Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

accessnow

The persecution of the information security community in Latin America

August 2021

*This report builds on research and analysis by the **Harvard Law School Cyberlaw Clinic, based at the Berkman Klein Center for Internet & Society**, with researchers **Fernanda Gomez Balderas and Payton Wulff led by Jessica Fjeld, Lecturer on Law and the Assistant Director of the Cyberlaw Clinic**. Access Now is responsible for the content, and any errors, omissions, or misrepresentations are ours alone.*

accessnow

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report was made possible, in part, by the shared knowledge of the civil society organizations working daily to defend digital security researchers in Latin America. We are so grateful for your time, your confidence, and your interest in this topic. For their insights and expertise, and help identifying case studies in Colombia, we would like to thank Fundación Karisma. For insight on the information security community in Argentina and help identifying current cases of persecution of digital security researchers, we would like to thank Fundación Vía Libre. For a better understanding of the cybersecurity landscape in Mexico, and insight on the persecution of digital security researchers in other Latin American countries, we would like to thank ARTICLE 19, particularly regarding the chapters on Mexico and Central America, and Brazil and South America. We would also like to thank attorney Jazmin Aquino for providing additional information and guidance on the infosec community in Mexico. Finally, we would like to give special thanks to Centro de Autonomía Digital, its executive director Sara Zambrano, and attorney Carlos Soria, for sharing their first-hand knowledge and experience with Ola Bini's case and continued support of this report. Our case study on the persecution of Ola Bini was greatly enriched through their ongoing willingness to share their lived experiences with us.

INTRODUCTION

Digital security researchers are the unsung heroes of cybersecurity. Their work identifying and reporting on vulnerabilities or weaknesses in digital infrastructures, such as the internet, software code, and information systems, benefits all of us by making these systems more secure. Despite the clear value of their work, governments worldwide have not only underappreciated digital security researchers, but have also persecuted them for finding and reporting on vulnerabilities. This report aims to bring greater awareness to governments' adverse treatment of digital security researchers, both under the law and in practice, with a particular focus on governments' response to digital security research in four Latin American countries: Argentina, Colombia, Ecuador, and Mexico.

By "digital security researchers," we mean researchers, software developers, technical experts, and other actors in the information security community who—among their other activities—identify and report on vulnerabilities in digital systems to benefit the public at large. This community is also sometimes described as the "infosec," or information security community. Often, politicians and other government actors may lack a technical understanding of what digital security research entails, painting it as malicious "hacking" and publicly perpetuating the harmful narrative that digital security research should be punished. Those engaged in "ethical hacking," or hackers for good, represent a critical pillar of the infosec community; without these digital security research pioneers, global cybersecurity would be jeopardized and users placed at increased risk. By locating, analyzing, and exposing infosec vulnerabilities, digital security researchers make the internet and information systems more secure by strengthening them against data breaches and other forms of cybersecurity attacks. In addition, digital security research often promotes human rights, such as the right to free expression and the right to privacy, by uncovering and reporting on harms conducted by public and private actors via technology, such as the use of spyware or malware on certain groups in society.

By "persecute," we mean generally any activity carried out by a government or an entity acting in concert with the government to punish, sanction, harass, or intimidate digital security researchers. Persecutions have taken many forms, including criminal prosecution, civil legal action, regulatory or administrative sanctions, physical harassment, surveillance, and other extralegal means of intimidation. The motivations behind these persecutions are not always clear. Sometimes a government may wish to keep a vulnerability out of public attention to avoid scrutiny, and therefore try to silence the messenger, i.e., the digital security researcher that discovered the flaw. In other cases, the persecution may be a result of insufficient care in drafting or updating legal frameworks. Over the last several years, many countries have enacted cybercrime laws that do not explicitly exempt digital security research from their scope, creating significant legal uncertainty and risk for digital security researchers.

For each country featured in this report (Argentina, Colombia, Ecuador, and Mexico), we first identify the relevant legal framework and highlight some of the country's federal laws which could be used to impose criminal or civil liability on digital security researchers at a national level. We then describe examples of persecutions of digital security researchers in these countries, illustrated through case studies that identify individual digital security researchers who have recently faced persecution for their vulnerability research or association with the infosec community. We conclude by making a set of recommendations to increase support for and protection of digital security researchers' work in Latin America going forward.

I. ARGENTINA

LEGAL FRAMEWORK AND ANALYSIS

In Argentina, there are various laws that could be used to punish digital security researchers for reporting on vulnerabilities in IT infrastructures, including multiple provisions of Argentina's federal criminal code (Código Penal). Certain provisions of Argentina's intellectual property regime could also impose both civil and criminal liability on digital security researchers, in instances where their disclosures reproduce, and thus by definition, infringe, sections of copyrighted code. Here, we identify and analyze some of the key provisions of Argentinean law that are likely to be used in legal action against digital security researchers.

In the past, Argentinean law enforcement has invoked cybercrime laws against digital security researchers for conducting vulnerability research. For example, Article 183 of the Código Penal was used to question the activities of software developer Joaquín Sorianello in 2015.[1] Under Art. 183, in relevant part, anyone who alters, destroys, or disables data, documents, or computer programs or information systems will be punished by up to one year in prison.[2] Although "alter" could be interpreted very broadly, "destroy" and "disable" suggest that there must be some type of damage done to violate this article.[3]

Art. 157 bis of the criminal code could also easily be used to criminalize the work of digital security researchers. Art. 157 bis (in relevant part) punishes anyone who knowingly and illegitimately, or in violation of confidentiality and security systems, accesses, in any way, a databank of personal data, or anyone who illegitimately provides or reveals information from a databank of personal data that is protected as secret by the law.[4]

Depending on what is considered to be "knowingly" and "illegitimately" under Art. 157 bis, digital security researchers are likely punishable. Under the plain meanings of "knowingly" and "illegitimately," digital security researchers are aware that in most cases their access is "illegitimate." For example, a digital security researcher that observes a vulnerability in a company's database and

[1] *See* "Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica," La Nación, August 2, 2016. Available at 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."

[3] *Supra* n. 1. Judicial interpretation of this article in Joaquín Sorianello's case determined that Sorianello had not violated this law because no damage was done to the computer system he was researching. The judge noted that while Sorianello did access the systems, he did not damage the systems but instead found vulnerabilities and reported those vulnerabilities to the company in order to improve the systems. This interpretation recognizes the social utility of digital security research.

[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 un (1) a cuatro (4) años."

must hack into the system to find the code responsible for the vulnerability in order to report the vulnerability to the company would arguably *know* their access was *illegitimate*.

