Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

accessnow

La persecución de la comunidad de la seguridad informática en América Latina

Agosto del 2021

*Este informe está basado en investigaciones y análisis de la **Clínica de Ciberderecho de la Facultad de Derecho de Harvard, ubicada en el Berkman Klein Center for Internet & Society**, y cuenta con el trabajo de investigación de **Fernanda Gómez Balderas y Payton Wulff, encabezado por Jessica Fjeld, profesora de Derecho y directora adjunta de la Clínica de Ciberderecho**. Access Now es responsable del contenido aquí presentado y cualquier error, omisión o mala interpretación serán puramente nuestros.*

accessnow

TABLA DE CONTENIDOS

AGRADECIMIENTOS

El presente informe fue posible, en parte, gracias al conocimiento compartido de las organizaciones de la sociedad civil que trabajan a diario para defender a investigadores e investigadoras de seguridad digital de América Latina. Valoramos enormemente su tiempo, su confianza y su interés en este tema. Agradecemos a Fundación Karisma por sus aportes y experiencia y por ayudarnos a identificar casos de estudio en Colombia. Gracias, además, a Fundación Vía Libre por sus perspectivas sobre la comunidad de la seguridad informática en Argentina y su ayuda en la identificación de casos actuales de persecución de investigadores e investigadoras de seguridad digital. Para comprender mejor el panorama de ciberseguridad en México y conocer sobre la persecución de estas personas en otros países latinoamericanos, recibimos la ayuda de ARTÍCULO 19, en particular con respecto a los capítulos sobre México y América Central, y Brasil y América del Sur. Queremos agradecer, además, a la abogada Jazmín Aquino por brindarnos información y orientación adicional sobre esta comunidad en México. Por último, agradecemos especialmente al Centro de Autonomía Digital, a su directora ejecutiva, Sara Zambrano, y al abogado Carlos Soria, por compartir con nosotros conocimiento y experiencia de primera mano respecto del caso de Ola Bini y su constante apoyo en la elaboración de este informe. Nuestro caso de estudio sobre la persecución de Ola Bini se vio muy enriquecido gracias a su continua voluntad de compartir sus experiencias con nuestro equipo.

INTRODUCCIÓN

Quienes se dedican a la investigación de la seguridad digital son los héroes no reconocidos de la ciberseguridad. Su trabajo de identificación y denuncia de vulnerabilidades y debilidades en infraestructuras digitales, como el internet, el código de software y los sistemas informáticos, nos benefician gracias a que logran que estos sistemas sean más seguros. A pesar del evidente valor de su trabajo, los Gobiernos de todo el mundo no solo menosprecian a estas personas, sino que también las persiguen por encontrar e informar vulnerabilidades. Este informe apunta a crear más consciencia sobre el trato perjudicial de los Gobiernos en relación con investigadores(as) de seguridad digital, tanto en la ley como en la práctica. Se centra, particularmente, en la respuesta de los Gobiernos a investigaciones de seguridad digital en cuatro países latinoamericanos: Argentina, Colombia, Ecuador y México.

Al usar el término "investigadores(as) de seguridad digital", nos referimos a investigadores(as), desarrolladores(as) de software, especialistas del ámbito técnico y demás actores de la comunidad de la seguridad de la información que, entre sus tantas otras actividades, identifican y denuncian vulnerabilidades en los sistemas digitales para beneficiar al público en general. A esta comunidad se la conoce también como la comunidad "infosec", o de seguridad informática. A menudo, las figuras políticas y demás agentes gubernamentales carecen de un entendimiento técnico de lo que implica la investigación sobre seguridad digital, y la presentan como "hackeo" malicioso y perpetúan públicamente la narrativa dañina de que la investigación sobre seguridad digital debe ser penalizada. Quienes se dedican al "hacking ético" o son hackers para el bien general representan un pilar esencial de la comunidad de infosec. Sin la investigación pionera sobre seguridad digital, la ciberseguridad mundial estaría en peligro y usuarios y usuarias correrían un riesgo mayor. Al localizar, analizar y exponer vulnerabilidades de infosec, la investigación sobre seguridad digital hace que internet y los sistemas informáticos sean más seguros: los fortalece contra violaciones de datos y otros ataques a la ciberseguridad. Además, la investigación de seguridad digital, a menudo, promueve los derechos humanos, como la libertad de expresión y el derecho a la privacidad, revelando y denunciando daños ocasionados por entes públicos y privados a través de la tecnología, como el uso de *spyware* o *malware* contra ciertos grupos sociales.

Con "perseguir", nos referimos, en general, a cualquier actividad llevada a cabo por un Gobierno o ente que actúe en conjunto con el Gobierno con el fin de castigar, sancionar, acosar o intimidar a quienes investigan sobre seguridad digital. Las persecuciones se pueden dar de muchas formas: procesamiento penal, acciones judiciales civiles, sanciones regulatorias o administrativas, acoso físico, vigilancia, y otros medios de intimidación extralegal. Las motivaciones que impulsan dichas persecuciones no siempre son claras. En ocasiones, un Gobierno puede desear mantener la vulnerabilidad oculta de la atención pública para evitar el escrutinio y, por consiguiente, intenta silenciar al mensajero; es decir, a la persona que, investigando, descubrió la falla. En otros casos, la persecución puede ser el resultado de una insuficiente atención en la elaboración o actualización de marcos legales. Durante los últimos años, muchos países promulgaron leyes en materia de ciberdelincuencia que no eximen explícitamente a investigadores(as) de seguridad digital de su alcance, lo que crea gran incertidumbre jurídica y supone un riesgo para estas personas.

En cada país que se aborda en este informe (Argentina, Colombia, Ecuador y México), primero identificamos el marco legal relevante y destacamos algunas leyes federales del país que podrían usarse para imponer responsabilidad legal penal o civil a investigadores(as) de seguridad digital a escala nacional. Luego, damos ejemplos de persecución de investigadores(as) en dichos países, ilustrados mediante casos de estudio que identifican a personas investigadoras de la seguridad digital que han sido perseguidas recientemente por sus trabajos de investigación de vulnerabilidades o por su asociación con la comunidad de infosec. Nuestra conclusión incluye una serie de recomendaciones para aumentar, de ahora en adelante, el apoyo y la protección de las personas que se dedican a este tipo de investigación en América Latina.

I. ARGENTINA

MARCO LEGAL Y ANÁLISIS

En Argentina, existen varias leyes que podrían usarse para sancionar a quienes informen vulnerabilidades en infraestructuras IT, incluidas múltiples disposiciones del Código Penal de la Nación Argentina. Ciertas disposiciones del régimen de propiedad intelectual de Argentina también podrían imponer responsabilidades legales civiles y penales a investigadores(as) de seguridad digital, en casos en los que sus revelaciones reproducen —y, por lo tanto, infringen— secciones de código protegido por derechos de autor. En este documento identificamos y analizamos algunas de las disposiciones clave de la legislación argentina que, probablemente, se usen para justificar acciones legales contra personas que investiguen la seguridad digital.

En el pasado, la fuerza pública argentina ha recurrido a las leyes de ciberdelincuencia para usarlas contra personas que investigan la seguridad digital y llevan a cabo investigaciones sobre vulnerabilidades. Por ejemplo, el artículo 183 del Código Penal se utilizó para cuestionar las actividades del desarrollador de software Joaquín Sorianello en el 2015.[1] En virtud del artículo 183, "[s]erá reprimido con prisión de [hasta] un año [...] el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos".[2] Si bien "alterar" puede interpretarse de manera más amplia, "destruir" e "inutilizar" sugieren que debe haber algún tipo de daño para que

[1] *Consulte* "Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica", La Nación, 2 de agosto del 2016. Disponible en https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088/

[2] Código Penal, art. 183: "Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

ocurra la violación del artículo.[3]

Otro artículo que también podría usarse para penalizar el trabajo de investigación sobre seguridad digital es el artículo 157 bis del Código Penal. Esta disposición (en la parte relevante para este documento) sanciona a quien "a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales" o a quien "ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley".[4]

Según cómo se interpreten los términos "a sabiendas" e "ilegítimamente" utilizados en el art. 157 bis, es probable que quienes se dediquen a la investigación de la seguridad digital puedan ser sancionados. Según los significados básicos de dichos términos, estas personas son conscientes de que, en la mayoría de los casos, su acceso es "ilegítimo". Por ejemplo, puede decirse que, si un(a) investigador(a) de seguridad digital ve una vulnerabilidad en la base de datos de una empresa y hackea el sistema para encontrar el código responsable de tal vulnerabilidad a fin de informarla a la empresa, esta persona *sabría* que su acceso fue *ilegítimo*.

El art. 153 bis del Código Penal también usa lenguaje poco específico que podría interpretarse para penalizar a investigadores(as) de seguridad digital. Dicho artículo sanciona a quien "a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido".[5]

Una vez más, el requisito de intencionalidad del artículo 153 bis, "a sabiendas", es lo suficientemente general como para ser usado para procesar las actividades de investigación de vulnerabilidades. Podría decirse que las personas que investigan la seguridad digital siempre tienen consciencia de que acceden a sistemas sin autorización. El estatuto no reconoce que, a pesar de que cuentan con el conocimiento necesario, quienes investigan la seguridad digital generalmente tienen la intención específica de beneficiar a la sociedad exponiendo vulnerabilidades y mejorando los sistemas de seguridad, en lugar de malas intenciones para cometer delitos. Al reducir la intencionalidad al mero conocimiento, el estatuto no reconoce esta distinción. El uso de lenguaje poco preciso en el art. 153 bis también plantea la pregunta de qué

[3] *Supra* n. 1. La interpretación judicial de este artículo en el caso de Joaquín Sorianello determinó que Sorianello no había violado esta ley, debido a que no había causado daño alguno en el sistema informático que estaba investigando. La jueza observó que, si bien Sorianello había accedido a los sistemas, no los había dañado, sino que había encontrado vulnerabilidades y las había informado a la empresa con el objetivo de mejorar los sistemas. Esta interpretación reconoce la utilidad social de la investigación sobre seguridad digital.

[4] Código Penal, art. 157 bis: "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno (1) a cuatro (4) años".

[5] Código Penal, art. 153 bis: "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

constituye una autorización y quién da autorización para el acceso lícito a tales sistemas.

Además del derecho penal, ciertas disposiciones de las leyes de propiedad intelectual de Argentina podrían usarse para sancionar a las personas que investigan la seguridad digital. Según el régimen de propiedad intelectual argentino, las protecciones de derechos de autor se extienden al código informático y al código objeto, así como a la compilación de datos en una base de datos.[6] Quienes investigan la seguridad digital podrían, por ende, infringir los derechos de autor si sus revelaciones exigieran la reproducción de parte de un código de software. El titular de los derechos de autor del código de software podría iniciar acciones civiles por violación contra una persona que investigue la seguridad digital.

