

CONCLUSIÓN JURÍDICA DEL PATRÓN

La represión transnacional constituye una violación del derecho a la libertad de expresión sin fronteras y del principio de no injerencia arbitraria. Su uso confirma la existencia de un sistema de control que trasciende el ámbito territorial del Estado; y, en términos interamericanos, afecta asimismo la **libertad de investigación, opinión, expresión y difusión por cualquier medio (art. IV DADH)**, y puede implicar injerencias sobre la **vida privada y familiar (art. V DADH)** y sobre la **correspondencia (art. X DADH)** cuando las amenazas o presiones se sostienen mediante intrusión o control comunicacional sobre el entorno familiar en Cuba.

PATRÓN 9: BRECHA DIGITAL ESTRUCTURAL Y MONOPOLIO ESTATAL COMO MECANISMOS DE CONTROL

El control estatal de la infraestructura, los altos costos y la baja calidad del servicio configuran una brecha digital estructural que limita el acceso a la información y refuerza la desigualdad. Estas condiciones no son neutrales, sino funcionales al control del flujo informativo.

CONCLUSIÓN JURÍDICA DEL PATRÓN

La restricción estructural del acceso a Internet vulnera el derecho a la información y a la participación, y contradice las obligaciones estatales de garantizar un acceso equitativo a las tecnologías de la información; en

el marco interamericano, esta afectación incide de manera directa en la **libertad de investigación, opinión, expresión y difusión (art. IV DADH)**, en el **derecho de participación en el gobierno (art. XX DADH)** y en el principio de **igualdad ante la ley (art. II DADH)** cuando el diseño monopólico y restrictivo opera como barrera estructural para el debate público, el acceso a información plural y la participación cívica efectiva.

PATRÓN 10: AUTOCENSURA Y RETRAIMIENTO DIGITAL POR MIEDO

El efecto acumulado de todos los patrones anteriores genera un clima de miedo que conduce a la autocensura. La reducción de la participación digital, el abandono de espacios de expresión y el ocultamiento de identidad son respuestas racionales frente a un entorno hostil.

CONCLUSIÓN JURÍDICA DEL PATRÓN

El efecto inhibidor documentado constituye una violación indirecta pero real de la libertad de expresión. Conforme a los estándares internacionales, el simple hecho de generar miedo suficiente para silenciar el discurso público constituye una restricción ilegítima de derechos fundamentales; y, en clave interamericana, afecta el contenido esencial de la **libertad de investigación, opinión, expresión y difusión (art. IV DADH)**, con repercusiones sobre la **participación en el gobierno (art. XX DADH)**, así como sobre la **reunión (art. XXI DADH)** y la **asociación (art. XXII DADH)** cuando el retraimiento digital reduce la organización cívica y el espacio deliberativo.

ANÁLISIS JURÍDICO CUBANO: BASES LEGALES QUE FACILITAN LA VIGILANCIA DIGITAL EN CUBA

MONOPOLIO ESTATAL DE LAS TELECOMUNICACIONES Y CONTROL DE LA INFRAESTRUCTURA

El control estatal sobre las telecomunicaciones constituye el pilar estructural de la vigilancia digital en Cuba. La Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) mantiene el monopolio absoluto de los servicios de telefonía fija, móvil y acceso a Internet, sin competencia privada ni mecanismos independientes de supervisión.

Este monopolio permite al Estado:

- Controlar el tráfico de datos entrante y saliente del país.
- Implementar bloqueos selectivos o generales.
- Identificar usuarios, dispositivos y ubicaciones.
- Limitar o degradar el servicio de forma discrecional.
- Ejecutar apagones de Internet a nivel nacional o local.

La ausencia de pluralidad de proveedores y de regulación independiente impide cualquier forma de control ciudadano o judicial sobre las prácticas de vigilancia, creando un entorno técnicamente propicio para la interceptación masiva de comunicaciones.

CONSTITUCIÓN DE LA REPÚBLICA (2019): RECONOCIMIENTO FORMAL SIN GARANTÍAS REALES

La Constitución cubana de 2019 reconoce formalmente derechos como:

- La intimidad y la vida privada (art. 48)
- La inviolabilidad de las comunicaciones (art. 50)
- La libertad de pensamiento, conciencia y expresión (art. 54)

Sin embargo, estos derechos están subordinados a cláusulas amplias e indeterminadas vinculadas a la *"seguridad del Estado"*, el *"orden público"* y los *"fines de la sociedad socialista"*. Estas cláusulas funcionan como habilitaciones abiertas para restringir derechos sin control judicial efectivo.

Además, la Constitución carece de:

- Un tribunal constitucional independiente.
- Mecanismos de control de constitucionalidad accesibles.
- Recursos efectivos contra actos de vigilancia o censura.

En la práctica, el reconocimiento constitucional de derechos digitales queda vacío de contenido operativo.

DECRETO-LEY 370 Y NORMATIVAS ADMINISTRATIVAS: CRIMINALIZACIÓN DEL DISCURSO DIGITAL

El **Decreto-Ley 370/2018, "Sobre la informatización de la sociedad en Cuba"**, constituye el principal instrumento normativo que regula el uso de las tecnologías de la información y la comunicación en el país. Si bien formalmente se presenta como una norma orientada a promover el desarrollo tecnológico, su diseño, contenido y forma de aplicación revelan un enfoque centrado en el control, la seguridad y la subordinación del espacio digital a los intereses del Estado.

A diferencia de los marcos regulatorios adoptados en sistemas democráticos, el **Decreto-Ley 370** no reconoce la libertad de expresión digital como un derecho autónomo ni establece salvaguardas efectivas frente a la injerencia estatal. Por el contrario, integra explícitamente la informatización al aparato de seguridad nacional, vinculando el uso de las tecnologías al *"fortalecimiento de la defensa"*, la *"seguridad del Estado"* y el *"orden interior"*.

Este enfoque convierte a la normativa digital en un instrumento funcional a la vigilancia, más que en un marco de protección de derechos.

CENTRALIZACIÓN DEL CONTROL TECNOLÓGICO Y AUSENCIA DE CONTRAPESOS

El **Decreto-Ley 370** consolida el control estatal absoluto sobre las telecomunicaciones al otorgar al Ministerio de Comunicaciones, en coordinación con el Ministerio del Interior y las Fuerzas Armadas Revolucionarias, amplias facultades de regulación, fiscalización y control del ecosistema digital.

Este diseño tiene consecuencias directas:

- No existe pluralidad de proveedores ni independencia técnica.
- No hay autoridades reguladoras autónomas.
- No se establecen mecanismos de supervisión judicial previa.
- No se reconoce el derecho a la notificación ni a la impugnación efectiva frente a actos de vigilancia o sanción.

La combinación de monopolio estatal de infraestructura, control normativo y ausencia de contrapesos institucionales crea un entorno estructuralmente propicio para la vigilancia masiva y la restricción arbitraria de derechos.

EL ARTÍCULO 68: CRIMINALIZACIÓN DE LA EXPRESIÓN EN ENTORNOS DIGITALES

El núcleo represivo del **Decreto-Ley 370** se encuentra en su artículo 68, que tipifica como contravención administrativa una serie de conductas vinculadas al uso de las tecnologías de la información.

En particular, el inciso **68(i)** sanciona ***"difundir, a través de las redes públicas de transmisión de datos, información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas."***.

El **Decreto-Ley 370**, al tipificar como contravención en su **artículo 68(i)** la difusión en redes públicas de "**información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas**", introduce una cláusula **abiertamente indeterminada**: conceptos como *"interés social"*, *"moral"* o *"buenas costumbres"* carecen de definición normativa precisa y permiten lecturas expansivas y cambiantes, lo que compromete la **previsibilidad** exigible a cualquier restricción sancionadora (el ciudadano no puede anticipar razonablemente qué conductas quedan prohibidas). En ese contexto, la norma habilita un **riesgo estructural de censura indirecta**: aun sin prohibir expresamente una opinión, la amenaza de sanción por categorías vagas favorece la aplicación selectiva y genera **efecto inhibidor** (autocensura), especialmente cuando se usa para castigar crítica pública o difusión de información de interés público bajo etiquetas morales o de "interés social" definidas por la autoridad.

Este precepto, por tanto, presenta **graves incompatibilidades con los estándares internacionales** adicionales:

a) Vaguedad e indeterminación normativa

Los conceptos utilizados *"interés social"*, *"moral"*, *"buenas costumbres"* carecen de definición legal precisa. Esta indeterminación impide a las personas prever qué conductas están prohibidas, vulnerando el principio de legalidad reconocido en el **artículo 15 del Pacto Internacional de Derechos Civiles y Políticos**.

b) Criminalización del discurso crítico

En la práctica, esta disposición ha sido utilizada para sancionar:

- Opiniones políticas,
- Denuncias de violaciones de derechos humanos,
- Críticas a autoridades,
- Difusión de información independiente,
- Contenidos satíricos o de opinión.

Ello convierte al artículo 68(i) del **Decreto-Ley 370** en una **cláusula de censura por contenido**, incompatible con el **artículo 19 del PIDCP** y con la jurisprudencia del Comité de Derechos Humanos, que prohíbe sancionar expresiones por resultar molestas, críticas o incómodas para el poder.

c) Ausencia de exigencia de daño real o incitación a violencia

La norma no exige que la información cause un daño concreto, ni que incite a la violencia o al odio, lo que refuerza su carácter desproporcionado y arbitrario.

SANCIONES ADMINISTRATIVAS COMO MECANISMO DE CENSURA INDIRECTA

El **Decreto-Ley 370** establece un régimen sancionador que incluye:

- Multas elevadas;
- Decomiso de dispositivos electrónicos;
- Suspensión o cancelación de licencias;
- Clausura de servicios o actividades; y
- Confiscación definitiva de equipos.

Estas sanciones, aplicadas en el contexto de la expresión digital, tienen un efecto claramente inhibidor. La confiscación de un teléfono móvil o una computadora equivale, en la práctica, a la exclusión del espacio público digital, afectando no solo la libertad de expresión, sino también el acceso a información, el trabajo, la educación y la comunicación familiar.

