INFORME ECUADOR-EXAMEN PERIÓDICO UNIVERSAL-EPU

DERECHO DE PRIVACIDAD Y SEGURIDAD DIGITAL

Este reporte conjunto ha sido elaborado, consolidado y revisado por:

FUNDACIÓN MIL HOJAS

En coalición con estas organizaciones: la Asociación de Familiares y Amigos de Personas Desaparecidas en el Ecuador , -ASFADEC-; Fundación Lucha Anticorrupción; Comité Permanente por la Defensa de los Derechos Humanos; Nos Faltan Tres, Fundación IR "Iniciativas para la Reinserción"; Fundación Desafío; FUNDAMEDIOS; Diálogo Diverso.

En preparación para el Examen Periódico Universal (EPU) de Ecuador ante el Consejo de Derechos Humanos de Naciones Unidas.

FUNDACIÓN MIL HOJAS

http://www.milhojas.is/

Correo electrónico:

info@fundamedios.org

DERECHO DE PRIVACIDAD Y SEGURIDAD DIGITAL

PRESENTACIÓN INSTITUCIONAL

www.milhojas.is

Informe elaborado por Martha Roldós, Directora de la Fundación Mil Hojas y por la académica María José Calderón, PhD. [1]

La Fundación Mil Hojas nació en el 2013 con personería legal panameña y desde hace dos años tiene personería legal ecuatoriana. Su objetivo es estimular el acceso a la información pública, libertad de prensa, libertad de expresión al disenso y a la promoción de una mayor participación ciudadana en la supervisión de la gestión pública.

Nuestra vinculación con el Examen Periódico Universal (EPU) surge de la necesidad de visibilizar la situación de los derechos digitales como acceso al internet y libertad en redes y de las garantías a la privacidad tanto off line como on-line de personas.

[1] Son las mismas autoras del informe de privacidad anterior, presentado por la coalición entre Fundación Milhojas y Usuarios Digitales. La Dra. Calderón escribió la parte correspondiente a Usuarios Digitales, organización a la que entonces pertenecía.

METODOLOGÍA

1. Información fue levantada con información disponible desde 2017 hasta la actualidad, donde se analizan las recomendaciones que se realizaron al respecto en el EPU anterior.

2. Está compuesta por dos secciones relacionadas a la transgresión de esos derechos en el caso ecuatoriano. En el primero se analiza el derecho a la privacidad y en la segunda el derecho al acceso y uso del internet.

3. En relación con el tema sobre privacidad, se analizan sus componentes físicos y virtuales sobre casos reportados de vulneración del anonimato, la seguridad y privacidad en línea. Este ítem considera igualmente el acoso e intimidación a nivel personal. La vulneración de este derecho fue realizada por el Estado ecuatoriano.

4. En relación a la limitación del acceso, el análisis se basa en monitoreos que se realizan en la web y redes sociales en busca de suspensiones, bloqueos o intrusiones, que atentan contra el acceso. Igualmente, se realizaron investigaciones sobre temas relevantes en la opinión pública, periodistas críticos al gobierno cuya información y sitios periodísticos, tienden a ser víctimas de *throttling*.

INTRODUCCIÓN: DERECHO A LA PRIVACIDAD

1. La privacidad es un derecho humano fundamental y un pilar para el ejercicio democrático, ninguna persona puede ser objeto de vigilancia arbitraria o ilegal de su vida privada, correspondencia. El Derecho Humano a la privacidad en la Declaración Universal de los Derechos Humanos (Art.12) establece la condición en la cual nadie puede ser considerado objeto-sujeto de injerencias arbitrarias o ilegales en su vida privada, familia, hogar o correspondencia. La Constitución ecuatoriana reconoce y garantiza a las personas el Derecho a la Protección de Datos de Carácter Personal (Art. 66 n. 19); el Derecho a la intimidad personal y familiar (Art. 66 n. 20); el Derecho a la inviolabilidad y al secreto de la correspondencia física y virtual para cualquier tipo o forma de comunicación (Art. 66 n. 21).

2. El Derecho a la privacidad prevé la condición de permanecer libre del ámbito del Estado en la esfera privada, y a la vez, poder determinar quién posee su información personal y cómo se la usa. Es preciso recordar que la privacidad está estrechamente relacionada con la seguridad personal, que en sí misma es un Derecho fundamental. El Estado es el agente prioritario para proteger y respetar el Derecho a la intimidad o

privacidad y por tanto, abstenerse de incurrir en actividades que amenacen o lesionen la integridad personal que es un bien jurídico protegido.[2]

3. Se reconoce que el ejercicio del derecho a la privacidad se vincula con el real ejercicio de otros derechos civiles y políticos (Art. 19) como los derechos a la libertad de expresión, opinión, circulación y reunión. La privacidad es condición necesaria para el ejercicio de la libertad de expresión, incluyendo la realizada en plataformas digitales de cualquier naturaleza: redes sociales, blogs, filtraciones de información ("leaks"), etc.

4. El derecho de privacidad se relaciona con el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual para cualquier tipo o forma de comunicación (Constitución de Ecuador Art. 66 n. 21).