Asimismo, la violación de derechos de autor en Argentina también se puede castigar mediante sanciones penales. Según el art. 71 del régimen de propiedad intelectual, "[s]erá reprimido con la pena establecida por el artículo 172 del Código Penal, el que defraude los derechos de propiedad intelectual", lo que puede incluir hasta seis años de prisión.[7] El amplio alcance de lo que podría constituir defraudar derechos de propiedad intelectual implica que este artículo brinda otra vía para que funcionarios, empresas y demás actores argentinos califiquen como delitos las actividades legítimas de quienes investigan la seguridad digital.[8]

Caso de estudio

En el último tiempo, han ocurrido varios casos de persecución, penal o de otra índole, a investigadores(as) de seguridad digital en Argentina. En este informe, nos centramos en dos de los casos más recientes que identificamos en nuestra investigación: los casos de Javier Smaldone y Gaspar Ortmann.[9]

[6] Régimen Legal de La Propiedad Intelectual, Ley 11.723, art. 1: "A los efectos de la presente Ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; (...)"
[7] Régimen Legal de la Propiedad Intelectual, Ley 11.723, art. 71: "Será reprimido con la pena establecida por el artículo 172 del Código Penal, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta Ley". Código Penal, art. 172: "Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño".
[8] Practical Law de Westlaw, "Copyright litigation in Argentina: overview, Practical Law Country Q&A w-010-2109" indica que "en principio, cualquier tipo de violación intencional de los derechos de autor está sujeta a las sanciones provistas en el artículo 71 del Régimen de la Propiedad Intelectual".
[9] Como mencionamos previamente, el desarrollador de software Joaquín Sorianello también estuvo involucrado en un caso prominente en el 2016, que luego fue desestimado. Este informe no analizará su caso en profundidad.

Javier Smaldone es investigador de seguridad digital y un reconocido experto informático en la comunidad de infosec de Argentina. En el pasado, Smaldone ha llevado a cabo investigaciones de seguridad en el uso de máquinas de voto electrónico en Argentina, y ha declarado ante el Senado argentino para compartir su conocimiento experto sobre el tema y desaconsejar el uso de tales dispositivos. Smaldone tiene un blog personal en el que, a menudo, critica las prácticas de ciberseguridad del Gobierno, y también es muy activo en su cuenta personal de Twitter en relación con estos temas.[10]

En octubre del 2019, la policía argentina detuvo a Smaldone para interrogarlo por sospecha de hackeo y filtración de datos de sistemas del Gobierno, un escándalo que luego fue conocido como "La Gorra Leaks 2.0".[11] La policía detuvo a Smaldone durante 12 horas antes de devolverle la libertad. Las autoridades también allanaron su casa, e incautaron y revisaron varios de sus teléfonos, computadoras y pen drives.

Días después de su arresto, Smaldone, conociendo su propia inocencia, solicitó los documentos de los tribunales que la policía había presentado para obtener la orden de arresto. Le sorprendió descubrir que la principal "prueba" que había usado la policía para obtener la orden habían sido sus tuits en los que hablaba y hacía un análisis de la filtración de datos "La Gorra Leaks 2.0".

Además, Smaldone se percató de que la policía había estado llevando a cabo una investigación en su contra durante algunos meses. Su investigación incluía: el "ciberpatrullaje" de la cuenta de Twitter de Smaldone y sus cuentas de otras redes sociales; la solicitud de los registros telefónicos de su celular personal a su proveedor de servicios móviles para obtener la ubicación de su teléfono y sus registros de llamadas entrantes y salientes; la solicitud a la empresa WhatsApp de la información de su cuenta, incluidas las direcciones IP utilizadas en conexión durante los meses anteriores a la investigación; la solicitud de registros de su uso de la tarjeta de transporte público "Sube" durante el año anterior a la investigación; la vigilancia de Smaldone en lugares públicos y la toma de fotografías de su persona; la colocación de cámaras de vigilancia fuera de la casa de los hijos de Smaldone.[12] Este escandaloso nivel de vigilancia por sí solo debería considerarse persecución, especialmente teniendo en cuenta que la policía no contaba con pruebas fehacientes de la participación de Smaldone en las filtraciones de datos antes de comenzar con la investigación.

Aunque nunca se lo acusó oficialmente conforme al Código Penal, el caso de Smaldone ejemplifica cómo alguien con conocimiento técnico de los sistemas IT y asociado a la comunidad de infosec puede ser perseguido sin causa justa. Básicamente, la policía argentina perfiló a Smaldone como un hacker criminal debido a su conocimiento técnico y por su rol vocero en la denuncia y el análisis de hackeos mediante su cuenta de Twitter, y quizás también debido a sus opiniones

[10] El blog de Smaldone está disponible en: https://blog.smaldone.com.ar/. Su cuenta de Twitter es @mis2centavos (https://twitter.com/mis2centavos?lang=en)
[11] Para ver más información sobre el caso, visite: https://www.eff.org/es/deeplinks/2019/11/raid-javier-smaldone-argentinian-authorities-have-restarted-their-harassment-e
[12] Smaldone analiza toda esta información en su posteo de blog "Allanado y detenido por tuitear", de su autoría, que publicó el 25 de enero del 2020. https://blog.smaldone.com.ar/2020/01/25/allanado-y-detenido-por-tuitear/

críticas sobre cómo el Gobierno ha manejado estos asuntos en el pasado. Como resultado, fue sujeto de intimidación e invasión de la privacidad.

El caso de Smaldone ejemplifica cómo la narrativa en torno a los hackeos puede perjudicar a quienes investigan la seguridad digital de manera legítima o a quienes son meramente miembros conocidos de la comunidad de infosec. Quienes ocupan posiciones de poder a menudo perpetúan esta narrativa dañina debido a sus propias motivaciones políticas o su falta de conocimiento técnico de estos conceptos, o ambos. Según expresa en su blog, Smaldone considera que este caso es nada más y nada menos que una persecución política, y ahora le preocupa qué más puede sucederle a él o a otras personas que trabajen en el espacio de infosec en Argentina en el futuro.

Gaspar Ariel Ortmann es gerente de ingeniería en la empresa de viajes Despegar[13] y disfruta buscar vulnerabilidades en infraestructuras IT en su tiempo libre para ayudar a fortalecer estas tecnologías. En el 2019, Ortmann descubrió una vulnerabilidad en el sistema de Home Banking del Banco Nación que permitía a los usuarios modificar el precio del dólar estadounidense sin que el sistema de seguridad del banco verificara el precio. Como resultado, los usuarios podían comprar dólares por menos y venderlos por más de su valor de cambio real. Ortmann llevó a cabo múltiples transacciones él mismo para demostrar la vulnerabilidad.[14]

Luego, Ortmann intentó revelar esta vulnerabilidad a los funcionarios de seguridad del banco, comunicándose por correo electrónico, LinkedIn, y WhatsApp. Tras no recibir respuestas, escribió una carta con capturas de pantalla de las transacciones que había llevado a cabo que demostraban la vulnerabilidad y, luego, la entregó personalmente en una sucursal del banco.

A pesar de haber informado la vulnerabilidad de buena fe y haber tomado los pasos necesarios para devolver las ganancias de las transacciones que hizo como parte de la investigación, Ortmann fue procesado penalmente de todos modos.[15] Hace poco, en diciembre del 2020, el juez a cargo del caso Ortmann decidió desestimar el asunto. El juez explicó que Ortmann no había accedido de manera indebida al sistema informático, debido a que, como cliente del banco, tenía acceso al sistema de Home Banking. El juez también señaló la utilidad pública de la revelación de Ortmann.

El resultado del caso Ortmann establece un precedente a favor de la investigación de seguridad y la revelación de vulnerabilidades que, con suerte, será recordado por las fuerzas públicas argentinas y el Poder Judicial en el futuro. Sin embargo, este caso también es prueba de que, sin los mecanismos necesarios para la revelación de vulnerabilidades, quienes investigan la seguridad digital aún arriesgan sus reputaciones y corren el riesgo de verse involucrados en procedimientos legales al informar las vulnerabilidades que encuentran.

[13] Despegar es una “empresa de viajes líder en América Latina… que opera en 20 países”. Investor.desgapar.com, “Company Profile”. Disponible en https://investor.despegar.com/home/default.aspx
[14] Sebastián Gamen, “Caso Gaspar Ariel Ortmann, otra sentencia a favor del hacking ético”. Perfil. 11 de diciembre del 2020. Disponible en https://www.perfil.com/noticias/opinion/sebastian-gamen-caso-gaspar-ariel-ortmann-otra-sentencia-a-favor-del-hacking-etico.phtml
[15] Ibíd.

II. COLOMBIA

MARCO LEGAL Y ANÁLISIS

Colombia cuenta con una serie de leyes penales, incluidos el Código Penal y la Ley de Delitos Informáticos, que podrían usarse para sancionar a las personas que investigan la seguridad informática por varias razones, entre las que se incluyen el acceso a sistemas informáticos, la interceptación y revelación de datos informáticos, y la violación de datos personales. Además, Colombia cuenta con leyes de derechos de autor y de propiedad intelectual (Ley sobre Derechos de Autor), así como también regulaciones de protección de datos personales (Ley de Protección de Datos Personales)[16] que podrían utilizarse para imponer multas y otras sanciones. En los siguientes párrafos, mencionamos detalladamente las disposiciones que podrían ser empleadas por el Gobierno en contra de investigadores e investigadoras de seguridad informática.

En el 2009, se promulgó la Ley de Delitos Informáticos 1273 como parte del Código Penal.[17] Esta ley incorporó nuevos delitos penales en base al Convenio de Budapest sobre Ciberdelincuencia.[18] Entre las disposiciones que podrían utilizarse en contra de las personas que investigan la seguridad digital, se encuentra el art. 269A, que aborda el acceso abusivo a sistemas informáticos. El artículo señala que:

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".[19]

Un problema recurrente en el marco penal colombiano sobre la ciberdelincuencia es la ausencia de intencionalidad de causar daños o de obtener un beneficio económico como parte del delito.[20] Una persona investigadora de la seguridad informática podría ser responsable penalmente de acceder a un sistema informático "no protegido", independientemente de su intención. Para

[16] En general, las regulaciones de protección de datos personales tienden a apoyar los derechos humanos, en particular la privacidad, en la esfera digital, y esta referencia no pretende desalentar su adopción o aplicación. Sin embargo, en casos individuales, es posible que estas leyes se empleen en contra de miembros de la comunidad de infosec, por ejemplo, cuando su trabajo expone la deficiencia de la seguridad de datos sensibles que los lleva a acceder a tales datos.
[17] La Ley de Delitos Informáticos del 2009 pasó a formar parte de los capítulos I y II, título VII bis de la Protección de la Información y de los Datos del Código Penal.
[18] Colombia ratificó plenamente el Convenio de Budapest sobre Ciberdelincuencia en el 2020. *Consulte*: Consejo de Europa; "Columbia joined the Budapest Convention on Cybercrime", (2020), disponible en https://www.coe.int/en/web/cybercrime/-/colombia-joined-the-budapest-convention-on-cybercrime
[19] Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
[20] Fundación Karisma, Rutas de Divulgación, (2019), p. 22. Disponible en: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf

agravar las razones de preocupación, si una persona descubre que un sistema tiene una vulnerabilidad y la informa, esta persona puede ser declarada responsable en lo penal, aunque no haya causado ningún daño o perjuicio.