Art. 153 bis of the criminal code also has broad language that could be used to criminalize digital security research. Art. 153 bis punishes anyone who knowingly logs in, without authorization or exceeding the authorization they possess, to an information system with restricted access.[5]

Once again, the intent requirement of Art. 153 bis, "knowingly," is general enough to be used to prosecute vulnerability research; digital security researchers arguably always have knowledge of the fact that they are logging in to systems without authorization. The statute fails to recognize that despite having the requisite knowledge, security researchers' specific intentions in performing this type of work are usually to benefit society by exposing vulnerabilities and enhancing security systems, rather than the malicious intent to commit a crime. By reducing the inquiry of intent to mere knowledge, the statute fails to account for this distinction. The vague language of Art. 153 bis also raises questions about what constitutes authorization and who gives authorization for lawful access to such systems.

Beyond criminal law, certain provisions of Argentina's intellectual property laws could be used to sanction digital security research. Under Argentina's intellectual property regime, copyright protections extend to computer source and object code, as well as the compilation of data in a database.[6] Digital security researchers could thus infringe on copyright holders' rights if their disclosures require them to reproduce a portion of software code. The software code's copyright holder could conceivably initiate civil proceedings for infringement against a digital security researcher.

Additionally, copyright infringement in Argentina can also be punished by criminal sanctions. Per Art. 71 of the intellectual property regime, any "fraud" against the intellectual property rights of another can result in the criminal penalties specified in Art. 172 of the criminal code, which include up to six years in prison.[7] The broad scope of what could constitute fraud against intellectual property rights means this article provides yet another avenue for Argentinean officials, companies, and others to characterize the legitimate activities of digital security researchers as criminal acts.[8]

---

[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."

[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] Westlaw's Practical Law "Copyright litigation in Argentina: overview, Practical Law Country Q&A w-010-2109," notes that "in principle, any type of willful infringement of copyright is subject to the penalties provided by section 71 of the Copyright Law."

Case Study

There have been a number of recent examples of digital security researchers being persecuted, criminally or otherwise, in Argentina. Here, we focus on two of the most recent cases that we have identified in our research, the cases of Javier Smaldone and Gaspar Ortmann.[9]

Javier Smaldone is a security researcher and IT expert who is well known in the Argentinean infosec community. In the past, Smaldone has performed security research on Argentina's use of e-voting machines, and he has testified in front of the Argentinean Senate to share his expertise on the topic and advise against the use of such devices. Smaldone maintains a personal blog that is often critical of the government's cybersecurity practices, and he is also active on his personal Twitter account regarding such issues.[10]

In October 2019, Argentinian police detained Smaldone for questioning under suspicion of hacking and leaking data from government systems, a hacking scandal that later became known as "La Gorra Leaks 2.0."[11] The police detained Smaldone for a total of 12 hours before releasing him. Authorities also raided Smaldone's home, seizing and searching various of Smaldone's phones, computers, and pen drives.

In the days following his arrest, Smaldone, knowing his own innocence, requested the court documents that the police submitted to obtain a warrant for his arrest. He was surprised to discover that the main "evidence" the police used to obtain a warrant were his Tweets discussing and analyzing the "La Gorra 2.0" data leaks.

In addition, Smaldone realized that the police had been building their investigation against him over a period of a few months. Their investigation included: "cyber-patrolling" Smaldone's Twitter and other social media accounts; requesting Smaldone's personal cell phone records from his mobile service provider for the location of his phone and his incoming and outgoing call records; requesting Smaldone's account information from WhatsApp, including the IP addresses used in connection over the months leading up to the investigation; requesting records of Smaldone's use of the public transit card "Sube" over the year leading up to the investigation; surveilling Smaldone in public and taking photos of him; and putting surveillance cameras outside of Smaldone's children's home.[12] This egregious level of surveillance alone should be considered persecution, especially considering that the police had no real evidence of Smaldone's involvement in the data leaks prior to commencing their investigation.

While Smaldone was never formally charged under the criminal code, his case exemplifies how someone with technical knowledge of IT systems who is associated with the infosec community

[9] As previously mentioned, software developer Joaquín Sorianello was also involved in a prominent case in 2016 that was subsequently dismissed. This report will not discuss his case in greater detail.
[10] Smaldone's blog is available at: https://blog.smaldone.com.ar/. His Twitter account is @mis2centavos (https://twitter.com/mis2centavos?lang=en).
[11] More information about the case available at: https://www.eff.org/es/deeplinks/2019/11/raid-javier-smaldone-argentinian-authorities-have-restarted-their-harassment-e
[12] Smaldone discusses all of this information in his blog post "Allanado y detenido por tuitear," authored and posted by him on January 25, 2020. https://blog.smaldone.com.ar/2020/01/25/allanado-y-detenido-por-tuitear/

can be persecuted without just cause. The Argentinean police essentially profiled Smaldone as a criminal hacker because of his technical expertise and his vocal role in reporting and analyzing hacks via his Twitter account, and perhaps also because of his critical views on how the government has handled these issues in the past. As a result, he was subjected to intimidation and invasions of privacy.

Smaldone's case exemplifies how the narrative around hacking can be harmful to those performing legitimate security research or those merely known to be members of the infosec community. Those in positions of power often perpetuate this harmful narrative due to their own political motivations or their lack of technical understanding of these concepts, or both. According to his blog, Smaldone views his case as nothing short of a political persecution, and he is now worried about what else could happen to him or others working in Argentina's infosec space in the future.

Gaspar Ortmann is an engineering manager at the travel company Despegar[13] who enjoys looking for vulnerabilities in IT infrastructure in his spare time to help strengthen these technologies. In 2019, Ortmann discovered a vulnerability in the HomeBanking system of Banco Nación that allowed users to modify the US dollar price without the bank's security system verifying that price. As a result, users could buy US dollars for less and sell them for more than their actual exchange value. Ortmann carried out multiple transactions himself to demonstrate the vulnerability.[14]

Ortmann then attempted to disclose this vulnerability to security officials at the bank, reaching out to them via email, LinkedIn, and WhatsApp. After receiving no response, he prepared a letter with screenshots of the transactions he carried out that demonstrated the vulnerability, which he then personally delivered to a branch of the bank.

Despite reporting the vulnerability in good faith and taking the necessary steps to return the profits from the transactions conducted as part of the research to the bank, Ortmann was still criminally prosecuted.[15] Recently, in December 2020, the judge overseeing Ortmann's case decided to dismiss the matter. The judge explained that Ortmann did not improperly access a computer system, because as a bank client, Ortmann had access to the HomeBanking system. The judge also noted the public utility of Ortmann's disclosure.

The outcome of Ortmann's case sets a precedent in favor of security research and vulnerability disclosure that will hopefully be remembered by the Argentinean law enforcement and judiciary in the future. However, his case also demonstrates that without adequate vulnerability disclosure mechanisms, digital security researchers are still risking their reputations, and opening themselves up to the possibility of being involved in legal proceedings to report on the vulnerabilities they find.

