28 de junio de 2021

Secretaría de Derechos Humanos de la República de Ecuador

Sra. Bernarda Ordóñez Moscoso
Secretaria de Derechos Humanos.

Sr. Felipe Ochoa
Subsecretario de Derechos Humanos

Nos dirigimos respetuosamente a la Secretaría de Derechos Humanos con el propósito de **presentar preocupaciones sobre la causa judicial abierta contra el experto en seguridad informática Sr. Ola Bini en Ecuador**, un caso que resulta de gran interés para la competencia de la Secretaría de Derechos Humanos dadas las violaciones al debido proceso y otros derechos involucrados. *Esta comunicación es particularmente relevante dada la reinstalación de la audiencia evaluatoria y preparatoria de juicio del Sr. Ola Bini* ***el 29 de junio,*** *que debería recibir la atención especial de la Secretaría*. La Secretaría de Derechos Humanos también parece legítimamente posicionada para examinar las irregularidades y violaciones que cercan el caso del Sr. Bini.

La Electronic Frontier Foundation (EFF) es una organización internacional sin ánimo de lucro que defiende los derechos humanos en el mundo digital.[1] Fundada en 1990, la EFF defiende los derechos humanos de los usuarios mediante litigios de impacto, análisis de políticas, activismo de base y desarrollo tecnológico. La misión de la EFF es garantizar que la tecnología apoye los derechos humanos de todas las personas del mundo. La EFF cuenta con más de 30.000 seguidores en 99 países de todo el mundo.

El caso del Sr. Bini tiene profundas implicaciones y se sitúa en el centro de la garantía de los derechos humanos y del debido proceso, un caso emblemático en el contexto de la aplicación arbitraria de leyes penales demasiado amplias a los expertos en seguridad. El caso del Sr. Bini representa una oportunidad única para que el Gabinete de la Secretaría

[1] Vea más de nuestro trabajo en https://www.eff.org/

de Derechos Humanos considere y vele por los derechos de los expertos en seguridad en la era digital. Los expertos en seguridad protegen los computadores de los que todos dependemos y protegen a las personas que han integrado los dispositivos electrónicos en su vida cotidiana, como los defensores de los derechos humanos, los periodistas, los activistas y los disidentes, entre muchos otros. Para llevar a cabo la investigación en materia de seguridad, debemos proteger a los expertos en seguridad y garantizar que dispongan de las herramientas necesarias para realizar su trabajo.

Desde nuestra fundación en 1990, la EFF se ha preocupado por el empleo de las leyes de ciberdelincuencia para perseguir a los tecnólogos que se dedican a la exploración de la tecnología de vanguardia, donde con demasiada frecuencia se confunden investigaciones de seguridad que resultan beneficiosas con un mal comportamiento. Nos hemos opuesto en los tribunales a la persecución o intimidación de los tecnólogos, en particular de los expertos en seguridad digital, y hemos intervenido para defender a los investigadores de seguridad de los malentendidos de las fuerzas del orden[2].

Debido a la relevancia de este caso de cibercrimen emergente en América Latina, del 29 de julio al 2 de agosto de 2019, la EFF realizó una visita *in situ* a Ecuador para investigar las denuncias de injusticia relacionadas con el caso del Sr. Bini, y continuó monitoreando su procesamiento legal en los años posteriores.

A continuación, encontrará los principales puntos que deseamos poner en conocimiento de la Secretaría como contribución para que su oficina pueda examinar el asunto. En primer lugar, explicamos cómo el trabajo de los expertos en seguridad es crucial para garantizar los derechos y la seguridad de todos. En segundo lugar, discutimos cómo la trayectoria de trabajo del Sr. Bini es coherente con la mejora de la protección de las personas en el uso diario de la tecnología. En tercer lugar, planteamos las preocupaciones de la EFF en relación con el enjuiciamiento del Sr. Bini, como las violaciones del debido proceso y otros derechos, la debilidad del caso contra el experto en seguridad teniendo en cuenta las pruebas disponibles públicamente, y el preocupante marco político que rodea el caso.