5. La defensa del derecho a la privacidad enfrenta nuevos retos con las nuevas tecnologías de vigilancia y la explosión del internet. En el ámbito de las comunicaciones, la privacidad, seguridad y anonimato factores decisivos para el pleno ejercicio del derecho a la privacidad; Hacer pública una identidad anónima en las comunicaciones, tiene un efecto intimidatorio en los afectados para la denuncia de víctimas de violencia y abuso, que se pueden inhibir de denunciarlas por temor a la doble victimización. Para enfrentar estos nuevos retos, las Naciones Unidas recientemente crearon la figura del Relator Especial sobre el Derecho a la Privacidad.[3]

6. En el año 2013 la Asamblea General de Naciones Unidas reafirmó el derecho a la privacidad y reconoció la naturaleza global y amplia del internet como un factor coadyuvante hacia el desarrollo en sus distintas formas, alertando a los países la necesidad de proteger los derechos de las personas en internet.[4] Dicho postulado se ha reafirmado en todos los sistemas de protección de derechos humanos. El 27 de junio de 2016, el Consejo de Derechos Humanos de Naciones Unidas aprueba la resolución A/HRC/32/L.20 para la "Promoción, protección y disfrute de los derechos humanos en Internet".[5]

---

[2]Reporte sobre las Consecuencias de la Vigilancia Estatal de las Comunicaciones sobre el ejercicio de los Derechos Humanos a la Privacidad pág. 6 y 7 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement
"22. La intimidad se define como la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otros y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados. El derecho a la intimidad también es la capacidad de las personas para determinar quién posee información acerca de ellos y cómo se utiliza dicha información.
23. Si es que las personas han de ejercer su derecho a la intimidad en el ámbito de las comunicaciones, deben estar en condiciones de garantizar que estas sean privadas, seguras y, si así lo desean, anónimas. La confidencialidad de las comunicaciones supone que las personas pueden intercambiar información en un ámbito que está fuera del alcance de otros miembros de la sociedad, el sector privado y, en última instancia, el propio Estado. La seguridad de las comunicaciones implica que las personas deberían poder verificar que sus comunicaciones sean recibidas únicamente por los destinatarios a las que están dirigidas, sin injerencias ni modificaciones, y que todas las comunicaciones que reciban estén también libres de injerencias. El anonimato de las comunicaciones es uno de los adelantos más importantes facilitados por Internet, que permite a las personas expresarse libremente sin temor a represalias o condenas."
[3] http://www.un.org/spanish/News/story.asp?NewsID=31995#.V_Omt_nhDIU
[4] En el actual Código Orgánico Integral Penal (COIP) del Ecuador se tipifica como delito la divulgación de información de archivos dirigidas obtenidas de un medio electrónico o de telecomunicaciones, materializando la violación del secreto, intimidad y privacidad (Art.229)
[5] http://www.hiperderecho.org/wp-content/uploads/2016/07/naciones_unidas_derechos_internet_bloqueos.pdf

7. En la sesión 27 del anterior examen periódico universal que tuvo lugar en Ginebra en 2017, se dieron varias recomendaciones al Ecuador. Entre ellas la 118.74 propuesta por Liechtenstein que recomiendan a Ecuador "armonizar toda la legislación relativa a la vigilancia de las comunicaciones con las normas internacionales de derechos humanos y, en especial, probar la necesidad y proporcionalidad de toda vigilancia de las comunicaciones."[6]

8. En el Grupo de Trabajo de la misma sesión la recomendación de Liechtenstein apunta también a los órganos de inteligencia del Ecuador. En el numeral 9.16 de la sección B sobre "Privacidad y Derechos Humanos" llama al estado ecuatoriano a "Tomar las medidas necesarias para asegurar que todas las operaciones de los gobiernos de inteligencia sean supervisadas por un mecanismo de supervisión independiente."[7]

9. En mayo de 2021 la Asamblea Nacional del Ecuador aprobó la "Ley para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad."[8] Pese a lo prometedor del título de la ley esta tenía varios artículos que implicaban censura. [9] La ley fue vetada parcialmente por el CEO del despacho jurídico, pese a ello tropecé con varios obstáculos: Vamos a presentar el tema con otra perspectiva. La condición para recibir el sin mayores recortes tenemos que esperar por un periódica. [10]

Instituciones y Marco Legal

10. En marzo de 2018 el entonces presidente Lenin Moreno eliminó vía decreto la Secretaría Nacional de Inteligencia SENAIN[11]. La SENAIN era un ente centralizado con dependencia directa de la Presidencia de la República creado en 2009. Este órgano fue señalado por múltiples denuncias de espionaje por fuera de la ley contra activistas, periodistas y políticos por el solo hecho de discrepar.[12] Las actividades de espionaje de la SENAIN sobre objetivos políticos, sin investigación penal dirigida por la Fiscalía; abarcaba tanto seguimientos, grabaciones y filmaciones, como el espionaje digital con intercepción y adulteración de comunicaciones en varias plataformas, así como el monitoreo de las actividades de sus objetivos en redes sociales.