Asimismo, este tipo de conducta se define como "abusiva", aunque la única razón aparente para calificarla de esta manera es la ausencia de autorización para el acceso a un sistema informático. Si una persona accede por accidente a un sistema no protegido, podría ser sancionada en virtud del artículo 269A.

Otra disposición clave es el art. 296C, que sanciona la interceptación de datos informáticos. El artículo señala que:

"El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".[21]

En este artículo, no queda claro si la interceptación puede ser el resultado de un acceso a un sistema informático mientras se buscan vulnerabilidades. Al igual que con el art. 269A, no se hace referencia a la intención de causar daños, lo que abre la posibilidad de que el artículo tenga una cantidad mayor de aplicaciones.

Además, el art. 269D, que sanciona el daño informático, también podría ser problemático. Este artículo responsabiliza "[a]l que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos".[22]

La "alteración" de datos informáticos, software o un sistema de procesamiento informático, en contraposición con las demás conductas detalladas en la ley, no necesariamente implica un daño al sistema o a los datos. Además, existe el riesgo de que, al acceder un sistema con vulnerabilidades que la persona investigadora no conoce a la perfección, se causen alteraciones o daños, por los que podría responsabilizarse a tal persona.[23]

El art. 269H también incluye algunas situaciones en las que las penas aumentan entre un 50 % y un 75 %. Estos agravantes incluyen:
"(1) Si la conducta se cometiere sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales. (…)
(4) Revelando o dando a conocer el contenido de la información en perjuicio de otro. (…)

[21] Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
[22] Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
[23] Fundación Karisma, Rutas de Divulgación, (2019), p. 22. Disponible en: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf

(5) Obteniendo provecho para sí o para un tercero".[24]

Este artículo aumenta el riesgo que corren investigadores(as) de seguridad digital que identifiquen vulnerabilidades en sistemas o redes gubernamentales. Según el art. 269H (1), no es necesario demostrar la intención o el motivo: la pena se puede aumentar por la mera razón de que el sistema pertenezca al Gobierno. El párrafo (4) también es ambiguo y potencialmente peligroso para la investigación de seguridad, ya que informar una vulnerabilidad se puede interpretar como revelación de información. Finalmente, el párrafo (5) sí incluye un elemento que debería ser parte de todos los delitos cibernéticos: la intención de obtener un beneficio. Idealmente, la quinta condición debería estar incluida, junto con la provocación de daños, en todas las situaciones que presenta la Ley 1273.

Colombia también sanciona las violaciones a los derechos de autor mediante el Código Penal y la Ley sobre Derechos de Autor N° 23 de 1982. De conformidad con la ley colombiana, las personas que investigan la seguridad informática pueden ser procesadas por infracción de derechos de autor. En este sentido, el software es una obra literaria y puede ser registrado según los artículos 1, 2, 4 y 7[25] del Decreto 1360 de 1989, que regula el registro de software en el Registro Nacional del Derecho de Autor. El reconocimiento y la protección del software también se recogen en los artículos 3,[26] 4,[27] y 23[28] de la Decisión 351 del Acuerdo de Cartagena de 1993.

El Código Penal incluye tres delitos penales de violación a derechos de autor que son penados con

[24] Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles, de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

[25] Artículo 1 De conformidad con lo previsto en la ley 23 de 1982 sobre Derechos de Autor, el soporte lógico (software) se considera como una creación propia del dominio literario. Artículo 2 El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción de programa y el material auxiliar. Artículo 4 El soporte lógico (software), será considerado como obra inédita, salvo manifestación en contrario hecha por el titular de los derechos de autor. Artículo 7 La protección que otorga el derecho de autor al soporte lógico (software), no excluye otras formas de protección por el derecho común.

[26] Artículo 3 (…) "Programa de ordenador (Software): Expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador -un aparato electrónico o similar capaz de elaborar informaciones- ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso".

[27] Artículo 4 La protección reconocida por la presente Decisión recae sobre todas las obras literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer, y que incluye, entre otras, las siguientes: (...) l) Los programas de ordenador.

[28] Artículo 23 Los programas de ordenador se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto. En estos casos, será de aplicación lo dispuesto en el artículo 6 bis del Convenio de Berna para la Protección de las Obras Literarias y Artísticas, referente a los derechos morales. Sin perjuicio de ello, los autores o titulares de los programas de ordenador podrán autorizar las modificaciones necesarias para la correcta utilización de los programas.

prisión: violación a los derechos morales de autor (artículo 270),[29] defraudación a los derechos patrimoniales de autor (artículo 271),[30] y violación a los mecanismos de protección de los derechos patrimoniales de autor (artículo 272).[31] La violación a los derechos morales incluye la mutilación o transformación de una obra literaria, mientras que la violación a los derechos patrimoniales incluye la reproducción y distribución de obras literarias, entre otras cosas. Específicamente, el art. 271 indica que la reproducción de estas obras mediante el uso de medios informáticos será sancionada cuando el autor esté motivado por la obtención de un beneficio económico, ya sea directo o indirecto. Dado que puede interpretarse que la investigación de vulnerabilidades puede generar un beneficio económico indirecto para quien la lleve a cabo, como la mejora de su reputación, esos delitos podrían usarse para perseguir a estas personas. Identificar vulnerabilidades y acceder a sistemas informáticos puede implicar acceder a código e instrucciones de programación que, cuando se replican (aunque sea incidentalmente) o se

[29] Artículo 270. Violación a los derechos morales de autor. Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veintiséis punto sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien: (…) 3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico. PARÁGRAFO. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

[30] Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley, sin autorización previa y expresa del titular de los derechos correspondientes: 1. Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones. (…) 3. Alquile o, de cualquier otro modo, comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas. (...) 5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título. (…) PARÁGRAFO. La reproducción por medios informáticos de las obras contenidas en el presente artículo será punible cuando el autor lo realice con el ánimo de obtener un beneficio económico directo o indirecto, o lo haga a escala comercial.

[31] Artículo 272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones. Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis punto sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes, quien: 1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados. 2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada. 3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo o sistema, que permita a los titulares del derecho controlar la utilización de sus obras o fonogramas, o les posibilite impedir o restringir cualquier uso no autorizado de estos. 4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos.

transforman, pueden resultar en la violación de derechos de autor.[32] Asimismo, las actividades de investigación digital pueden procesarse según el párrafo 3 del art. 272, que sanciona a cualquier persona que elimine o evada un sistema "que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de estos". Obtener acceso a un sistema puede equivaler a evadirlo o tomar el control del código y, consecuentemente, las personas que lo hagan podrían ser consideradas responsables.

La Ley sobre Derechos de Autor sanciona las violaciones a los derechos de autor con encarcelamiento (art 232) y multas (art. 233). Al igual que el Código Penal, el art. 232 enumera una serie de conductas ilícitas que pueden resultar en tres y hasta seis meses de prisión. Estas conductas incluyen la reproducción y modificación de una obra, pero las penas son considerablemente menores que las de los delitos analizados previamente.

Por otra parte, el artículo 12[33] de la Ley 1915 del 12 de julio del 2018 (que modifica la Ley sobre Derechos de Autor y establece nuevas disposiciones) impone penas civiles ante ciertas conductas, que incluyen la evasión no autorizada de medidas tecnológicas para controlar el acceso a una obra. Existen algunas excepciones a la responsabilidad legal, que incluyen la ingeniería inversa de buena fe. Sobre todo, la ley exime de responsabilidad legal si las acciones fueron realizadas con la única intención de identificar y analizar las fallas y vulnerabilidades de las tecnologías que codifican y decodifican información. Para aprovechar esta exención, sin embargo, se debe obtener legalmente una copia de la obra o una muestra del trabajo y hacer un esfuerzo de buena fe por conseguir la autorización,[34] lo cual podría ser todo un desafío debido a la hostilidad de muchas instituciones hacia investigadores e investigadoras.

---

[32] En el 2014, Diego Gómez, estudiante de Biología, fue procesado por haber subido la tesis doctoral de otra persona a Scribd para que otros estudiantes la consulten. La pena variaba entre cuatro y ocho años. El 24 de mayo del 2017, fue declarado inocente debido a que no había divulgado la obra, porque ya era pública, ni había buscado obtener rédito, y su conducta había tenido un propósito educativo. Sin embargo, esta resolución fue apelada. El 4 de diciembre del 2017, el fallo inicial fue confirmado y Gómez fue declarado inocente.
Aunque este caso no involucra a un investigador de seguridad digital, se incorporó en este informe para mostrar que la legislación actual colombiana en materia de derechos de autor puede representar una amenaza a la comunidad y otras personas que usen internet. Además, ayuda a enfatizar la falta de proporcionalidad de la sanción por violación de derechos de autor en relación con el uso justo. Consulte: Fundación Karisma "Campaña de crowdfunding busca ayudar a biólogo acusado penalmente por compartir una investigación académica en línea", Fundación Karisma, 12 de junio del 2017. Disponible en: https://web.karisma.org.co/campana-de-crowdfunding-busca-ayudar-a-biologo-acusado-penalmente-por-compartir-una-investigacion-academica-en-linea/; Fundación Karisma, "El caso de Diego Gómez termina", 15 de diciembre del 2017. Disponible en: https://web.karisma.org.co/compartir-no-es-delito-sharing-is-not-a-crime/

[33] Artículo 12. Medidas tecnológicas e información sobre gestión de derechos. Independientemente de que concurra una infracción al derecho de autor o a los derechos conexos, incurrirá en responsabilidad civil quien realice cualquiera de las siguientes conductas: a) Sin autorización eluda las medidas tecnológicas efectivas impuestas para controlar el acceso a una obra, interpretación o ejecución o fonograma protegidos, o que protegen cualquier derecho de autor o cualquier derecho conexo al derecho de autor frente a usos no autorizados (…)

[34] Artículo 13. Excepciones a la responsabilidad por la elusión de las medidas tecnológicas. Las excepciones a la responsabilidad consagrada en los literales a) y b) del artículo anterior son las siguientes, las cuales serán aplicadas en consonancia con los parágrafos de este artículo. a) Actividades de buena fe no infractoras de ingeniería inversa realizadas a la copia de un programa de computación obtenida legalmente, siempre que los elementos particulares de dicho programa no hubiesen estado a disposición inmediata de la persona involucrada en dichas actividades, con el único propósito de lograr la interoperabilidad de un programa de computación creado independientemente con otros programas. b) Actividades de buena fe no infractoras, realizadas por un investigador que haya obtenido legalmente una copia, interpretación o ejecución no fijada o muestra de una obra, interpretación o ejecución o fonograma, y que haya hecho un esfuerzo de buena fe por obtener autorización para realizar dichas actividades, en la medida necesaria, y con el único propósito de identificar y analizar fallas y vulnerabilidades de las tecnologías para codificar y decodificar la información.