[2] Vea más en <https://www.eff.org/issues/coders>.

Creemos que la Secretaría de Derechos Humanos puede desempeñar un papel relevante al vincular la protección de los expertos en seguridad con la misión más amplia de defender los derechos humanos en el país.

El trabajo de los expertos en seguridad es vital para salvaguardar los derechos y la seguridad de todos

Al identificar y revelar las vulnerabilidades del software y el hardware, los expertos en seguridad mejoran la seguridad de todos los usuarios que dependen de los sistemas de información para su vida diaria y su trabajo. Sin embargo, con demasiada frecuencia se ven amenazados por leyes destinadas a evitar intrusiones malintencionadas, incluso cuando su propio trabajo es todo menos malintencionado. La tecnología de la comunicación digital y las herramientas de protección de la privacidad, como el cifrado de extremo a extremo, han hecho que el trabajo de los periodistas, abogados y defensores de los derechos humanos sea más seguro frente a los ciberdelincuentes y el acoso de los regímenes represivos. Por desgracia, estos impresionantes avances en materia de privacidad y seguridad han puesto en aprietos a los tecnólogos que construyen esas herramientas y los someten cada vez más al mismo acoso.

La EFF explicó los riesgos de leyes de ciberdelincuencia excesivamente amplias, y las amenazas de su interpretación amplia por parte de las autoridades policiales, en nuestro documento de 2018 *Protegiendo los derechos de los investigadores de seguridad en las Américas*[3]. El documento se basa en los derechos reconocidos por la Convención Americana sobre Derechos Humanos, y en ejemplos de la jurisprudencia de América del Norte y del Sur, para analizar cómo estos derechos humanos fundamentales se aplican a los investigadores de seguridad y cómo podríamos interpretar mejor las salvaguardias de derechos humanos para proteger el trabajo de seguridad digital que es cada vez más vital para garantizar nuestros derechos y nuestra seguridad en el uso cotidiano de la tecnología.

Basándonos en nuestro análisis jurídico de las leyes penales, el documento refleja la preocupación por la posibilidad de que se extienda el acoso y el enjuiciamiento de los expertos en seguridad que construyen software seguro en las Américas[4]. Muchas

[3] Vea más en <https://www.eff.org/coders-rights-americas>.
[4] La EFF ha informado sobre algunos de esos casos: *Buenos Aires censura y allana a los tecnólogos que arreglan su defectuoso sistema de voto electrónico* (<https://www.eff.org/pt-br/node/86903>); *Querido Canadá: Acceder a la información disponible públicamente en Internet no es un delito*

disposiciones sobre ciberdelincuencia que no aclaran la definición de intención maliciosa y daño real pueden convertir el trabajo general de los expertos en seguridad en delitos de responsabilidad objetiva. Nuestro documento recomienda que tanto la intención como el daño real formen parte de la definición de responsabilidad penal en las leyes de ciberdelincuencia. Sin estos elementos, la ley puede suponer una carga para el derecho fundamental a la libertad de expresión y el trabajo socialmente beneficioso de los investigadores de seguridad, permitiendo que las disposiciones se interpreten de forma amplia para atacar injustamente a las personas. Se puede abusar fácilmente de estas leyes para acosar a los investigadores de seguridad que se comprometen a proteger el interés público.

El enjuiciamiento y la detención del desarrollador de código abierto de origen sueco, el Sr. Ola Bini, en Ecuador en abril de 2019, ilustra la creciente gravedad de esta cuestión en América Latina.

