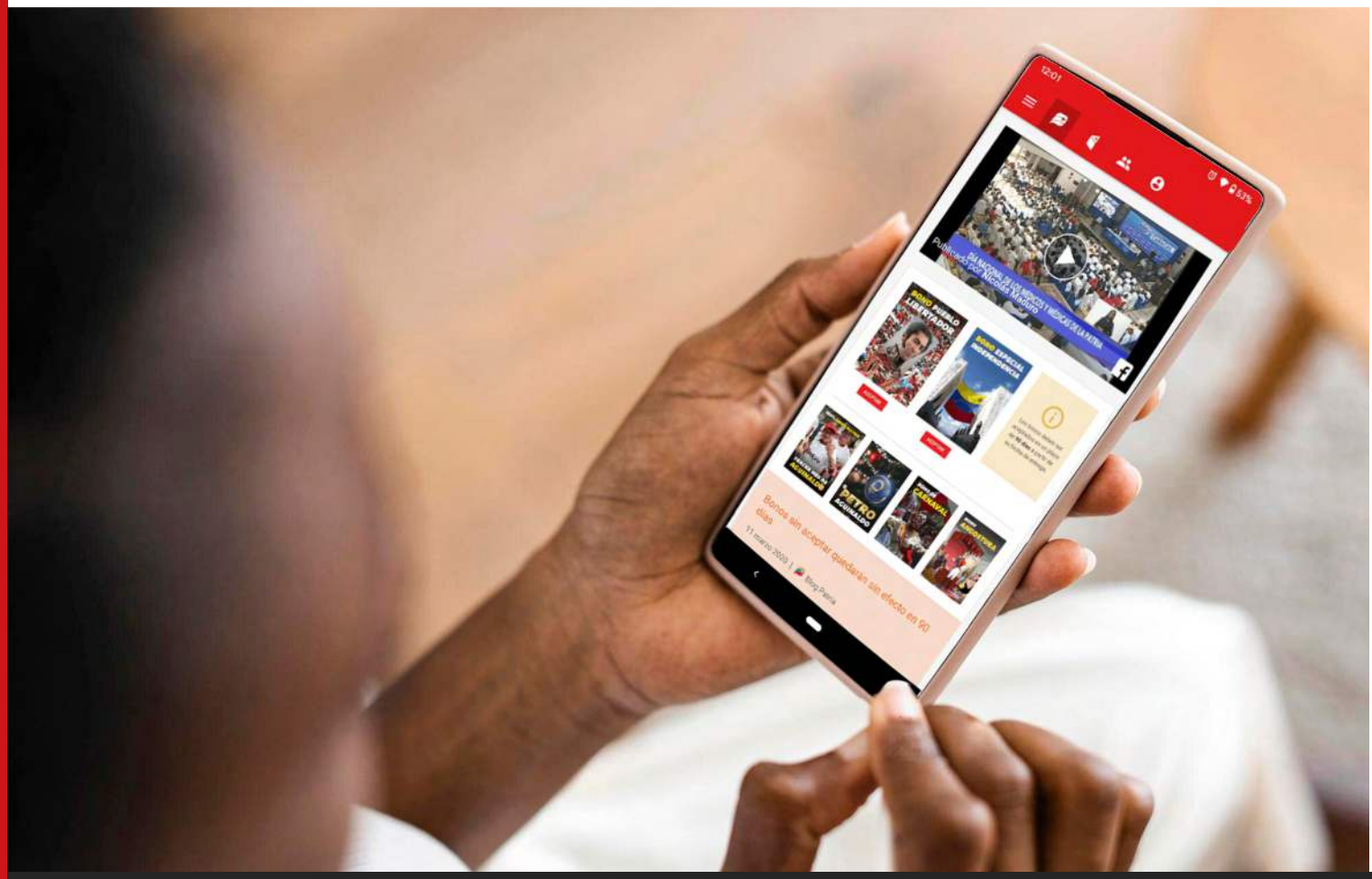
Privacidad y gestión de datos personales en Venezuela.

Evaluación de las aplicaciones ***VePatria*** y ***VenApp*** desde una perspectiva de derechos humanos.



Esta investigación fue realizada entre marzo y septiembre de 2024, por **Espacio Público.**

espacio público

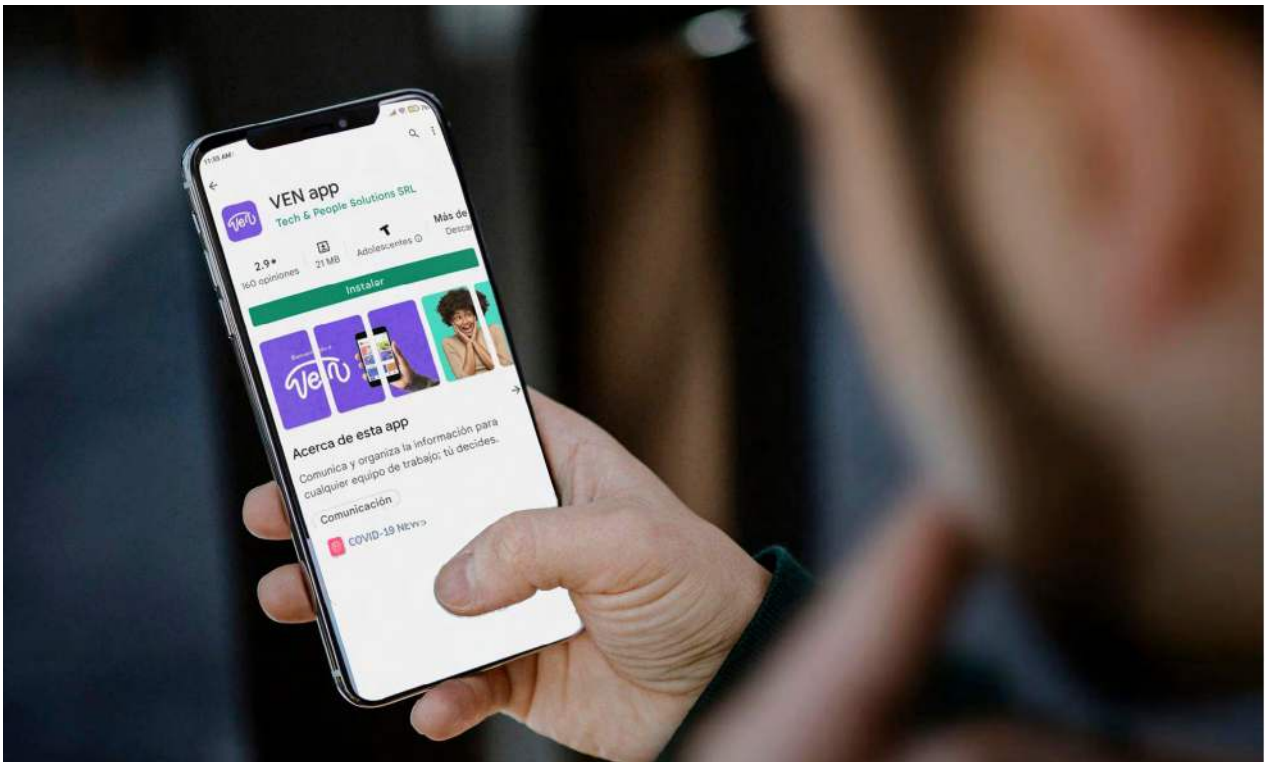
Resumen Ejecutivo

La investigación titulada “Privacidad y gestión de datos personales en Venezuela” analiza la situación crítica de los derechos humanos y la protección de datos personales en el país. Contextualiza la crisis estructural que afecta a Venezuela, caracterizada por la falta de independencia en los poderes públicos y un entorno gubernamental que criminaliza la contraloría ciudadana. Este contexto ha llevado a condiciones socioeconómicas adversas y a la aparición de un sistema de gobernanza disfuncional que limita los derechos civiles, provocando un incremento en la represión y la violación de derechos fundamentales.