11. No obstante, con el cierre de la SENAIN el Estado no ha realizado una desclasificación de los expedientes obtenidos ilegalmente más allá de los casos puntuales de dos personas contra las que se realizaron expedientes no sólo de

---

[6] **UPR of Ecuador (3 rd Cycle – 27th session) Thematic list of recommendations**
Source of position: A/HRC/36/4 - Para. 118
[7] Document: United Nations A/HRC/WG.6/27/L.2
Human Rights Council
Working Group on the Universal Periodic Review
Twenty-seventh session
Geneva, 1–12 May 2017
[8] ECUADOR SE UBICA A LA VANGUARDIA EN LA LUCHA CONTRA LA VIOLENCIA SEXUAL DIGITAL Y LOS DELITOS INFORMÁTICOS
[9] Para erradicar la violencia digital en Ecuador no es necesario restringir la libertad de expresión y
[10] Para erradicar la violencia digital en Ecuador no es necesario restringir la libertad de expresión
[11] https://www.elcomercio.com/actualidad/seguridad/leninmoreno-eliminacion-senain-inteligencia-austeridad.html
[12] https://periodismodeinvestigacion.com/2021/01/06/asi-persiguio-correa-a-villavicencio/

seguimiento y espionaje sino operaciones de inteligencia que iban desde la falsa incriminación en un delito[13] hasta el intento de secuestro.[14]

12. Al cierre de la SENAIN le siguió la creación del Centro De Investigaciones Estratégica CIES que se presenta como una institución de inteligencia con una hoja de ruta diferente de la de persecución política de la SENAIN.[15] Sin embargo, no se creó ninguna instancia de supervisión independiente a las actividades a realizar por parte de la nueva institución como indicaba la recomendación 9.16. La supervisión que realiza la contraloría general de la nación al CIES como antes a la SENAIN es al gasto y no a la legalidad de sus operaciones.

13. En el pasado la desaparecida Secretaría Nacional de Información SENAIN contaba con la colaboración de otras instituciones del Estado, sobre todo la Dirección Nacional de Registro de Datos Públicos DINARDAP,[16] creada en 2010 mediante la Ley del Sistema de Registro de Datos Públicos como la institución llamada a ***"consolidar, estandarizar y administrar la base única de datos de todos los Registros Públicos."***[17]para facilitar la compilación de la información de sus objetivos de seguimiento. Desde 2017 esta institución ha tenido cambios positivos y ha sido una de las impulsoras de la ley de datos personales. Sin embargo, debido a la falta de reglamento y de la creación del ente regulador no se ha revisado lo sucedido con las bases de datos controladas por la DINARDAP.

Nuevas leyes e iniciativas legales

14. El país ha avanzado legalmente con la promulgación de la Ley de Datos Personales, el 26 de mayo de 2021.[18] La ley ecuatoriana se inspira en el Reglamento General de Protección de Datos Europeo y los preceptos dados por los órganos de la Unión Europea. Previamente a la promulgación de esta ley, la protección a la privacidad existía como una declaración de principio en la Constitución Ecuatoriana y en algunos artículos del Código Penal, sobre todo respecto a la intrusión en la correspondencia electrónica y websites. Más allá de ello una serie de temáticas vinculada a la privacidad y los datos personales no era ni siquiera abordada. Y sobre lo que estaba regulado no existía voluntad o capacidad técnica por parte de los órganos de justicia y control para implementarlos, sobre todo cuando quien cometía la intrusión era el Estado.

15. En esa medida, la ley es un avance. Su objeto y finalidad es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección.

---

[13] https://www.eluniverso.com/noticias/2018/10/26/nota/7016981/no-conocia-que-senain-investigaba-galo-lara/

[14] https://www.eluniverso.com/noticias/2018/07/12/nota/6855185/fernando-balda-publica-informacion-desclasificada-senaim-sobre/

[15] https://www.cies.gob.ec/retos

[16] La Dirección Nacional de Registro de Datos Públicos fue creada por la Ley del Sistema Nacional de Registro de Datos Públicos http://direcciondedatospublicos.jimdo.com/leyes/sinardap/

[17] Numeral 5, Art. 31 de la Ley del Sistema Nacional de Registro de Datos Públicos

[18] https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

16. Tampoco se ha designado a la fecha a la Autoridad de Protección de Datos Personales[19] contemplada en la ley y de la cual depende fundamentalmente su implementación. Con ello la ley está promulgada pero realmente no ha entrado en vigor.

17. Aunque la ley también habla de los datos biométricos como parte de los datos personales, en la ley no se aborda el tratamiento de las cámaras de vigilancia públicas y privadas que con gran densidad existen sobre todo en los centros urbanos del país.

18. En junio de 2021 se promulgó la ·Ley para Prevenir la Violencia, el Acoso Digital y la Violación a la Intimidad", más allá de la declaración de principios el proyecto que salió de la Asamblea era más bien en una ley que vulneraba la libertad de expresión.[20] El veto parcial de la presidencia de la república corrigió los aspectos más preocupantes del proyecto, pero la ley resultante resultó bastante vaga y no cumplió con las expectativas de las organizaciones de mujeres que reclamaban al Estado enfrentar los fenómenos de violencia, acoso digital y violación de la intimidad.[21]

19. En enero 20 de enero de 2022 se presentó ante la Asamblea Nacional una iniciativa de ley llamada "Proyecto de Ley Orgánica de Ciberseguridad, Seguridad Sistémica y Acceso a la Verdad de los Hechos" donde se mezclan de manera confusa conceptos vinculados a la ciberseguridad con los de "verdad de los hechos". La ley inicia su tratamiento a fines de marzo.