Caso de estudio

Juliana Peña es ingeniera en software, colombiana, y recibió atención mediática y del Gobierno cuando identificó un problema de seguridad en el censo digital colombiano. El eCenso empezó a estar disponible al público el 9 de enero del 2018 bajo la gestión del Departamento Administrativo Nacional de Estadística, también conocido como el DANE. Juliana informó que el sitio web no lograba brindar la seguridad adecuada para quienes lo usaban, ya que guardaba sus contraseñas sin cifrado efectivo. Según explicó Peña, al completar ella misma el censo, "la página me mostró mi contraseña en la pantalla cuando terminé mi registro. Esto me dio la sospecha de que la página almacena la contraseña en texto plano. Lo pude confirmar usando la opción de 'Olvidé mi contraseña', la cual me envió por email mi contraseña en texto".[35]

Además, luego de navegar la página del censo, no había manera de cambiar la contraseña. Si el DANE almacenaba las contraseñas sin medidas de seguridad, podía poner en riesgo cuentas de usuarios en diferentes páginas web en las que hubieran usado la misma contraseña. Peña denunció la falta de seguridad como un error terrible del Gobierno.[36]

Unos días después, Peña aclaró que, aunque las contraseñas no se almacenaban en texto plano, el sistema utilizaba cifrado simétrico (el cual es reversible) y que la clave estaba disponible al público para cualquiera que quisiera verla. En cambio, sugirió usar un *hash-salt* no reversible.[37]

El DANE declaró que la información que daba Peña era falsa. El Departamento emitió una declaración por escrito en la que explicaba que la herramienta se atenía a estrictos parámetros de seguridad. Cuando una persona se registra, según el DANE, su contraseña solo se envía de manera personal y exclusiva si la persona la olvida. Según el DANE, Peña carecía de la experiencia y el conocimiento suficientes para emitir tales declaraciones, las cuales, según el Departamento, no tenían respaldo fáctico.[38]

Aunque el DANE recalcó que su sistema funcionaba con parámetros de alta seguridad, otras personas, como Julián Alarcón y Mauricio Duque, también criticaron la plataforma.[39] Carolina Botero, de Fundación Karisma, indicó que Peña no podría haber alertado al DANE antes de hacer

[35] La W, "La página del eCenso almacena mal tu contraseña, no la uses". Juliana Peña, WRadio, 15 de enero del 2018. Disponible en: https://www.wradio.com.co/noticias/actualidad/la-pagina-del-ecenso-almacena-mal-tu-contrasena-no-la-uses-juliana-pena/20180115/nota/3689816.aspx
[36] La W, "La página del eCenso almacena mal tu contraseña, no la uses". Juliana Peña, WRadio, 15 de enero del 2018. Disponible en: https://www.wradio.com.co/noticias/actualidad/la-pagina-del-ecenso-almacena-mal-tu-contrasena-no-la-uses-juliana-pena/20180115/nota/3689816.aspx
[37] Juliana Peña, "Actualización: Las contraseñas del eCenso no están precisamente guardadas en texto plano, pero sigue siendo muy feo el asunto", 13 de enero del 2018. Disponible en: https://julip.co/2018/01/actualizacion-contrasenas-censo/
[38] DANE, "El DANE responde a afirmaciones falsas sobre la seguridad del eCenso", 2018. Disponible en: https://www.dane.gov.co/index.php/actualidad-dane/4455-el-dane-responde-a-afirmaciones-falsas-sobre-la-seguridad-del-ecenso Redacción El Tiempo, "El DANE defiende la seguridad del censo", 18 de enero del 2018. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ante-criticas-el-dane-defiende-la-seguridad-de-la-plataforma-para-el-censo-172244
[39] Carolina Botero Cabrera, "Lección 1 del e-censo: no matar a la mensajera", El Espectador, 18 de enero del 2018. Disponible en: https://www.elespectador.com/opinion/leccion-1-del-e-censo-no-matar-la-mensajera-columna-734171/

públicas sus declaraciones porque el Gobierno colombiano carece de mecanismos o canales de comunicación mediante los cuales las personas puedan informar problemas de seguridad digital.[40]

Como consecuencia de la reacción del DANE y la falta de reconocimiento de su error, Peña pasó a ser el blanco de los medios.[41] Un grupo de desarrolladores y desarrolladoras de Colombia y Fundación Karisma defendieron a Peña.[42] El 19 de enero del 2018, enviaron un correo electrónico al Gobierno en el que solicitaron una reunión para hablar de las posibilidades de colaboración en asuntos de seguridad informática y de la reivindicación de Peña.[43]

La reunión tuvo lugar el 24 de enero y culminó en una resolución amistosa.[44] El Gobierno indicó que había creado un Puesto de Mando Unificado (PMU) para monitorear permanentemente la plataforma del eCenso. Las autoridades también reconocieron las "valiosas contribuciones de la comunidad de desarrolladores, ciudadanos y Juliana Peña para mejorar la plataforma del eCenso". El DANE indicó que "no hay dudas de las buenas intenciones de Juliana Peña y de su ética profesional respecto de sus comentarios".[45] Colombia.Dev y Fundación Karisma hicieron de mediadores entre el Gobierno colombiano y Peña para evitar que ella sufriera otras consecuencias negativas. El DANE también se comprometió a analizar las sugerencias de la comunidad de la seguridad informática y a tener abiertas sus puertas para recibir informes sobre el funcionamiento del sistema o cualquier recomendación.[46]

El caso de Juliana Peña expuso los pocos o inexistentes medios para informar vulnerabilidades, fallas en la seguridad, y violaciones de datos en el Gobierno colombiano. Durante años, las cuatro entidades a cargo de solucionar problemas de seguridad informática eran parte del Ministerio de Defensa. Recientemente, otras autoridades han tomado un rol activo, como el Ministerio de las Tecnologías de la Información y las Comunicaciones, también conocido como

[40] Carolina Botero Cabrera, "Lección 1 del e-censo: no matar a la mensajera", El Espectador, 18 de enero del 2018. Disponible en: https://www.elespectador.com/opinion/leccion-1-del-e-censo-no-matar-la-mensajera-columna-734171/
[41] Redacción El Espectador, "Afirmaciones de bloguera Juliana Peña son falsas, irresponsables y apresuradas". DANE, 18 de enero del 2018. Disponible en: https://www.elespectador.com/economia/afirmaciones-de-bloguera-juliana-pena-son-falsas-irresponsables-y-apresuradas-dane-article-733982/
[42] Consulte: "Carta abierta al DANE", 19 de enero del 2018. Disponible en: https://github.com/colombia-dev/carta
Consulte también: Johann Echavarria, "Resumen sobre el censo virtual del DANE; Los hallazgos de seguridad de Juliana Peña y las respuestas del DANE y Colombia Dev", 21 de enero del 2018. Disponible en: https://medium.com/@abrupto/resumen-sobre-el-censo-virtual-del-dane-los-hallazgos-de-seguridad-de-juliana-pe%C3%B1a-y-las-db42040132e5
[43] Consulte: correo electrónico de Colombia.Dev enviado a una figura del Gobierno: https://github.com/colombia-dev/carta/blob/master/contacto_dane.md
Consulte también: DANE, "El DANE ratifica que el eCenso es seguro", 2018. Disponible en: https://www.dane.gov.co/index.php/actualidad-dane/4459-el-dane-ratifica-que-el-ecenso-es-seguro
[44] Consulte: Johann Echavarria, "Segunda parte sobre el censo del DANE, Juliana Peña, la seguridad y Colombia Dev", 30 de enero del 2018. Disponible en: https://medium.com/@abrupto/segunda-parte-sobre-el-censo-del-dane-juliana-pe%C3%B1a-la-seguridad-y-colombia-dev-49f5114223e5
[45] Comunicado de prensa del DANE, PMU y desarrolladores(as) de software sobre el eCenso 2018, 29 de enero del 2018. Disponible en: https://github.com/colombia-dev/carta/blob/master/comunicado.pdf
[46] Comunicado de prensa del DANE, PMU y desarrolladores(as) de software sobre el eCenso 2018, 29 de enero del 2018. Disponible en: https://github.com/colombia-dev/carta/blob/master/comunicado.pdf

el MinTIC.[47] Los obstáculos a los que se enfrenta el pueblo colombiano al encontrar una vulnerabilidad son: (i) el miedo a una reacción hostil o a sanciones legales; (ii) barreras legales o falta de marco legal para su protección; (iii) falta de medios para comunicarse con el Gobierno y falta de políticas bien definidas; y (iv) ausencia o insuficiencia de coordinación entre el Gobierno y las partes involucradas.[48] La comunidad de investigación de seguridad informática y las organizaciones sin fines de lucro, como Fundación Karisma, se han esforzado para construir canales de comunicación con las autoridades gubernamentales para mejorar la situación.

III. ECUADOR

MARCO LEGAL Y ANÁLISIS

En Ecuador podrían usarse múltiples leyes para sancionar a investigadores(as) por informar vulnerabilidades en sistemas informáticos, que incluyen distintos artículos del código penal ecuatoriano: el Código Orgánico Integral Penal. Asimismo, el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación —la ley de propiedad intelectual de Ecuador— podría usarse también para imponer sanciones administrativas, responsabilidad legal civil o, en casos poco frecuentes, responsabilidad penal, a la comunidad de infosec, si la divulgación viola un código con derechos de autor u otros materiales con derechos de autor.[49] En este documento, identificamos y analizamos algunas de las disposiciones clave que ya han sido usadas o probablemente se usen en acciones legales contra personas que investiguen la seguridad digital en Ecuador.