El informe se centra en la evaluación de dos aplicaciones gubernamentales, *VePatria* y *VenApp*, que, aunque podrían servir a fines legítimos en un contexto democrático, en realidad parecen ser utilizadas para prácticas represivas y de control social. Los ciudadanos se ven obligados a proporcionar información personal a través de estas plataformas para acceder a servicios y recursos públicos, lo que compromete su privacidad y expone sus datos a un uso inadecuado por parte del Estado. Esta situación es denunciada como una violación a la privacidad y a los derechos humanos en el contexto de un gobierno que carece de una política garantista.

Metodológicamente, la investigación utiliza un análisis del marco legal vigente en Venezuela, un análisis de cumplimiento de los principios sobre protección de datos personales desarrollados por la Organización de Estados Americanos y Naciones Unidas, así como un estudio técnico de las aplicaciones mediante herramientas como Mobile Security Framework (MobSF) y Exodus Privacy. A través de estas herramientas e instrumentos, se identifican riesgos de seguridad en la gestión de datos y se evalúa el cumplimiento de principios internacionales sobre privacidad y protección de datos. Sin embargo, se destaca la ausencia de un marco legal robusto y la falta de políticas transparentes que regulen el tratamiento de la información personal.

La conclusión del informe subraya que el Estado venezolano no pro-



porciona garantías adecuadas para la protección de datos personales. A pesar de su extensa experiencia en la gestión de información, el gobierno carece de voluntad política para implementar medidas que resguarden la privacidad de los datos de los ciudadanos. Esto crea un entorno en el que se vulneran los derechos humanos, limitando la efectividad de las aplicaciones en beneficio de la ciudadanía y favoreciendo prácticas de control arbitrario.

Finalmente, las recomendaciones emitidas en el informe apuntan hacia la necesidad de establecer un marco legal robusto que garantice la protección de datos personales tanto a nivel estatal como privado. Este enfoque es esencial para permitir un ejercicio real de los derechos humanos en Venezuela, donde la evaluación crítica de las aplicaciones gubernamentales se funda en una revisión exhaustiva y fundamentada del contexto sociopolítico y normativo del país. La investigación también destaca la importancia de visibilizar estas violaciones para promover un cambio significativo en la gestión de los derechos humanos en el contexto venezolano.

Introducción

Venezuela atraviesa una crisis estructural que afecta el ejercicio y la garantía de los derechos humanos de su población, dentro y fuera del país. La falta de independencia entre los poderes públicos derivó en la ausencia de institucionalidad democrática y consolidó una gobernanza disfuncional guiada por esquemas arbitrarios, que criminaliza la contraloría ciudadana y rechaza abiertamente la rendición de cuentas.

En los últimos 10 años, a las limitaciones progresivas a derechos civiles y políticos se le sumaron peores condiciones socioeconómicas que estallaron en ciclos de alta conflictividad sin precedentes en la historia reciente del país. Esto incrementó lógicas represivas [1] asociadas a la discriminación por razones políticas, restricciones para la libertad de expresión y de contenidos, así obstáculos al trabajo de los medios de comunicación y periodistas. La necesidad de responder a estas crisis llevó a la implementación de tecnologías de la información atravesadas por el mismo enfoque opaco y poco transparente de la gestión gubernamental.

El presente informe busca evaluar dos aplicaciones promovidas por el Estado venezolano a fin de identificar si cumplen o no con los principios regionales y globales de protección de datos personales y aproximarse a los desafíos puntuales en la materia a partir de estas dos aplicaciones como expresión parcial de las políticas gubernamentales.

Para ello se abordará una primera sección sobre el marco legal general, que dará cuenta los instrumentos vigentes que favorecen y entorpecen una política estructural y garantista de protección de datos. Seguidamente se desarrolla una abordaje de la situación general del derecho a la privacidad y protección de datos personales con referencias a eventos puntuales que involucran el desempeño público y privado al respecto. Con ello se introduce al origen, contexto y variaciones de aplicaciones analizadas en función del contexto,

1 Al respecto: https://manifestar.org/2014-una-decada-de-represion-impunidad-y-resistencia/

lo que deriva en los resultados de la investigación tras la revisión del cumplimiento o no de los principios y evaluaciones de seguridad a partir de dos herramientas de análisis técnico. Y cierra con una serie de conclusiones y recomendaciones tanto a nivel público estatal como en términos de las responsabilidades de las empresas privadas en la gestión de datos.

Marco legal general

En Venezuela no existe una ley que regule la protección de datos personales pero diferentes legislaciones contemplan ámbitos específicos que se aplican a la gestión de datos e información personal. El instrumento más importante de estos es la Constitución Nacional que reconoce el derecho de toda persona a la protección de su vida privada e intimidad, además de indicar que regulará el uso de la información para garantizar dicha protección[2]. Y en otra sección contempla el derecho de acceder a la información propia, personal o sobre sí mismo que consten en registros privados y públicos[3].

A este marco constitucional le siguen en jerarquía legal varias consideraciones que son más explícitas sobre el principio de *habeas data*. Por ejemplo, la **Ley Orgánica del Tribunal Supremo de Justicia**[4] en el artículo 167 dispone el derecho a conocer los datos propios, la finalidad de dicha tenencia así como reconoce la posibilidad de exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de datos cuando resulten inexactos o agraviantes. Además contempla el recurso judicial cuando la administración de la base de datos no responda a los requerimientos.

La **Ley de Infogobierno**[5] establece la obligación a las instituciones públicas de notificar lo siguiente: las formas de recolección de información; su propósito, uso y con quién será compartida la información; además de ofrecer opciones de acceso, ratificación, supresión y oposición al uso de la misma; y las medidas de seguridad para su protección.

---

2 Artículo 60 de la Constitución Nacional. Recuperado en: https://venezuela.justia.com/federales/constitucion-de-la-republica-bolivariana-de-venezuela/titulo-iii/capitulo-iii/#articulo-60

3 Artículo 28 de la Constitución Nacional. Recuperado en: https://venezuela.justia.com/federales/constitucion-de-la-republica-bolivariana-de-venezuela/titulo-iii/capitulo-i/#articulo-28

4 Recuperado en: https://www.venelogia.com/uploads/PDF/Ley-TSJ-2010.pdf

5 Recuperado en: https://www.asambleanacional.gob.ve/leyes/sancionadas/ley-de-infogobierno

Por su parte, la **Ley Especial contra Delitos Informáticos**[6] contempla expresamente la *violación a la privacidad de la información*, la cual es entendida como apoderse o modificar intencionalmente información personal sin consentimiento de su dueño; la *violación a la privacidad de las comunicaciones* que es el acceso, captura, intercepcion, interferencia, reproducción, modificación, desviación o eliminación de cualquier mensaje de datos o señal de transmisión o comunicación ajena; y la revelación *indebida de información de carácter personal* a la que define como la difusión de la data o información obtenidos sin consentimiento por los medios indicados en los delitos anteriores.