Sistemas de espionaje y vigilancia

20. En el país no existe monitoreo del tratamiento y almacenamiento de datos que se da al gran volumen de data generado por los sistemas de cámaras de vigilancia (también conocidos como "ojo de águila"). El más extenso sistema es el de las cámaras del ECU911 y en la ciudad de Guayaquil -el puerto principal del país- existe también la red de la Corporación de Seguridad Ciudadana. Estos omnipresentes sistemas de cámaras son manejados autónomamente por las entidades correspondientes sin supervisión de otras entidades.

21. Según la investigadora Melissa Chang en el reportaje del New York Times: "Ecuador cuenta con un sistema nacional de 4.300 cámaras y 16 centros de

---

[19] Pese a que en rueda de prensa en julio de 2021 sobre el ataque digital a la página de CNT, las ministras de telecomunicaciones y de gobierno del país, señalaron que la falta de creación del ente de protección de datos el país no tenía capacidad de reaccionar ante sucesos como la filtración de bases de datos y los ataques cibernéticos a la privacidad, aún no se ha creado el ente para la protección de datos La creación de ente para protección de datos está pendiente

[20] Para erradicar la violencia digital en Ecuador no es necesario restringir la libertad de expresión

[21] *"El problema de la ley fundamental es que los artículos que sancionan directamente a la violencia sexual en el ámbito digital (tres en total)* ***no llenan las expectativas del propósito manifiesto de la ley ni las demandas de las activistas."*** Isabella Nuques, promotora de la iniciativa de ley.
La Violencia Sexual Digital es un femicidio indirecto – Los puntos ciegos de la ley

monitoreo. Para combatir el crimen, detectar emergencias o tal vez espiar. Llamado ECU-911. Diseñado y construido principalmente por dos empresas chinas (CEIEC y Huawei), comprado con la ayuda de un préstamo bancario chino."[22]

22. Parte de este sistema funciona también con software de reconocimiento de imagen, principalmente comprado a China.[23] En otra entrega de la investigación del New York Times se señala que el sistema de cámaras del Servicio Integrado de Seguridad ECU 911 también era monitoreado por la ex SENAIN.[24] Después del reportaje del New York Times no ha habido una respuesta satisfactoria por parte del Estado ecuatoriano.

23. Adicional al riesgo de abuso por parte de las autoridades locales sobre los sistemas de *surveillance* comprados a empresas chinas se suma el riesgo del hecho que China puede acceder a información sensible de inteligencia ecuatoriana a través del de un ECU-911 equipado con equipos y software adquiridos en los últimos años a empresas chinas.[25]

24. La falta de normativa e institucionalidad que garantice por el monitoreo de las actividades de vigilancia (surveillance) en el país hacen que el país siga apareciendo en las listas de los países involucrados en quienes adquieren software y equipos cuestionables como reportó Citizen Lab.[26] La carrera por nuevos equipos y sistemas no desapareció con los cambios de gobierno.

25. En la medida de ello, si bien la presión parece haber disminuido desde la época del régimen de Rafael Correa[27], quienes residen en Ecuador no tienen aún garantías claras de no ser investigados ilegalmente por las instituciones de inteligencia en el Estado. Desde el EPU anterior, no se puede señalar la implementación de mejores prácticas con miras a someter los mecanismos de vigilancia al estado de derecho.

26. Un problema adicional en el tema de la vigilancia es que la falta de transparencia y rendición de cuentas no sólo de los operativos sino también de los equipos llevó a que varios de estos desaparecieran. El Estado ya no tiene el monopolio de la vigilancia, sino que otros grupos no estatales tienen la capacidad de realizar actividades de espionaje en el país.[28]

Seguridad informática y Filtraciones de datos personales

---

[22] https://twitter.com/melissakchan/status/1121017696743776257?s=20&t=8l2R3o2Fz-kCTXndyGRmVg

[23] Expuesto en la nota del New York Times Made in China, Exported to the World: The Surveillance State
In Ecuador, cameras capture footage to be examined by police and domestic intelligence. The surveillance system's origin: China.
https://twitter.com/Cascabelito09/status/1121147431402516480?s=20&t=6XVJ9haP2yozq7t-dP1bBQ

[24] In a Secret Bunker in the Andes, a Wall That Was Really a Window
Before a video interview with an Ecuadorean intelligence chief, I thought I was adjusting a dimmer switch. What I inadvertently revealed broke our story open.

[25] China accede a información sensible de inteligencia ecuatoriana a través del ECU-911

[26] Running in Circles, Uncovering the Clients of Cyberespionage Firm Circles

[27] Un par de los ejemplos citados en el informe para el EPU 2017
Así persiguió Correa a Villavicencio
La Senain gastó $ 7,1 millones para vigilar a Galo Lara

[28] EL RETORNO DE LA SENAIN

27. Otra amenaza a la privacidad son las filtraciones masivas de bases de datos y el ransomware que exponen y comprometen la información de millones de ecuatorianos.