[13] Despegar is a "leading online travel company in Latin America… [o]perating across 20 countries." Investor.desgapar.com, "Company Profile." Available at https://investor.despegar.com/home/default.aspx.
[14] Sebastián Gamen, "Caso Gaspar Ariel Ortmann, otra sentencia a favor del hacking ético." Perfil. December 11, 2020. Available at https://www.perfil.com/noticias/opinion/sebastian-gamen-caso-gaspar-ariel-ortmann-otra-sentencia-a-favor-del-hacking-etico.phtml.
[15] Ibid.

II. COLOMBIA

LEGAL FRAMEWORK AND ANALYSIS

Colombia has a variety of criminal laws, including the "Código Penal" and "Ley de Delitos Informáticos," that could be used to sanction information security researchers for a variety of reasons, including access to computer systems, interception and disclosure of computer data, and personal data violations, among others. In addition, Colombia has copyright and intellectual property laws ("Ley sobre Derechos de Autor"), as well as data protection regulations ("Ley de Protección de Datos Personales")[16] that could be used to impose fines and other sanctions. In the following paragraphs, we detail a number of the provisions that are likely to be employed by the government against information security researchers.

In 2009, the Law 1273 de 2009 "Ley de Delitos Informáticos" (Cybercrime Law) was enacted as part of the Criminal Code.[17] It created new criminal offenses based on the Budapest Convention on Cybercrime.[18] Among its provisions that could be used against digital security researchers is Art. 269A, regarding the abusive access to a computer system. The article states that:

> "[a]nyone who, without authorization or acting differently than agreed, accesses partially or totally a computer system protected or not protected with a security measure, or who remains inside the system against the will of the person who has a legitimate right to exclude him or her, will be imprisoned from 48 to 96 months and fined with the equivalent of 100 to 1000 minimum monthly wages."[19]

A constant problem with the Colombian criminal framework on cybercrime is the absence of requiring intent to cause harm or intent to obtain an economic benefit as an element of the crime.[20] An information security researcher could be held criminally liable for accessing a "not protected" computer system, regardless of their intention. Compounding the reasons for concern, if someone finds out the system has a vulnerability and manages to report it, this person can be held criminally liable even though they did not cause any damage or harm.

Further, this kind of conduct is defined as "abusive," although the only apparent reason to describe it that way is the absence of authorization to access a computer system. If someone accidentally

[16] In general, data protection regulations tend to be supportive of human rights, particularly privacy, in the digital sphere, and this reference is not meant to discourage their adoption or enforcement. However, in individual instances, it is possible for these laws to be employed against members of the infosec community, for example when their work in exposing the lack of security around sensitive data leads them to access that data.
[17] The Ley de Delitos Informáticos of 2009 became part of Chapters I and II, Title VII Bis "De la Protección de la Información y de los Datos" (Information and Data Protection) of the Código Penal.
[18] Colombia fully ratified the Budapest Convention on Cybercrime in 2020. *See* Council of Europe; Columbia joined the Budapest Convention on Cybercrime (2020), available at 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. Available at: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf .

accesses an unprotected system, they could be sanctioned under article 269A.

Another key provision is Art. 296C, which sanctions the interception of computer data. The article states that:

> "[a]nyone that in the absence of a judicial order intercepts computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data will be imprisoned from 36 to 72 months."[21]

Under this article, it is unclear whether data interception can result from accessing a computer system while looking for vulnerabilities. As under Article 269A, there is no reference to the intention to cause harm, which opens the door to apply to a broader number of applications.

Moreover, Art. 269D, sanctioning computer damage, could also be problematic. This article holds liable "[a]nyone who lacking an attribution or without a right destroys, damages, deletes, deteriorates, alters, or suppresses computer data or a computer processing system or any of its elements or software."[22]

The "alteration" of computer data, software, or a computer processing system, as opposed to the other conduct detailed in this law, does not necessarily entail damaging the system or data. Also, there is a risk that when accessing a system with vulnerabilities that the researcher is not perfectly familiar with, they may inadvertently cause alteration or damage, for which they could then be held liable.[23]

Article 269H also includes some situations in which sanctions will increase by 50% to 75%. These aggravating circumstances include:

> "(1) When the conduct is executed on networks or computing systems or communicating systems belonging to the State or the government. (…)
> (4) Revealing the information or data causing harm to someone else. (…)
> (5) Obtaining a benefit for him/her or another person."[24]

This article intensifies the risk for information security researchers that might identify vulnerabilities

[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 trasporte 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. Available at: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf .
[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.

in governmental systems or networks. Under Article 269(H) (1), there is no need to demonstrate intention or motive; the sanction can be increased for the sole reason that the system belongs to the government. Paragraph (4) is ambiguous too and potentially dangerous to security research as the reporting of a vulnerability could be construed as revealing information. Finally, paragraph (5) does include an element that should be part of all cybercrime offenses: a motive to obtain a benefit. Ideally, this fifth condition should be included, along with causing harm, in all the scenarios presented in the Law 1273.

Colombia also sanctions violations of copyright via the Código Penal and the Law 23 de 1982 "Ley sobre Derechos de Autor" (Copyright Law). Under Colombian law, information security researchers can be prosecuted for copyright infringement. In this sense, the software is a literary work and it can be registered according to articles 1, 2, 4, and 7[25] of the "Decreto 1360 de 1989," which regulates the registration of software in the Registro Nacional del Derecho de Autor (National Copyright Office). Software's recognition and protection was also stated in articles 3,[26] 4,[27] and 23[28] of the 1993 Decisión 351 of the Acuerdo de Cartagena.

The Código Penal includes three criminal offenses of copyright infringement that are punished with imprisonment: author's moral rights violations (Article 270),[29] authors' economic rights violations

[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."

[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 veinte seis 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. PARAGRAFO. 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.

(Article 271),[30] and violation of the mechanisms protecting copyright (Article 272).[31] Moral rights violations encompass mutilating or transforming a literary work; while economic rights violations include literary works' reproduction and distribution, among others. Specifically, Article 271 indicates that the reproduction of these works using computing means will be sanctioned when the author is motivated by getting an economic benefit, whether it is direct or indirect. Since vulnerability research could be presumed to have an indirect economic benefit to practitioners, such as enhancing their reputations, these offenses could be used to persecute them. Identifying vulnerabilities and accessing computing systems can entail access to the code and programming instructions that, when replicated (even if incidentally) or transformed, can result in copyright infringement.[32] Additionally, digital researchers' activities can be prosecuted under Article 272, paragraph 3, which sanctions anyone who deletes or evades a system that allows copyright holders to control their works' rights or makes it impossible for them to restrict any unauthorized use. Gaining access to a system might amount to evading it and getting control over the code, and, consequently, researchers could be held accountable.

The "Ley sobre Derechos de Autor" sanctions copyright infringement with prison (Article 232) and fines (Article 233). Similar to the "Código Penal", Article 232 lists a series of illicit conduct that may result in three to six months in prison. This conduct includes the reproduction and modification of a

[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.