La **Ley sobre Protección a la Privacidad de las Comunicaciones**[7] tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas. La ley establece que las comunicaciones privadas son inviolables y que solo pueden ser interceptadas o monitoreadas por orden judicial. La ley también establece que las empresas de telecomunicaciones deben tomar medidas para proteger la privacidad de sus clientes y están obligadas a tomar todas las medidas necesarias para garantizar la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones de sus usuarios.

La ley establece que el que arbitraria, clandestina o fraudulentamente grabe o se imponga de una comunicación entre otras personas, la interrumpa o impida, será castigado con prisión de tres a cinco años. En la misma pena incurrirá, salvo que el hecho constituya delito más grave, quien revele, en todo o en parte, el contenido de una comunicación privada.

Esta *Ley sobre Protección y Privacidad de las Comunicaciones* autoriza a las autoridades como policías y auxiliares de la administración de justicia a intervenir, impedir o interceptar comunicaciones para

---

6 Recuperado en: https://venezuela.justia.com/federales/leyes/ley-especial-contra-los-delitos-informaticos/gdoc/

7 Recuperado en: https://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/

fines de investigación penal[8]. Reconoce expresamente que tal acción debe ser solicitada y ordenada por Juzgado de Primera Instancia en un tiempo limitado y razonado. De no cumplirse el procedimiento la intervención sería ilegal, sin efecto probatorio, y contempla penas de hasta cinco años de prisión para los responsables.

La **Ley de Transparencia y Acceso a la Información de Interés Público**[9] no hace referencia alguna a datos o informaciones personales, ni establece procedimientos sobre su uso, a diferencia del proyecto de ley precedente del año 2016 que, además de definir su alcance, establecía el cese de la reserva cuando se tratare de investigaciones sobre violaciones a los derechos humanos o delitos de lesa humanidad. El acceso estaría condicionado por la decisión de un tribunal.

En una **sentencia de 2011**[10], la Sala Constitucional del Tribunal Supremo de Justicia estableció un marco normativo de carácter vinculante para la protección de datos personales en Venezuela. Este fallo define nueve principios esenciales, como la finalidad, la calidad, la exactitud y la seguridad de los datos, que deben ser cumplidos por cualquier norma o sistema que trate información de personas naturales o jurídicas.

La sentencia calificó como un derecho humano a la protección de datos de carácter personal. Estableció que toda normativa o sistema sobre datos personales que contenga información de cualquier tipo referida a personas físicas o jurídicas debe garantizar los siguientes principios:

> **Autonomía de la voluntad.** La necesidad de un consentimiento previo, libre, informado, inequívoco y revocable para el uso o recopilación de datos personales.

---

8 a) Delitos contra la seguridad o independencia del Estado;
b) Delitos previstos en la Ley Orgánica de Salvaguarda del Patrimonio Público;
c) Delitos contemplados en la Ley Orgánica sobre Sustancias Estupefacientes y Psicotrópicas; y
e) Delitos de secuestro y extorsión.

9 Recuperado en: https://www.asambleanacional.gob.ve/storage/documentos/documentos/ley-de-transparencia-y-acceso-a-la-informacion-publica-20210930233602.pdf

10 Expediente N° 04-2395. Recuperado en: https://vlexvenezuela.com/vid/german-jose-mundarain-hernandez-311569838

Legalidad. La recopilación de datos debe estar definida y limitada por un rango legal establecido.

Finalidad y calidad. La recopilación de datos personales debe responder a motivos o causas predeterminadas que no sean contrarias al ordenamiento jurídico constitucional.

Temporalidad o conservación. La conservación de los datos se extiende hasta el logro de los objetivos para los cuales han sido elaborados, o que justificaron su obtención y tratamiento.

Exactitud y autodeterminación. Los datos deben mantenerse exactos, completos y actualizados, respondiendo a la situación de la persona a la que se refiere. Y toda actividad que comporte la recopilación de datos personales puede ser objeto de control, el cual posee cada ciudadano/a frente a la información que le concierne.

Previsión e integralidad. La tutela de los derechos fundamentales vinculados con la recopilación de datos personales, debe plantearse inicialmente en relación con la protección del individuo contra la recopilación, el almacenamiento, la utilización y la transmisión ilimitada de dicha información.

Seguridad y confidencialidad. Es la necesaria garantía de confidencialidad, de no alteración de datos por terceros y del acceso a tales datos por parte de las autoridades competentes de conformidad con la ley. Por lo tanto, deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.

Responsabilidad. La violación del derecho a la protección de datos personales debe generar de conformidad con el ordenamiento jurídico aplicable, sanciones de tipo civil, penal y administrativas, según sea el caso.

Tutela. Toda persona tiene derecho constitucional a acceder a la información que los entes estatales y privados tengan sobre

sí misma. Es un derecho protegido por el marco legal y constitucional. La negación de este derecho es una violación grave de los derechos humanos.

Por último, se reseña una **providencia administrativa N°171** de la Comisión Nacional de Telecomunicaciones[11], que constituye una norma sublegal, e impone el deber de entregar varios datos personales a cambio de obtener el contrato para una línea telefónica, móvil o fija. Entre los datos se encuentran el documento de identidad, la firma, la impresión dactilar, el domicilio, su dirección de correo electrónico y una foto digital de su rostro, tomada al momento y en el sitio de la transacción. Este último procedimiento fue incorporado también como condición para concretar diligencias sobre líneas telefónicas, como cambios de equipos o de tarjetas SIM.

En general, de las disposiciones normativas referidas se entiende que cualquier dato personal o sobre bienes patrimoniales que reposen en instituciones privadas o públicas, deben ser tratadas con diligencia y responsabilidad bajo el reconocimiento y tratamiento que tienen las personas sobre sus datos. Algunas normativas, aunque aisladas, pueden servir de base para exigir mayores criterios y mecanismos de protección actualizados, acorde a los estándares actuales.

Por otra parte, existen iniciativas que resultan excesivas para la recolección de datos sensibles sin mayores garantías para las personas usuarias en materia de protección frente a vulnerabilidades digitales o ante la divulgación de información con actores de riesgo. En la práctica es esta voluntad no garantista la que se impone, ya que a pesar del carácter vinculante de varios de los principios internacionales de protección de datos personales en la jurisprudencia local, estos son escasamente referidos o aplicados.

11 Recuperado en: https://conatel.gob.ve/wp-content/uploads/2024/08/gaceta_41265.pdf

Situación general

En Venezuela el poco avance en un sistema legislativo se conjugó con el desarrollo de una crisis institucional a largo plazo que avanza hacia esquemas punitivos o sostiene restricciones innecesarias y desactualizadas respecto a las dinámicas que impone la conexión en línea; así como respecto a los avances en la región en materia de estándares internacionales de protección de derechos humanos.

La gestión de datos personales en Venezuela no es transparente ni rinde cuentas[12]. El Estado venezolano a través de diferentes entidades maneja a discreción bases de datos, desde el registro público civil hasta el electoral, sin dar a conocer a los responsables de la gestión, ni explicar el uso o los mecanismos de seguridad y protección. Por el contrario, los avances del Estado están orientados a prácticas restrictivas que limitan arbitrariamente el derecho a la privacidad, la mayoría de las veces con fines represivos; además de omitir abiertamente sus responsabilidades y obligaciones en materia de protección de datos personales y sensibles.