El informe de denuncia documenta que la mayoría de los declarantes/denunciantes, el **83% (166 de 200)** ha sido sancionado, citado o amenazado (sin contabilizar aquellos que han sufrido otras represalias y consecuencias) en relación directa con sus publicaciones y/o comunicaciones digitales, lo que demuestra que estas disposiciones no son meramente formales, sino que se aplican de manera activa como herramienta de control.

DÉFICIT DE GARANTÍAS PROCESALES Y AUSENCIA DE CONTROL JUDICIAL EFECTIVO

El procedimiento sancionador previsto por el **Decreto-Ley 370** agrava aún más su impacto sobre los derechos humanos:

- Las sanciones pueden imponerse de forma inmediata.
- Los recursos se tramitan ante la misma autoridad administrativa que impone la sanción.
- El acceso a la vía judicial es posterior, limitado y poco efectivo.
- No existe obligación de motivación reforzada.
- No se prevé reparación integral ni compensación por daños.

Además, el propio decreto excluye expresamente la posibilidad de reclamar indemnización por los perjuicios derivados de las sanciones, lo que deja a las personas afectadas en una situación de indefensión estructural.

Este diseño contraviene los artículos **2 y 14 del PIDCP**, que exigen recursos efectivos y garantías judiciales frente a violaciones de derechos.

CONTRADICCIONES INTERNAS DEL DECRETO Y USO INSTRUMENTAL DE LA LEGALIDAD

Aunque el **Decreto-Ley 370** reconoce formalmente la protección de los datos personales y la inviolabilidad de las comunicaciones, estas garantías quedan vacías de contenido al coexistir con disposiciones que obligan a proveedores y usuarios a entregar información a las autoridades sin orden judicial ni criterios de proporcionalidad.

Esta contradicción normativa evidencia que la protección de datos es meramente declarativa, mientras que el acceso estatal a la información digital opera sin límites claros.

En la práctica, el decreto legitima un modelo de vigilancia preventiva, incompatible con los estándares desarrollados por las Naciones Unidas sobre el derecho a la privacidad en la era digital, entre otros, en AGNU, Res. 73/179, The right to privacy in the digital age (2018), A/RES/73/179, y en CDH, Res. 34/7 (A/HRC/RES/34/7, 2017) y CDH, Res. 42/15 (A/HRC/RES/42/15, 2019).

CONEXIÓN DIRECTA CON LOS HALLAZGOS DEL INFORME DE DENUNCIA

Los hallazgos empíricos recogidos en este informe confirman el uso sistemático del **Decreto-Ley 370**, junto con otras normas administrativas y penales, como fundamento para:

- Multas por publicaciones en redes sociales.
- Citaciones e interrogatorios basados en contenido digital.
- Decomiso de dispositivos.
- Amenazas y advertencias oficiales.
- Represalias indirectas contra familiares.

Aunque no siempre se invoca explícitamente el número del decreto, la tipología de las sanciones, el lenguaje utilizado por las autoridades y la naturaleza de las conductas reprimidas coinciden plenamente con el marco habilitado por el **Decreto-Ley 370**.

Esto permite concluir que el **Decreto-Ley 370** constituye el **soporte jurídico central de la política de vigilancia digital en Cuba**, al proporcionar una base legal amplia, ambigua y funcionalmente orientada al control del discurso público.

El **Decreto-Ley 370** no puede ser analizado como una norma técnica de informatización, sino como un instrumento normativo de control político en el entorno digital. Su redacción ambigua, su régimen sancionador desproporcionado, la ausencia de garantías judiciales y su articulación con los órganos de seguridad del Estado lo convierten en un pilar estructural de la vigilancia digital documentada en este informe.

Lejos de proteger derechos, el decreto habilita un sistema que normaliza la censura, la vigilancia y la represión de la expresión en línea, en abierta contradicción con los estándares internacionales de derechos humanos aplicables a la era digital.

CÓDIGO PENAL (LEY 151/2022): AMPLIACIÓN DEL CONTROL PUNITIVO

El Código Penal Cubano vigente refuerza el marco represivo al incorporar figuras penales amplias y ambiguas que pueden aplicarse a la actividad digital, entre ellas:

- **Delitos contra el orden constitucional:** El Código Penal cubano tipifica una serie de delitos contra el orden constitucional que, por su formulación amplia y ambigua, permiten su aplicación a conductas estrictamente expresivas desarrolladas en entornos digitales. Estas figuras no exigen necesariamente el uso de la violencia ni la comisión de actos materiales concretos, sino que sancionan comportamientos que las autoridades consideren contrarios al "*orden constitucional*" o a la estabilidad del sistema político.
  En la práctica, esta redacción habilita la criminalización de publicaciones en redes sociales, opiniones políticas, llamados a la protesta pacífica o denuncias públicas que cuestionen a las autoridades. La ausencia de una definición precisa del bien jurídico protegido y la amplitud del concepto de "*afectación al orden constitucional*" generan un margen de discrecionalidad incompatible con el principio de legalidad penal reconocido en el derecho internacional de los derechos humanos. Este tipo de disposiciones permite convertir el ejercicio legítimo de la libertad de expresión en una conducta penalmente reprochable, especialmente cuando se ejerce a través de plataformas digitales con amplio alcance.
- **Propaganda contra el orden constitucional:** El delito de propaganda contra el orden constitucional constituye uno de los mecanismos más utilizados para reprimir la expresión política en Cuba. Su formulación permite sancionar la difusión de ideas, opiniones o mensajes que las autoridades interpreten como contrarios al sistema político vigente, sin exigir que exista incitación directa a la violencia o a la comisión de actos delictivos.
  En el contexto digital, esta figura se ha utilizado para perseguir publicaciones en redes sociales, comentarios críticos, contenidos audiovisuales y mensajes difundidos por mensajería privada. El carácter subjetivo del concepto de "propaganda" y su desvinculación de un daño concreto convierten esta figura en

una herramienta idónea para silenciar el disenso. Desde la perspectiva del derecho internacional, la criminalización de la propaganda política resulta incompatible con el **artículo 19 del Pacto Internacional de Derechos Civiles y Políticos**, que protege de manera reforzada el discurso político, incluso cuando resulta incómodo u ofensivo para las autoridades.

- **Difusión de noticias falsas:** El Código Penal cubano sanciona la difusión de "*noticias falsas*" cuando estas puedan causar alarma, desorden o afectar el orden público. Esta figura, ampliamente criticada por organismos internacionales, presenta graves problemas de compatibilidad con la libertad de expresión debido a su vaguedad y a la ausencia de criterios objetivos para determinar qué información es falsa.
  En el entorno digital, esta disposición ha servido para perseguir a personas que difunden información no oficial, denuncias ciudadanas, reportes sobre protestas o críticas a la gestión gubernamental. La norma no exige prueba de intención dolosa ni de daño real, lo que permite su aplicación discrecional contra cualquier contenido que contradiga la versión oficial de los hechos.
  Los estándares internacionales han sido claros en advertir que las leyes contra la "*desinformación*" o las "*noticias falsas*" no deben utilizarse para sancionar el debate público ni el periodismo independiente. La Relatoría Especial para la Libertad de Expresión de la ONU ha señalado que este tipo de figuras, cuando no están estrictamente delimitadas, generan un efecto inhibidor incompatible con una sociedad democrática.
- **El delito de Desacato (art. 185)**, que consiste en aplicar sanción penal a quien "*verbal o extra verbalmente, mediante escrito o gestos, en su presencia o de otra u otras personas, o a través de cualquier medio de comunicación, amenace, calumnie, difame, insulte, injurie, ultraje u ofenda en su dignidad o decoro, a un funcionario público, autoridad o a sus agentes o auxiliares, en ejercicio de sus funciones o en ocasión o con motivo de ellas*", es decir, cualquier manifestación sobre cualquier funcionario o auxiliar de cualquier organismo del régimen, y que aplica la sanción de privación de libertad de seis meses a un año, pero que se agrava en el caso de críticas a altos mandos del régimen, con sanción de uno a tres años de privación de libertad. Este delito proscribe toda crítica a la gestión del aparato gobernante.
- **Colaboración con medios o entidades extranjeras:** El Código Penal también contempla figuras que penalizan la colaboración con entidades extranjeras o la difusión de información que supuestamente favorezca intereses externos. En el contexto cubano, estas disposiciones se han aplicado contra periodistas independientes, activistas, defensores de derechos humanos y personas que mantienen contacto con medios internacionales o plataformas extranjeras.
  En el ámbito digital, esta figura se traduce en la criminalización de entrevistas, publicaciones en medios fuera del país, cooperación con organizaciones internacionales o simple intercambio de información a través de Internet. La amplitud del tipo penal permite equiparar el ejercicio de la libertad de expresión transnacional con conductas de traición o desestabilización, en abierta contradicción con el derecho a la libertad de expresión sin fronteras consagrado en el **artículo 19 del PIDCP.**
  La utilización de esta figura refuerza un esquema de aislamiento informativo y control del discurso, en el que cualquier vínculo comunicacional externo puede ser reinterpretado como una amenaza a la seguridad del Estado.
- **Sanción accesoria de comiso (art. 52)**: permite a las autoridades "*desposeer al sancionado de los bienes u objetos que sirvieron o estaban destinados para la perpetración del delito*", sanción que "*alcanza, los efectos o instrumentos del delito a que se refieren los apartados anteriores, que se encuentren en posesión o propiedad de terceros no responsables*".
- **Sanción accesoria de Confiscación de bienes (art. 53)**, consistente en "*desposeer al sancionado de sus bienes, total o parcialmente, transfiriéndolos a favor del Estado*".

En conjunto, estas disposiciones del Código Penal cubano configuran un marco jurídico que permite la criminalización de la expresión digital mediante tipos penales amplios, ambiguos y carentes de salvaguardias efectivas. Su aplicación selectiva y discrecional, en combinación con el **Decreto-Ley 370** y los mecanismos de vigilancia digital documentados en este informe, conforma un sistema normativo orientado no a la protección de derechos, sino al control del discurso público y la disuasión del disenso.