Antecedentes del experto en seguridad Ola Bini

El Sr. Bini es conocido mundialmente como experto en seguridad informática y defensor de una Internet segura y abierta. El Sr. Bini es conocido principalmente por su trabajo sin ánimo de lucro sobre el protocolo de comunicación segura, OTP, y por sus contribuciones a la implementación en Java del lenguaje de programación Ruby. Ha contribuido al proyecto DECODE de la Unión Europea,[5] una iniciativa destinada a proporcionar herramientas para que las personas tengan el control de sus datos. También ha contribuido al proyecto Certbot[6] de la EFF, que proporciona seguridad fácil de usar a millones de sitios web de todo el mundo. Se trasladó a Ecuador durante su empleo en la consultora global ThoughtWorks, que tiene una oficina en Quito, y posteriormente cofundó

(<https://www.eff.org/pt-br/deeplinks/2018/04/dear-canada-accessing-publicly-available-information-internet-not-crime>). *Con una redada a Javier Smaldone, las autoridades argentinas han reiniciado su acoso a los críticos del voto electrónico* (<https://www.eff.org/pt-br/deeplinks/2019/11/raid-javier-smaldone-argentinian-authorities-have-restarted-their-harassment-e>).

[5] Más información en <https://decodeproject.eu>. El proyecto DECODE proporciona herramientas que permiten a los individuos controlar si mantienen su información personal en privado o la comparten para el bien público

[6] Certbot es una herramienta de software libre y de código abierto para utilizar automáticamente los certificados de Let's Encrypt, que proporcionan a las personas los certificados digitales que necesitan para habilitar la seguridad HTTPS para los sitios web, de forma gratuita. Let's Encrypt es una autoridad certificadora gratuita sin ánimo de lucro, que ha crecido hasta convertirse en la mayor autoridad certificadora del mundo. La seguridad de la web moderna depende de HTTPS y de las autoridades de certificación que soportan HTTPS. Vea más en <https://certbot.eff.org/about/>.

una organización sin ánimo de lucro dedicada a crear herramientas de seguridad fáciles de usar (el *Centro de Autonomía Digital*)[7].

Como muestra esta breve descripción, la **reputación mundial del Sr. Ola Bini en la comunidad de la seguridad de la información es principalmente como "constructor" de software seguro**. **No se le conoce como el tipo particular de investigador de seguridad que comprueba los fallos en el software o los servicios intentando "entrometerse" en ellos**. Aunque no hay nada malo en probar y encontrar fallos en la seguridad, el Sr. Bini es conocido por su trabajo defensivo: asegurarse de que las herramientas de privacidad están diseñadas para que otros no puedan entrar en ellas. Por lo tanto, su detención e investigación por "ataque a la integridad de sistemas informáticos" en abril de 2019 fue sorprendente y tuvo poco sentido. Las circunstancias de su detención fueron igualmente desconcertantes.

Detención del Sr. Ola Bini

La detención del Sr. Ola Bini en abril de 2019 estuvo precedida por una rueda de prensa horas después de que el gobierno nacional expulsara a Julian Assange de la embajada de Ecuador en Londres, y se ha encuadrado como parte de un proceso de defensa de Ecuador frente a las represalias de los asociados de Wikileaks. Durante la entrevista, la entonces Ministra del Interior de Ecuador anunció que el gobierno estaba a punto de detener a individuos que supuestamente estaban involucrados en el intento de establecer un supuesto centro de piratería en Ecuador, incluyendo dos hackers rusos, un colaborador de Wikileaks y una persona cercana a Julian Assange.[8] Sin embargo, no se han aportado pruebas que respalden estas afirmaciones.

Tras la detención, la Policía Nacional de Ecuador anunció en Twitter que "mediante la utilización de plataformas digitales de redes sociales, [el ciudadano] transmitía contenido de connotación social (divulgación de información) a través de sitios web, entre los más destacados, #Wikileaks. El sujeto utilizaba perfiles falsos". Este anuncio iba acompañado de una fotografía de los libros de programación que cualquier programador podría tener y

[7] Vea más en https://autonomia.digital
[8] Vea más en <https://www.eluniverso.com/noticias/2019/04/11/nota/7279946/jackers-rusos-miembro-wikileaks-viven-ecuador-denuncia-maria-paula/>.

de dispositivos informáticos comunes, como memorias USB y llaves de seguridad, que habían sido confiscados en el domicilio del Sr. Bini y de su persona[9].