28. El país ha sufrido varios ataques cibernéticos vinculados a grandes bases de datos. Estos casos se repetido en este período sin que se haya implementado hasta ahora de forma efectiva protocolo de prevención, información, manejo, investigación y remediación de tales sucesos. En tales ocasiones el Estado ecuatoriano ha fallado en informar a la ciudadanía de lo sucedido, han demorado en corregir lo sucedido y los responsables tampoco han respondido ante la justicia por lo sucedido. Los afectados no tienen idea hasta el día de hoy del alcance de la afectación.

29. Más allá del problema de la vulneración digital y la amenaza a la información de la ciudadanía el mal manejo de los sucesos es la norma en Ecuador ya sea que las bases de datos afectadas sean de instituciones públicas o privadas. La forma de enfrentar las denuncias es la negación, luego el tardío reconocimiento para proceder luego de este a negar posibles consecuencias debido a la información filtrada o hacer un adecuado seguimiento sin ninguna autoridad de control que garantice transparencia y rendición de cuentas respecto de estos sucesos.

Casos de filtraciones y amenazas a bases de datos personales

30. En septiembre de 2019 la firma internacional de seguridad digital vpnMentor[29] reveló mediante un informe[30] la filtración masiva de los datos millones de ecuatorianos. Casi la totalidad de la población nacional, incluidos los datos de más de 6,7 millones de menores de edad.[31]

31. Como recogió la prensa nacional, la responsable de la filtración de los datos fue una empresa consultora ecuatoriana uno de cuyos dos directivos había trabajado para el gobierno del presidente Correa justo cuando implementaban el Sistema Nacional de Información. De alguna manera las bases de datos recopiladas por el Estado terminaron estando en el servidor de una empresa privada de un exfuncionario.

32. En 2021 se dio un ataque a la base de datos de la Corporación Nacional de Telecomunicaciones CNT.[32] Pese a que la información sobre el probable

---

[29] "VPN Mentor es el sitio web de revisión de VPN (red privada virtual) más grande del mundo. Su laboratorio de investigación es un servicio que se esfuerza por ayudar a la comunidad en línea a defenderse de las amenazas cibernéticas, al tiempo que educa a las organizaciones sobre cómo proteger los datos de sus usuarios. Ellos junto con el portal de tecnología Zdnet.com lanzaron este lunes 16 de septiembre la noticia."
La peor filtración de datos en la historia del Ecuador al descubierto

[30] Report: Ecuadorian Breach Reveals Sensitive Personal Data
Almost entire population of Ecuador has data leaked

[31] "Sobre los niños, el portal Zdnet.com publicó lo siguiente: "Al mirar este índice también nos dimos cuenta de que había entradas para niños, algunos de los cuales nacieron tan recientemente como esta primavera. Por ejemplo, encontramos 6,77 millones de entradas para niños menores de 18 años. Estas entradas contenían nombres, cédulas, lugares de nacimiento, domicilios y sexo (...) Con la excepción de los últimos años, el resto de las entradas de la base de datos están en sintonía con los informes públicos sobre la tasa de natalidad del país", apunta. Esta filtración, dice el portal, no solo expone a los niños a posibles robos de identidad, sino que también los pone en peligro físico porque sus domicilios se han dejado expuestos en línea para que cualquiera los pueda encontrar."
La peor filtración de datos en la historia del Ecuador al descubierto

[32] CNT sufrió ataque informático de 'alta sofisticación', la denuncia se investiga en Fiscalía

ransomware ya estaba en la prensa internacional, nacional y en conocimiento de la ciudadanía, las autoridades solo emitían comunicados de prensa neutros hablando solo de fallas en el sistema.[33] Las autoridades aceptaron ante la ciudadanía luego de varias quejas lo que estaba sucediendo[34] mediante una rueda de prensa brindada por las ministras de Telecomunicaciones y Gobierno. En ella no se permitió preguntas de la prensa. En consecuencia, el tema de lo sucedido en CNT no fue adecuadamente comunicado por el gobierno mientras circulaban versiones sobre lo realmente sucedido en redes sociales.[35] Las autoridades ofrecieron compensación a los perjudicados por la filtración pero sin que hubiera claridad del real impacto de la filtración.[36]

33. Otras instituciones públicas que han sufrido filtración de datos son el Ministerio de Salud. En julio de 2021 las autoridades del MSP admitieron públicamente que existió una filtración de datos de 1.5 millones de ciudadanos. La data filtrada contenía información como nombres, número de cédula, número de teléfono y si se habían contagiado o no con la Covid-19.[37]

34. Otra entidad pública atacada fue la Agencia Nacional de Tránsito quienes presentaron denuncia del hecho.

35. No sólo la información de los ecuatorianos en plataformas públicas se ha visto amenazada sino también aquella que se encuentra en instituciones privadas, como fue el caso del Banco del Pichincha.