También es relevante indicar que el Código Penal establece en su artículo 80.1 una serie de circunstancias agravantes del delito penal, en especial el inciso ñ) y q):

> "*Artículo 80.1 Son circunstancias agravantes de la responsabilidad penal de las personas naturales cometer el delito:*

ñ) contra personas o bienes relacionados con la defensa, la seguridad nacional, el ciberespacio, las reservas materiales o vinculados con actividades priorizadas para el desarrollo económico y social del país;

q) facilitando la ejecución del hecho,... o agravando sus consecuencias; mediante la utilización de las tecnologías de la información y la comunicación, las telecomunicaciones y sus servicios."

Todo este entramado legal contradice de manera directa los estándares internacionales en materia de libertad de expresión, legalidad penal y protección frente a injerencias arbitrarias, y constituye uno de los pilares fundamentales del modelo de vigilancia digital identificado en el presente estudio.

LA LEY DEL PROCESO PENAL (LEY NO. 143/2021) HABILITA AMPLIAMENTE EL CIBERPATRULLAJE

La Ley No. 143/2021 "Del Proceso Penal", vigente desde enero de 2022, consolida un marco procesal que **normaliza la recolección y tratamiento de información** (incluida la de naturaleza digital) como parte de la investigación penal, bajo la lógica de "necesidad" para el esclarecimiento del hecho. En sus disposiciones preliminares, la propia norma reconoce que **la correspondencia y "demás formas de comunicación" son inviolables, pero acto seguido establece que pueden ser interceptadas o registradas** por "resolución expresa de *autoridad competente*" en los casos y formalidades que la misma Ley determina (art. 10).

El punto crítico, para efectos de vigilancia digital, es **cómo queda definido el perímetro de esa "*autoridad competente*"**. La Ley describe como "*autoridad actuante*" —con potestades dentro del proceso penal— **a la Policía, al instructor penal, al fiscal y al tribunal** (art. 13.1). En consecuencia, **la habilitación para interceptar/registrar comunicaciones prevista en el art. 10 no queda, por diseño, asociada de forma inequívoca a un control judicial previo e independiente**, sino que se inserta en un esquema donde actores de persecución penal integran el núcleo decisorio del proceso.

A ello se suma un **mecanismo de acceso a datos particularmente amplio**: la Ley impone a "*órganos, organismos, organizaciones y demás entidades de cualquier naturaleza*" el deber de **suministrar informes, datos y antecedentes** a la Policía, instructor penal, fiscal o tribunal cuando estos lo requieran para investigar o juzgar un delito, en un plazo fijado (hasta 20 días, prorrogable ordinariamente) y con advertencia de responsabilidades, incluso penales, por incumplimiento (art. 49). En la práctica, esta cláusula de auxilio obligatorio **crea una autopista legal para requerimientos de datos a operadores, proveedores, empleadores, instituciones y cualquier entidad** que custodie información relevante (metadatos, registros, trazas, listados, etc.).

La propia Ley legitima, además, el uso de **"medios científico-técnicos y las tecnologías de la información y la comunicación"** dentro de actuaciones y diligencias del proceso penal (art. 47). Aunque la norma enuncia deberes de integridad, autenticidad y confidencialidad de datos, en términos estructurales **normaliza el recurso a herramientas técnicas** (captura, procesamiento, preservación y traslado de información) como parte ordinaria de la investigación sin control judicial, lo que abre un espacio funcional absoluto para prácticas intrusivas.

Finalmente, la Ley contiene reglas de **entrada y registro** que —por su naturaleza— se proyectan inevitablemente sobre el ámbito digital (incautación de teléfonos, ordenadores, memorias, documentos, soportes y contraseñas en la práctica). En particular, **si no hay consentimiento**, se permite el registro mediante "resolución fundada" de la Policía o del instructor penal **con aprobación del fiscal** (art. 307.2), e incluso se prevén autorizaciones específicas del fiscal para registros fuera del horario ordinario (art. 307.3). A esto se añade que, durante diligencias ordenadas, **pueden realizarse grabaciones o filmaciones** que se incorporan al proceso (art. 50), reforzando un marco en el que la captura de información (también audiovisual y digital) se vuelve rutinaria.

En suma, la Ley 143/2021 articula un **ecosistema procesal que permite intervención y obtención de información digital** mediante: (i) habilitación expresa para interceptar/registrar comunicaciones (art. 10), (ii) una definición amplia de "*autoridad actuante*" (art. 13), (iii) obligaciones generales de entrega de datos por parte de entidades (art. 49), (iv) legitimación del uso de TIC en diligencias (art. 47) y (v) registros con control predominantemente fiscal (art. 307). Todo ello resulta especialmente problemático cuando el estándar internacional de protección de la vida privada exige **legalidad, necesidad y proporcionalidad**, además de **controles efectivos e independientes** para medidas altamente intrusivas como la interceptación de comunicaciones y el acceso a datos.

LEY 162/2023 DE LA COMUNICACIÓN SOCIAL

Esta Ley establece los propósitos, partidistas y sectarios, de los sistemas de comunicación social (art. 5), controlados por el "*Instituto de Información y Comunicación Social*" (art. 6), cuyos propósitos es controlar el aparato propagandístico del régimen (art. 7) y proscribir cualquier desviación de este propósito, definiendo los "*contenidos*" como material potencialmente "*subversivo*" y altamente peligroso para el Estado (art. 13), por lo que justifica el monopolio del Estado sobre toda forma de comunicación social (arts. 14, 27 y 28), articulando el control de los periodistas o comunicadores (arts. 35 y 36), poniendo extremos límites a la "*comunicación social en el ciberespacio*" (arts. 51 a 54), definiendo la "*comunicación política*" y limitándola al extremo de servir la expresión, únicamente, del "*pensamiento revolucionario*" (arts. 55 y 56).

MARCO LEGAL CUBANO COMPLEMENTARIO: DECRETO-LEY 35/2021, LEY 149/2022 Y NORMATIVA ASOCIADA

El **Decreto-Ley 35/2021** ("De las Telecomunicaciones, las TIC y el Uso del Espectro Radioeléctrico") constituye el **marco sectorial transversal** que habilita la gobernanza estatal de redes, servicios y operadores. Desde su propio objeto y fines, vincula explícitamente la regulación de telecomunicaciones/TIC con objetivos de **seguridad**: "contrarrestar... agresiones... en el ciberespacio" y salvaguardar la "seguridad e invulnerabilidad" en beneficio de la **Seguridad y Defensa Nacional** y el **Orden Interior**, entre otros fines. Esta formulación, por su amplitud, funciona como "puerta de entrada" para medidas técnicas y administrativas de aseguramiento y control sobre infraestructura y servicios digitales, bajo racionalidades de defensa/orden público.[10]

En ese mismo diseño, el DL-35 refuerza el rol del **Ministerio de Comunicaciones (MINCOM)** como autoridad rectora con capacidad normativa: el artículo 71 dispone que el MINCOM "establece las disposiciones normativas" que deben cumplir operadores y proveedores para "garantizar la seguridad" de redes y servicios. Paralelamente, se establecen **deberes** que conectan directamente con riesgos de vigilancia o control: por ejemplo, se prevé que se "impida" el uso de servicios para atentar contra la seguridad/orden interior, y se incluye la obligación de **entregar al MINCOM la información que este determine** para el cumplimiento de sus funciones. Este tipo de deberes, si no se acompaña de garantías robustas (límites claros, control independiente, trazabilidad y recursos efectivos), puede traducirse en incentivos normativos para la **monitorización preventiva** o requerimientos amplios de datos a intermediarios.

Como **normativa asociada** de ciberseguridad, la **Resolución 105/2021 (MINCOM)** aprueba el "*Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad*" y prevé un esquema de coordinación donde la Dirección de Ciberseguridad del MINCOM actúa "en coordinación" con los ministerios de las **FAR** y del **Interior**, facultada para implementar acciones complementarias para su cumplimiento.[11] Esta arquitectura institucional es relevante porque integra, en la práctica, la gestión de "incidentes" y flujos de información técnica con estructuras de seguridad del Estado, lo que incrementa el riesgo de que categorías amplias de "ciberseguridad" se utilicen para justificar medidas intrusivas.

Por su parte, la **Ley 149/2022 de Protección de Datos Personales** introduce un marco formal de derechos (acceso, rectificación, cancelación/oposición) y crea un **sistema de control nacional** de registros y bases de datos personales: dispone que el **Ministro de Justicia** debe crear dicho control nacional y ejercer la "máxima supervisión", y que los responsables declaren la existencia de sus bases en el plazo previsto.[12] Sin embargo, la Ley también contiene **excepciones amplias** que pueden debilitar la tutela en contextos sensibles: permite denegar o no dar curso a solicitudes, entre otros supuestos, por razones de "bienestar general", "orden público" o "interés de la defensa y la seguridad nacional". Además, prevé que diversos altos cargos —incluido el **Ministro del Interior**— estén facultados para autorizar transferencias internacionales de datos "en el ámbito de sus competencias", lo que confirma el peso institucional de los órganos de seguridad en el ecosistema de tratamiento de datos.

Finalmente, como desarrollo reglamentario técnico, la **Resolución 58/2022 (MINCOM)** aprueba el "Reglamento para la Seguridad y Protección de los Datos Personales en Soporte Electrónico", justificándolo por el avance de

[10] https://www.mincom.gob.cu/sites/default/files/marcoregulatorio/d-l_35-21_sobre_telecomunicaciones-tic_y_uso_de_ere.pdf
[11] https://csirt.biocubafarma.cu/storage/marco_regulatorio/r_105-21_modelo_de_actuacion_nacional.pdf
[12] https://www.minjus.gob.cu/sites/default/files/archivos/publicacion/2022-08/goc-2022-o90_0_0.pdf

la informatización y la necesidad de complementar la legislación de seguridad TIC con requerimientos de seguridad específicos para datos personales. Este reglamento —junto con la obligación legal de notificar incidentes de ciberseguridad a la autoridad competente— refuerza un enfoque de **seguridad/gestión centralizada** del dato personal, que puede mejorar prácticas de protección técnica, pero también ampliar canales de reporte e intervención si no se acota con garantías, transparencia y control independiente.