Por nuestra experiencia trabajando con la comunidad de la seguridad de la información durante más de 30 años, los expertos en seguridad digital de todo el mundo suelen tener hábitos y comportamientos que las personas ajenas a esta comunidad pueden considerar excéntricos o sospechosos. Dado que los investigadores de seguridad estudian los riesgos de privacidad y seguridad asociados a las tecnologías emergentes, tienden a coleccionar hardware técnico, cifrar todas sus comunicaciones y bloquear sus ordenadores. Aquellos que construyen software de seguridad son más conscientes de su privacidad y seguridad, al igual que alguien que trabaja con pacientes de COVID-19 es más consciente de cómo protegerse contra el virus. Poseer este tipo de dispositivos y preservar la seguridad de las comunicaciones y los equipos propios no es un delito, pero puede hacer pensar a quienes no están familiarizados con esta comunidad que hay algo malo.

El seguimiento de la EFF al caso del Sr. Bini

Visita a Quito y nuestras conclusiones sobre el carácter político de la acusación del Sr. Bini

En julio de 2019, EFF realizó una visita *in situ* en Quito para investigar nuestras preocupaciones de que las autoridades de Ecuador siguieran procesando el caso legal contra el Sr. Bini sin detalles sobre el supuesto ataque digital, o sobre lo que había sido hackeado, además de las irregularidades iniciales del caso.

En nuestro viaje, la EFF habló con periodistas, políticos, abogados y académicos, junto con el Sr. Bini y su equipo de defensa. Aprendimos más sobre la sentencia de *Habeas Corpus* que liberó al Sr. Bini después de 70 días de encarcelamiento, que ha calificado su detención como ilegal y arbitraria. Para entonces, los abogados del Sr. Bini nos dijeron que habían contabilizado más de 60 violaciones del debido proceso en el juicio[10]. Los

[9] Ver en: <https://www.planv.com.ec/historias/politica/ola-bini-el-agente-wikileaks>.
[10] Véase en <https://twitter.com/calilo84/status/1152257124040368130>. En cuanto a la detención de Ola Bini, su defensa ha detallado una serie de irregularidades en un comunicado de prensa <https://goatsing.wordpress.com/2019/04/13/press-release-on-the-detention-of-ola-bini-2/>.

periodistas nos reiteraron la falta de pruebas contra el Sr. Bini, ya que nadie pudo darles descripciones concretas de lo que había hecho el experto en seguridad.

Celebramos una conferencia de prensa al final de nuestra visita a Quito, en la que concluimos que el enjuiciamiento del Sr. Bini representaba "un caso político, no un caso criminal[11]". Un factor importante que afectaba a la situación del juicio era la percepción de las consecuencias políticas de abandonar el caso, o de continuar con el enjuiciamiento. Los detalles sobre quién es responsable, o quién se beneficia de la acusación del Sr. Bini, variaban según con quién habláramos. Sin embargo, nos inquietó hasta qué punto el efecto político de la inocencia o la culpabilidad del Sr. Bini parecía afectar a la investigación. Basándonos en las entrevistas y en las circunstancias del caso, **hicimos hincapié en que la inocencia o la culpabilidad del Sr. Bini es un hecho que debe determinarse en un juicio justo que siga las debidas garantías procesales, al margen de sus ramificaciones políticas**.