En 2019, el gobierno nacional[13] anunció la aprobación de 50 mil euros para la compra de *Cellebrite UFED Touch2*, unos dispositivos para hackear y extraer datos de teléfonos celulares, que son ampliamente usados por gobiernos represivos a nivel mundial. De acuerdo a la plataforma *Surveillance Watch*[14], dedicada a la documentación de las conexiones dentro de la industria de la vigilancia, Venezuela cuenta con seis tecnologías de vigilancia, además de *Cellebrite*, a saber: Blue Coat Systems (EE.UU), Digital Clues (Israel), Finfisher (Ale-

12 Entre 2018 y 2024, Espacio Público realizó seis peticiones de información a diferentes entes públicos (Presidencia, Ministerio de la Defensa, Ministerio del Interior, Vicepresidencia, Servicio de Administración, Identificación y Extranjería) sobre la gestión de datos personales, criterios de seguridad y protección de los datos respecto a diferentes iniciativas o políticas gubernamentales. Ninguna de las solicitudes fue respondida.

13 Venezolana de Televisión (2019). Jefe de Estado aprueba más de 12 millones de euros o su equivalente en petros para modernización del CICPC. Recuperado en: https://web.archive.org/web/20191115014106/https://www.vtv.gob.ve/millones-euros-petros-modernizacion-cicpc/

14 Recuperado en: https://www.surveillancewatch.io/

mania), Gamma Group (Reino Unido), Hacking Team (Italia) y Protei (Russia). En ninguno de los casos existe información pública disponible al respecto.

También en 2019, el Estado a través de la operadora pública estatal CANTV, clonó la página web *voluntariosxvenezuela.com* para robar información de las personas usuarias que subían sus datos para registrarse como voluntarias en la distribución de ayuda humanitaria[15]. La página fue una iniciativa del Poder Legislativo del momento, integrado en su mayoría por la oposición política al Gobierno Nacional. Luego, en abril de 2020, se registró otro episodio de *phishing* ejecutado por el Estado, esta vez a través de la plataforma *Héroes de la Salud*[16] para el registro de personal médico, iniciativa también promovida por sectores de oposición.

A partir del año 2020 se empezaron a registrar detenciones por publicaciones a través de aplicaciones de mensajería instantánea, específicamente *WhatsApp*; en su mayoría por difusión de información de interés público. Hasta 2023 se identificaron 20 detenciones arbitrarias por este motivo, la mayoría de las personas son acusadas en supuestos delitos de odio tras compartir información a través de estados o grupos de *WhatsApp*[17].

Al tratarse de una aplicación de mensajería instantánea, estas prácticas para castigar y limitar la expresión implican al menos esquemas básicos de vigilancia de contenidos con fines represivos. Los contenidos fueron compartidos en grupos con gran cantidad de usuarios; y a su vez, los estados permiten distintos niveles de alcance, por lo que terceros pueden tener acceso a las publicaciones. El uso de

---

15 Espacio Público (2019). El Estado roba información a usuarios web con página de phishing. Recuperado en: https://espaciopublico.ong/el-estado-roba-informacion-a-usuarios-web-con-paginas-de-phishing/

16 VeSinFiltro (2020). Informe Preliminar: Phishing del gobierno de Maduro contra plataforma Héroes de la Salud. Recuperado en: https://vesinfiltro.com/noticias/2020-04-26-phishing_heroes_salud

17 Espacio Público lleva un registro histórico de casos de violaciones a la libertad de expresión, lo que incluye la detención arbitraria de personas por la libre difusión de contenidos a través de diferentes medios, incluidas aplicaciones de mensajería instantánea. Al respecto consultar en: https://espaciopublico.ong/incitacion-al-odio-balance-de-una-ley-criminalizante-y-los-desafios-del-problema-real/

WhatsApp exige el registro de un número telefónico, dato que está al alcance de terceros y cuyo uso para perseguir implica una vulneración de la privacidad al constituir un mal uso de datos personales a través de dispositivos tecnológicos.

El uso de medios de comunicación públicos para promover la estigmatización hacia activistas, personas defensoras de derechos humanos, militantes de partidos de oposición, periodistas y trabajadores de la prensa, considerados de la "oposición política", es una práctica frecuente por parte de altos funcionarios. Esta práctica se apoya en el uso indebido de datos personales a los que se accede, sea a través de información disponible en redes sociales o posiblemente en bases de datos de instituciones públicas.

En abril de 2017, se inició una campaña de descalificación[18] hacia personas manifestantes que participaron en convocatorias opositoras. A través de la cuenta oficial en X del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), se difundieron fotos tomadas en las protestas con foco en los rostros de activistas sociales y personas defensoras de derechos humanos, que fueron calificados como «delincuentes». Esto dio lugar a la creación de etiquetas como #SonTerroristas y #DenunciaTuZona que se mantuvieron durante semanas. En este contexto, se dieron varias declaraciones de funcionarios en el canal del Estado, *Venezolana de Televisión*, que difundieron datos personales de "dirigentes opositores" que incluían direcciones, e incitaban a la persecución.

Los mecanismos de persecución a través del *Doxing*[19] se reactivaron a finales de julio de 2024 en el contexto de las elecciones presidenciales. Se registraron casos de detenciones por publicaciones en estados de *WhatsApp* y publicaciones de material audiovisual en redes sociales que criticaban al gobierno nacional, en una lógica de

18 Al respecto, las personas afectadas adelantaron una denuncia ante la Fiscalía. Más en: https://espaciopublico.ong/wp-content/uploads/2017/04/Denuncia-Instigaci%-C3%B3n-ODIO-Estado-venezolano-Espacio-P%C3%BAblico.pdf

19 El doxing es un tipo de ciberataque que implica la recopilación y publicación no autorizada de datos personales identificables de un individuo. A través de diversas técnicas, los atacantes buscan vulnerabilidades en la privacidad digital para exponer información sensible y perjudicar a sus víctimas.

delación promovida desde el Estado[20]. Autoridades ofrecieron líneas telefónicas[21], promovieron el uso de aplicaciones, incluida *VenApp*[22], para denunciar a personas manifestantes que participaron en protestas o divulgaron contenidos críticos al Gobierno Nacional. Se usó información como fotos, videos, direcciones y contenidos de redes sociales para criminalizar a las personas por su expresión política, y con ello facilitar sus detenciones arbitrarias. Cuerpos de seguridad difundieron videos que mostraban la presunta captura de personas tras su aparición en videos de protestas o donde se expresaban en contra del gobierno[23].

Por otra parte, algunas empresas privadas no distan mucho de la experiencia pública en cuanto a prácticas poco transparentes, situación que se ha hecho evidente en casos de especial riesgo como espionaje estatal o ataques a operadoras telefónicas.

La empresa española *Telefónica*, casa matriz de *Movistar Venezuela*, reveló en su informe de transparencia[24] de 2021 que intervino más de 20 % de las líneas telefónicas y de internet de sus clientes en el país por órdenes del gobierno, la mayoría sin mediación de una orden judicial. Esto representó un total de 1.584.547 líneas de clientes en Venezuela.

Además de las intervenciones, un total de 997.679 líneas fueron afectadas por solicitudes de metadatos, que según *Telefónica* tienen como objetivo obtener datos históricos referidos a:

---

20 Varios casos fueron documentados por Espacio Público, pero no se ofrecen detalles por razones de seguridad y protección de las víctimas y sus familias.