[32] In 2014, Diego Gomez, a Biology student, was prosecuted for having uploaded someone else's master's thesis to Scribd so other students could consult it. The penalty ranged from four to eight years. On May 24, 2017, he was found innocent because he did not disclose the work, as it was already public, nor looked for any profit, and his conduct had an educative purpose. However, the decision was appealed. On December 4, 2017, the initial judgment was confirmed and he was found not guilty. Even though this case does not involve a digital security researcher, it has been included to show that current Colombian copyright legislation can pose a threat to the community and other Internet users. Also, it helps to stress copyright infringement sanction's lack of proportionality in relation to fair use. See: Fundación Karisma "Campaña de crowdfunding busca ayudar a biólogo acusado penalmente por compartir una investigación académica en línea," Fundación Karisma, June 12, 2017. Available at: https://web.karisma.org.co/campana-de-crowdfunding-busca-ayudar-a-biologo-acusado-penalmente-por-compartir-una-investigacion-academica-en-linea/; Fundacion Karisma, "El caso de Diego Gómez termina," December 15, 2017. Available at: https://web.karisma.org.co/compartir-no-es-delito-sharing-is-not-a-crime/ .

work, but the penalties are considerably lower than the other crimes analyzed previously.

Moreover, Article 12[33] of the Law 1915 of July 12, 2018 (which modifies the "Ley sobre Derechos de Autor" and establishes new provisions) imposes civil penalties for certain conduct, including the unauthorized avoidance of technological measures to control access to a work. There are certain exceptions to liability, including good faith reverse engineering. Most importantly, the law exempts from liability if the actions were performed with the only intention of identifying and analyzing the flaws and vulnerabilities of technologies to code and encode information. In order to take advantage of this exemption, however, researchers must legally obtain a copy or work sample and make a good faith effort to get authorization,[34] both of which could be a challenge given many institutions' hostility to researchers.

Case Study

Juliana Peña is a Colombian software engineer who gained media and government attention when she identified a security problem with the Colombian digital census. The e-census became available on January 9, 2018, and was administered by the "Departamento Administrativo Nacional de Estadística," also known as DANE (National Administrative Department of Statistics). Juliana reported that the website failed to provide adequate security for its users because it saved their passwords without effective encryption. As Peña explained, when she filled out the census herself, "The website showed me my password on the screen when I finished my registration. This made me suspect that the website stores the password in plain text. I could confirm it using the option 'Forgot my password' because I received an email with it."[35]

Moreover, after searching through the census website, there was no way to modify the password. If DANE stored the passwords without security measures, it could risk users' accounts on various websites on which they had used the same passwords. Peña denounced the lack of security as a

[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.

[35] La W, ""La página del eCenso almacena mal tu contraseña, no la uses": Juliana Peña," WRadio, January 15, 2018. Available at: https://www.wradio.com.co/noticias/actualidad/la-pagina-del-ecenso-almacena-mal-tu-contrasena-no-la-uses-juliana-pena/20180115/nota/3689816.aspx.

terrible mistake by the government.[36]

Days after, she clarified that although the passwords were not stored in plain text, the system used symmetric encryption (which is reversible) and that the key was publicly available for anyone who wanted to look at it. Instead, she suggested using a non-reversible hash-salt.[37]

DANE declared Peña's information was false. It issued a written statement explaining that the tool abided by strict security parameters. Once a user signs up, DANE said, their password will only be sent in a personal and exclusive way if they forget it. According to DANE, Peña lacked experience and sufficient knowledge to make those declarations, which DANE asserted had no factual support.[38]

Even though DANE stressed that their system operated with high-security parameters, other people like Julián Alarcón and Mauricio Duque also criticized the platform.[39] Carolina Botero, from Fundación Karisma, indicated that Peña might not have alerted DANE before going public because the Colombian government lacks mechanisms or communication channels via which individuals can report digital security problems.[40]

As a result of DANE's reaction and failure to recognize their mistake, Peña was targeted by the media.[41] A group of Colombian developers and Fundación Karisma advocated on behalf of Peña.[42] On January 19, 2018, they sent an email to the government requesting a meeting to talk about possibilities of collaboration on information security matters and Peña's revindication.[43]

---

[36] La W, ""La página del eCenso almacena mal tu contraseña, no la uses": Juliana Peña," WRadio, January 15, 2018. Available at: 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," January 13, 2018. Available at: https://julip.co/2018/01/actualizacion-contrasenas-censo/

[38] DANE, "El DANE responde a afirmaciones falsas sobre la seguridad del eCenso," 2018. Available at: 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," January 18, 2018. Available at: 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, January 18, 2018. Available at: https://www.elespectador.com/opinion/leccion-1-del-e-censo-no-matar-la-mensajera-columna-734171/ .

[40] Carolina Botero Cabrera, "Lección 1 del e-censo: no matar a la mensajera," El Espectador, January 18, 2018. Available at: 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," January 18, 2018. Available at: https://www.elespectador.com/economia/afirmaciones-de-bloguera-juliana-pena-son-falsas-irresponsables-y-apresuradas-dane-article-733982/

[42] See: "Open Letter to DANE,"January 19, 2018. Available at: https://github.com/colombia-dev/carta .
See also: Johann Echavarria, "Resumen sobre el censo virtual del DANE, Los hallazgos de seguridad de Juliana Peña y las respuestas del DANE y Colombia Dev," January 21, 2018. Available at: https://medium.com/@abrupto/resumen-sobre-el-censo-virtual-del-dane-los-hallazgos-de-seguridad-de-juliana-pe%C3%B1a-y-las-db42040132e5

[43] See: Colombia.Dev email sent to a government official: https://github.com/colombia-dev/carta/blob/master/contacto_dane.md .
See also: DANE, "El DANE ratifica que el eCenso es seguro," 2018. Available at: https://www.dane.gov.co/index.php/actualidad-dane/4459-el-dane-ratifica-que-el-ecenso-es-seguro .

The meeting took place on January 24, and resulted in an amicable resolution.[44] The government indicated that they had created a Unified Command Post (Puesto de Mando Unificado– PMU) to monitor the platform of the eCensus permanently. The authorities also recognized the "valuable contributions made by the developers' community, citizens, and Juliana Peña to improve the eCensus's platform." DANE stated that they "have no doubt on Juliana Peña's good intentions and her professional ethics in regards to her comments."[45] Colombia.Dev and Fundación Karisma acted as mediators between the Colombian government and Peña to prevent her from suffering further negative consequences. DANE also committed to analyzing the information security community's suggestions and having their doors open to receive reports on the system operation or any recommendations.[46]

Juliana Peña's case exposed the scarce or nonexistent means to report vulnerabilities, security flaws, and data breaches to the Colombian government. For years, the four entities in charge of solving information security problems were part of the Ministry of Defense. Recently, other authorities have taken an active role, such as the Ministerio de las Tecnologías de la Información y las Comunicaciones (Ministry of Information Technologies and Communications), also known as MinTIC.[47] The hurdles Colombian individuals face when they find a vulnerability are: (i) fearing a hostile reaction or legal sanctions; (ii) legal barriers or lack of a legal framework that protects them; (iii) lack of means to communicate with the government and a well-defined policy; and (iv) lack or insufficient coordination among the government and parties involved.[48] The information security research community and non-profit organizations like Fundación Karisma have worked to build communication channels with governmental authorities to improve this situation.