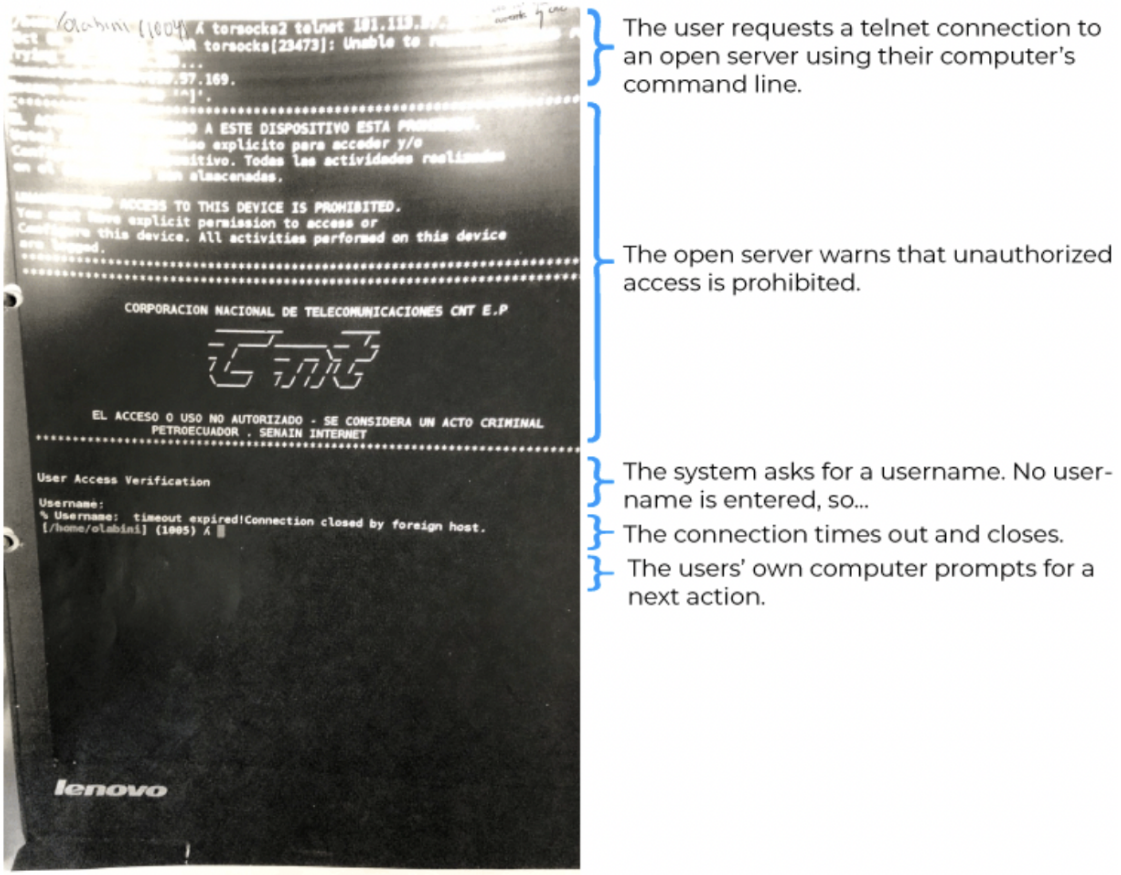
Las pruebas disponibles públicamente muestran un caso débil contra el Sr. Bini, basado en malentendidos de la tecnología

El 16 de agosto de 2019, justo después de nuestra misión en Ecuador, los medios de comunicación locales publicaron una foto que se utilizó para apoyar una acusación de que el Sr. Bini entró ilegalmente en un router de la Corporación Nacional de Telecomunicaciones (CNT), información que se utilizó en posteriores audiencias.

La foto era una captura de pantalla, que se muestra a continuación, supuestamente tomada del teléfono móvil del Sr. Bini. La prensa informó de que el teléfono fue desbloqueado por la policía después de que las imágenes de seguridad incautadas revelaran el PIN del Sr. Ola Bini cuando utilizó su teléfono en el ascensor de su propia oficina: " La cámara captó el momento en que el informático se acercaba al ascensor y digitaba la clave de ocho dígitos en la pantalla de su teléfono celular."[12] Esta prueba no era la alegada por los fiscales. Como explicó la EFF en un informe del 23 de agosto de 2019,[13] la captura de pantalla era, en cambio, consistente con alguien que revisó un servidor de acceso público

[11] Véase en https://www.eff.org/deeplinks/2019/08/ecuador-political-actors-must-step-away-ola-binis-case.
[12] Véase, por ejemplo, la siguiente noticia: <https://www.elcomercio.com/actualidad/ola-bini-fiscalia-celular-cnt.html>.
[13] Véase en <https://www.eff.org/deeplinks/2019/08/telnet-not-crime-unconvincing-prosecution-screenshot-leaked-ola-bini-case>.

y **obedeció** las advertencias de los servidores sobre el uso y el acceso. La captura de pantalla (con nuestras anotaciones):



Bloque1:
El usuario solicita una conexión telnet a un servidor abierto usando la línea de comandos de una computadora.