AUSENCIA DE GARANTÍAS PROCESALES Y CONTROL JUDICIAL

Un elemento central del sistema de vigilancia digital en Cuba es la ausencia de controles judiciales independientes sobre:

- Interceptación de comunicaciones.
- Acceso a dispositivos.
- Uso de información digital como prueba.
- Medidas de vigilancia personal.

No existen mecanismos efectivos de autorización judicial previa, notificación posterior ni recursos de impugnación accesibles para las personas afectadas. Esto vulnera de forma directa los estándares establecidos por:

- El artículo 17 del PIDCP.
- La jurisprudencia del Comité de Derechos Humanos.
- Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (Principios de Necesidad y Proporcionalidad).

CONVERGENCIA ENTRE MARCO LEGAL, TECNOLOGÍA Y REPRESIÓN

El análisis conjunto del marco normativo cubano permite concluir que la vigilancia digital no es una desviación ni una práctica informal, sino un componente estructural del sistema de control estatal.

La combinación de:

- Monopolio tecnológico,
- Legislación ambigua,
- Ausencia de controles judiciales,
- Criminalización del disenso,
- Uso de sanciones administrativas y penales,
- Represión física complementaria,

configura un entorno en el que la vigilancia digital se convierte en una herramienta de gobernanza autoritaria.

Este contexto normativo explica y da sustento jurídico-político a los patrones empíricos documentados en el presente informe de denuncia, permitiendo comprender por qué la vigilancia digital en Cuba no opera como una excepción, sino como una política pública sostenida.

ANÁLISIS JURÍDICO INTERNACIONAL DE LOS PATRONES DE VIGILANCIA DIGITAL IDENTIFICADOS

CIBERPATRULLAJE Y MONITOREO SISTEMÁTICO DE REDES

ESTÁNDAR INTERNACIONAL APLICABLE

La información recogida en el informe de denuncia evidencia la existencia de un sistema estructurado de **Ciberpatrullaje estatal**, consistente en la observación, seguimiento y análisis sistemático de la actividad de personas usuarias en redes sociales, plataformas digitales y servicios de mensajería. Este monitoreo no se limita a contenidos públicos, sino que se extiende a espacios percibidos como privados o semiprivados, como grupos cerrados, mensajes directos o intercambios entre contactos.

Desde la perspectiva del derecho internacional de los derechos humanos, este tipo de prácticas afecta directamente al núcleo del derecho a la libertad de expresión, protegido por el **artículo 19** de la **Declaración Universal de Derechos Humanos** y del **Pacto Internacional de Derechos Civiles y Políticos (PIDCP)**. **La**

Observación General Nº 34 del Comité de Derechos Humanos es clara al señalar que la vigilancia o supervisión de la expresión, incluso cuando no conlleva sanciones inmediatas, puede constituir una restricción ilegítima si genera un efecto inhibidor o disuasorio sobre el ejercicio del derecho.

El Consejo de Derechos Humanos ha consolidado este estándar, entre otras, mediante las resoluciones A/HRC/RES/20/8 (2012) y A/HRC/RES/26/13 (2014), afirmando que los mismos derechos que las personas tienen fuera de línea deben ser protegidos en línea —en particular la libertad de expresión— y que los Estados no deben interferir arbitrariamente en el flujo de información en Internet.[13]

Los datos del informe de denuncia muestran que una amplia mayoría de los declarantes/denunciantes ha sido confrontada por autoridades con publicaciones, mensajes o interacciones digitales, en muchos casos durante citaciones o interrogatorios. Este uso de la actividad digital como insumo represivo demuestra que el Ciberpatrullaje no es una práctica pasiva u ocasional, sino un mecanismo activo de vigilancia política. La reiteración de estos hechos permite afirmar que existe una política de observación sistemática del discurso en línea, orientada a identificar, clasificar y eventualmente sancionar expresiones consideradas críticas.

Desde un enfoque jurídico, este patrón constituye una forma de censura indirecta, prohibida por el derecho internacional, ya que no requiere prohibiciones explícitas para restringir la libertad de expresión: basta con generar un entorno de supervisión constante que induzca a la autocontención y al silencio.

TEST DE LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD

El monitoreo sistemático de redes sociales y plataformas digitales:

- **No cumple el requisito de legalidad**, al no estar sustentado en normas claras, públicas y previsibles.
- **No supera la prueba de necesidad**, al aplicarse de manera masiva y no individualizada.
- **Resulta desproporcionado**, al generar un control permanente sobre la expresión ciudadana sin relación directa con un fin legítimo concreto.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

Los datos recabados muestran que:

- Un **76,50%** de los declarantes/denunciantes (153 de 200) afirmó que **autoridades cubanas mencionaron o reprocharon sus publicaciones o mensajes digitales en múltiples ocasiones, de forma explícita o velada, durante citaciones o interrogatorios**. Un **12,00%** (24 de 200) reportó que esto ocurrió **al menos una vez**, mientras que solo un **11,50%** (23 de 200) indicó que nunca le fueron mencionados contenidos digitales en procesos de citación e interrogatorios.
- El **57,50%** de los declarantes/denunciantes (115 de 200) señaló que **las autoridades mostraron o mencionaron capturas de sus publicaciones**, mientras que el **47,00%** (94 de 200) indicó que durante **interrogatorios se les comentó explícitamente que estaban siendo vigiladas en redes sociales**.
- **Las autoridades mencionaron mensajes privados** de aplicaciones de mensajería cifrada o semiprivada (como WhatsApp, Telegram o Signal) en el **42,50%** de los casos (85 de 200 declarantes, cifra que consolida las menciones de mensajes en grupos y mensajes en chats privados), mencionando **mensajes en grupos** privados en el **29,50%** (59 de 200) y **mensajes en conversaciones uno-a-uno** en el **33,00%** de los casos (66 de 200). Incluso **audios privados** fueron mencionados en el **20,00%** de los casos (40 de 200). El uso de capturas y referencias a mensajes privados demuestra una práctica sistemática de vigilancia, no incidental.

Estos elementos configuran un patrón de **Ciberpatrullaje permanente**, incompatible con los estándares internacionales sobre libertad de expresión.

[13] Consejo de Derechos Humanos, Resolución 20/8, A/HRC/RES/20/8 (5 de julio de 2012); y Resolución 26/13, A/HRC/RES/26/13 (26 de junio de 2014), La promoción, protección y disfrute de los derechos humanos en Internet.

BLOQUEOS Y CORTES DE INTERNET Y APLICACIONES

ESTÁNDAR INTERNACIONAL APLICABLE

El análisis de las respuestas revela un uso recurrente de interrupciones del servicio de Internet, bloqueos de plataformas y degradación intencional de la conectividad, especialmente en contextos de movilización social, fechas políticamente sensibles o tras la difusión de contenidos críticos. Estas prácticas configuran uno de los mecanismos más visibles y extendidos de control digital.

El marco jurídico internacional es inequívoco al respecto. El marco jurídico internacional es inequívoco al respecto: el Consejo de Derechos Humanos ha condenado expresamente las medidas que interrumpen el acceso a Internet o limitan la difusión de información en línea, por ser incompatibles con el derecho a la libertad de expresión, y ha reiterado esta posición en resoluciones posteriores.[14]

Asimismo, la **Observación General Nº 37** del Comité de Derechos Humanos reconoce que el acceso a Internet es hoy un elemento esencial para el ejercicio del derecho de reunión pacífica, especialmente cuando las protestas y movilizaciones se organizan, documentan o difunden a través de medios digitales. En este sentido, los apagones o bloqueos no afectan únicamente a la expresión individual, sino que inciden directamente en el derecho a la participación política y a la protesta pacífica.

El análisis de los datos muestra que las interrupciones no se producen de forma aleatoria ni responden a fallas técnicas aisladas. Por el contrario, se concentran temporalmente en momentos de alta sensibilidad política, como protestas, fechas simbólicas o juicios relevantes, lo que refuerza su carácter intencional. El uso de bloqueos selectivos, reducción deliberada de velocidad y limitaciones al uso de VPN evidencia una estrategia orientada a dificultar la circulación de información sin recurrir a prohibiciones formales.

TEST DE LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD

Desde la prueba de legalidad, necesidad y proporcionalidad, estas prácticas resultan claramente incompatibles con los estándares internacionales. No existen bases legales claras, no se aplican de forma individualizada y producen afectaciones masivas desproporcionadas, lo que permite calificarlas como restricciones arbitrarias al ejercicio de derechos fundamentales.

Los cortes:

- No están regulados por normas claras ni sometidos a control judicial.
- Se aplican de forma generalizada y preventiva.
- Carecen de proporcionalidad al afectar a poblaciones enteras, incluso sin relación con protestas o hechos concretos.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- Sufren **cortes selectivos de Internet el 77,50%** de los declarantes/denunciantes (155 de 200).
- Sufren **bloqueos selectivos de servicios o páginas el 63,00%** de los declarantes/denunciantes (126 de 200).
- Entre las prácticas reportadas con mayor frecuencia se encuentran el **corte total de datos móviles o conectividad dirigido a la línea personal** (**52%**, 104 de 200) y los **cortes que afectaron simultáneamente a la línea propia y a otras del entorno inmediato mientras otros usuarios de la misma zona mantenían conectividad** (**51%**, 102 de 200).
- Asimismo, se reportaron **apagones totales de conectividad y/o llamadas en determinadas zonas** (**47,50%**, 95 de 200), **fallos en servicios de mensajería o llamadas durante protestas u otros eventos sensibles** (**49%**, 98 de 200) y **reducción extrema e intencionada de la velocidad de navegación (throttling)** (**47%**, 94 de 200).
- A estas interferencias se suman los **bloqueos de plataformas y contenidos**: un **44,50%** (89 de 200) reportó **bloqueo de redes sociales específicas** como Facebook, X o YouTube; un **36%** (72 de 200) indicó el **bloqueo habitual de páginas web si no se utiliza VPN**; y un **36,50%** (73 de 200) señaló **imposibilidad de acceso a**

[14] Consejo de Derechos Humanos, Resolución 32/13, A/HRC/RES/32/13 (1 de julio de 2016); Resolución 38/7, A/HRC/RES/38/7 (5 de julio de 2018); y Resolución 57/29, A/HRC/RES/57/29 (11 de octubre de 2024), La promoción, protección y disfrute de los derechos humanos en Internet.

páginas de medios independientes u organismos internacionales. También aparece un elemento adicional de alta gravedad: el **bloqueo o imposibilidad de uso de VPN** (**22,50%**, 45 de 200).