Como punto de partida, el código penal de Ecuador incluye leyes en materia de ciberdelincuencia que ya se han utilizado para procesar la investigación de seguridad digital. Por ejemplo, Ola Bini, investigador de seguridad cuya prominente situación se detalla en el caso de estudio de más abajo, está actualmente procesado según el art. 234 del código penal. Dicho artículo penaliza el acceso no autorizado a un sistema informático con la intención, entre otras cosas, de “explotar

[47] Fundación Karisma, Rutas de Divulgación, (2019), p. 8. Disponible en: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf
[48] Fundación Karisma, Rutas de Divulgación, (2019), p. 16. Disponible en: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf
[49] El art. 131 del estatuto extiende la protección de los derechos de autor al software como obra literaria, e incluye al software expresado como código fuente o código objeto. Sin embargo, el art. 134 enumera las actividades relacionadas con el software que están permitidas sin autorización, incluidas las actividades llevadas a cabo en una copia del software obtenida legítimamente con el único propósito de comprobar, investigar o corregir su funcionamiento o su seguridad en el mismo u otros programas. Art. 134(4). Por lo tanto, es probable que quienes investigan la seguridad digital recurran a este artículo como un puerto seguro ante las acusaciones de violación de derechos de autor que se originen a partir de la investigación llevada a cabo en software.

ilegítimamente" tal acceso.[50] El lenguaje del estatuto es lo suficientemente amplio en alcance como para cubrir la investigación de vulnerabilidades. En el estatuto, no se especifica qué constituye un acceso no autorizado, quién debe autorizar el acceso, qué constituye una autorización, ni qué tipo de acceso se permite una vez obtenida la autorización.

El art. 234 es aún más problemático porque no contempla adecuadamente la intención de la persona que accede al sistema. Sin mayor claridad sobre qué constituye una intención de explotación ilegítima del acceso no autorizado a un sistema informático, el acceso a un sistema con la intención de encontrar e informar vulnerabilidades podría considerarse una forma de explotación ilegítima según el estatuto.

Otra disposición sobre ciberdelincuencia del código penal ecuatoriano que podría penalizar la investigación de seguridad digital es el art. 232, que sanciona los ataques a la integridad de los sistemas informáticos.[51] El estatuto enumera diversas acciones prohibidas, que incluyen alterar la infraestructura tecnológica de un sistema sin el consentimiento de su propietario.[52] A pesar de que el uso del término "alterar" probablemente implique alguna acción adicional al mero acceso al sistema, no está claro cuándo un sistema ha sido lo suficientemente alterado como para generar una responsabilidad legal. Dependiendo del sistema, quizás el mero acceso a este resulte en alguna forma de alteración. Por lo tanto, el uso de verbos tan generales como "alterar" podría ser expansivo y alcanzar para penalizar la investigación de infosec.

Las disposiciones destinadas a proteger la privacidad también podrían usarse para atacar a investigadores(as) de seguridad digital. Por ejemplo, los artículos 229 y 230 del código penal de Ecuador sancionan la divulgación ilegal de una base de datos y la interceptación ilegal de datos,

[50] Código Orgánico Integral Penal, art. 234: "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años".

[51] Inicialmente, Ola Bini fue acusado de conformidad con este artículo, como explicamos en mayor profundidad en el caso de estudio de la sección de más abajo.

[52] Código Orgánico Integral Penal, art. 232: "Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad".

respectivamente.[53] Si bien ambos artículos mencionan conductas que la mayoría de las personas investigadoras de seguridad digital llevarían a cabo, también remarcan los requisitos de intencionalidad que pueden evitar su aplicación a cierta investigación de seguridad digital. Por ejemplo, una revelación ilegal según el art. 229 exige la violación voluntaria e intencional del secreto, la intimidad y la privacidad de las personas. Es poco probable que las personas que investigan la seguridad digital tengan esta intención al informar una vulnerabilidad. Sin embargo, debido a que el Gobierno a menudo califica la investigación de seguridad digital como hackeo malicioso, podría argüir que quienes llevan a cabo estas investigaciones satisfacen el requisito de intencionalidad en ciertos casos.

El art. 230(1) también exige que una interceptación ilegal de datos incluya que quien los intercepta actúe en provecho personal o en el de un tercero. Si bien "provecho" y "tercero" tienen un alcance tan amplio que podrían incluir la investigación de seguridad digital en esta disposición, el requisito de intencionalidad agravada, al menos, sugiere que existen casos en los que la interceptación de datos no será penalizada en virtud del estatuto; la investigación de seguridad que beneficia al público en general podría ser uno de esos casos.

Otros artículos más generales del código penal de Ecuador podrían, previsiblemente, utilizarse para penalizar la investigación de seguridad digital y otras actividades relacionadas. A modo de ejemplo, el art. 195 prohíbe que las personas posean infraestructura, programas, equipos o bases de datos que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil.[54] El lenguaje de este estatuto es tan amplio que puede ser usado para penalizar a quienes tengan en su posesión tecnologías de doble uso de manera más general, a pesar de que tan amplia interpretación del artículo parecería ir más allá de lo pretendido por quienes lo formularon.

Otro ejemplo de una disposición más general que se podría aplicar a un caso de investigación de seguridad es el art. 178, que ampliamente sanciona las violaciones a la privacidad, que incluyen acceder, examinar, reproducir, diseminar, entre otras cosas, los datos personales de otro individuo

[53] Código Orgánico Integral Penal, art. 229: "Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años". Art. 230: "Interceptación ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (…)"

[54] Código Orgánico Integral Penal, art. 195: "Infraestructura ilícita. La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles".

sin su consentimiento o autorización legal.[55] Sin ningún tipo de puerto seguro para la investigación y denuncia de vulnerabilidades, quienes investigan la seguridad digital en Ecuador podrían fácilmente violar esta disposición del código penal en repetidas ocasiones; por ejemplo, cualquier investigación de seguridad que acceda a una base de datos con datos personales de otras personas representaría una violación de esta disposición.

Caso de estudio

Ola Bini: un ejemplo ilustre de la persecución de la investigación de seguridad digital por parte del Gobierno ecuatoriano es el caso de Ola Bini. El caso de Bini se ha vuelto paradigmático respecto de cuán grave puede ser la persecución. En este informe, resumimos los procesos penales contra Bini y damos detalles sobre otras formas de persecución que se han utilizado para amenazarlo y acosarlo a él y a quienes lo rodean, durante los últimos dos años.

Ola Bini es un desarrollador de software sueco que reside en Ecuador desde el 2013. Muchos lo consideran uno de los mejores programadores y expertos en seguridad digital del mundo. Ha trabajado en varios proyectos de software de código abierto para mejorar la seguridad y la privacidad de quienes usan internet. Cuando llegó a Ecuador en el 2013, estaba trabajando en software de código abierto para la firma de consultoría tecnológica global ThoughtWorks. En el 2017, Bini y otros colegas de ThoughtWorks decidieron abandonar la empresa para crear Centro de Autonomía Digital (CAD), una organización sin fines de lucro con sede en Quito que se centra en el desarrollo de software de código abierto y en la mejora de la privacidad de software. Actualmente, Bini ocupa el puesto de director técnico en CAD.

En abril del 2019, las autoridades ecuatorianas arrestaron a Bini.[56] No había acusaciones formales en su contra en el momento de su arresto, aunque parece que la causa tuvo que ver con la revocación del asilo de Julian Assange, arrestado unas pocas horas antes que Bini. Según una entrevista con el abogado de Bini, Carlos Soria, Ola había entablado una amistad con Assange durante su asilo en Ecuador y lo visitó en la embajada ecuatoriana aproximadamente una docena de veces en el transcurso de varios años. Cuando Bini fue arrestado, no había pruebas de que hubiera quebrantado alguna ley. Su orden de arresto se refería a él como un "hacker ruso", a pesar de que él no es de Rusia y que ser hacker no es un delito.

Tras su arresto, Bini fue privado de libertad sin tener acceso a un abogado ni a un traductor. Las autoridades tampoco se comunicaron con la embajada sueca, omisión que se considera una violación del derecho internacional que rige el acceso y la notificación consulares. Soria tiene la

[55] Código Orgánico Integral Penal, art. 178: "Violación a la intimidad. La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley".

[56] Para ver más información sobre el caso, visite: https://www.amnesty.org/download/Documents/AMR2808712019SPANISH.pdf

hipótesis de que las autoridades no sabían por qué mantenían bajo su custodia a Bini, ya que no había pruebas que lo vincularan a ningún delito, y que el Gobierno probablemente estaba intentando decidir qué quería hacer con él durante ese tiempo. Bini estuvo privado de libertad durante 70 días mientras la fiscalía incautaba y examinaba sus dispositivos tecnológicos personales y sus comunicaciones privadas para intentar encontrar pruebas en su contra.

Finalmente, Bini fue acusado de violar el art. 232 del código penal por un presunto ataque a la integridad de sistemas informáticos. Desde la fecha de su acusación inicial, la fiscalía tuvo 90 días para llevar a cabo una investigación formal y recopilar pruebas del supuesto ataque de Bini al sistema informático. Al terminar esos 90 días, la fiscalía decidió acusar a otra persona como cómplice de Bini, lo que Soria describe como una maniobra legal para ganar 30 días más para buscar evidencia en contra de Bini.

Al pasar 28 de esos 30 días, la fiscalía decidió enmendar las acusaciones iniciales contra Bini para alegar que, en cambio, él había violado el art. 234 del código penal por acceso no autorizado a un sistema informático. Esta movida le dio al equipo legal defensor de Bini solo dos días antes de su siguiente audiencia para formular una estrategia legal completamente nueva para defenderlo contra esa nueva acusación. Las pruebas presentadas por la fiscalía para respaldar la nueva acusación era una única captura de pantalla extraída del teléfono de Bini, que mostraba una pantalla de inicio de sesión de Telnet, aunque no había pruebas de que Bini hubiera intentado acceder más allá de la interfaz de inicio de sesión que se mostraba en la foto.

Ahora, a casi dos años de la fecha de su arresto, el caso de Bini está acercándose lentamente a un juicio.[57] A pesar de que su equipo defensor está ansioso por probar su inocencia en el juicio, su caso se ha pospuesto muchas veces. En su audiencia previa al juicio en diciembre del 2020, la jueza rechazó desestimar el caso de Bini, a pesar de que su equipo legal había presentado durante más de cinco horas las más de 120 violaciones civiles y procesales que sus abogados habían documentado a lo largo del caso; violaciones que, según Soria, deberían dejar sin efecto el caso en su totalidad. La jueza, en cambio, pospuso la audiencia previa al juicio, la cual finalmente programaría el juicio de Bini, para marzo del 2021. Sin embargo, fue recién el 22 de junio del 2021 que dicha audiencia tuvo lugar. La jueza, basándose en pruebas y argumentos escasos, decidió proceder e ir a juicio.

Además de lo que Bini ha estado sufriendo en el sistema jurídico, también ha sido víctima de muchas formas extralegales de acoso durante todo su caso. Por ejemplo, ha sido objeto de vigilancia constante desde que fue liberado por la policía. Lo han seguido, le han tomado fotos y drones han seguido su automóvil como parte de dicha vigilancia. Consecuentemente, Bini ha tenido que contratar un guardaespaldas para mayor protección.