Bloque 2:
El servidor abierto advierte que los accesos no autorizados, están prohibidos.

Bloque 3:
El sistema pide un nombre de usuario, que no es ingresado, por lo tanto…
El tiempo de conexión expira y se cierra.
La computadora del usuario inquiere por la siguiente acción.

Como explicaron los tecnólogos de la EFF, los conocedores de los shells y utilidades de línea de comandos de estilo Unix que aparecen en la foto la reconocerían

fácilmente como la fotografía de la pantalla de un ordenador portátil, que muestra una "sesión telnet," un protocolo de comunicación inseguro que se ha abandonado en gran medida para las tecnologías de cara al público). Nuestro equipo de tecnología lo explicó:

> "Las interacciones de la línea de comandos generalmente fluyen por la página cronológicamente, de arriba a abajo, incluyendo tanto los comandos textuales escritos por el usuario, como las respuestas de los programas que el usuario ejecuta. La imagen muestra, en orden, a alguien - (presumiblemente Bini, dado que el prompt de su ordenador local muestra "/home/olabini") - solicitando una conexión, vía Tor, a un servicio telnet abierto ejecutado en un ordenador remoto.
>
> Telnet es un sistema de comunicación de sólo texto, y el programa local se hace eco de la advertencia del servicio remoto contra el acceso no autorizado. El servicio remoto pide entonces un nombre de usuario como autorización. A continuación, el sistema remoto cierra la conexión con un error de "tiempo de espera", porque la persona que se conecta no ha respondido.
>
> La última línea de la captura de pantalla muestra el programa telnet saliendo, y devolviendo al usuario a la línea de comandos de su propio ordenador."

Concluimos que **la captura de pantalla en sí misma no demostraba nada más allá de los procedimientos normales que los profesionales de la seguridad informática llevan a cabo como parte de su trabajo**:

> " Un usuario descubre un servicio telnet abierto, y se conecta a él por curiosidad o preocupación. La máquina remota responde con un mensaje del propietario del dispositivo, con una advertencia de no conectarse sin autorización. El usuario opta por respetar la advertencia y no continuar."

Los medios de comunicación también filtraron una parte de una conversación entre el Sr. Bini y su administrador de sistemas, Ricardo Arguello, una figura muy conocida en las comunidades de redes y de software libre de Ecuador. Aunque la conversación completa no se hizo pública, la imagen de arriba y nuestro análisis también pueden explicar la fracción del siguiente extracto en el que el Sr. Bini envió la captura de pantalla de arriba, a la que Arguello respondió: "Es un router. Hablaré con mi contacto en la CNT".

Como explicó nuestro equipo de tecnología, si alguien encontrara un servicio abierto de forma insegura al acceso telnet en la vasta Internet, eso es lo que podría hacer de forma razonable y responsable: enviar un mensaje a alguien que pudiera informar al propietario del servicio, con pruebas de que su sistema está abierto a que cualquiera se conecte. Y en esas condiciones, la respuesta de Arguello es justo lo que un colega podría responder: que se pondría en contacto con alguien que pudiera desconectar el servicio de telnet, potencialmente inseguro, o ponerlo detrás de un cortafuegos.

Usar Tor no es un delito

Según el informe del Sr. Bini sobre la audiencia preparatoria de juicio, el abogado de la CNT se basó injustamente en el uso de Tor, una herramienta común de seguridad en Internet, como indicación de comportamiento ilegal[14] El periodista de *El Comercio*, Valentín Díaz, entendió estas preocupaciones, diciendo "¡Qué peligro! Periodistas, activistas, abogados, ingenieros y gente que en general almacena datos sensibles usamos @torproject. No es que queramos cometer ilegalidades. Es lo responsable. No puedo navegar por donde sea exponiendo mi identidad y -de paso- la de mis contactos."[15]