[44] See: Johann Echavarria, "Segunda parte sobre el censo del DANE, Juliana Peña, la seguridad y Colombia Dev,"January 30, 2018. Available at: https://medium.com/@abrupto/segunda-parte-sobre-el-censo-del-dane-juliana-pe%C3%B1a-la-seguridad-y-colombia-dev-49f5114223e5

[45] DANE, PMU, and Software developers' Press Release on the ECensus 2018, January 29, 2018. Available at: https://github.com/colombia-dev/carta/blob/master/comunicado.pdf .

[46] DANE, PMU, and Software developers' Press Release on the ECensus 2018, January 29, 2018. Available at: https://github.com/colombia-dev/carta/blob/master/comunicado.pdf .

[47] Fundación Karisma, Rutas de Divulgación, (2019), p. 8. Available at: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf .

[48] Fundación Karisma, Rutas de Divulgación, (2019), p. 16. Available at: https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf .

III. ECUADOR

LEGAL FRAMEWORK AND ANALYSIS

In Ecuador, multiple laws could be used to punish digital security researchers for reporting on vulnerabilities in information systems, including various articles of Ecuador's criminal code, the Código Orgánico Integral Penal. In addition, Ecuador's intellectual property law, Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, could also be used to impose administrative sanctions, civil liability, or in rare cases, criminal liability, on infosec researchers, if the disclosure they make infringes copyrighted code or other copyrighted materials.[49] Here, we identify and analyze some of the key provisions that have been used or are likely to be used in legal action against digital security researchers in Ecuador.

As a starting point, Ecuador's criminal code includes cybercrime laws that have already been used to prosecute digital security research. For example, security researcher Ola Bini (whose prominent case is discussed in greater detail in the Case Study section below) is currently being prosecuted under Art. 234 of the criminal code. Art. 234 criminalizes unauthorized access to an information system with the intent to, among other things, "illegitimately exploit" such access.[50] The statute's language is broad enough that its scope could cover vulnerability research. The statute does not specify what constitutes unauthorized access: who needs to authorize access, what constitutes authorization, and what type of access is allowed when authorization is obtained.

Art. 234 is further problematic because it does not adequately contemplate the intent of the person accessing the system. Without further clarity on what constitutes the intent to illegitimately exploit unauthorized access to an information system, accessing a system with the intent of finding and reporting vulnerabilities could be considered a form of illegitimate exploitation under the statute.

Another cybercrime law in Ecuador's criminal code that could criminalize digital security research is Art. 232, which punishes attacks on the integrity of information systems.[51] The statute lists many prohibited actions, including altering a system's technological infrastructure without the owner's

[49] Art. 131 of the statute extends copyright protection to software as a literary work, including software expressed as source code or object code. However, Art. 134 lists activities related to software that are allowed without authorization, including activities carried out on a legitimately obtained copy of the software with the sole purpose of testing, investigating, or correcting its operation or its security of the same or other programs. Art. 134(4). Digital security researchers can thus likely use this article as a safe harbor from copyright infringement claims originating from research on software.
[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] Ola Bini was first charged under this Article, as explained in greater detail in the Case Study section below.

consent.[52] Though use of the word "alter" likely implies that some additional action beyond merely accessing the system is required, it is not clear when a system is sufficiently altered for liability to arise. Depending on the system, perhaps even gaining access to it would require some form of alteration to the system. Therefore, the use of such vague verbs like "alter" could be expansive enough to criminalize infosec research.

Laws aimed at protecting privacy could also be used to target digital security researchers. For example, Articles 229 and 230 of Ecuador's criminal code punish the illegal disclosure of a database and the illegal interception of data, respectively.[53] While both articles prescribe conduct that most digital security researchers likely engage in, both articles also have heightened intent requirements that might prevent their application to some digital security research. For example, an illegal disclosure under Art. 229 requires voluntary and intentional violation of the secrecy, intimacy, and privacy of people. Digital security researchers likely do not have this intent when reporting a vulnerability. However, because the government often characterizes digital security research as malicious hacking, it might contend that security researchers do meet this heightened intent requirement in some instances.

Art. 230(1) similarly requires that an illegal interception of data include the interceptor of the data acting for personal benefit or for the benefit of a third party. While "benefit" and "third party" are broad enough that digital security research could possibly still be captured under the scope of this provision, the heightened intent requirement at least suggests that there are instances involving the illegal interception of data that will not be punishable under the statute; security research that benefits the public at large could be one of those instances.

Other, more general articles of Ecuador's criminal code could also foreseeably be used to criminalize digital security research and related activities. For example, Art. 195 prohibits anyone from possessing the infrastructure, programs, equipment, or databases that would allow them to

[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."

[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. …"

reprogram, modify, or alter the identification information of mobile terminal equipment.[54] The language of the statute is broad enough that it could be used to punish those who have in their possession dual-use technologies more generally, despite that such a broad interpretation of the statute would seemingly go beyond what was intended by lawmakers.

Another example of a more general law that could be applied to a specific instance of security research is Art. 178, which broadly punishes violations of privacy, including accessing, examining, reproducing, or disseminating, amongst other things, the personal data of another person without consent or legal authorization.[55] Without providing some sort of safe harbor for vulnerability research and reporting, digital security researchers in Ecuador could easily violate this provision of the criminal code many times over; for example, any security research accessing a database with other people's personal data would seem to violate this provision.

Case Study

Ola Bini – A prominent example of the Ecuadorian government persecuting digital security research is the case of Ola Bini. Bini's case has become paradigmatic of how severe such persecution can be. Here, we provide a summary of the criminal proceedings against Bini, as well as details of other forms of persecution that have been used to threaten and harass him, and those around him, over the past two years.

Ola Bini is a Swedish software developer who has resided in Ecuador since 2013. He is considered by many to be one of the top programmers and digital security experts in the world. He has worked on several open-source software projects to improve the security and privacy of internet users. When he arrived in Ecuador in 2013, he was working on open-source software for the global technology consultancy firm ThoughtWorks. In 2017, Bini and other colleagues from ThoughtWorks decided to leave ThoughtWorks to start Centro de Autonomía Digital ("CAD"), a non-profit organization based in Quito that focuses on developing open-source software and enhancing the privacy of software. Bini currently serves as CAD's technical director.