Todo este conjunto de evidencias confirma que los cortes constituyen una **herramienta de control social y político**, y no una medida técnica neutral.

INTERCEPTACIÓN DE COMUNICACIONES, SPYWARE Y ACCESO NO AUTORIZADO

ESTÁNDAR INTERNACIONAL APLICABLE

Uno de los hallazgos más graves del informe de denuncia es la existencia de indicios consistentes de **interceptación de comunicaciones privadas y acceso no autorizado a cuentas y dispositivos personales**. Este patrón incluye la lectura de mensajes, el acceso a cuentas desde ubicaciones desconocidas, la modificación de contraseñas, el envío de mensajes sin consentimiento y la mención de contenidos privados durante interrogatorios oficiales.

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establece la prohibición absoluta de injerencias arbitrarias o ilegales en la vida privada, la correspondencia y las comunicaciones. Este principio ha sido desarrollado ampliamente por el Consejo de Derechos Humanos en el informe **A/HRC/27/37**, que subraya que la vigilancia digital, especialmente cuando es masiva o indiscriminada, constituye una injerencia grave que solo podría justificarse bajo condiciones extremadamente restrictivas.[15]

Los informes del Relator Especial sobre la libertad de expresión, en particular (**A/HRC/29/32** y **A/HRC/32/38**, refuerzan esta interpretación al afirmar que el cifrado y el anonimato son elementos esenciales para el ejercicio de los derechos humanos en la era digital, y que su debilitamiento o el acceso no autorizado a comunicaciones privadas socavan la libertad de expresión, la privacidad y la seguridad personal.

El patrón identificado en el informe de denuncia sugiere que estas prácticas no responden a investigaciones individuales autorizadas judicialmente, sino a un esquema de vigilancia generalizada. La reiteración de accesos no autorizados, la mención de mensajes privados por parte de autoridades y la ausencia de garantías procesales indican la existencia de mecanismos de interceptación incompatibles con el derecho internacional.

Además, la posible utilización de herramientas de espionaje digital o técnicas de intrusión informática agrava la vulneración, al introducir riesgos adicionales de manipulación de información, fabricación de pruebas y persecución selectiva. En este contexto, la vigilancia digital deja de ser una medida excepcional para convertirse en una herramienta estructural de control político.

TEST DE LEGALIDAD, NECESIDAD Y PROPORCIONALIDAD

La interceptación:

- Carece de base legal accesible.
- No está sujeta a autorización judicial independiente.
- Es indiscriminada y no limitada a casos concretos.
- Utiliza tecnologías intrusivas incompatibles con estándares de proporcionalidad.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- Un **49,50%** de los declarantes/denunciantes (99 de 200) reportó **haber recibido avisos de sesiones abiertas desde ubicaciones desconocidas**, mientras que un **46,50%** (93 de 200) detectó **intentos o cambios de contraseña no iniciados por la propia persona**. Asimismo, un **37%** (74 de 200) afirmó que **se enviaron mensajes desde sus cuentas sin su autorización**, y un **23,50%** (47 de 200) **detectó aplicaciones desconocidas instaladas en su teléfono sin consentimiento**.
- Adicionalmente, un **37,50%** de los declarantes/denunciantes (75 de 200) señaló que **las autoridades les mencionaron directamente sus mensajes privados**, reforzando la presunción de acceso indebido a

[15] En la misma línea, la Asamblea General de la ONU ha reiterado —como estándar universal— que la privacidad debe ser protegida también 'en la era digital' y que las injerencias mediante vigilancia e interceptación solo son compatibles con el derecho internacional bajo criterios estrictos de legalidad, necesidad y proporcionalidad, con salvaguardas efectivas." (AGNU, Res. 73/179, "The right to privacy in the digital age" (2018), A/RES/73/179).

comunicaciones personales. Solo un **15%** (30 de 200) indicó no haber notado nunca signos de intervención en cuentas o dispositivos.
- Estos indicadores describen un **patrón de acceso no autorizado a cuentas y dispositivos**, compatible con prácticas de intrusión digital y vigilancia técnica.
- A esta dinámica se suma la **intrusión coercitiva directa por parte de las autoridades**, documentada de manera consistente en las respuestas del cuestionario. En global, **el 65,50% de los declarantes/denunciantes (131 de los 200) fueron obligados a desbloquear sus teléfonos, a entregar sus contraseñas, a permitir la revisión de su contenido o a mostrar sus redes sociales**.
- Sin mandato judicial alguno, un **48,00%** de los declarantes/denunciantes (**96 de 200**) reportó que **fueron obligados por las autoridades a desbloquear su teléfono** durante una detención o interrogatorio; un **33,00%** (**66 de 200**) indicó que **se les exigieron contraseñas** de acceso a sus cuentas o dispositivos; y un **37,50%** (**75 de 200**) señaló que las autoridades **revisaron o copiaron fotos, documentos o chats** almacenados en sus teléfonos. Asimismo, un **33,00%** (**66 de 200**) fue obligado a **mostrar sus redes sociales** a agentes estatales.
- Solo un **4%** (8 de 200) indicó no haber sufrido ninguna anomalía.

Todo este conjunto de evidencias confirma un patrón de **vigilancia digital intrusiva**, compatible además con prácticas de spyware.

VIGILANCIA FÍSICA DIGITALIZADA Y CONTROL DEL ESPACIO PÚBLICO

ESTÁNDAR INTERNACIONAL APLICABLE

La evidencia recopilada permite identificar un patrón claro de **vigilancia física activada o intensificada como consecuencia directa de la actividad digital** de los declarantes/denunciantes. Este fenómeno demuestra que la vigilancia en Cuba no opera de manera aislada en el entorno virtual, sino que se proyecta deliberadamente sobre el espacio físico, configurando un **sistema híbrido de control** que combina herramientas digitales con prácticas presenciales tradicionales.

La observación recurrente de seguimientos personales, presencia policial frente a domicilios, visitas de advertencia y patrullaje selectivo tras publicaciones críticas sugiere la existencia de **mecanismos de identificación y selección previos**, basados en la actividad en redes sociales, mensajería digital o intercambios comunicacionales en línea. En este sentido, la vigilancia física digitalizada funciona como una **fase posterior del control digital**, destinada a materializar la presión estatal en la vida cotidiana de las personas vigiladas.

Desde la perspectiva del derecho internacional, esta articulación resulta particularmente preocupante. **La Observación General Nº 37 del Comité de Derechos Humanos** establece que la vigilancia del espacio público, especialmente cuando está vinculada al ejercicio de derechos fundamentales como la expresión o la reunión pacífica, debe ser excepcional, estrictamente necesaria y sujeta a salvaguardias claras. La vigilancia permanente o reiterada, activada por el ejercicio legítimo de la expresión digital, constituye una restricción indirecta e ilegítima de derechos.

Además, la instalación de cámaras frente a viviendas o la presencia constante de agentes en el entorno inmediato introduce un componente de **control territorial y psicológico**, que trasciende a la persona directamente vigilada e impacta en su familia, vecindario y red social. Esta dimensión expansiva refuerza el carácter disuasorio de la vigilancia y amplifica su efecto inhibidor, afectando el tejido social más allá del individuo.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

La vigilancia física:

- No responde a órdenes judiciales individualizadas.
- Se activa tras actividad digital legítima.
- Genera un efecto disuasorio incompatible con una sociedad democrática.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- Tras realizar publicaciones, enviar mensajes o participar en intercambios críticos en redes sociales u otros medios digitales, un **60,50%** (**121 de 200**) de los declarantes/denunciantes afirmó haber comprobado

vigilancia física de manera frecuente, mientras que un **24,00%** (**48 de 200**) indicó haberla experimentado **de forma ocasional**. En conjunto, un **84,50%** (**169 de 200**) reporta **algún grado de vigilancia física posterior a su actividad digital**. Solo un **4,50%** (**9 de 200**) afirmó no haber observado vigilancia física, y un **11%** (**22 de 200**) manifestó no estar seguro.

- La modalidad más frecuentemente observada fue la **presencia de personas vigilando frente a sus casas**, reportada por el **68,50%** de los declarantes/denunciantes (**137 de 200**). A ello se suman las **visitas de advertencia por parte de autoridades o agentes**, señaladas por el **60 %** (**120 de 200**), que constituyen una forma explícita de presión presencial vinculada a la actividad digital previa.
- Asimismo, un **53,50%** (**107 de 200**) reportó **seguimientos mediante motos o automóviles**, y un **49,50%** (**99 de 200**) indicó la **presencia recurrente de patrullas frente a su vivienda**. Estas prácticas sugieren un control sistemático del movimiento y del entorno inmediato de las personas vigiladas.
- En menor proporción, pero con especial gravedad, un **13,50%** (**27 de 200**) reportó la **instalación o presencia de cámaras frente a la vivienda**, lo que introduce un componente de vigilancia permanente y tecnológicamente mediada del espacio doméstico. Un **11%** (**22 de 200**) señaló **otros tipos de vigilancia física**, que incluyen observación encubierta esporádica, conversaciones informales de agentes o advertencias transmitidas vía telefónica o a través de terceros.

Todo este conjunto de evidencias confirma la existencia de un **sistema híbrido de vigilancia digital-física**.

USO DE NORMAS JURÍDICAS Y SANCIONES PARA CASTIGAR LA EXPRESIÓN DIGITAL

ESTÁNDAR INTERNACIONAL APLICABLE

El informe de denuncia documenta el uso sistemático de normas administrativas y penales para **castigar expresiones realizadas en entornos digitales**, lo que revela un patrón de instrumentalización del derecho interno como mecanismo de control del discurso público. Multas, investigaciones y procesos penales son activados en respuesta directa a publicaciones, mensajes, audios, memes o contenidos compartidos en redes sociales o aplicaciones de mensajería.