21 Cuenta de Instagram de la Delegación Distrito Capital del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC). Recuperado en: https://www.instagram.com/reel/C-OHvjSpBQB/?igsh=MWFyNnlwYW84eG9iZg==

22 TalCual (30 de julio de 2024). Maduro pide denunciar en la VenApp a opositores que hayan «agredido al pueblo». Recuperado en: https://talcualdigital.com/maduro-pide-denunciar-en-la-venapp-a-opositores-que-hayan-agredido-al-pueblo/ / Más en: https://manifestar.org/la-represion-poselectoral-y-exposicion-de-datos-personales/

23 Tik Tok, gnbnuevaluchad112. Recuperado en: https://www.tiktok.com/@gnbnuevaluchad112/video/7400192472883711238

24 Recuperado en: https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf

- Nombre y dirección del usuario registrado.

- Datos para identificar el origen y destino de una comunicación. Esto incluye número de teléfono y nombres de usuario para servicios de internet.

- Fecha, hora y duración de una comunicación.

- Tipo de comunicación e identidad de los equipos de comunicación (como números IMSI e IMEI).

- Localización del dispositivo del usuario.

La empresa fue consultada al respecto a través de una petición de información que nunca fue respondida. Esto resulta especialmente grave al considerar que la empresa facilitó prácticas violatorias de derechos humanos al ofrecer al Estado, sin justificaciones legítimas y razonables, información sobre comunicaciones privadas en un contexto político represivo, lo que pudo sumar a procesos judiciales y detenciones arbitrarias contra sectores criminalizados.

A inicios de 2024 se conoció públicamente de la ocurrencia de un ataque a la operadora telefónica *Digitel*, una de las tres operadoras que dominan el mercado local, con aproximadamente ocho millones de usuarios/as, según datos de 2020. Según un portal especializado[25], el ciberataque ocurrió el 30 de enero, mientras que la empresa anunció en su página web que detectó una amenaza de seguridad en su sistema y bloqueó "temporalmente" sus servidores para prevenir hackeos y filtraciones de información. Pero no fue sino el 1° de febrero que comunicó formalmente, sin dar mayores detalles, la "incidencia ocurrida en días pasados".

Los datos personales de millones de usuarios fueron divulgados el 12 de febrero por un grupo de hackers que usaron el *ransomware Medusa* para acceder a la red de la empresa y encriptar la información de sus servidores. Los clientes no recibieron ningún tipo de aviso,

25 Asilo Digital. 2 de febrero de 2024. ¿Qué está pasando con el hackeo a Digitel? seguimiento en vivo. Recuperado de: https://www.asilodigital.com/que-esta-pasando-con-digitel/

advertencia, notificación o explicación al respecto. Ante una petición de información realizada a la empresa[26] respecto al ataque y su impacto en la seguridad de los datos de los usuarios, la empresa se limitó a indicar que no tenía responsabilidad ni obligación legal en ofrecer ese tipo de información.

En general, esto pone en evidencia la falta de medidas a implementar por parte de los entes, organismos y/o empresas para proteger los datos de los usuarios; no se gestionaron mecanismos para informar debidamente a los usuarios sobre los riesgos, los alcances del daño y las medidas de contención.

26 Espacio Público y VeSinFiltro realizaron una petición de información a la empresa Digitel en mayo de 2024, la cual no fue debidamente respondida.

Aplicaciones, tecnologías de la información y manejo de datos personales

Desde hace 15 años, el Estado venezolano ha desarrollado y usado recursos tecnológicos para la gestión de datos personales a fin de facilitar el ejercicio de derechos civiles, políticos y sociales. La creación del pasaporte biométrico, la incorporación de captahuellas en el sistema electoral, y la construcción de un sistema biométrico para la seguridad alimentaria, fueron avances progresivos pero constantes que se gestaron de forma paralela a la disminución de garantías democráticas e institucionales.

VePatria

Para el sistema biométrico de acceso a alimentos se creó en 2015 el *Carnet de la Patria*, un documento inteligente con Códigos QR que almacena datos personales, a partir del cual se reguló la distribución de alimentos. El Carnet se instaló en medio de una crisis caracterizada por la inflación y la escasez, lo que condicionó a la población a someterse a la cesión de sus datos como casi la única opción para acceder a alimentos a precios asequibles, en medio de una pobreza generalizada[27].

En 2018, se consultó al Estado a través de una petición de información sobre los responsables de la gestión de los datos personales recogidos a través del *Carnet de la Patria*, qué tipo de sistemas de información se usaron, qué mecanismos garantizaban la seguridad de la información, y cómo los usuarios podían acceder a sus datos. La solicitud de información hecha al Poder Ejecutivo nunca fue respondida.

Tras la instalación estatal de un sistema biométrico para regular el acceso a alimentos, diferentes entes privados también hicieron uso

27 Al respecto: https://accesoalajusticia.org/coaccion-social-y-control-politico-a-traves-del-carnet-de-la-patria/

de la huella digital para ofrecer sus servicios: bancos, farmacias, restaurantes y locales de diverso tipo han incorporado este sistema. A la fecha, se masificó el uso del *Biopago,* un dispositivo desarrollado por el Estado a través de la banca pública para el pago de bienes y servicios mediante la autenticación biométrica, sin el uso de tarjetas de crédito o débito, que puede ser usado desde distintos bancos privados[28], lo que supone al menos la divulgación de datos de los clientes de la banca privada a la pública, con un alcance desconocido.

Al sistema biométrico se articularon más programas de asistencia social, como diferentes tipos de "bonificaciones". En definitiva, el Estado incrementó la dependencia al sistema biométrico como única opción para acceder a subsidios y planes de asistencia pública, en medio de una emergencia humanitaria compleja, además de extenderlo a todo tipo de pagos para el acceso a múltiples bienes y servicios. Así se consolidó entonces el *Sistema Patria*[29] que comprende cuatro aplicaciones: *VeQR* y **VePatria** que gestionan el *Carnet de la Patria; VeMonedero* y *Billetera Móvil*, que funcionan para la consulta de saldo y medios de pago de los subsidios.

VenApp

En diciembre de 2022, el Poder Ejecutivo inició la promoción de la aplicación *VenApp* como una herramienta para "la conexión directa de los usuarios con el presidente Maduro", a fin de brindar respuestas inmediatas a las comunidades que requieren atención en materia de servicios públicos. *Línea 58* es la sección específica para dichas demandas en fallas de servicios como agua, electricidad, vialidad, infraestructura pública, etc. La aplicación ha sido ampliamente promovida por autoridades públicas, ofreciéndola muchas veces como única opción para canalizar y dar respuesta a los problemas en los servicios públicos.

28 Más en: https://efectococuyo.com/economia/biopago-bancos-privados-2021/

29 Recuperado en: https://www.patria.org.ve/

De acuerdo con la sección de términos y condiciones, *VenApp* es una aplicación móvil y página web, ambas de intermediación comercial y con diversos servicios asociados, desarrollados por la sociedad de comercio VEN CORPORATION, C.A. Es una plataforma que ofrece varios servicios, y *Línea 58* es uno de ellos, por lo que está integrado a otros servicios distintos al de denuncia a las autoridades.