In April 2019, Bini was arrested by Ecuadorian authorities.[56] There were no formal charges against him at the time of his arrest, though it appears his arrest was made in connection with the revocation of asylum of Julian Assange, who was arrested a few hours before Bini. According to an

[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."
[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] More information about the case available at: https://www.amnesty.org/download/Documents/AMR2808712019SPANISH.pdf

interview with Bini's lawyer Carlos Soria, Bini had befriended Assange during his asylum in Ecuador and visited Assange at the Ecuadorian embassy approximately a dozen times over the course of many years. There was no evidence at the time of his arrest that Bini had broken any laws. The warrant for his arrest called him a "Russian Hacker," despite the fact that Bini is not Russian, nor is being a hacker a crime.

Upon arrest, Bini was held in custody without access to a lawyer or a translator. The authorities also did not contact the Swedish embassy, an omission which is regarded as a violation of international law governing consular notification and access. Soria hypothesizes that the authorities did not know why they were keeping Bini in custody, as there was no evidence linking him to any crime, and that the government was likely trying to figure out what they wanted to do with him during this time. Bini was held in custody for 70 days while prosecutors seized and examined his personal technology and his private communications to try to find evidence against him.

Eventually, Bini was charged with violating Art. 232 of the criminal code for an alleged attack on the integrity of computer systems. From the date of his initial charge, the prosecution had 90 days to carry out a formal investigation and gather evidence of Bini's alleged attack on a computer system. After the 90 days were up, the prosecution decided to charge another person as an accomplice to Bini, which Soria describes as a legal maneuver to gain an additional 30 days to find evidence against Bini.

After 28 days of the 30-day period had passed, the prosecution decided to amend its original charges against Bini to allege that he instead violated Art. 234 of the criminal code for unauthorized access to a computer system. This move left Bini's legal defense team with only two days before Bini's next hearing to formulate an entirely new legal strategy to defend against this new charge. The evidence the prosecution presented in support of the new charge was a single screenshot, found on Bini's phone, which showed a telnet login screen, though there was no additional evidence that Bini tried to proceed past the login prompt in the photo.

Now, almost two years since the date of his arrest, Bini's case is slowly moving towards trial.[57] Though his defense team is eager to prove his innocence at trial, his case has been delayed many times. At his pre-trial hearing in December 2020, the judge declined to dismiss Bini's case, despite the fact that his legal team presented for over five hours on the 120-plus civil and procedural violations his attorneys have documented throughout his case; violations that, according to Soria, should render the whole case null. The judge instead postponed the pre-trial hearing, which would finally schedule Bini's trial, until March 2021. But it wasn't until June 22, 2021 that the pre-trial hearing took place. The judge, based on scarce evidence and arguments, decided to move on to trial.

Apart from what Bini has been facing in the legal system, he has also been the victim of many extralegal forms of harassment throughout the duration of his case. For example, Bini has been the subject of continued surveillance since he was released from police custody. This surveillance has included Bini being followed, having photos taken of him, and drones following his car. As a result,

[57] More information about the case available at:
https://www.fundamedios.org.ec/alertas/jueza-yadira-proano-es-separada-del-caso-ola-bini/

Bini has had to hire a bodyguard for additional protection.

Though they have no definitive proof, Bini and his defense team suspect the government is behind this surveillance. For this reason, Bini filed a Habeas Data[58] lawsuit against various governmental institutions in hopes of discovering whether the Ecuadorian government has given authorities an official order to surveil and track Bini, and if so, to make public any information the authorities have gathered on Bini as a result of the ordered surveillance. His Habeas Data hearing, initially meant to take place in October 2020, was most recently rescheduled for March 12, 2021. However, that, too, was postponed. At the hearing, the government sent a new attorney to represent it in those proceedings, without notifying the court in advance of the change. As a result, the judge postponed the proceedings yet again and gave the government additional time to file with the court its change of legal representation[59]. Bini's team, however, believes this is nothing more than yet another procedural maneuver by the government to continue delaying the process.

Centro de Autonomía Digital has also faced significant harassment throughout Bini's case for its affiliation with Bini. For example, something as simple and essential to daily business operations as opening and maintaining a bank account has become a difficulty for CAD. Multiple banks have closed its accounts without cause or explanation, which the organization believes are efforts to block it from operating. In addition, CAD's offices have also been broken into. During the burglary some CAD's informatic equipment was taken[60], giving CAD strong suspicion that the offense was carried out by the police.

Assuming that Bini gets a fair trial eventually, Bini's lawyer Carlos Soria hopes that the trial will not only prove Bini's innocence but also serve as a precedent to ensure that digital security researchers and other technical software developers will not be criminalized for their work in the future. Soria is hopeful that Bini's case can bring greater public understanding to the infosec community's work and perhaps increase scrutiny on governmental actors that have been abusing their power to persecute researchers for this work that the government actors themselves so clearly do not understand.

[58] See: OAS, "Relation between Privacy Protection, Data Protection and Habeas Data." Available at: http://www.oas.org/dil/data_protection_privacy_habeas_data.htm

[59] More information about the case available at: https://twitter.com/ODJEcuador/status/1374801302396542979

[60] More information about the case available at: https://www.elpais.cr/2019/08/01/fiscalia-ecuatoriana-vincula-a-una-persona-mas-al-caso-del-programador-sueco-ola-bini/

IV. MEXICO

LEGAL FRAMEWORK AND ANALYSIS

Mexico has substantial criminal legislation, including the Código Penal Federal and other specialized criminal laws, that could be employed to punish information security researchers. It also has other laws, in areas like intellectual property (Ley Federal del Derecho de Autor) that could be used to impose fines and other administrative sanctions. In this section, we highlight some of the provisions that the government could use against information security researchers. Additionally, considering that the legislative branch has been very active on the subject, four recent bills are analyzed.

First, Article 211 bis 1,[61] from the Código Penal Federal (Federal Criminal Code), punishes unauthorized access to computer systems and computer devices that result in the modification, deletion, or suppression of information stored in computer systems or computer devices protected by a security mechanism. People can be punished with six months to two years in prison and a fine. Besides, taking a glance at or copying that information is sanctioned with three months up to a year in jail.

Similarly, Article 211 bis 2[62] punishes unauthorized access to computer systems and computer devices owned by the State or related to public security, if that access results in the modification, deletion, or suppression of information. Sanctions go from one year to four years in prison for state-owned systems and devices and four to ten years in the case of public security-related systems and devices. Article 211 bis 4[63] provides similar penalties for the unauthorized modification, deletion, or suppression of information stored in computers belonging to financial institutions, if they are protected by a security mechanism. In this case, the penalty is six months to four years in

[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.

prison. In case the information is "acknowledged" or copied, the person can be imprisoned for three months to two years.