Aunque no cuentan con pruebas concluyentes, Bini y su equipo de defensa sospechan que el Gobierno es el responsable de estas actividades de vigilancia. Por este motivo, Bini interpuso

[57]Para ver más información sobre el caso, visite: https://www.fundamedios.org.ec/alertas/jueza-yadira-proano-es-separada-del-caso-ola-bini/

una demanda de *habeas data*[58] contra varias instituciones gubernamentales con la esperanza de descubrir si el Gobierno ecuatoriano ha dado a las autoridades la orden oficial de vigilarlo y rastrearlo y, de ser así, de hacer pública toda la información que las autoridades hayan recopilado sobre él como producto de esa vigilancia ordenada. Su audiencia de *habeas data*, que inicialmente debía tener lugar en octubre del 2020, se reprogramó para el 12 de marzo de 2021. Sin embargo, esa instancia también se pospuso. En la audiencia, el Gobierno envió nueva representación legal para esos procedimientos, sin notificar por anticipado al tribunal acerca del cambio. Como resultado, se pospusieron nuevamente los procesos y se le dio al Gobierno más tiempo para presentar ante el tribunal el cambio de representación legal[59]. El equipo de Bini, sin embargo, piensa que esto no es más que otra maniobra procesal del Gobierno para continuar demorando el proceso.

Centro de Autonomía Digital también ha sufrido acoso significativo durante el caso de Bini por su afiliación con él. Por ejemplo, algo tan simple y esencial como las operaciones comerciales diarias de abrir y mantener una cuenta bancaria se volvieron tarea difícil para CAD. Múltiples bancos cerraron sus cuentas sin causa ni explicación, lo que, según la organización, son esfuerzos para bloquear sus operaciones. Además, las oficinas de CAD también fueron asaltadas. Durante la entradera, algunos equipos informáticos de CAD fueron sustraídos[60], lo que suscitó la sospecha de CAD de que la acción había sido perpetrada por la policía.

Asumiendo que Bini tendrá un juicio justo tarde o temprano, su abogado, Carlos Soria, espera que el juicio no solo pruebe la inocencia de su cliente, sino que establezca un precedente para garantizar que quienes se dedican a la investigación de seguridad digital y al desarrollo técnico de software no sean penalizados por su trabajo en el futuro. Soria confía en que el caso de Bini provocará un mayor entendimiento público del trabajo de la comunidad de infosec y, quizás, un aumento en el escrutinio de los actores gubernamentales que han estado abusando de su poder para perseguir a investigadores(as) por el trabajo que ellos mismos claramente no comprenden.

[58] Consulte: OEA, “Relation between Privacy Protection, Data Protection and Habeas Data”. Disponible en: http://www.oas.org/dil/data_protection_privacy_habeas_data.htm
[59] Para ver más información sobre el caso, visite: https://twitter.com/ODJEcuador/status/1374801302396542979
[60] Para ver más información sobre el caso, visite: https://www.elpais.cr/2019/08/01/fiscalia-ecuatoriana-vincula-a-una-persona-mas-al-caso-del-programador-sueco-ola-bini/

IV. MÉXICO

MARCO LEGAL Y ANÁLISIS

México cuenta con una considerable legislación penal, que incluye el Código Penal Federal y otras leyes penales especializadas, que podrían ser utilizadas para sancionar a la comunidad de investigación de seguridad informática. También cuenta con otras leyes en materia de propiedad intelectual (Ley Federal del Derecho de Autor) que podrían emplearse para imponer multas y otras sanciones administrativas. En esta sección, destacaremos algunas de las disposiciones a las que el Gobierno podría recurrir para usarlas en contra de investigadores(as) de seguridad informática. Adicionalmente, considerando que el Poder Legislativo ha estado muy activo en el asunto, analizamos cuatro proyectos de ley recientes.

En primer lugar, el art. 211 bis 1,[61] del Código Penal Federal penaliza el acceso no autorizado a sistemas informáticos y a dispositivos informáticos que resulte en la modificación, eliminación o supresión de información almacenada en tales sistemas o dispositivos protegidos por un mecanismo de seguridad. Las personas pueden ser sancionadas con penas de prisión de entre seis meses y dos años, y multas. Además, visualizar o copiar esa información conlleva la sanción de tres meses a un año de prisión.

Asimismo, el artículo 211 bis 2[62] penaliza el acceso no autorizado a sistemas y dispositivos informáticos de propiedad estatal o relacionados con la seguridad pública, si tal acceso resulta en la modificación, eliminación o supresión de información. Las sanciones varían de uno a cuatro años en prisión para sistemas y dispositivos del Estado y de cuatro a 10 años en el caso de sistemas y dispositivos relacionados con la seguridad pública. El artículo 211 bis 4[63] contempla

[61] (ADICIONADO, D.O.F. 17 DE MAYO DE 1999)
ARTÍCULO 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

[62] Artículo 211 BIS 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

[63] Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

penas similares para la modificación, eliminación o supresión sin autorización de información almacenada en computadoras que pertenezcan a instituciones financieras, si están protegidas por un mecanismo de seguridad. En este caso, la pena es de seis meses a cuatro años de prisión. Si la información se "conoce" o copia, la persona puede ser encarcelada de tres meses a dos años.

A diferencia de lo que sucede en otros países, estos tres artículos mencionan que los sistemas informáticos o las computadoras deben contar con la protección de un mecanismo de seguridad. Sin embargo, al igual que en los otros países que hemos analizado, la ley no exige la intención de causar daños. Acceder a un sistema informático y ver la información que contiene podría ser suficiente para que el Gobierno utilice este artículo para sancionar a una persona que investigue la seguridad informática en busca de vulnerabilidades.

El Código Penal Federal también incluye el artículo 424 bis[64], relacionado con la producción, distribución y venta ilegal de copias de obras, fonogramas, videogramas o libros protegidos por la Ley Federal del Derecho de Autor. La responsabilidad legal penal solo se puede imponer en virtud de esta disposición si el perpetrador actuó intencionalmente con el propósito de obtener un beneficio económico. Por lo tanto, es menos probable que investigadores(as) de seguridad digital de México estén bajo amenazas de sanciones penales por derechos de autor.

El artículo 426[65] podría usarse contra la comunidad de investigación de seguridad informática, ya que sanciona las interferencias a transmisiones satelitales y de cable. Específicamente, la ley establece que las siguientes conductas serán sancionadas con prisión entre seis meses y cuatro años y entre 300 a 3000 días multa:

> "I. A quien fabrique, modifique, importe, distribuya, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal; (…)
>
> III. A quien fabrique o distribuya equipo destinado a la recepción de una señal de cable encriptada portadora de programas, sin autorización del distribuidor legítimo de dicha

[64] Artículo 424 bis. Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa:
I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior; II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación, o III. A quien grabe, transmita o realice una copia total o parcial de una obra cinematográfica protegida, exhibida en una sala de cine o lugares que hagan sus veces, sin la autorización del titular del derecho de autor o derechos conexos.

[65] Artículo 426. Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, en los casos siguientes:
I. A quien fabrique, modifique, importe, distribuya, venda o arriende un dispositivo o sistema para descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal;
II. A quien realice con fines de lucro cualquier acto con la finalidad de descifrar una señal de satélite cifrada, portadora de programas, sin autorización del distribuidor legítimo de dicha señal;
III. A quien fabrique o distribuya equipo destinado a la recepción de una señal de cable encriptada portadora de programas, sin autorización del distribuidor legítimo de dicha señal, o
IV. A quien reciba o asista a otro a recibir una señal de cable encriptada portadora de programas sin la autorización del distribuidor legítimo de dicha señal.

señal;

IV. A quien reciba o asista a otro a recibir una señal de cable encriptada portadora de programas sin la autorización del distribuidor legítimo de dicha señal".

Una persona que investigue la seguridad y haya creado un dispositivo capaz de decodificar una señal cifrada podría ser penalizada por la mera acción de la "fabricación". No existe requisito de probar que el dispositivo haya sido utilizado y con qué intención, como causar daños, ni con qué resultado, como haber provocado algún daño.

La Ley de Instituciones de Crédito también incluye algunas sanciones penales que podrían ser usadas contra investigadores(as) de seguridad informática. El artículo 112 QUÁTER[66] indica que cualquiera que cometa los siguientes actos sin "causa legítima" o sin consentimiento será encarcelado entre tres y nueve años y se le impondrá una multa:

"I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada;

II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada".

Además de la falta de intención maliciosa, no queda claro qué es una "causa legítima". Esto plantea la preocupante pregunta de que el mero acceso a cualquiera de estos dispositivos o tecnologías y la visualización de la información bastarían para imponer una sanción. Sobre la base de una interpretación literal del artículo, solo se necesita que el motivo de la persona que accede sea "obtener" información confidencial. Sin un requisito de que la intención sea también usar la información para explotarla o causar daños, la disposición resulta peligrosamente amplia. Además, no está claro si es necesario que la información solo sea visualizada o sea descargada o copiada.

El artículo 112 SEXTUS[67] penaliza el uso de credenciales indebidas para acceder a información. Específicamente, cualquiera que use un medio tecnológico para "suplantar la identidad" de una

[66] Artículo 112 QUÁTER. Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:
I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o
II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

[67] Artículo 112 SEXTUS. Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientas mil Unidades de Medida y Actualización, a quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de una autoridad financiera o de alguna de sus áreas o de alguno de los sujetos a que se refiere el artículo 3 de esta Ley, o de un servidor público, directivo, consejero, empleado, funcionario, o dependiente de éstas, en los términos establecidos por el artículo 116 bis 1 de la presente Ley.

autoridad financiera o un funcionario público, director, concejal o empleado, será sancionado con prisión de tres a nueve años y multado. Al igual que otros artículos mencionados, este tampoco requiere una intención maliciosa ni la intención de obtener rédito, ni la provocación de un daño en particular que resulte del accionar. No menciona situación alguna sobre las consecuencias de la suplantación, como la obtención de rédito o el beneficio personal. Esto conlleva a la posibilidad concreta de que se sancione a una persona investigadora que use las credenciales de alguien más para probar un sistema.

El Tratado entre México, Estados Unidos y Canadá (USMCA) condujo a una serie de reformas de leyes mexicanas, incluida la legislación en materia de derechos de autor y propiedad intelectual. La Ley Federal del Derecho de Autor reconoce al software como obra protegida en virtud del artículo 13, mientras que el artículo 101 recoge su definición. El artículo 112 prohíbe la importación, fabricación, distribución y el uso de dispositivos o la prestación de servicios destinados a eliminar protecciones técnicas de software o programas informáticos, y transmisiones a través del espectro electromagnético, entre otros.[68] El capítulo V, sobre las medidas de protección tecnológica y los proveedores de servicios de internet, contiene los artículos 114 bis a 114 OCTIES.[69] Las violaciones a las medidas de protección técnica contienen una serie de excepciones descriptas en el artículo 114 QUÁTER. Por ejemplo, la sección III del artículo 114 QUÁTER exime las actividades llevadas a cabo por alguien con buena fe y con la autorización del propietario del dispositivo, sistema o red, con el único propósito de probar, investigar o corregir sus medidas de seguridad.[70] La persona que hace la prueba o investigación debe tener el consentimiento del propietario; de lo contrario, la excepción no aplica. La Ley Federal del Derecho de Autor contiene sanciones administrativas basadas en los derechos de autor (artículos 229 y 230) y razones comerciales (artículos 231 al 236).[71] En virtud del artículo 232 bis, se le impondrán multas a quien produzca, reproduzca, fabrique, distribuya, importe, comercialice, arriende, almacene, transporte, ofrezca o ponga a disposición del público dispositivos, mecanismos, productos o sistemas para evadir medidas de protección tecnológica.[72] Como se explica anteriormente, el alcance de esta conducta es amplio, abarca numerosos

[68] Artículo 112. Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior.