36. Las primeras alertas sobre el banco datan de inicios de 2021.[38] A los pocos días vinieron sendos comunicados del banco y tarjetas de crédito vinculadas negando cualquier filtración de la información de sus clientes.[39] Finalmente el banco admitió los problemas, pero negó que hubieran consecuencias.[40] Luego de esta aclaración en febrero de 2021, nuevamente se presentaron problemas a mediados de año respondidas por varios comunicados de la institución bancaria. En el primero, el banco negaba que se hubiera producido algún ataque.[41] Posteriormente el banco señaló en otro comunicado que los impedimentos de acceso a su plataforma digital se debían a mantenimiento.[42] Meses después, luego de que los servicios digitales del Banco colapsaron varios días, la institución emitió un comunicado reconociendo haber sufrido un "incidente de ciberseguridad" sin brindar más información.[43] Como

---

[33] https://twitter.com/CNTinforma/status/1415787232166830088?s=20&t=ZhjC_KeLdgdI8riznUZcPw
[34] Ecuador State Telecom Company Fighting Ransomware Attack: Govt
[35] https://twitter.com/1ZRR4H/status/1417903899143458821?s=20&t=w5WkMWIK_Z1agWJnxrdRnQ
Ver esta publicación de Usuarios Digitales
https://twitter.com/usuariosdigital/status/1416189131181469698?s=20&t=dKixuABwAniyWGpBbX-Mlw
[36] CNT compensará a usuarios por el ataque informático que sufrió
[37] Ministerio de Salud ratificó la filtración de datos y apunta a periodista y ciudadanos que dieron la alerta
https://www.elcomercio.com/tendencias/sociedad/msp-filtracion-datos-plataforma-pandemia.html
[38] https://twitter.com/usuariosdigital/status/1360015093849849862?s=20&t=edGdGLQjyivrLS08DhFBbg
[39] https://twitter.com/usuariosdigital/status/1360015711469510666?s=20&t=edGdGLQjyivrLS08DhFBbg
[40] Banco Pichincha indica que los recursos financieros de sus clientes no se vieron comprometidos por filtración de información
[41] Banco Pichincha niega filtración de datos
[42] https://twitter.com/BancoPichincha/status/1161283828981338112?s=20&t=edGdGLQjyivrLS08DhFBbg
[43] https://twitter.com/BancoPichincha/status/1447628963858296834?s=20&t=edGdGLQjyivrLS08DhFBbg

en el caso de las filtraciones previas la información de lo sucedido aparecía en fuentes no oficiales.[44]

El caso de Ola Bini, experto en criptografía y software de privacidad

37. Según la organización internacional Electronic Frontier Foundation, el caso Ola Bini tiene una serie de vicios en el proceso jurídico originadas en motivaciones políticas. El 11 de abril del año 2019, el programador y experto en ciberseguridad, Ola Bini fue detenido en el Ecuador, como sospechoso de desestabilización contra el gobierno de Lenin Moren y de hackeo de la red de comunicaciones de la Compañía Nacional de Telecomunicaciones CNT. El delito que ambas entidades alegan es el acceso no consentido a un sistema informático del Estado ecuatoriano. En el centro del debate del caso Ola Bini está el reclamo de la legitimidad del hacking ético. La defensa de Bini indica que su entrada al portal de CNT fue para compartir la vulnerabilidad del mismo con Ricardo Argüello quien tenía un contrato de seguridad de CNT. En la imagen que Bini envió a Argüello se observa un encabezado de CNT y el mensaje: “El acceso o uso no autorizado – se considera un acto criminal Petroecuador – Senain – Internet”.

38. A más del alegato de la defensa de Ola Bini de que el proceso tuvo su orígen en motivaciones políticas, el manejo del mismo desde la detención del acusado y el manejo de los tiempos procesales se ha considerado irregular. En octubre del 2020, la defensa de Bini presentó un recurso de habeas data para probar que lo estaban vigilando. Luego de siete meses, un tribunal se lo concedió. A través de este recurso, Ola Bini y su defensa recibieron información adicional con las que señalan que pueden probar que los equipos de Inteligencia de Ecuador no contaban con pruebas para incriminarlo ni detenerlo. En declaraciones a “La Barra Espaciadora” la defensa de Ola Bini señaló: *“El habeas data puede ser visto como un éxito, pero hay que recordar que lo presentamos en octubre y tomó alrededor de dos meses para que se iniciara la audiencia, cuatro meses más para que la audiencia termine, y ocho meses después no tenemos aún la resolución”*.

ACCESO Y USO DE INTERNET EN ECUADOR

Usos y brecha digital

39. Según los datos del Instituto Nacional de Estadisticas y Censos el porcentaje de hogares con acceso a internet en Ecuador pasó de 45,5% a 53,2%. El porcentaje de personas que utilizan internet ha pasado 59,2% a 70,7%. La proporción de personas con celular activado pasó de 59,9% a 62,9%. La población que utiliza smartphones pasó de 76,8% al 81,8% de 2019 a 2020. Y el analfabetismo digital bajó del 11,4% al 10,2%. [45] Estas cifras presentan una mejora respecto a las que presentamos en el

---

[44] https://noticiasseguridad.com/hacking-incidentes/como-hackearon-el-banco-pichincha-la-institucion-bancaria-mas-grande-de-ecuador/

[45] Encuesta Multipropósito Tecnología de la Información y Comunicación TIC

informe del Examen Periódico Universal anterior. El acceso a internet a nivel nacional pasó de del 32,8% al 53,2%.