Ante la falta de información regular y actualizada sobre las contrataciones públicas, se desconocen los términos de los servicios prestados a la administración pública. Desde la vocería gubernamental ha sido divulgada como una creación del Gobierno Nacional[30], mientras que una investigación periodística señala que la aplicación fue desarrollada por una firma panameña, bajo la dirección de André Golabek, un brasileño vinculado a una empresa de comunicación política. Dicha empresa está involucrada con cientos de cuentas falsas que difundieron desinformación en apoyo a candidatos en Bolivia, gobernantes en Venezuela y funcionarios en Panamá, Bolivia y República Dominicana[31].

La aplicación ha sido ampliamente utilizada para mediar el acceso a servicios públicos, incluída la atención médica de urgencia en hospitales públicos, la gestión de operaciones quirúrgicas y entrega de insumos médicos[32]. Recientemente, en el marco de la represión de las protestas poselectorales, Maduro anunció el 30 de julio[33] una modificación de la aplicación, la creación de una opción para que los usuarios "denuncien a los que han atacado al pueblo para ir por ellos y hacer justicia"; la nueva categoría se denominó "guarimba

---

30 Venezolana de Televisión (2023). VenApp aplicación que facilita acceso a productos y soluciones de servicios públicos. Recuperado en: https://www.vtv.gob.ve/venapp-aplicacion-facilita-acceso-productos/

31 Cazadores de FakeNews (2023). Venqis: un brasileño, big data y una granja de trolls caribeña. Recuperado en: https://www.cazadoresdefakenews.info/venqis-un-brasileno-big-data-y-una-granja-de-trolls-caribena/

32 Al respecto: https://runrun.es/rr-es-plus/560820/venapp-tambien-se-sumo-a-la-campana-oficialista/

33 Transmisión en vivo en X, @NicolasMaduro, 30 de julio de 2024. Recuperado en: https://x.com/i/broadcasts/1rmxPoWDqqZJN

fascista"[34], e incluyó diferentes subcategorías de denuncias como *saqueos, alteración del orden público, desinformación y daños al patrimonio público*[35].

Tras el anuncio presidencial, se registró la salida de esta aplicación de las principales tiendas de descarga, lo que llevó al gobierno a activar vías de descarga alternas, incluidas algunas más riesgosas en materia de seguridad. En la página web de la aplicación[36] se indica expresamente que se deben otorgar permisos para instalar aplicaciones desconocidas, lo que lleva a la descarga de archivos riesgosos que no permiten en algunos casos correr los análisis de antivirus.

En definitiva, el Estado venezolano ha usado tecnologías de información y practica regularmente la recolección masiva de información personal sin cumplir con criterios básicos de responsabilidad, transparencia y contraloría. Contrario a los estándares internacionales, el Estado ignora activamente sus obligaciones en materia de protección de datos, al punto de no rendir cuentas, divulgar con terceros y empresas privadas datos personales de ciudadanos/as, sin explicar las condiciones ni los términos de tales intercambios, e incluso ha usado y modificado las plataformas para facilitar la persecución por razones políticas.

Para este informe, el objetivo es evaluar dos aplicaciones promovidas por el Estado venezolano, *VePatria* y *VenApp*, específicamente sus políticas de privacidad y algunas dinámicas de funcionamiento, a la luz de las garantías necesarias para la protección de datos personales desde la perspectiva de derechos humanos.

---

34 Forma despectiva de calificar a las protestas antigubernamentales por parte autoridades públicas.

35 Recuperado en: https://proboxve.org/publicacion/terrorenredes-venapp-la-aplicacion-que-evolucio-no-para-reprimir/

36 Recuperado en: https://www.venapp.com/

Análisis de resultados

A partir de los *Principios actualizados sobre la privacidad y protección de datos personales de la Organización de Estados Americanos*[37] junto a los *Principios que informan la privacidad y protección de datos personales* de la Relatoría especial sobre el derecho a la privacidad de Naciones Unidas[38], se desarrolló un cuestionario[39] para medir el cumplimiento general de tales principios en las aplicaciones *VePatria*[40] y *VenApp*[41] de acuerdo a sus políticas de privacidad. También se utilizaron dos herramientas: *Mobile Security Framework* (MobSF), para realizar pruebas estáticas de malware en ambas aplicaciones para identificar riesgos de seguridad en la gestión de datos; y *Exodus Privacy*[42] una plataforma que audita rastreadores incrustados en aplicaciones de Android.

Legitimidad

Ninguna de las aplicaciones detalla, cita o se refiere a alguna ley o instrumento que regule el tratamiento/recopilación de datos. A pesar de la falta de una ley de protección de datos, existen diferentes instrumentos que aunque aislados, ofrecen garantías legales mínimas para la protección de los datos, como la Ley Orgánica del Tribunal Supremo de Justicia[43] o Ley de Infogobierno[44], que establecen parcialmente varios de los principios de protección contemplados en los estándares internacionales.

---

37 Recuperado en: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

38 Recuperado en: https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data#:~:text=S%C3%ADmbolo%20ONU%20A%2F77%2F196%20Resumen%20Los%20principios%20que%20informan,de%20interpretaci%C3%B3n%20y%20de%20integraci%C3%B3n%20del%20ordenamiento%20normativo.

39 En Anexo.

40 Recuperado en: https://www.patria.org.ve/vePatria/politicas-privacidad/

41 Recuperado en: https://venapp.com/politica-de-privacidad-terminos-y-condiciones-de-uso/

42 Recuperado en: https://exodus-privacy.eu.org/en/

43 Ver arriba.

44 Ver arriba.

Transparencia y consentimiento
En ningún caso se específica la identidad o los datos de contacto del responsable específico de la gestión de datos. Solo en *VenApp* se dispone de un correo electrónico genérico de contacto, que no diferencia a los términos y condiciones de las políticas de privacidad. *VePatria* no dispone de ningún contacto.

VePatria tampoco específica los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, ni el tipo de información o datos que puede compartir. Por su parte *VenApp* lo hace de manera parcial, al indicar que **pueden compartir los datos con: fuerzas del orden público, agentes de salud pública, otras entidades gubernamentales, aeropuertos, y otros terceros según sea necesario**. Esto resulta especialmente grave ya que no específica condiciones legítimas mínimas para compartir la información, como la existencia de una orden judicial que dé cuenta de alguna investigación en curso. No se plantean ni detallan los motivos legales, legítimos y razonables que deberían cumplirse para poder compartir tales datos. No específica tipos de datos a compartir al referirse genéricamente a “datos personales”.

Pertinencia y necesidad
Ambas aplicaciones demandan cuentas creadas con usuario y contraseña para garantizar el acceso, esto significa la captura de datos como nombre, apellidos, correo electrónico y números de teléfono e incluso direcciones físicas. Y para el uso de determinados servicios exige datos sensibles como la ubicación georreferenciada en el caso de *VenApp* para la atención de las denuncias de servicios públicos, por ejemplo.

VePatria cuenta con varios formularios según los perfiles de los usuarios y los tipos de programas sociales que dispone, entre el tipo de información que recoge está situación laboral, tipo de sector con que trabaja el usuario, si es privado, público o independiente; nivel de estudios; tipos de oficios o entretenimientos favoritos; hasta el manejo de ingresos económicos; la frecuencia de alimentación (cuántas veces se alimenta la persona al día); si tienen alguna discapacidad, enfermedad, o recibe algún tratamiento médico.

VenApp establece los tipos de datos que recopila, a saber:

- Perfil del usuario (Nombre y apellido, correo electrónico, número de teléfono, nacionalidad, dirección, foto de perfil, provincia, ciudad, municipio, parroquia, información bancaria, incluyendo la utilizada para verificación de los pagos).