[69] El artículo 114 OCTIES es casi una reproducción de la sección 230 de la Ley de Decencia en las Comunicaciones de los Estados Unidos. Incorporó un sistema de notificación y baja que no funcionaba previamente en la jurisdicción mexicana.

[70] Artículo 114 QUÁTER. No se considerarán como violación de la presente Ley aquellas acciones de elusión o evasión de una medida tecnológica de protección efectiva que controle el acceso a una obra, interpretación o ejecución, o fonograma protegidos por esta Ley, cuando: (…) III. Las actividades realizadas por una persona de buena fe con la autorización del propietario de una computadora, sistema o red de cómputo, realizadas con el único propósito de probar, investigar o corregir la seguridad de esa computadora, sistema o red de cómputo.

[71] Las sanciones basadas en razones comerciales se incorporaron como resultado del USMCA.

[72] Artículo 232 bis. Se impondrá multa de mil hasta veinte mil veces el valor diario de la Unidad de Medida y Actualización a quien produzca, reproduzca, fabrique, distribuya, importe, comercialice, arriende, almacene, transporte, ofrezca o ponga a disposición del público, ofrezca al público o proporcione servicios o realice cualquier otro acto que permita tener dispositivos, mecanismos, productos, componentes o sistemas que:
I. Sean promocionados, publicados o comercializados con el propósito de eludir una medida tecnológica de protección efectiva; II. Sean utilizados preponderantemente para eludir cualquier medida tecnológica de protección efectiva, o
III. Sean diseñados, producidos o ejecutados con el propósito de eludir cualquier medida tecnológica de protección efectiva.

dispositivos y podría aplicarse de igual manera a personas que causan un daño real, como el robo de información o dinero, mientras que quienes investigan la seguridad informática justamente desean prevenir este tipo de problemas.

Por último, México aún no ha adoptado el Convenio de Budapest y mantiene un rol de observador. Sin embargo, a finales del 2020, el Poder Legislativo solicitó a la Secretaría de Relaciones Exteriores continuar con el trabajo de adhesión al Convenio.[73]

Proyectos de ley en materia de ciberseguridad

Desde el 2018, legisladores y legisladoras federales de México han presentado 11 proyectos de ley que se centran en la ciberseguridad.[74] Cuatro de ellos se analizan brevemente en este documento con el fin de destacar su preocupante contenido. En abril del 2021, la senadora Lucía Trasviña presentó un proyecto de ley en el que proponía crear una Ley General de Ciberseguridad y eliminar algunos artículos del Código Penal Federal (artículos del 211 bis al 211 bis 7).[75] Algunas disposiciones penales propuestas incluyen el acceso ilícito a sistemas informáticos (artículo 24); la interceptación de datos no autorizada (artículo 26); y la fabricación, el uso o la comercialización de software y dispositivos empleados para modificar, eliminar o suprimir datos almacenados en sistemas o dispositivos informáticos (artículo 28). Para este último delito penal, que tiene un alcance amplio, las penas podrían ser desproporcionadas: no establece la conexión entre estos dispositivos y software ni explica cómo podrían ser empleados.

En septiembre del 2020, el diputado Javier Salinas presentó un proyecto de ley para reformar la fracción XXIX-M del artículo 73 de la Constitución de México.[76] A principios del 2021, el cuerpo legislativo organizó una reunión parlamentaria abierta para debatir el proyecto de ley.[77] Se

[73] Consulte: Senado de la República, "Urgen a la SRE concluir la adhesión al Convenio sobre Ciberdelincuencia", Senado de la República, 20 de diciembre del 2020. Disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/50022-urgen-a-la-sre-concluir-la-adhesion-al-convenio-sobre-ciberdelincuencia.html

[74] Senador José Ramón Enríquez Herrera: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/11/asun_4102523_20201104_1601648158.pdf; diputada María Eugenia Hernández Pérez: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/01/asun_3986616_20200108_1578514711.pdf y http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/08/asun_4059385_20200812_1597257570.pdf; senadora Alejandra Lagunes Soto Ruiz: http://sil.gobernacion.gob.mx/Archivos/Documentos/2018/10/asun_3760770_20181023_1540294391.pdf; diputado Carlos Iván Ayala Bobadilla: http://sil.gobernacion.gob.mx/Archivos/Documentos/ 2020/08/asun_4059591_20200812_1597257015.pdf; diputado José Salvador Rosas Quintanilla: http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/03/asun_4144555_20210302_1614965083.pdf; senador Gustavo Madero Muñoz: http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/03/asun_4161702_20210325_1613504011.pdf

[75] Disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf

[76] Consulte: Cámara de Diputados, "Promueve Javier Salinas facultar a Congreso de la Unión para legislar en materia de ciberseguridad". Disponible en: http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2020/Septiembre/28/6500-Promueve-Javier-Salinas-facultar-a-Congreso-de-la-Union-para-legislar-en-materia-de-ciberseguridad. Consulte también: Cámara de Diputados, "Impulsa Javier Salinas iniciativa de reforma a la Constitución, para facultar al Congreso a fin de que pueda legislar en materia de ciberseguridad". Disponible en: http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2020/Febrero/04/4232-Impulsa-Javier-Salinas-iniciativa-de-reforma-a-la-Constitucion-para-facultar-al-Congreso-a-fin-de-que-pueda-legislar-en-materia-de-ciberseguridad

[77] Cámara de Diputados, "Análisis de la reforma a la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad", YouTube, 26 de febrero del 2020. Disponible en: https://www.youtube.com/watch?v=qCJerA-wm2M

propone darle al Congreso las facultades para legislar sobre "seguridad nacional, que incluye la ciberseguridad y la protección de los derechos humanos digitales"[78]. La exposición de los motivos es ambigua y hace referencia a los ciberataques, el ciberespionaje, las noticias falsas, la desinformación, y el *sexting*, entre otros. Muchos de los términos se usan incorrectamente, como el robo de identidad y la suplantación de identidad. Según ARTÍCULO 19, el proyecto no hace una distinción entre la conducta y el uso de la tecnología.[79] Además, no queda claro cómo algunos temas, como el *sexting*, se relacionan con la seguridad nacional. No caben dudas de que esta es una de las principales razones por las que la sociedad civil ha instado a abrir el debate y escuchar a las partes interesadas.

Anteriormente, la senadora Lucía Trasviña[80] y el senador Miguel Mancera[81] habían presentado dos proyectos. Ambas propuestas son muy generales e incorporan delitos penales poco precisos que sancionan actividades tecnológicas legítimas y cotidianas,[82] en contra de la investigación de seguridad informática. El proyecto de Trasviña proponía incluir delitos que describían acciones que pueden darse cuando investigadores(as) digitales identifican problemas de seguridad. Como destacamos en otras secciones de este documento, utilizan términos como "acceso ilegítimo" o "no autorizado". Las acciones de acceder o interferir equivaldrán automáticamente a una sanción sin dejar espacio para informar estas vulnerabilidades. El proyecto de Mancera es igualmente preocupante. Muchos de los delitos propuestos podrían representar una amenaza para quienes investigan la seguridad digital. Por ejemplo, el artículo 55 de la propuesta de ley sobre ciberseguridad sancionaría la búsqueda de vulnerabilidades si no se tiene una autorización para hacerlo. Este artículo también es confuso, debido a que indica que la conducta será penalizada ya sea que se haya llevado a cabo con o sin permiso. Además, algunas de las actividades prohibidas, como acceder a una cuenta de servicios provistos a través de internet, no deberían considerarse un asunto de ciberseguridad nacional y podrían ser reguladas en otros tipos de leyes a escala local, según el sistema penal mexicano.

[78] Proyecto de ley del diputado Javier Salinas. Disponible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/10/asun_3953044_20191029_1569348687.pdf
[79] Artículo 19, Reforma constitucional en materia de Ciberseguridad podría explotarse para censurar y arremeter contra manifestaciones legítimas de la sociedad", 10 de febrero del 2021. Disponible en: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/
[80] Proyecto de ley de la senadora Lucía Trasviña. Disponible en: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-19-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf
[81] Proyecto de ley del senador Miguel Mancera. Disponible en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf
[82] R3D, "Urgente, Parlamento Abierto y Respeto a Derechos Humanos en Legislación sobre Ciberseguridad", R3D, 22 de septiembre del 2021. Disponible en: https://r3d.mx/2020/09/22/urgente-parlamento-abierto-y-respeto-a-derechos-humanos-en-legislacion-sobre-ciberseguridad/

Caso de estudio

Chris Vickery: el 14 de abril del 2016, Chris Vickery, investigador de seguridad informática y ciudadano de EE. UU., encontró una base de datos de 132 GB que contenía 93,4 millones de datos personales de mexicanos en la nube de Amazon (Amazon Web Services).[83] Vickery verificó que era accesible públicamente y, mediante capturas de pantalla, explicó cómo se podía acceder a la base de datos.[84] "No se requería ninguna contraseña ni autenticación, de ningún tipo. Estaba configurada completamente para el acceso público. ¿Por qué? No tengo idea".[85] Informó sobre sus hallazgos al Instituto Nacional Electoral, también conocido como el INE. Dicho instituto verificó la información y determinó que pertenecía a la base de datos otorgada a Movimiento Ciudadano, un partido político; por lo tanto, el INE sancionó al partido. La base de datos de datos se dio de baja de la nube de Amazon el 22 de abril.[86]
Movimiento Ciudadano admitió que había subido y almacenado la información con el propósito de revisarla. Sin embargo, también intentó echarle la culpa al investigador de seguridad. Alegó que un tercero había hackeado su cuenta de Amazon Web Services: "[p]ara hacer pública la información que estaba salvaguardada en los servidores de Amazon Web Services fue necesario violar las medidas de seguridad a través de métodos altamente especializados, característicos de hackers profesionales".[87] El partido afirmó que Amazon les había notificado sobre el acceso ilegal a su cuenta. Movimiento Ciudadano inició una denuncia penal en contra de "los hackers" ante la autoridad a cargo de los delitos electorales.[88]