Utilizar la herramienta Tor para acceder y navegar por Internet no es un delito, ni debe considerarse un comportamiento sospechoso. Tor es un navegador de código abierto, gestionado por voluntarios, que se basa en una fuerte encriptación para proporcionar una sólida protección de la privacidad en la navegación y las comunicaciones en línea[16]. Originalmente desplegado en Estados Unidos con el propósito principal de proteger las comunicaciones de la Marina, actualmente es utilizado por periodistas, activistas de derechos humanos, militares, agentes de la ley, profesionales de la informática, blogueros y otros[17]. Al proteger las identidades y ubicaciones de los usuarios, Tor ofrece una protección crucial a los periodistas y sus fuentes, a los testigos que se enfrentan al acoso y a los defensores de los derechos humanos y disidentes políticos amenazados en su vida o integridad física, entre otros. También se utiliza comúnmente para proteger contra el rastreo comercial y otras invasiones más mundanas de la privacidad

[14] Véase el post del Sr. Ola Bini en: <https://twitter.com/olabini/status/1339689974275432454>.
[15] Ver en: <https://twitter.com/v4li3nte/status/1339758702904176640>.
[16] Vea más en <https://www.torproject.org/>.
[17] Véase en <https://2019.www.torproject.org/about/torusers.html.en>.

demasiado comunes en línea. Los que construyen software seguro también suelen utilizar Tor, porque saben que la herramienta protegerá sus comunicaciones.
El Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha destacado que:

> "El cifrado y el anonimato, separados o en su conjunto, crean una zona de privacidad para proteger opiniones y creencias. Por ejemplo, permiten las comunicaciones privadas y pueden encubrir una opinión frente al escrutinio externo, algo particularmente importante en los entornos políticos, sociales, religiosos o jurídicos hostiles. Cuando los Estados imponen censuras ilegales a través del filtrado y otras tecnologías, el uso del cifrado y el anonimato puede permitir a los ciudadanos superar los obstáculos y acceder a informaciones e ideas sin la intromisión de las autoridades. Los periodistas, investigadores, abogados y miembros de la sociedad civil pueden utilizar el cifrado y el anonimato para protegerse a sí mismos (y a sus fuentes, clientes y asociados) de la vigilancia y el acoso. La capacidad de buscar en la red, elaborar ideas y comunicarse de manera segura es tal vez, para muchos, la única manera de explorar aspectos básicos de su identidad como el género, la religión, la etnia, el origen nacional o la sexualidad."[18]

Evolución reciente del caso del Sr. Ola Bini

Más recientemente, en abril de 2021, un Juez Constitucional aceptó parcialmente el recurso de *Habeas Data* del Sr. Bini**,** presentado originalmente en octubre de 2020 contra la Policía Nacional, el Ministerio de Gobierno y el Centro de Inteligencia Estratégica (CIES). La decisión ha determinado al CIES proporcionar información relacionada con si el organismo ha llevado a cabo actividades de vigilancia contra el experto en seguridad. **La sentencia considera que el CIES negó indebidamente dicha información al Sr. Bini, al no ofrecer una respuesta oportuna a su anterior solicitud de información[19]**.

[18] Véase el *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, David Kaye (A/HRC/29/32), párrafo 12. Véase en: <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32>.
[19] Vea más en: <https://ecuadortoday.media/2021/04/29/victoria-parcial-para-ola-bini-juez-reconocio-infraccion-del-cies-al-negar-entrega-de-informacion/>.

En la causa penal, **la audiencia evaluatoria y preparatoria de juicio se reanudará el 29 de junio**, más de dos años después de la detención del Sr. Bini. La audiencia se suspendió por última vez en diciembre de 2020.

Las repetidas suspensiones y reanudaciones de la audiencia preliminar plantean preocupaciones en materia de derechos humanos que también deben ser examinadas por la Secretaría. La Relatoría Especial para la Libertad de Expresión de la CIDH expresó su preocupación por el hecho de que el juicio del Sr. Ola Bini continuara en suspenso durante el año 2020. Como señala el informe anual de la Relatoría Especial para la Libertad de Expresión (RELE) para el año 2020, las audiencias preparatorias de juicio fueron suspendidas y reprogramadas por lo menos cinco veces durante ese año[20]. Desde la detención del Sr. Bini en abril de 2019, los presuntos cargos y las pruebas en su contra siguen esperando una evaluación adecuada por parte del tribunal, y el Sr. Bini, como sospechoso sometido a juicio, sigue privado del pleno disfrute de sus derechos.