- Datos demográficos basados en el perfil, cookies, google analytics e incluso a través de encuestas.

- Contenido creado (uso de los canales, los reportes, denuncias, solicitudes, y sugerencias que realizan. Esto puede incluir comentarios, fotografías, ubicación u otros, así como mensajes directos o por correo, como por ejemplo preguntas, sugerencias de mejora o quejas).

- Datos de listas de contactos, para la comunicación interna entre usuarios.

- Datos de ubicación para el envío de reportes de incidentes georreferenciados.

- Datos de uso como tiempo de permanencia en la aplicación, los flujos de navegación, fecha y la hora de acceso, fallos de la app, y otras actividades del sistema.

En ambos casos se trata de información relevante para la gestión se servicios que ofrecen, pero la ausencia de criterios que reconozcan y por lo tanto presten atención especial a la protección de estos datos sensibles, representa un factor de riesgo para los usuarios/as ante la falta de garantías sobre uso debido y seguro.

Tratamiento y conservación limitados

En ambos casos, las finalidades para el uso de la información no son lo suficientemente explícitas y detalladas. Por lo que resulta difícil determinar si estos fines son compatibles, o no, con la información recopilada. Si nos centramos en la gestión directa de servicios como atención a fallas de servicios geolocalizada o la asistencia social en función del acceso o no a recursos económicos, podría ser legítima la solicitud de cierta información personal; sin embargo en ambos

casos el problema radica en la abierta posibilidad de compartir la información con terceros según criterios legales no explícitos, que no tienen que responder a órdenes judiciales, por lo cual el intercambio y la divulgación de los datos no tiene fines claros en ningúna de las dos aplicaciones. Además, tampoco establecen tiempo límite justificado para la conservación de los datos.

En el caso de *VePatria* plantea generalidades "como potenciar la organización del Poder Popular y las Misiones Sociales en Venezuela" o que los fines están "siempre dentro de la competencia y atribuciones de vePatria, conectar el Carnet de la Patria con el movimiento Somos Venezuela", sin detallar tales competencias ni atribuciones y además plantea la posibilidad de compartir la información con el "Movimiento Somos Venezuela", un partido político promovido por el Gobierno Nacional.

VenApp plantea que su recopilación tiene los siguientes fines: mejora de servicios, soporte al cliente, promociones, servicios del desarrollador, procedimientos y requisitos legales e intercambio y divulgación de datos. En los últimos dos casos nuevamente ignora el criterio de orden judicial cuando se trata de investigaciones oficiales, no plantea los motivos por los cuales las entidades gubernamentales podrían acceder de forma legítima a los datos, y tampoco cita legislaciones específicas que justificaría un potencial acceso a la información de las personas usuarias. La sola petición de organismos reguladores, entidades gubernamentales no es un criterio válido en sí mismo que justifique acceso a información y datos personales por parte de autoridades, lo que es más riesgoso en contextos no democráticos.

Confidencialidad

En ambas aplicaciones, se plantea la posibilidad de compartir la información con terceros bajo criterios poco claros e incluso ilegítimos, como el caso de *VenApp* que de forma explícita dice poder compartir datos de usuarios con fuerzas del orden público, agentes de salud pública y otras entidades gubernamentales, sin definir motivaciones razonables o demandar órdenes judiciales. Además indica que divulgará la información en caso de que sea lo más apropiado por asuntos de seguridad, sin embargo, no define en detalle bajo qué

criterios divulgar los datos es apropiado, o no, o cuáles serían esos asuntos de seguridad, de qué o de quién, y tampoco indica quién establece tal condición ni bajo qué mecanismos o procedimientos se define dicha decisión.

VePatria por su parte dice garantizar "la confidencialidad de los datos personales de los usuarios que se registren mediante los formularios". También señala que "Sin perjuicio de sus facultades legales, sólo efectuaremos tratamiento de datos personales respecto a aquellos que han sido entregados voluntariamente." Sin embargo, no específica en qué consiste ese tratamiento de datos ni establece mecanismos sobre sus atribuciones al respecto, las cuales son referidas sin detalle para notificar que puede compartir la información con el partido político "Movimiento Somos Venezuela".

Seguridad de los datos

En ninguna de las aplicaciones se hace referencia, al menos general, a las medidas para resguardar la seguridad de la información suministrada por las personas usuarias. En el caso de *VePatria* sólo se plantea el uso de "sistemas muy avanzados que se actualizan constantemente" para invocar seguidamente y reiterar la posibilidad de compartir los datos personales por "motivos legales", sin especificar normativas específicas ni referir expresamente la necesidad de una orden judicial, ni los actores a los cuales sería divulgada la información. *VenApp* por su parte sólo indica que sus medidas son "robustas", sin ofrecer mayor información.

VePatria y *VenApp* tampoco refieren ni hacen explícita su obligación de informar de manera oportuna a las personas usuarias sobre potenciales riesgos de seguridad respecto a sus datos personales.

El informe de análisis estático de MobSF (Mobile Security Framework) sobre las aplicaciones en estudio encontró varios problemas de seguridad y acceso a la información de los usuarios. De acuerdo con el análisis de los factores de riesgos asociados a seguridad e información que demandan, *VePatria* tiene un índice de 45/100 y un riesgo medio. *VenApp* indica un riesgo alto con una calificación de 37/100. Estas aplicaciones solicitan mucha información y permisos pero no garantizan adecuadamente la privacidad de los datos recolectados. Sobre la seguridad de la aplicación resaltan los siguientes aspectos: Las aplicaciones están firmadas con el esquema de firma v1, lo que las expone a la vulnerabilidad Janus[45] en Android 5.0-8.0; las aplicaciones se pueden instalar en versiones antiguas de Android que tienen vulnerabilidades sin parchear.

En lo relativo a los datos sensibles almacenados se encontró información sensible como contraseñas y claves almacenados en texto plano en el código fuente de las aplicaciones, se solicitan permisos

45 La vulnerabilidad de Janus es una falla de seguridad descubierta en Android que permitía a atacantes modificar el código de aplicaciones sin que el sistema operativo lo detectara. Esto se lograba manipulando los archivos APK (Android Package Kit) de manera que el sistema operativo considerara la aplicación como legítima, incluso si se había introducido código malicioso.

innecesarios, como el acceso a la ubicación y al historial de llamadas. Y además las aplicaciones se comunican con servidores que podrían ser maliciosos.

Y sobre problemas de seguridad de nivel informativo, las aplicaciones recogen información sensible en los registros de depuración, lo que podría permitir a los atacantes acceder a esta información; y utilizan componentes exportados que no están protegidos adecuadamente, lo que podría permitir también acceso a atacantes.

En general, las aplicaciones *VePatria* y *VenApp* tienen problemas de seguridad que podrían facilitar el acceso a datos sensibles, el espionaje de los usuarios y causar otros daños.

Se realizó un análisis estático a través de la plataforma *Exodus*. Los resultados revelan una diferencia en sus prácticas de recopilación de datos y permisos solicitados, pero coinciden en general con el análisis de MobSF.

VePatria no presenta rastreadores conocidos y solicita únicamente tres permisos, uno de los cuales se clasifica como “peligroso” o “especial”, según los estándares de *Google*. Aunque este último punto requiere una evaluación más detallada, en general, *VePatria* parece ser menos intrusivo en términos de privacidad del usuario que *VenApp*. Esta última muestra un comportamiento mucho más riesgoso; se identificaron siete rastreadores diferentes y exige hasta 44 permisos, incluyendo 11 considerados “peligrosos” o “especiales”. Esta cantidad y tipo de permisos indican una recopilación intensiva de datos del usuario, lo que podría representar un riesgo significativo para su privacidad.

