

En el marco de **RightsCon 2023** la Misión de Observación del caso Ola Bini organizó una sesión para analizar la sentencia que ratificó la inocencia del experto informático por unanimidad respecto del proceso político-judicial que enfrenta desde abril de 2019 en Ecuador.<sup>1 2</sup>

En dicha sesión, donde participaron organizaciones de sociedad civil de diversos países, se llegó a las **siguientes conclusiones:**

**1. Primero**, según el Tribunal, toda la prueba documental presentada por la Fiscalía General del Estado (FGE) es impertinente y no conducente. Esto quiere decir que ninguno de estos elementos conducía a una verdad procesal a los efectos de probar ningún delito. Entre las supuestas pruebas figuraban los movimientos migratorios de Bini, el registro de sus visitas a Julian Assange en la embajada ecuatoriana en Londres, su contrato de servicio de internet, la cantidad de elementos informáticos de los que era propietario, traducciones de conversaciones privadas mantenidas con diversos contactos a través de distintas aplicaciones de mensajería, entre otras.

La debilidad probatoria de este caso ha quedado de manifiesto a tal punto que, actualmente, la propia Corporación Nacional de Telecomunicaciones (CNT), presunta víctima del supuesto acceso no consentido ha desistido de apelar el fallo en cuestión.

Con este posicionamiento sobre la prueba documental, el Tribunal no sólo se ajustó a derecho, sino que también cerró las puertas a una posible aplicación del llamado derecho penal de autor, esto es: a aplicar el derecho penal en función de lo que una persona representaría en cuanto a su identidad, vínculos o actividad. Pero también cerró las puertas a aplicar la Ley en función del derecho penal del enemigo, es decir, aplicarla a partir de una interpretación política y arbitraria sobre lo que significa la seguridad del Estado y quiénes podrían amenazarla.

En tal sentido, se rechazó el intento de la FGE de tildar a un activista digital, experto en seguridad informática y defensor de derechos digitales, como un peligro para la seguridad pública y del Estado. En cuanto a otros casos de persecución, invocar la cuestión de la impertinencia y no conducencia es clave para evitar peligrosas interpretaciones de criminalización, así como para resguardar sus actividades orientadas a fortalecer la seguridad informática y defender derechos en línea

<sup>1</sup> La sentencia fue dictada por los jueces Coello Serrano Pablo Marcelo, Altamirano Cárdenas Fanny Isabel y Maroto Sánchez Milton Iván.

<sup>2</sup> RightsCon es la cumbre mundial líder sobre derechos humanos en la era digital, organizada por [Access Now](https://www.accessnow.org/).

**2. Segundo,** el Tribunal sólo tomó como prueba factible de ser analizada la famosa fotografía que fue filtrada a medios de prensa, antes de formar parte del expediente. Al respecto, el Tribunal, retomando las intervenciones de los peritos de la FGE y de la CNT, concluyó que dicha fotografía es insuficiente para probar el delito investigado. Es más, entendió que con esta prueba no puede verificarse, ni siquiera, que los comandos allí ilustrados tan siquiera fueron ejecutados realmente.

Tomando en cuenta las intervenciones de los propios peritos de la CNT, el Tribunal también recordó, acertadamente, que no es una prueba digital lo que no surge de *logs*, o puede ser comprobado por logs. En suma, las representaciones gráficas (que pueden ser sujetas a manipulación) no son prueba de delitos informáticos. Se necesitan pericias forenses digitales para tal fin. Pericias que ni la Fiscalía ni CNT solicitaron para este caso.

En cuanto a otros procesos de persecución, esto ayuda a clarificar qué tipo de pruebas pueden ser técnicamente válidas para probar supuestos ilícitos informáticos. Y, fundamentalmente, este elemento de la sentencia muestra que el trabajo de las personas expertas en materia de seguridad no cuenta con las garantías necesarias en Ecuador ni en el resto de la región. El desconocimiento técnico por parte de las fiscalías y policías que investigan estos casos, en marcos de persecución a personas expertas de seguridad digital, demanda explicaciones a niveles básicos urgentemente.

El Tribunal, sin embargo, en este punto, no abordó la cuestión de la veracidad de la fotografía en cuestión, así como las circunstancias de su inclusión en el expediente. Esto es un tema a tener en cuenta en la continuación del proceso penal.

**3. Tercero,** para despejar cualquier malinterpretación, la sentencia ofrece un abordaje técnico y restringido sobre lo que significa “acceso no consentido” a un sistema informático, telemático o de telecomunicaciones, aun cuando no se haya demostrado el cometimiento de dicho delito en este caso.

El Tribunal, nuevamente retomando lo planteado por los peritos de la CNT, sostuvo que, para este caso, debería haberse probado la vulneración de algún sistema de seguridad del sistema de la CNT supuestamente afectado para probar un “acceso no consentido”. Es decir, no alcanza con afirmar, como lo hicieron CNT y FGE, que Bini habría accedido sin consentimiento a un ruteador de la CNT porque, supuestamente, habría realizado una conexión vía Telnet y utilizando Tor, pasando por la ONT (Optical Node Terminal) de propiedad de la CNT.

# Ola Bini es inocente

Una sentencia clave para la defensa de los derechos digitales

En este punto vale resaltar que, también a contramarcha de lo que intentaron posicionar CNT y FGE, el Tribunal no consideró el uso de Tor como indicativo de una conducta criminal. No reproducir estas posturas es clave no sólo para que los/as investigadores/as en seguridad digital desarrollen su trabajo y activismo, sino también para todos/as quienes quieren navegar en internet de manera segura y resguardando su privacidad.

En definitiva y por defecto, sin acceso no consentido, tampoco puede darse ninguna intencionalidad de explotación ilegítima. Es más, el Tribunal dejó claro que el supuesto sistema al que CNT dijo que Bini había accedido ni siquiera estaba en producción en la fecha en la que se habría cometido el supuesto ilícito.

En cuanto a otros casos de expertos/as digitales, este posicionamiento del Tribunal refuerza la doctrina técnica sobre lo que implica acceder sin consentimiento a un sistema restringido. Esto también deja más certezas para quienes hacen investigación en seguridad digital e informática para la defensa de los derechos en línea, contando con más garantías de no persecución y criminalización.

**Todos estos elementos constituyen precedentes clave** para otros casos de personas expertas en seguridad informática y defensores/as de derechos digitales perseguidos/as que deben ser ratificados. Además, estos elementos son relevantes para resguardar el trabajo de dichos expertos y defensores en torno a garantizar los derechos humanos en línea.

Por lo expuesto, las organizaciones de sociedad civil de la Misión **demandamos a las autoridades judiciales ecuatorianas correspondientes ratificar el estado de inocencia de Bini en la instancia de apelación.**

**La Misión de Observación seguirá monitoreando el desarrollo del caso** con el fin de asegurar el cumplimiento de las garantías de debido proceso.



La Libre



intervozes  
coletivo brasil de  
comunicação social

Fundación  
karisma



CDH  
COMITÉ PERMANENTE  
POR LA DEFENSA DE LOS  
DERECHOS HUMANOS

@ DERECHOSDIGITALES  
Derechos Humanos y Tecnología en América Latina



APC  
ASSOCIATION FOR  
PROSECUTIVE  
COMMUNICATIONS



DERECHOS Y JUSTICIA  
OBSERVATORIO



Asociación de Software Libre del Ecuador