Desde el derecho internacional de los derechos humanos, esta práctica vulnera principios fundamentales. **La Observación General Nº 34** establece que las restricciones a la libertad de expresión deben estar previstas en leyes claras, perseguir fines legítimos y ser estrictamente necesarias y proporcionales. El uso de normas vagas o ambiguas para sancionar expresión política o de interés público constituye una violación directa del principio de legalidad.

Asimismo, tanto el Comité de Derechos Humanos como la Comisión Interamericana han reiterado que el derecho penal no puede ser utilizado como herramienta para silenciar la crítica, y que incluso las sanciones administrativas pueden generar un efecto disuasorio equivalente cuando se aplican de forma selectiva o intimidatoria. En este sentido, la activación de procesos legales por expresión digital no solo castiga conductas individuales, sino que **envía un mensaje disciplinador al conjunto de la sociedad**.

El uso de estas normas se inscribe, por tanto, en una estrategia más amplia de control, donde el marco legal deja de cumplir una función protectora y se transforma en un **instrumento de represión indirecta**, incompatible con los estándares internacionales sobre libertad de expresión y debido proceso.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

Las sanciones:

- No cumplen con el principio de legalidad estricta.
- Se aplican de manera selectiva.
- Buscan disuadir la crítica, no proteger derechos.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- A **77** de los 200 declarantes (el **38,50%**) les **realizaron una investigación penal** formal.
- A **35** de los 200 declarantes (el **17,50%**) les iniciaron una **acusación penal formal**.
- A **61** de los 200 declarantes (el **30,50%**) les **impusieron una medida cautelar** formal o de facto.
- A **47** de los 200 declarantes (el **23,50%**) les **impusieron una multa administrativa** por sus publicaciones.

- Las sanciones suelen ir precedidas de **advertencias, amenazas o prohibiciones informales**, lo que refuerza su carácter disuasorio. Un **58%** de los declarantes/denunciantes (**116 de 200**) recibió **advertencias o restricciones adicionales por mantener comunicaciones con determinadas personas**, y un **46,50%** (**93 de 200**) fue **amenazado directa o veladamente** con consecuencias más graves si persistía en su actividad digital.
- De la muestra de 200 declarantes/denunciantes, **sólo 32 de ellos no sufrieron sanciones o amenazas, penales y/o administrativas derivadas de sus comunicaciones digitales**.

Todo este conjunto de evidencias confirma la existencia del uso de normativa violatoria de la legislación internacional apoyada por un sistema represivo penal para perseguir, intimidar y castigar el libre ejercicio de la expresión, denuncia, asociación y reunión.

REPRESALIAS OFFLINE DERIVADAS DE EXPRESIÓN ONLINE

ESTÁNDAR INTERNACIONAL APLICABLE

Las prácticas de vigilancia digital documentadas en este informe se encuentran estrechamente vinculadas a **represalias presenciales**, que incluyen citaciones, interrogatorios, detenciones, amenazas, restricciones laborales y sanciones en espacios educativos o comunitarios. Estas medidas no aparecen como hechos aislados, sino como respuestas previsibles y sistemáticas a la actividad digital de las personas afectadas.

Desde la óptica del derecho internacional, estas represalias constituyen una forma de restricción indirecta de la libertad de expresión. La Declaración de las Naciones Unidas sobre los defensores de derechos humanos prohíbe expresamente cualquier forma de represalia, intimidación o sanción por el ejercicio legítimo de derechos fundamentales, incluyendo la expresión y la denuncia.

La combinación de vigilancia digital y represalias offline refuerza el carácter coercitivo del sistema documentado. La expresión digital deja de ser un acto abstracto para convertirse en un factor de riesgo de **consecuencias físicas y sociales tangibles**, lo que incrementa el costo percibido de participar en el debate público. Este mecanismo resulta especialmente eficaz para inhibir la expresión crítica sin necesidad de recurrir a censura directa o prohibiciones formales.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

Las represalias indirectas constituyen violaciones autónomas, incluso cuando no derivan en condenas formales.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- A **116** de los 200 declarantes (el **58%**) les **prohibieron o advirtieron** de no tener relación con ciertas personas.
- A **93** de los 200 declarantes (el **46,50%**) les **amenazaron directa o veladamente** con acciones punitivas.
- A **77** de los 200 declarantes (el **38,50%**) les **realizaron una investigación penal** formal.
- A **35** de los 200 declarantes (el **17,50%**) les iniciaron una **acusación penal formal**.
- A **61** de los 200 declarantes (el **30,50%**) les **impusieron una medida cautelar** formal o de facto.
- A **47** de los 200 declarantes (el **23,50%**) les **impusieron una multa administrativa** por sus publicaciones.
- Un **61%** de los declarantes/denunciantes afirmó haber sido **interrogado en oficinas de la policía** política, la PNR o el MININT, al igual que un **61%** también reportó **interrogatorios en su vivienda, lugar de trabajo o en la vía pública**. Estas acciones evidencian la **traducción directa de la vigilancia digital en medidas represivas presenciales**, incluidas sanciones administrativas y penales.
- Un **60%** fue **citado formalmente** por estas autoridades.
- Un **55%** indicó haber sido **detenido**.

Todo este conjunto de evidencias confirma un sistema de represión con cobertura generalizada, inmerso en una operativa de vigilancia, control y persecución policial y penal, mediante una integración de todos los aparatos del Estado en dicha labor.

REPRESALIAS CONTRA FAMILIARES

ESTÁNDAR INTERNACIONAL

Uno de los hallazgos más graves del informe de denuncia es la extensión deliberada de las represalias hacia familiares de personas activas digitalmente. Amenazas, citaciones, vigilancia y sanciones laborales dirigidas a familiares configuran un patrón de **castigo indirecto**, destinado a ejercer presión emocional y social sobre la persona vigilada.

El derecho internacional es claro al respecto. El **artículo 17 del PIDCP** protege la vida privada y familiar, y los estándares sobre defensores de derechos humanos prohíben expresamente las represalias contra terceros como forma de coerción. Este tipo de prácticas agrava la violación original, al instrumentalizar vínculos afectivos como herramienta de control estatal.

La afectación a familiares no solo amplía el alcance de la represión, sino que refuerza su eficacia disuasoria, al introducir un dilema moral que trasciende la esfera individual. La vigilancia digital se convierte así en un mecanismo de **control colectivo**, que fragmenta redes de apoyo y debilita la solidaridad social.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

Las represalias contra familiares constituyen una forma agravada de persecución.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- Un **66,50%** de los declarantes/denunciantes (**133 de 200**) reportó que **algún familiar fue amenazado**.
- Un **51,50%** de los declarantes/denunciantes (**103 de 200**) indicó que sus familiares fueron **citados policialmente**.
- Un **32,50%** de los declarantes/denunciantes (**65 de 200**) que fueron **detenidos**.
- Un **50,50%** de los declarantes/denunciantes (**101 de 200**) señaló **vigilancia física contra familiares**.
- Un **22,50%** de los declarantes/denunciantes (**45 de 200**) reportó **pérdida de empleo** de algún familiar como consecuencia indirecta de la actividad digital de la persona vigilada.
- Un **74,50%** de los declarantes/denunciantes **(149 de 200) tienen familia directa afectada por amenazas, citaciones, detenciones, vigilancia o pérdida del empleo como consecuencia de publicaciones atribuibles sólo a los declarantes/denunciantes**, incluyendo parejas (**40,50%, 81 de 200**), hijos e hijas (**34,00%, 68 de 200**), madres o padres (**26,00%, 52 de 200**) y hermanos/as (**29,50%, 57 de 200**).
- Si incluimos otros tipos de allegados, **176 de los 200 declarantes/denunciantes (un 88% del total) han sufrido, por sus publicaciones, la afectación de sus familiares o allegados inocentes con amenazas, citaciones, detenciones, vigilancia o pérdida del empleo**.

Todo este conjunto de evidencias demuestra que el control estatal no se dirige únicamente a la persona que se expresa o comunica en Internet, sino que se proyecta hacia su red afectiva como mecanismo de **intimidación ampliada**. Esta extensión tiene un impacto especialmente disuasorio: incrementa el costo percibido de expresarse, reduce la capacidad de organización social y fragmenta vínculos comunitarios, operando como una forma de coerción indirecta que multiplica el alcance de la vigilancia digital.

Este patrón reviste especial gravedad porque desplaza la sanción desde la conducta individual hacia el **entorno afectivo**, generando una lógica de *"responsabilidad por asociación"* que amplifica el miedo y erosiona el tejido social. La amenaza a familiares funciona como mecanismo de censura indirecta: incrementa el costo percibido de expresarse, reduce la denuncia y debilita redes de solidaridad. En términos de impacto, la vigilancia deja de ser un fenómeno individual y se convierte en una herramienta de **control social extensivo**.

REPRESIÓN Y VIGILANCIA TRANSNACIONAL

ESTÁNDAR INTERNACIONAL

El informe de denuncia evidencia que las prácticas de vigilancia y coerción no se limitan al territorio nacional, sino que se proyectan más allá de las fronteras, afectando a personas que residen en el exterior. Amenazas, advertencias y presiones ejercidas a través de familiares dentro de Cuba constituyen una forma de **represión transnacional**, reconocida crecientemente por el sistema de Naciones Unidas.

Los informes del ACNUDH (**Primer estándar global contra vigilancia masiva**, **Reconocimiento de spyware y vigilancia transnacional**, **Portal con todos los informes hasta 2024**) han señalado que los Estados pueden incurrir en violaciones de derechos humanos incluso cuando actúan indirectamente fuera de su territorio, especialmente cuando utilizan mecanismos de intimidación, vigilancia o coerción contra personas en el extranjero.