Repercusiones internacionales y la Secretaría de Derechos Humanos de Ecuador

El informe de la CIDH y el seguimiento del caso por parte de la EFF ilustran la **resonancia internacional del procesamiento del Sr. Ola Bini**. Las controversias e irregularidades en torno a este caso, algunas de ellas resaltadas en esta carta, han hecho que el caso forme parte de la discusión en diferentes espacios internacionales dedicados a la protección de los derechos humanos en su intersección con la tecnología (por ejemplo, el Foro de Gobernanza de Internet, el Foro Latinoamericano de Gobernanza de Internet, RightsCon)[21], así como han desencadenado declaraciones de organismos de derechos humanos, como la ONU,[22] y de entidades de derechos humanos, como Amnistía Internacional[23]. Grupos de derechos humanos y digitales, como APC, Artículo 19, Derechos Digitales, Access Now, Fundación Karisma, también han seguido de cerca la evolución del caso.

---

[20] Véase en: <www.oas.org/es/cidh/docs/anual/2020/capitulos/rele.PDF>, párrafo 545.
[21] Véase, por orden, en: <https://www.accessnow.org/join-our-statement-for-the-protection-of-digital-rights-defenders/>; <https://www.eff.org/pt-br/deeplinks/2019/08/eff-se-suma-organizaciones-de-america-latina-que-se-oponen-la-acusacion-de-ola>; y <https://rightscon2019.sched.com/event/QX9W/the-imprisonment-of-ola-bini-building-solidarity-and-protecting-the-community>.
[22] Ver en: <https://freeolabini.org/es/LetterUN/>.
[23] Ver en: <https://www.amnesty.org/es/documents/amr28/0871/2019/es/>.

La nueva administración de Ecuador, a través de la Secretaría de Derechos Humanos, tiene una oportunidad clave para evaluar y dar seguimiento a las denuncias de violaciones de derechos en el proceso del señor Bini. Durante nuestra visita a Quito en 2019, buscamos presentar nuestras preocupaciones sobre el caso extendiendo nuestras invitaciones de reunión a la Fiscal General y a la entonces Ministra del Interior, pero no hemos obtenido respuesta. Celebramos las declaraciones de la Secretaria de Derechos Humanos en el sentido de que el organismo estudiará las denuncias de violaciones de derechos cometidas en el país.[24] La Secretaría está legítimamente posicionada para examinar las irregularidades y las violaciones de los derechos humanos que cercan el caso del Sr. Bini, así como de seguir la evolución de su proceso y vigilar que el experto en seguridad pueda recibir un juicio adecuado y justo.

Conclusión

Esta carta pone en conocimiento de la Secretaría la preocupación de la EFF por el procesamiento del Sr. Bini, basada en nuestra larga labor de lucha contra la persecución penal injusta de los expertos en seguridad. Señalamos las violaciones de las garantías procesales y de otros derechos ya reconocidas en las decisiones judiciales, la endeblez del caso contra el Sr. Bini teniendo en cuenta las pruebas disponibles públicamente, la inquietante pauta de reprogramación o suspensión de las audiencias previas al juicio, y la necesidad de garantizar al Sr. Bini un juicio justo separado del marco politizado que ha rodeado su procesamiento desde el principio.

La Secretaría de Derechos Humanos está bien posicionada para examinar las irregularidades y violaciones relacionadas con el caso del Sr. Bini, e instamos respetuosamente a tal institución a que evalúe y dé seguimiento a dichas quejas de injusticia, así como a que vele por que el Sr. Bini pueda recibir un juicio justo. Le agradecemos de antemano su atenta consideración, quedando a disposición de la Secretaría para cualquier aclaración.

[24] Ver en:<https://www.facebook.com/LaPostaEc/videos/781619866053286>.