As opposed to other countries, these three articles mention that the computing system or computer needs to be protected by a security mechanism. However, as in the other countries we have looked at, the law fails to require an intent to cause harm. Accessing a computing system and seeing the information it stores could be enough for the government to use this article to penalize an information security researcher looking for system vulnerabilities.

The Federal Criminal Code also includes Article 424 bis[64] related to illegal reproduction, distribution, and selling of copies of works, phonograms, videograms, or books protected under the Federal Copyright Law. Criminal liability can only be imposed under this provision if the perpetrator acted intentionally with the motive to obtain an economic benefit. Therefore, it is less likely that digital security researchers in Mexico would be threatened with criminal copyright penalties.

Article 426[65] could be used against information security researchers. It criminalizes interference with satellite and cable transmissions. Specifically, the law states that the following conduct will be penalized with six months to four years prison and the equivalent of 300 to 3,000 days fine:

> "I. Anyone who manufactures, modifies, imports, distributes, sells, or rents a device or system to decode a program carrying encrypted satellite signal without the authorization of the legal distributor. (…)
>
> III. Anyone who manufactures or distributes devices meant for receiving a program carrying cable signal without the legal distributor's authorization.
>
> IV. Anyone who receives or helps someone else to receive a program carrying encrypted cable signal without the authorization of the legal distributor."

A security researcher who created a device capable of decoding an encrypted signal could be penalized for the sole action of "manufacturing." There is no requirement to prove that the device

[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.

was used and with what intent, like causing harm, and result, such as damaging something.

The "Ley de Instituciones de Crédito" (Credit Institutions Law) also has some criminal sanctions that might be used against information security researchers. Article 112 Quater[66] indicates that anyone who commits the following acts without a "legitimate cause" or consent will be imprisoned for three to nine years and fined:

> "I. Accesses the devices or electronic, optical or any other kind of technological means of the Mexican banking system to obtain economic resources, confidential or reserved information;
>
> II. Alters or modifies the functioning mechanism of the devices or electronic, optical or any other kind of technological means used to make cash available for clients to obtain economic resources, confidential or reserved information."

Apart from the lack of malicious intent, it is unclear what is a "legitimate cause." It raises the troubling question that merely accessing any of those devices or technologies and seeing information would be enough to be penalized. Based on a literal interpretation of the article, it is only necessary that the person accessing has as their motive to "obtain" confidential information; without a requirement that their intent also be to use that information to exploit it or cause harm, the provision is dangerously broad. Moreover, it is not clear if that information needs only to be seen or needs to be downloaded or copied.

Under Article 112 Sextus,[67] the use of improper credentials to access information is criminalized. Specifically, anyone using a technological means to "impersonate" the financial authority or a public officer, director, counsel, or employee, will be imprisoned from three to nine years and fined. As others in this report, this article does not require either malicious intent or the intent to obtain profits, or any particular damage resulting from the action. It fails to mention any scenario about the result from that impersonation, like obtaining profits or a personal benefit. This leads to the very real possibility that a researcher who uses someone's credentials to test a system could be penalized.

The United States-Mexico-Canada Agreement (USMCA) led to a series of reforms of Mexican laws, including copyright and intellectual property legislation. The "Ley Federal del Derecho de Autor" (Federal Copyright Law) recognizes software as protected work under Article 13, while Article 101

[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.

establishes its definition. Article 112 prohibits importing, manufacturing, distributing, and using devices, or offering services aiming to eliminate technical protections of software or computing programs, and transmissions via the electromagnetic spectrum, among others.[68] Chapter V, on technological protection measures and Internet service providers, covers Articles 114 Bis to 114 Octies.[69] Violations to technical protection measures have a series of exceptions outlined in Article 114 Quater. For instance, section III of Article 114 Quater exempts activities performed by anyone with good faith and the authorization of the owner of the device, system, or network, with the sole purpose to test, research, or correct its security measures.[70] The person testing or researching must have the owner's consent or the exception will not apply. The "Ley Federal del Derecho de Autor" has administrative sanctions based on copyright (Articles 229 and 230) and commercial reasons (Articles 231 to 236).[71] Under Article 232 bis, anyone who produces, reproduces, manufactures, distributes, imports, commercializes, rents, stores, transports, offers, or makes available to the public devices, mechanisms, products, or systems to avoid technological protection measures will be fined.[72] As explained previously, the scope of the conduct is broad, entails numerous devices, and could apply equally to people causing actual harm, like stealing information or money, and information security researchers who want to prevent these kinds of problems.

Finally, Mexico has not yet adopted the Budapest Convention and has an observer role. However, in late 2020, the legislative branch asked the Ministry of Foreign Relations to continue working to adhere to the Convention.[73]

[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] Article 114 Octies is almost a reproduction of Section 230 of the Communications Decency Act of the United States. It incorporated a notice and take down system which did not operate previously in the Mexican jurisdiction.

[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] The sanctions based on commercial reasons were added as a result of the 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.

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

Cybersecurity bills

Since 2018, Mexican federal legislators have presented 11 bills focusing on cybersecurity.[74] Four of them are briefly analyzed to highlight their troubling content. In April 2021, Senator Lucía Trasviña introduced a bill proposing to create a "Ley General de Ciberseguridad" (General Cybersecurity Law) and eliminate some articles of the Federal Criminal Code (Articles 211 bis to 211 bis 7).[75] Some of the criminal provisions proposed include illicit computer systems access (Article 24); unauthorized data interception (Article 26); and manufacturing, use, or commercialization of software and devices employed to modify, delete, or suppress data stored in computer systems or devices (Article 28). For this last criminal offense, penalties might be disproportionate; it is wide and fails to establish the connection between these devices and software and how they might be employed.

In September 2020, Deputy Javier Salinas introduced a bill to reform fraction XXIX-M of Article 73 of the Mexican Constitution.[76] In early 2021, legislators organized an open parliament to discuss the bill.[77] The proposal is to give Congress powers to legislate on "national security, which include cybersecurity and digital human rights protection."[78] The statement of reasons is ambiguous and references cyberattacks, cyberespionage, fake news, disinformation, and sexting, among others. Numerous terms are misused, like identity theft and impersonation. According to ARTICLE 19, the bill does not distinguish between the conduct and the use of technology.[79] Further, it is unclear how some topics, like sexting, are somehow related to national security. This is undoubtedly one of the main reasons civil society has called to open the discussion and listen to the stakeholders.