En este contexto, la actividad digital desde la diáspora no escapa al control estatal, y el espacio transnacional se incorpora al sistema de vigilancia mediante el uso de familiares como intermediarios involuntarios. Esta práctica amplía el alcance del control digital y vulnera el derecho a la libertad de expresión sin fronteras.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

El uso de familiares como mecanismo de presión configura una violación extraterritorial de derechos.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

133 de los 200 declarantes/denunciantes (el **66,50%** del total) reportaron **actos represivos contra ellos** (dentro de Cuba) **o sus familiares** (si el declarante/denunciante estaba fuera de Cuba) por publicaciones realizadas por el familiar (fuera el declarante/denunciante o un familiar suyo) que se encontraba fuera de Cuba. Sobre estos 133:

- Un **51,13%** de ellos (**68 de 133**) reportó **llamadas o mensajes amenazantes dirigidos a familiares dentro de Cuba**.
- Un **29,32%** de ellos (**39 de 133**) recibió **advertencias directas**.
- Un **15,79%** de ellos (**21 de 133**) indicó haber sido informado explícitamente de que debía **cesar su actividad digital** para evitar consecuencias sobre su familia.
- Un **1,5%** adicional (2 de 133), manifestó **otros hechos represivos o amenazantes sobre los familiares en la isla** por las publicaciones del familiar fuera de Cuba (citaciones y pérdida de la plaza universitaria de la hija).

Todo este conjunto de evidencias documenta que la vigilancia digital y sus efectos represivos operan más allá de las fronteras estatales, reforzando un ecosistema de control que afecta tanto a residentes en Cuba como a la diáspora, y que amplía el alcance de la coerción mediante la instrumentalización de vínculos familiares y afectivos.

BRECHA DIGITAL Y MONOPOLIO ESTATAL

ESTÁNDAR INTERNACIONAL

El entorno de vigilancia digital documentado se ve reforzado por **condiciones estructurales de acceso desigual a Internet**, derivadas del monopolio estatal del proveedor de servicios, los altos costos, las limitaciones técnicas y la baja calidad de la conectividad. Estas condiciones no son neutrales, sino que crean un entorno especialmente propicio para el control y la censura.

Las resoluciones del Consejo de Derechos Humanos han reconocido que el acceso a Internet es un habilitador clave de otros derechos, y que los Estados tienen la obligación positiva de promover un acceso asequible, equitativo y sin discriminación.[16] Cuando el Estado concentra el control de la infraestructura y restringe el acceso de manera estructural, se generan **limitaciones indirectas pero sistemáticas** al derecho a la información.

La brecha digital documentada en el informe de denuncia no solo limita la capacidad de informarse y expresarse, sino que profundiza desigualdades territoriales y sociales, afectando de manera desproporcionada a determinados grupos y regiones.

[16] Consejo de Derechos Humanos, Resolución 26/13, La promoción, protección y disfrute de los derechos humanos en Internet, A/HRC/RES/26/13 (26 de junio de 2014).

TEST DE LEGALIDAD Y PROPORCIONALIDAD

El monopolio estatal y las barreras económicas constituyen restricciones estructurales al derecho a la información.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- Un **80,00%** de los declarantes/denunciantes (**160 de 200**) considera que el acceso a Internet es **demasiado costoso** para un uso regular.
- Un **69,00%** de los declarantes/denunciantes (**138 de 200**) reportó **velocidades insuficientes** para informarse o acceder a contenidos audiovisuales.
- Un **49,50%** de los declarantes/denunciantes (**99 de 200**) indicó que el acceso a Internet está disponible solo en horarios limitados.
- Un **46,00%** de los declarantes/denunciantes (**92 de 200**) señaló problemas técnicos recurrentes del proveedor.
- Un **46,50%** de los declarantes/denunciantes (**93 de 200**) percibió desigualdades de acceso según la zona de residencia.
- Un **88,50%** de los declarantes/denunciantes (**177 de 200**) considera que estas limitaciones afectan de forma muy significativa su capacidad de informarse o participar en debates públicos.
- Solo un **7%** de los declarantes/denunciantes **(14 de los 200)** afirmó no haber experimentado dificultades relevantes de conectividad.

Todo este conjunto de evidencias documenta que **la combinación de altos costos, baja calidad del servicio, restricciones técnicas y bloqueos selectivos crea un entorno en el que el acceso a la información depende de factores económicos y políticos, y no del ejercicio libre de derechos**. En este sentido, **la brecha digital en Cuba no es un fenómeno accidental, sino un componente funcional del sistema de control, que refuerza la vigilancia digital y limita estructuralmente el pluralismo informativo**.

AUTOCENSURA Y RETRAIMIENTO DIGITAL

ESTÁNDAR INTERNACIONAL

Las prácticas descritas en los patrones anteriores producen un resultado previsible: la autocensura. El informe de denuncia documenta decisiones individuales de borrar contenido, reducir la participación en espacios digitales, abandonar grupos, cambiar de identidad digital o dejar de expresarse por temor a represalias.

El derecho internacional reconoce este fenómeno como **efecto inhibidor o chilling effect**, y lo considera una violación de la libertad de expresión incluso cuando no existe una sanción directa en todos los casos. **La Observación General Nº 34** subraya que el mero temor a la vigilancia o a represalias puede ser suficiente para restringir ilegítimamente el ejercicio de derechos.

La coexistencia de vigilancia digital, interferencias técnicas, sanciones legales, vigilancia física y represalias contra familiares crea un entorno en el que la autocensura se convierte en una estrategia racional de supervivencia. De este modo, la vigilancia digital cumple una función estructural: **reducir el espacio cívico sin necesidad de silenciar a todas las voces**, afectando al ecosistema comunicacional en su conjunto.

TEST DE LEGALIDAD Y PROPORCIONALIDAD

No es necesario castigar a todos: basta generar miedo estructural.

REFLEJO EN LOS HALLAZGOS BASADOS EN LAS 200 DECLARACIONES

- **El 55,50%** de los declarantes/denunciantes (**111 de 200**) **reportó haber modificado su comportamiento digital** como respuesta a la vigilancia y a las represalias asociadas.
- En concreto, un **24%** de los declarantes/denunciantes (**48 de 200**) afirmó que **dejó de publicar contenidos políticos** por temor.
- De forma complementaria, un **21%** (**42 de 200**) indicó que **borró publicaciones antiguas** con el mismo propósito.
- Un **13,50%** (**27 de 200**) señaló haber **abandonado grupos de WhatsApp, Telegram u otras plataformas** por temor.

- Un **21,50%** (**43 de 200**) afirmó haber **dejado de comunicarse con determinadas personas** para reducir su exposición.
- Un **18,50%** de los declarantes/denunciantes (**37 de 200**) afirma verse compelido a usar seudónimos.
- Un **19,00%** de los declarantes/denunciantes (**38 de 200**) reportó el **cierre o cambio de cuentas** en redes sociales o servicios de mensajería por temor.
- De los 200 declarantes/denunciantes, **160 expresaron un alto temor en alguno o varios de los canales de comunicación habituales**, siendo el promedio de temor de los 200 declarantes de **3,01 sobre un máximo de 5**.
- Los niveles promedio de miedo a denunciar o expresarse alcanzan valores elevados en **llamadas telefónicas** (**un promedio de temor del 3,37 sobre 5**), redes sociales como **Facebook** (**un promedio de temor del 3,31 sobre 5**) y **WhatsApp en grupos** (**un promedio de temor del 3,18 sobre 5**), mientras que se mantienen ligeramente inferiores —aunque aún significativos— en **videollamadas (un promedio de temor de 3,07 sobre 5)**, **Telegram** (**un promedio de temor del 2,80 sobre 5**), **WhatsApp uno a uno** (**media 2,80 sobre 5**) y **Signal** (**media 2,56 sobre 5**).

Todo este conjunto de evidencias documenta el alto nivel de temor en llamadas, redes y mensajería y que una parte sustantiva de la muestra adopta **múltiples estrategias de autocensura**, que afectan tanto a la producción de contenido como a las relaciones y dinámicas de participación en línea.

Nota adicional: a pesar de que la muestra contiene un gran número de familias de presos políticos y activistas de derechos humanos, los más resilientes a la represión, una proporción significativa de los declarantes/denunciantes, **el 55,50%** (111 de 200) **reportó haber modificado su comportamiento digital** como respuesta a la vigilancia y a las represalias asociadas. Por tanto, aunque un **44,50%** de los declarantes/denunciantes (**89 de 200**) indicó que no ha cambiado su comportamiento digital **a pesar del temor**, este dato no desvirtúa la existencia del efecto inhibidor, sino que debe interpretarse a la luz del contexto de la muestra, y nos da un indicativo claro de que la autocensura entre los no activistas de derechos humanos es aún más generalizada.

CONCLUSIONES DEL ANÁLISIS JURÍDICO NACIONAL E INTERNACIONAL

El análisis desarrollado a lo largo del presente bloque permite afirmar, con base empírica y jurídica suficiente, que la vigilancia digital en Cuba no constituye una práctica aislada, excepcional o limitada a contextos específicos, sino que responde a un **modelo estructural de control estatal**, diseñado y ejecutado mediante la convergencia de herramientas tecnológicas, marcos normativos restrictivos y prácticas administrativas y policiales sistemáticas.

Los hallazgos del informe de denuncia demuestran que las prácticas documentadas (Ciberpatrullaje, interceptación de comunicaciones, bloqueos de conectividad, vigilancia física derivada, uso de normas punitivas, represalias contra familiares, coerción transnacional y generación de autocensura) operan de manera coordinada y acumulativa, configurando un ecosistema de vigilancia incompatible con los estándares internacionales de derechos humanos.

Desde el punto de vista del **derecho interno**, el análisis evidencia que **el marco normativo cubano no actúa como un límite al poder estatal, sino como un habilitador de la vigilancia y la represión digital**. El monopolio estatal de las telecomunicaciones, la ausencia de órganos reguladores independientes, la inexistencia de control judicial efectivo y el uso de normas ambiguas, en particular el **Decreto-Ley 370** y determinadas figuras del Código Penal, configuran un sistema legal que permite:

- La vigilancia sin autorización judicial;
- La sanción de la expresión política mediante figuras imprecisas;
- La criminalización del disenso digital;
- La utilización del derecho administrativo y penal como instrumentos de intimidación.

Este entramado normativo vulnera de manera directa los principios de legalidad, necesidad, proporcionalidad y debido proceso, pilares esenciales del Estado de derecho conforme al derecho internacional.