40. Si bien se ve una mejora en las cifras nacionales, la brecha urbano rural es persistente en todos los rubros. Según las últimas cifras disponibles para 2020 mientras el porcentaje de hogares con acceso a internet a nivel urbano era de 61,7%, a nivel rural apenas llegaba al 34,7%. La brecha urbano rural se mantiene incluso para otros rubros como el uso del teléfono celular y en materia de analfabetismo digital, la población rural con 16,8% duplica el analfabetismo digital urbano cuyo porcentaje es del 7,5%.

Derechos Digitales y Pandemia

41. La pandemia provocó varios retos a la privacidad. En primer lugar, las plataformas para registro de contagio también tienen problemas de seguridad que pueden llevar al robo de las personas y sus propiedades.

42. Otro reto de la pandemia era la ceremonia en el hogar para evitar gastar mucho. Tampoco ha manejado mucho efectivo se va a meter su mano en mi asegura. Una mujer en general no se detiene y regreso a casa instalándolo.

43. En una resolución muy relevante aprobada recientemente por el Consejo de Derechos Humanos de las Naciones Unidas se "Condena inequívocamente las medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos, y exhorta a todos los Estados a que se abstengan de adoptar estas medidas, o cesen de aplicarlas". [46]

Bloqueo de Internet en Ecuador

44. En una resolución muy relevante aprobada recientemente por el Consejo de Derechos Humanos de las Naciones Unidas se "Condena inequívocamente las medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos, y exhorta a todos los Estados a que se abstengan de adoptar estas medidas, o cesen de aplicarlas". [47]

45. Los bloqueos pueden ser totales (conocidos como *shutdowns*) o parciales (*throttling*). El área también puede ser diferente, desde una afectación nacional a parcial.

46. En junio de 2017 el país sufrió un bloqueo parcial del internet que afectó a todo al país durante un fin de semana, pero no a todos los servicios de igual manera. Servicios bancarios se prestaban en cajeros, pero los servicios de internet por cable

[46] Resolución A/HRC/32/L.20
http://www.hiperderecho.org/wp-content/uploads/2016/07/naciones_unidas_derechos_internet_bloqueos.pdf
[47] Resolución A/HRC/32/L.20
http://www.hiperderecho.org/wp-content/uploads/2016/07/naciones_unidas_derechos_internet_bloqueos.pdf

de dos de las principales portadoras que brindan internet a hogares se interrumpieron. La navegación en internet y redes sociales fueron los servicios afectados. Las primeras en responder ante las protestas fueron las prestadoras del servicio de cable sin embargo por varios días no se apuntaba a la razón del corte. [48] Finalmente, en un comunicado se señaló brevemente que habría sufrido un daño en un cable submarino entre Panamá (capital de Panamá) y Manta (puerto ecuatoriano) donde se conecta el país al PCCS. El comunicado ni siquiera menciona que el cable con problemas era el Pacific Caribbean Cable System PCCS uno de los tres cables submarinos que sirve el Ecuador, justamente el que brinda la mayor cobertura. [49]

47. En este caso, la información tanto de la empresa privada que tiene la concesión como de las autoridades respectivas no fue transparente. La institucionalidad del país hasta el momento no garantiza transparencia cuando se dan este tipo de eventos, no existe un monitoreo adecuado del funcionamiento de los cables submarinos, ni de las prestadoras de servicio de internet. En el caso del PCCS las condiciones de la concesión fueron dudosas y de hecho, el día previo a la interrupción del servicio por el inexplicado suceso con el cable submarino, dichas condiciones habían vuelto a generar atención en las redes sociales. [50]

48. La regulación y la transparencia en torno a la regulación de la conectividad al internet es clave para garantizar el derecho a la conectividad.[51]

49. También hay bloqueos al acceso de ciertas páginas mediante el uso de DDoS u otros mecanismos.[52]

50. La Relatoría de Libertad de Expresión de la Comisión Interamericana de Derechos Humano RELE_CIDH y la Comisión Interamericana de Derechos Humanos CIDH citando a Netblocks[53], denunciaron que en el marco de las protestas de octubre de 2019 en Ecuador se habría restringido redes sociales. que redes sociales en el país.[54] Pese a ello el reporte de transparencia de Facebook para esas fechas no reporta interrupciones en esa red social.[55]

Acoso Digital

51. Los denominados "troll centers" y "bots" fueron utilizados desde gobierno desde el boom de las redes sociales en el pasado. Los *robots sociales,* trozos de código que generan contenido y usuarios en medios sociales reales que tienen usos pre-fabricados para acosar o para influenciar de manera negativa o positiva a los