Exactitud, Acceso, Rectificación, Cancelación, Oposición y Portabilidad

VenApp ofrece la posibilidad de corregir o actualizar la información a través de la configuración de privacidad, específicamente las asociadas a datos de ubicación, notificación de los reportes sobre denuncias de servicios, y las notificaciones de contenido (avisos sobre nuevos mensajes, ofertas o promociones); y mediante los permisos

del dispositivo, los vinculados a cámara y almacenamiento. La política de privacidad de *VenApp* no hace referencia a la posibilidad de modificar los datos personales necesarios para los inicios de sesión y el mantenimiento de las cuentas. Es posible enviar una solicitud de eliminación de la cuenta, sin embargo, la aplicación puede conservar los datos si es necesario para cumplir “requisitos legales”, sin mayores detalles.

VePatria no plantea expresamente en sus políticas el derecho de corregir o actualizar, pero si se pueden modificar los datos en los formularios. Tampoco establece los derechos de cancelación, oposición y portabilidad de los datos, ni en las políticas de privacidad ni como opción dentro de la aplicación.

Datos personales sensibles

Ninguna de las aplicaciones refiere ni reconoce explícitamente la existencia de datos personales sensibles, al tratarlos a todos como “información” o “datos personales”. En consecuencia, tampoco establece criterios o mecanismos específicos para su protección diferenciada.

Responsabilidad

Como se indicó en la sección de Transparencia, ninguna de las aplicaciones establece la identidad del responsable de la gestión de datos. Sólo en un caso se dispone un correo para cuestiones relativas a términos, condiciones y políticas de privacidad, sin individualizar la administración y tratamiento de los datos.

Conclusiones y recomendaciones

El Estado venezolano no ofrece garantías para la protección de datos personales a la población en general. A pesar de tener amplia experiencia en el manejo y gestión de bases de datos y su uso en tecnologías de la información de diversos tipos desde hace al menos 15 años, carece de voluntad política para la implementación de criterios realmente garantistas que protejan la privacidad de los datos, lo que resta condiciones para el ejercicio de derechos humanos.

La implementación de *VePatria* y *VenApp,* que podrían tener fines legítimos en un contexto democrático y respetuoso del Estado de Derecho, pierde efectividad para la ciudadanía en tanto termina siendo útil para prácticas represivas y de control social. A través de un acceso a recursos y servicios públicos condicionado a la entrega de información personal, se somete a los usuarios a un uso irresponsable y no transparente de sus datos, expone a las personas a criterios discrecionales que son usados con fines desconocidos sin ningún tipo de contraloría, lo que facilita accesos indebidos y dinámicas de persecución.

Es necesario un sistema integrado de normas, procedimientos y prácticas que garanticen de forma efectiva el derecho a la privacidad, bajo principios de transparencia, contraloría e independencia y demás criterios contemplados en los estándares regionales y globales de protección de datos.

Un sistema con principios garantistas debe excluir regulaciones o iniciativas excesivas en la recogida de datos sensibles, que faciliten dinámicas de control y seguimiento o uso indebido desde el Estado, terceros particulares o privados. Debe incluir mecanismos de acceso y control de la información por parte de las personas usuarias así como gestiones auditadas bajo mecanismos claros, determinados y conocidos, que permitan la actualización regular y responda a criterios objetivos y realistas de la gestión de datos a escala digital y *offline*. La independencia de poderes públicos en un auténtico sistema democrático es clave para concretar una gestión independiente y garante de los derechos humanos civiles y políticos relacionados

con el tratamiento de datos personales.

Por su parte, un sistema integrado junto a una práctica coherente con la perspectiva de derechos humanos dará un marco de acción claro a las empresas privadas para una gestión respetuosa de los derechos de los clientes y usuarios. Sin embargo, esto no justifica que las empresas promuevan o faciliten violaciones a los derechos humanos a través de la divulgación indiscriminada e injustificada de datos personales sensibles. La mayoría de las obligaciones estatales equivalen a responsabilidades para las empresas, que deben cumplir con leyes nacionales y que a su vez deben estar alineadas con los estándares internacionales de protección[46]. El principio del que deriva la obligación estatal o la responsabilidad empresarial es el mismo; **los datos son de las personas**, no de los Estados ni las empresas, y **en función de esa expresión básica de la identidad y dignidad humanas, tales datos deben ser protegidos**.

Al momento de solicitar datos personales, las empresas deben ser transparentes con respecto al uso que le darán a esta información; deben contar con una plataforma que garantice la seguridad de los datos para evitar posibles filtraciones. De igual forma, en el caso de que se vulnere la seguridad de la empresa y se filtren datos personales de sus clientes o beneficiarios, existen varias medidas que debe tomar la entidad para hacer un manejo adecuado de la situación, además de notificar de forma oportuna a las personas usuarias.

46 Naciones Unidas (2011). Principios rectores sobre las empresas y los derechos humanos. Recuperado en:https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf

ANEXO

Preguntas a partir de los *Principios actualizados sobre la privacidad y protección de datos personales* de la Organización de Estados Americanos y los *Principios que informan la privacidad y protección de datos personales* de la Relatoría especial sobre el derecho a la privacidad de Naciones Unidas.

Legitimidad

¿Se refiere a alguna ley o instrumento que justifique o regule el tratamiento/recopilación de datos?

Tratamiento y conservación limitados

¿Las finalidades para el uso de los datos son determinadas, específicas, explícitas y legítimas?

¿Las finalidades son compatibles con aquellas para las cuales se ha recopilado la información?

¿Se establece un tiempo límite justificado para la conservación de los datos?

Confidencialidad

¿Se garantiza la no divulgación de los datos personales, que no se pondrán a disposición de terceros, ni se emplearán para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley?

Exactitud de los datos

¿Se ofrece la posibilidad de corregir y actualizar la información, acorde a la finalidad legítima de mantener los datos en el tiempo?

Transparencia y consentimiento

¿Se especifica la identidad y datos de contacto del responsable de los datos?

¿Se especifican los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados?

¿Se especifica la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados?

Acceso, Rectificación, Cancelación, Oposición y Portabilidad

¿Se dispone de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar el acceso a esos datos personales?

¿Se dispone de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar la rectificación a esos datos personales?

¿Se dispone de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar la cancelación de los mismos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales?

Pertinencia y Necesidad

¿Los datos guardan una relación razonable con las finalidades para las cuales son recopilados y se tenga la intención de usarlos?

¿Los datos personales que manejan corresponden al mínimo requerido para la finalidad expresa?

Seguridad de los datos

¿Los Responsables de los Datos hacen explícitas las medidas de carácter administrativo y técnico necesarias para establecer salvaguardias de seguridad de los datos?

¿Los Responsables de los Datos hace explícita su obligación de informar oportunamente a los usuarios/as en caso de vulneraciones de seguridad que pongan en riesgo sus datos?

Datos personales sensibles

¿Se establece una protección explícita y específica para datos sensibles?

Responsabilidad

¿Se establece una figura responsable de la gestión de datos de manera explícita?

¿Se establecen mecanismos de contraloría y auditoría sobre la gestión de esa figura responsable de la gestión de los datos?