Desde la perspectiva del **derecho internacional de los derechos humanos**, los hechos documentados constituyen violaciones sistemáticas de obligaciones asumidas por el Estado cubano en virtud del **Pacto**

Internacional de Derechos Civiles y Políticos y de los estándares desarrollados por los mecanismos de Naciones Unidas y del sistema interamericano. En particular, se constata la vulneración reiterada de:

- El derecho a la libertad de expresión (art. 19 **PIDCP**);
- El derecho a la privacidad y a la inviolabilidad de las comunicaciones (art. 17 **PIDCP**);
- La libertad de reunión y asociación (arts. 21 y 22 **PIDCP**);
- El derecho a la participación política (art. 25 **PIDCP**);
- El derecho a la vida privada y familiar; y,
- El derecho a un recurso efectivo y a las garantías judiciales.

El análisis demuestra además que muchas de las prácticas identificadas no cumplen ninguno de los criterios exigidos por el derecho internacional para admitir restricciones legítimas: no están previstas en leyes claras, no responden a fines legítimos en sentido estricto, no son necesarias ni proporcionales, y carecen de control judicial independiente.

Especial relevancia adquiere el **efecto acumulativo** de estas prácticas. Aunque cada una de ellas, considerada aisladamente, ya constituye una vulneración, su aplicación conjunta configura un sistema de control estructural que produce un efecto inhibidor generalizado sobre el ejercicio de derechos. **La autocensura documentada no es una consecuencia colateral, sino el resultado previsible y funcional de un modelo diseñado para desalentar la participación cívica, limitar el flujo de información y desarticular el disenso.**

Asimismo, el informe de denuncia demuestra que la vigilancia digital en Cuba no se limita al territorio nacional, sino que se proyecta de manera transnacional mediante represalias indirectas contra familiares, amenazas y mecanismos de presión dirigidos a personas en el exterior. Este elemento agrava la responsabilidad internacional del Estado, al extender los efectos de la represión más allá de sus fronteras.

En conclusión, el análisis jurídico desarrollado en este bloque permite afirmar que:

1. **La vigilancia digital en Cuba constituye una política de Estado**, no una suma de excesos individuales.
2. **El marco legal vigente no protege derechos, sino que facilita su restricción**, mediante normas amplias, ambiguas y carentes de control efectivo.
3. **Las prácticas documentadas violan de forma sistemática múltiples derechos humanos**, tanto en su dimensión individual como colectiva.
4. **Existe un patrón estructural de control digital**, orientado a la prevención del disenso, la disuasión de la participación y la fragmentación del tejido social.
5. **El efecto inhibidor resultante equivale, en la práctica, a una forma de censura generalizada**, incompatible con los estándares democráticos mínimos.

Este conjunto de elementos permite sostener, con fundamento jurídico sólido, que la vigilancia digital en Cuba no responde a necesidades legítimas de seguridad, sino que constituye un mecanismo de control político que vulnera obligaciones internacionales vinculantes y exige una respuesta por parte de los mecanismos internacionales de protección de derechos humanos.

CONCLUSIONES GENERALES

El presente informe de denuncia permite concluir, a partir de evidencia empírica sistematizada y de un análisis jurídico exhaustivo, que la vigilancia digital en Cuba no constituye un conjunto de prácticas aisladas o excepcionales, sino un **sistema estructural, intencional y sostenido de control estatal**, orientado a restringir el ejercicio de derechos fundamentales y a neutralizar el disenso político y social.

Los hallazgos permiten identificar un **modelo integral de vigilancia y represión**, caracterizado por la convergencia de:

- Mecanismos tecnológicos de monitoreo y control del entorno digital;
- Un marco normativo ambiguo y punitivo;
- Ausencia de garantías judiciales efectivas;
- Uso instrumental del derecho administrativo y penal; y,
- Una articulación directa entre vigilancia digital y represión física.

Este sistema opera de forma acumulativa, generando un **efecto inhibidor estructural** sobre la libertad de expresión, la participación política y el acceso a la información, tanto dentro como fuera del territorio cubano.

El análisis de los diez patrones identificados demuestra que:

1. **La vigilancia digital es sistemática y no excepcional**, dirigida principalmente contra personas con actividad cívica, política, informativa o de denuncia, pero con efectos expansivos hacia la población general.
2. **El monitoreo de redes sociales, mensajes privados y comunicaciones digitales** se realiza sin base legal clara, sin autorización judicial independiente y sin control posterior, vulnerando de forma directa el derecho a la privacidad y a la libertad de expresión.
3. **Los bloqueos de Internet, la degradación deliberada del servicio y la restricción del uso de VPN** constituyen mecanismos de censura indirecta, utilizados de manera selectiva en contextos de movilización social o circulación de información crítica.
4. **La vigilancia digital se articula con prácticas represivas presenciales**, como citaciones, interrogatorios, detenciones, vigilancia física y hostigamiento, configurando un sistema híbrido de control que traslada la represión del entorno digital al espacio cotidiano.
5. **El uso del marco normativo interno, especialmente el Decreto-Ley 370 y el Código Penal, funciona como instrumento de criminalización del discurso**, mediante figuras amplias, vagas y carentes de garantías, incompatibles con el principio de legalidad y con los estándares internacionales de derechos humanos.
6. **Las represalias contra familiares y la vigilancia transnacional** evidencian una estrategia de coerción indirecta que amplía el alcance del control estatal más allá del individuo y del territorio nacional.
7. **La brecha digital estructural y el monopolio estatal de las telecomunicaciones** no son meras deficiencias técnicas, sino elementos funcionales del sistema de control, que limitan el acceso a la información y refuerzan la dependencia del Estado.
8. Como consecuencia de todo lo anterior, se constata un **fenómeno generalizado de autocensura y retraimiento digital**, que afecta la participación ciudadana, debilita el debate público y vacía de contenido el ejercicio efectivo de la libertad de expresión.

Desde una perspectiva jurídica, las prácticas documentadas vulneran de manera sistemática múltiples obligaciones internacionales asumidas por el Estado cubano, en particular las derivadas del:

- Pacto Internacional de Derechos Civiles y Políticos;
- Declaración Universal de Derechos Humanos;
- Estándares del Consejo de Derechos Humanos de la ONU;
- Jurisprudencia y doctrina de la Comisión Interamericana de Derechos Humanos.

El análisis demuestra que la vigilancia digital en Cuba **no cumple con los principios de legalidad, necesidad, proporcionalidad ni finalidad legítima**, y que se utiliza como un mecanismo estructural de control político, incompatible con un Estado de derecho y con los estándares mínimos de una sociedad democrática.

En consecuencia, el informe de denuncia concluye que el sistema de vigilancia digital documentado constituye una **violación grave, sistemática y continuada de derechos humanos**, con impactos individuales y colectivos, y con efectos especialmente graves sobre la libertad de expresión, la vida privada, la participación política y el ejercicio de la ciudadanía.

RECOMENDACIONES

RECOMENDACIONES AL ESTADO CUBANO

1. **Cesar de inmediato las prácticas de vigilancia digital arbitraria**, incluyendo el monitoreo de redes sociales, la interceptación de comunicaciones y el acceso no autorizado a dispositivos.
2. **Derogar o reformar de manera sustancial el Decreto-Ley 370**, eliminando disposiciones vagas o incompatibles con la libertad de expresión, y garantizando: criterios claros de legalidad; control judicial previo; recursos efectivos contra sanciones.
3. **Revisar el Código Penal**, en particular las figuras relacionadas con propaganda, orden constitucional y difusión de información, para asegurar su conformidad con el artículo 19 del PIDCP.

4. **Garantizar la independencia judicial y el acceso a recursos efectivos**, incluyendo mecanismos para impugnar actos de vigilancia, decomisos y sanciones administrativas.
5. **Poner fin al uso de represalias contra familiares**, reconociendo la prohibición absoluta de castigos colectivos o indirectos.
6. **Adoptar medidas para garantizar el acceso libre, asequible y no discriminatorio a Internet**, eliminando bloqueos, censura técnica y restricciones arbitrarias.
7. **Establecer salvaguardias legales claras contra la vigilancia masiva**, en línea con los Principios de Necesidad y Proporcionalidad reconocidos internacionalmente.

RECOMENDACIONES A LOS MECANISMOS INTERNACIONALES DE DERECHOS HUMANOS

1. **Que el Consejo de Derechos Humanos de la ONU examine de manera específica la situación de la vigilancia digital en Cuba**, en el marco de sus resoluciones sobre libertad de expresión y privacidad.
2. **Que los Relatores Especiales sobre libertad de expresión, privacidad y defensores de derechos humanos soliciten información formal al Estado cubano** sobre: prácticas de vigilancia; uso de tecnologías de interceptación; aplicación del **Decreto-Ley 370**.
3. **Que la CIDH incorpore estos hallazgos en sus informes temáticos y de país**, y evalúe la adopción de medidas cautelares cuando existan riesgos graves para personas vigiladas.
4. **Que se promueva el monitoreo internacional del impacto de la vigilancia digital transnacional**, especialmente en relación con la diáspora cubana.

RECOMENDACIONES A LA COMUNIDAD INTERNACIONAL Y ACTORES TECNOLÓGICOS

1. **Exigir transparencia a los proveedores de servicios y tecnologías** respecto a su cooperación con autoridades cubanas.
2. **Abstenerse de suministrar tecnologías de vigilancia o espionaje** que puedan ser utilizadas para reprimir derechos humanos.
3. **Apoyar programas de protección digital, alfabetización en seguridad digital y acompañamiento a víctimas**, especialmente defensores de derechos humanos, periodistas y activistas.

RECOMENDACIONES FINALES

El presente informe de denuncia demuestra que la vigilancia digital en Cuba no es un fenómeno técnico ni coyuntural, sino un **componente central de un modelo de control político**. Su persistencia erosiona de manera profunda el espacio cívico, inhibe la participación ciudadana y debilita el ejercicio de derechos fundamentales.

Frente a este escenario, resulta indispensable una respuesta internacional firme, sostenida y basada en estándares jurídicos claros, que reconozca la gravedad del fenómeno y contribuya a la protección efectiva de las personas afectadas.

La vigilancia digital, cuando se ejerce sin límites, sin control y con fines represivos, no solo vulnera derechos individuales: socava las bases mismas de una sociedad libre.

PRISONERS DEFENDERS

+34 647 564 741

info@prisonersdefenders.org

prisonersdefenders.org

PRISONERS
DEFENDERS