---

[48] Dos operadoras de cable alertan sobre problemas de internet por daño de cable submarino
[49] Mintel y Operadoras trabajan en conjunto para solucionar intermitencia en el servicio de Internet
[50] https://twitter.com/CarlosVerareal/status/880617570939936768?s=20&t=u9L8XGlEJ0iHGEhtyIX1wg; https://twitter.com/lahistoriaec/status/871417225231695873?s=20&t=u9L8XGlEJ0iHGEhtyIX1wg; curiosamente los medios que reportaron de este hecho, tienen la página a la que hacen referencia están inhabilitadas.
[51] Las pugnas por el control del mercado de la internet
[52] https://twitter.com/FUNDAMEDIOS/status/1373773806163083270?s=20&t=LMd3X7ZWaeOkNCcR8wcg2A https://twitter.com/VDSorg/status/1259984064020467713?s=20&t=LMd3X7ZWaeOkNCcR8wcg2A
[53] https://netblocks.org/ Evidence of social media disruptions in Ecuador as crisis deepens
[54] https://twitter.com/CIDH/status/1183475097727832066?s=20&t=w7WJqyYpa-c5dAmkDlv3AQ
[55] https://twitter.com/usuariosdigital/status/1260718244526206976?s=20&t=w7WJqyYpa-c5dAmkDlv3AQ

usuarios de redes sociales.[56] En el caso ecuatoriano, el fenómeno de la violación a la privacidad ha generado más cuidado y curiosidad.[57] En Ecuador todos los vinculados tienen hambre.

Recomendaciones

1. El Estado Ecuatoriano debe garantizar el Derecho a la Privacidad de los ciudadanos, tal como reza la Declaración Universal de derechos humanos: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Y garantizar el derecho a la libertad de expresión (art. 19) tal como reza la carta de derechos humanos de las Naciones Unidas: "*Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión*".

2. El Estado ecuatoriano debe investigar exhaustivamente y transparentar las operaciones y contratos de la ex Secretaría Nacional de Inteligencia, SENAIN. Respecto de la institución de inteligencia sucesora de la SENAIN, el Centro de Investigaciones Estratégicas CIES el Estado debe delimitar su accionar en el marco del respeto a los derechos humanos acorde a la Constitución y los instrumentos internacionales de los que el país es signatario. Se debe establecer que cualquier investigación sobre ciudadanos debe realizarse en el marco del debido proceso por las autoridades competentes, y no en un ambiente de espionaje e intimidación.

3. El Estado ecuatoriano debe desistir en el uso software de intrusión y control de dispositivos electrónicos e información de los ciudadanos. Los procesos de adquisición de equipos y software de vigilancia, mismos que deben alinearse en su uso a los estándares internacionales. En este sentido, se vuelve fundamental establecer sistemas de *checks and balances* para el aparato de inteligencia. Se debe investigar la pasada relación de instituciones del Estado con empresas globales poco transparentes con el uso de software de espionaje masivo.

4. El Estado ecuatoriano debe trabajar en la implementación de la nueva Ley de Protección de datos y en la creación de una cultura de protección de datos, que defienda los datos personales y a los ciudadanos contra el Big Data, ya sea que sea estatal o corporativo. En la institucionalización de la protección de datos personales por parte de un ente público, la Autoridad de Protección de Datos Personales que

[56] El uso de trolls y bots para el acoso de internet está desde los orígenes de las redes sociales. Este es el caso de Putin quien institucionalizaría su troll center. http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7. De la misma manera, se encuentran ya varios centros de investigación académico y organizaciones de la sociedad civil que monitorear el entorno digital y su impacto en la vida pública: http://politicalbots.org/

[57] Para erradicar la violencia digital en Ecuador no es necesario restringir la libertad de expresión y precisar mi parte en el grado nuevo .

establece la nueva ley, se debe evitar caer en la manipulación política de las autoridades de turno. Se vuelve imperativa la vigilancia de estas entidades por parte de la ciudadanía.

5. Los legisladores y el Estado ecuatoriano deben cuidar que los proyectos de ley y las leyes promulgadas en materia de derechos digitales, privacidad, contra el acoso digital y la ciberseguridad no sirvan de pretexto para la vulneración de otros derechos como los de la libertad de expresión y se alineen con los principios de los instrumentos internacionales en materia de derechos humanos.

6. El Estado ecuatoriano debe establecer normas, mecanismos y prácticas respetuosas del Derecho a la Privacidad para el manejo que los funcionarios públicos hagan los datos personales. El Estado ecuatoriano debe definir claramente, mediante tales normas y procedimientos, que la Ley Orgánica de Transparencia y Acceso a la Información Pública LOATIP hace referencia a la información que las instituciones y funcionarios públicos deben poner a disposición del público en virtud del Derecho al Acceso a la Información y que no puede utilizarse para obtener información de ciudadanos que no estén en tales funciones.
7. Más allá de los enunciados normativos, el Estado ecuatoriano debe proveer recursos efectivos, administrativos y judiciales, a los cuales los ciudadanos puedan acudir ante la vulneración de su derecho de privacidad.

8. El Estado ecuatoriano debe comprometerse a impulsar y participar de iniciativas regionales y globales a favor de la garantía del Derecho a la Privacidad y el Acceso al Internet y en la promoción del acceso a la información por medio de plataformas digitales, con énfasis en libertad de expresión y fiscalización ciudadana.

9. El Estado ecuatoriano debe garantizar la transparencia en la concesión, regulación y control de la infraestructura de internet y de los prestadores del servicio de conectividad. Los cortes e interrupciones del servicio deben ser debidamente investigados e informados.

10. El Estado ecuatoriano debe esforzarse en cerrar la brecha urbano rural en materia de conectividad y alfabetismo digital.