Amazon Web Services declaró que, cuando la empresa "fue notificada de que una base de datos no segura que contenía información sensible estaba alojada en la nube de AWS y era accesible públicamente a través de internet, siguió sus protocolos de seguridad estándar y confirmó que dicha base de datos ya no era accesible públicamente".[89] Además, el gerente de relaciones

[83] DataBreaches, "Personal info of 93.4 million Mexicans exposed on Amazon (UPDATED)," DataBreaches, 22 de abril del 2016. Disponible en: https://www.databreaches.net/personal-info-of-93-4-million-mexicans-exposed-on-amazon/
[84] Aristegui Noticias, "Subimos lista nominal de electores a Amazon y hubo "asalto cibernético": Movimiento Ciudadano", Aristegui Noticias, 27 de abril del 2016. Disponible en: https://aristeguinoticias.com/undefined/mexico/subimos-lista-nominal-de-electores-a-amazon-y-hubo-asalto-cibernetico-movimiento-ciudadano/; DataBreaches, "Movimiento Ciudadano admits it was their copy of the Mexican voter list on AWS, tries to deflect blame to researcher", DataBreaches, 27 de abril del 2016. Disponible en: https://www.databreaches.net/movimiento-ciudadano-admits-responsibility-for-mexican-voter-data-leak-on-amazon/
[85] Olga Sushko, "BREAKING: Massive Breach of Mexican Voter Data", MacKeeper, 22 de abril del 2016. Disponible en: https://mackeeper.com/blog/breaking-massive-data-breach-of-mexican-voter-data/
[86] Aristegui Noticias, "Subimos lista nominal de electores a Amazon y hubo "asalto cibernético": Movimiento Ciudadano", Aristegui Noticias, 27 de abril del 2016. Disponible en: https://aristeguinoticias.com/undefined/mexico/subimos-lista-nominal-de-electores-a-amazon-y-hubo-asalto-cibernetico-movimiento-ciudadano/; DataBreaches, "Movimiento Ciudadano admits it was their copy of the Mexican voter list on AWS, tries to deflect blame to researcher", DataBreaches, 27 de abril del 2016. Disponible en: https://www.databreaches.net/movimiento-ciudadano-admits-responsibility-for-mexican-voter-data-leak-on-amazon/
[87] Movimiento Ciudadano, "No hubo filtración, fue hackeo y ya fue denunciado ante la FEPADE: Movimiento Ciudadano", Movimiento Ciudadano, abril del 2016. Disponible en: https://movimientociudadano.mx/federal/boletines/no-hubo-filtracion-fue-hackeo-denunciado-ante-fepade-movimiento-ciudadano
[88] Ídem.
[89] DataBreaches, "Amazon denies Movimiento Ciudadano's claim that they were "hacked", DataBreaches, 28 de abril del 2016. Disponible en: https://www.databreaches.net/amazon-denies-movimiento-cuidadanos-claim-that-they-were-hacked/

públicas de Amazon en México afirmó que la información no estaba almacenada de manera segura, ya que no requería una contraseña y era visible en internet.[90] Movimiento Ciudadano no había usado medidas de seguridad para la base de datos.[91] Afortunadamente, el INE estuvo de acuerdo con esto y desestimó los argumentos de Movimiento Ciudadano, responsabilizando de la filtración al partido político.

El Tribunal Electoral ratificó la sanción del INE impuesta a Movimiento Ciudadano con una multa de USD 1,7 millones (MXN 34 158 411). Este Tribunal determinó que el partido político utilizaba el padrón de votantes de 2014-2015 para llevar a cabo actividades fuera del marco legal, como reproducir, almacenar y exponer la información en línea. La exposición de los datos fue grave, ya que la lista incluía datos sensibles de los y las votantes y otros datos personales, como la edad, la dirección, la fecha de nacimiento, la CURP (Clave Única de Registro de Población), la firma, los datos biométricos, y fotografías.[92]

Este caso de estudio difiere de algunos otros en el sentido de que el Gobierno rechazó la oportunidad de culpar de la violación al investigador, eligiendo responsabilizar al partido político. Al día de hoy, no hay casos en curso contra investigadores(as) de seguridad informática en México. No obstante, la comunidad de personas que se dedican a esto se sienten amenazadas y en un constante estado de temor de ser sancionadas por el Gobierno por sus actividades. Se protegen mediante el anonimato y son muy selectivas con la información que comparten a fin de no comprometer su trabajo.

RECOMENDACIONES PARA MEJORAR EL ECOSISTEMA DE LA INVESTIGACIÓN DE SEGURIDAD DIGITAL

La persecución de investigadores, investigadoras y aprendices de seguridad digital es un grave problema en todo el mundo. No es tarea sencilla construir un entorno en el que puedan realizar sus tareas sin temor a ser procesados penalmente, y requiere de muchos cambios en los marcos legales, las políticas públicas, las narrativas oficiales, la cobertura mediática, entre otras áreas. Las siguientes recomendaciones son un pantallazo inicial de cómo debería abordarse la protección de estas personas.

RECOMENDACIONES PARA REFORMAS DE LA LEGISLACIÓN:

Muchas de las leyes relevantes para la investigación de la seguridad digital que hemos mencionado en este informe incluyen términos y frases muy generales y mal definidas, como “acceso no autorizado o

[90] Aurora Zepeda, “¿Qué creen? ¡nos hackearon!: Dante Delgado; rechaza venta del padrón”, Excelsior, 28 de abril del 2016. Disponible en: https://www.excelsior.com.mx/nacional/2016/04/28/1089350
[91] DataBreaches, “Movimiento Ciudadano admits it was their copy of the Mexican voter list on AWS, tries to deflect blame to researcher”, DataBreaches, 27 de abril del 2016. Disponible en: https://www.databreaches.net/movimiento-ciudadano-admits-responsibility-for-mexican-voter-data-leak-on-amazon/
[92] Consulte: Tribunal Electoral, “Confirma TEPJF multa en contra de MC por publicación del listado nominal de electores en internet”, TEPJF, 20 de septiembre del 2018. Disponible en: https://www.te.gob.mx/front3/bulletins/detail/3408/0

ilegítimo", "alteración", "modificación" de los mecanismos de funcionamiento, que no consideran adecuadamente la intención del actor y si el acceso realmente resulta en algún tipo de daño o perjuicio. Si bien muchos delitos penales no incorporan la intencionalidad, a las personas que investigan la seguridad podría resultarles complicado demostrar este elemento. A menudo, no tienen un propósito real al investigar. Acceder a un sistema podría llevar a que descubran nuevas redes, accedan a una institución tras otra e identifiquen nuevas estructuras. Para abordar estos problemas, recomendamos que quienes formulan las leyes consideren las siguientes recomendaciones, como mínimo, al analizar propuestas o leyes existentes a escala federal en el país que afecten a investigadores(as) de seguridad:

1. **Modificar las leyes existentes que podrían ser usadas para sancionar a investigadores e investigadoras de seguridad digital** para que definan claramente qué actividades constituyen el "acceso ilegítimo" o "no autorizado" a un sistema informático o, en su lugar, definan ciertos tipos de acceso no autorizado "legítimo" que no serían penalizados por ley. Este tipo de acceso no autorizado legítimo debería incluir la investigación de seguridad digital llevada a cabo para el beneficio público.
2. **Identificar y modificar las leyes existentes que penalizan actos definidos en términos muy generales**, como el "acceso a sistemas informáticos" y la "evasión de mecanismos de seguridad".
3. **Incorporar un enfoque de buena fe a la revelación de vulnerabilidades o, en su lugar, crear una defensa afirmativa para la investigación de seguridad digital** con el fin de garantizar la protección de las personas que informen vulnerabilidades y amenazas a autoridades o entidades privadas.
4. **Modificar las leyes existentes para que exijan un requisito de intencionalidad agravada**, que vaya más allá del mero conocimiento en los casos de acceso no autorizado a sistemas informáticos o bases de datos.
5. **Revisar las disposiciones existentes en materia de ciberdelincuencia para garantizar que el costo de las medidas de seguridad razonables no se utilice para responsabilizar legalmente a las personas investigadoras** que revelen la ausencia de dichas medidas recurriendo a prácticas responsables de denuncia de vulnerabilidades.

RECOMENDACIONES PARA REFORMAS DE POLÍTICAS PÚBLICAS Y ADMINISTRATIVAS:

1. **Los Gobiernos deben buscar promover la revelación de vulnerabilidades en el sector público *y* en el privado** como objetivo clave en las políticas de ciberseguridad. Deben implementar **un proceso de equidad de vulnerabilidades** para sus propias operaciones, así como también **políticas de denuncia de vulnerabilidades** para servicios provistos por el Gobierno y sus propias instituciones. Los Gobiernos deben promover y apoyar el desarrollo de **políticas coordinadas en materia de vulnerabilidades** para todas las entidades que operen en sus jurisdicciones, asegurándose de que promuevan y protejan la cultura de la investigación de ciberseguridad y la cooperación de la comunidad. No solo deben contar con un proceso de revelación de vulnerabilidades para cuando se encuentran o descubren fallas tecnológicas en los sistemas del Gobierno, sino también asegurarse de que todas las ramas del Gobierno faciliten la revelación coordinada de vulnerabilidades (CVD) para la industria.
2. **Los Gobiernos deben trabajar en colaboración con la comunidad de infosec** y **desarrollar un mecanismo de transparencia para revelar las diversas sugerencias o recomendaciones en torno a las vulnerabilidades de seguridad en los sistemas del sector público** que se proponen cada año, junto con el tipo de informe, y si la recomendación fue implementada o no.
3. **Las autoridades no deben crear entornos hostiles para aquellos que expresan sus preocupaciones acerca de la seguridad informática**; específicamente, deben abstenerse de perseguir, desacreditar o difamar a personas que comunican sus preocupaciones acerca de los sistemas informáticos, los mecanismos de seguridad, las bases de datos y otras herramientas similares.
4. Las autoridades de Gobierno, mediante el uso de mecanismos adecuados a su estructura constitucional interna y su tradición jurídica, **deberían emitir directrices dirigidas a las fiscalías en torno a casos de seguridad informática que desalienten el procesamiento o brinden un margen de libertad de procesamiento** para evitar perseguir, acosar y penalizar a quienes lleven a cabo investigaciones de seguridad.
5. **Asegurar que la formulación de políticas y los procesos legislativos estén abiertos a** personas del ámbito académico, de la investigación de la seguridad informática, entidades del sector social y el público en general para que puedan participar activamente y expresar sus opiniones.

Para obtener más información, póngase en contacto con nosotros:

Gaspar Pisanu
(gaspar@accessnow.org)

Raman Jit Singh Chima
(raman@accessnow.org)

accessnow

Access Now (https://www.accessnow.org) defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.