---

[74] Senator Jose Ramon Enriquez Herrera: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/11/asun_4102523_20201104_1601648158.pdf; Deputy Maria Eugenia Hernandez Perez: http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/01/asun_3986616_20200108_1578514711.pdf and http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/08/asun_4059385_20200812_1597257570.pdf; Senator Alejandra Lagunes Soto Ruiz: http://sil.gobernacion.gob.mx/Archivos/Documentos/2018/10/asun_3760770_20181023_1540294391.pdf; Deputy Carlos Iván Ayala Bobadilla: http://sil.gobernacion.gob.mx/Archivos/Documentos/ 2020/08/asun_4059591_20200812_1597257015.pdf; Deputy Jose Salvador Rosas Quintanilla: http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/03/asun_4144555_20210302_1614965083.pdf; Senator Gustavo Madero Muñoz: http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/03/asun_4161702_20210325_1613504011.pdf.

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

[76] See: Cámara de Diputados, "Promueve Javier Salinas facultar a Congreso de la Unión para legislar en materia de ciberseguridad."Available at: 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. See also: 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."Available at : 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, February 26, 2020. Available at: https://www.youtube.com/watch?v=qCJerA-wm2M

[78] Deputy Javier Salinas's Bill. Available at: http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/10/asun_3953044_20191029_1569348687.pdf

[79] Articulo 19, Reforma constitucional en materia de Ciberseguridad podría explotarse para censurar y arremeter contra manifestaciones legítimas de la sociedad," February 10, 2021. Available at: https://articulo19.org/reforma-constitucional-en-materia-de-ciberseguridad-podria-explotarse-para-censurar-y-arremeter-contra-manifestaciones-legitimas-de-la-sociedad/

Previously, Senators Lucia Trasviña[80] and Miguel Mancera[81] introduced two bills. Both proposals are broad and introduce imprecise criminal offenses that penalize legitimate and everyday technology activities,[82] targeting information security researchers. Trasviñas's bill proposed to include offenses describing actions that can occur when digital researchers identify security issues; as stressed in other parts of this document, they use terms like illegitimate or unauthorized access. Accessing or interfering will automatically amount to sanctioning without leaving space to report these vulnerabilities. Similarly, Mancera's bill is troubling. Several of the proposed criminal offenses could pose a threat to digital security researchers. For instance, Article 55 of the proposed Cybersecurity law would punish looking for vulnerabilities if there is no authorization to do so. The article is also confusing because it states that the conduct will be penalized whether or not it is done without permission. Also, some of the prohibited activities, like accessing an account of services provided via the internet, should not be considered a matter of national cybersecurity and could be regulated in other kinds of laws at a local level in accordance with the Mexican criminal system.

Case Study

Chris Vickery – On April 14, 2016, Chris Vickery, an information security researcher and US citizen, found a 132GB database containing 93.4 million Mexicans' personal data on Amazon's cloud (Amazon Web Services).[83] Vickery verified that it was publicly accessible and explained how, providing screenshots.[84] "There was no password or authentication of any sort required. It was configured purely for public access. Why? I have no clue."[85] He informed the Instituto Nacional Electoral (National Electoral Institute), also known as INE, about his findings. INE verified the information and determined that it belonged to a database given to Movimiento Ciudadano, a political party; therefore, INE sanctioned the political party. The database was taken down from Amazon's cloud on April 22.[86]

[80] Senator Lucía Trasviña's Bill. Available at: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-19-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf
[81] Senator Miguel Mancera's Bill. Available at: 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 September 22, 2021. Availale at: https://r3d.mx/2020/09/22/urgente-parlamento-abierto-y-respeto-a-derechos-humanos-en-legislacion-sobre-ciberseguridad/
[83] DataBreaches, "Personal info of 93.4 million Mexicans exposed on Amazon (UPDATED)," DataBreaches, April 22, 2016. Available at: 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, April 27, 2016. Available at: 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, April 27, 2016. Available at: 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, April 22, 2016. Available at: 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, April 27, 2016. Available at: 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, April 27, 2016. Available at: https://www.databreaches.net/movimiento-ciudadano-admits-responsibility-for-mexican-voter-data-leak-on-amazon/

Movimiento Ciudadano admitted that it had uploaded and stored the information for reviewing purposes. However, it also attempted to cast blame on the security researcher. It alleged that a third individual had hacked its account on Amazon Web Services by "violating security protections using highly specialized methods proper of professional hackers."[87] The party claimed that Amazon had notified them about the illegal access to their account. Movimiento Ciudadano filed a criminal complaint against "the hackers" before the authority in charge of election crimes.[88]

Amazon Web Services declared that when the company "was notified that an unsecured database containing sensitive information was being hosted on the AWS Cloud and was publicly accessible via the internet, it followed [their] standard security protocols and confirmed that this database [was] no longer publicly accessible."[89] Further, Amazon Mexico's public relations manager said that the information was not stored securely as it had no password and was visible on the internet.[90] Movimiento Ciudadano had simply failed to secure the database.[91] Fortunately, INE agreed and dismissed Movimiento Ciudadano's arguments, holding the party responsible for the leak.

The Electoral Tribunal ratified INE's sanction of Movimiento Ciudadano with a fee of $ 1.7 million dollars ($34,158,411 Mexican pesos). The Electoral Tribunal determined that the political party utilized the 2014-2015 voter registration list for purposes outside of the legal framework, such as reproducing, storing, and exposing it online. The data exposure was severe as the list included sensitive data of electors and other personal data like age, address, date of birth, CURP (Mexico's equivalent of a Social Security or Social Insurance number), signature, biometrics, and pictures.[92]

This case study differs from some of the others in that the government declined the opportunity to blame the digital security researcher for the breach, choosing instead to hold the political party accountable. As of now, there are not any ongoing cases against information security researchers in Mexico. Nonetheless, information community researchers feel threatened and in a constant state of fear of being sanctioned by the government for their activities. They protect themselves through anonymity and are very selective with the information they share in order not to compromise their work.

[87] Movimiento Ciudadano, "No hubo filtración, fue hackeo y ya fue denunciado ante la FEPADE: Movimiento Ciudadano", Movimiento Ciudadano, April 2016. Available at: https://movimientociudadano.mx/federal/boletines/no-hubo-filtracion-fue-hackeo-denunciado-ante-fepade-movimiento-ciudadano
[88] Idem.
[89] DataBreaches, "Amazon denies Movimiento Ciudadano's claim that they were "hacked"", DataBreaches, April 28, 2016. Available at: https://www.databreaches.net/amazon-denies-movimiento-cuidadanos-claim-that-they-were-hacked/.
[90] Aurora Zepeda, "¿Qué creen? ¡nos hackearon!: Dante Delgado; rechaza venta del padrón,"Excelsior, April 28, 2016. Available at: 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, April 27, 2016. Available at: https://www.databreaches.net/movimiento-ciudadano-admits-responsibility-for-mexican-voter-data-leak-on-amazon/
[92] See: Electoral Tribunal, "Confirma TEPJF multa en contra de MC por publicación del listado nominal de electores en internet," TEPJF, September 20, 2018. Available at: https://www.te.gob.mx/front3/bulletins/detail/3408/0

INITIAL RECOMMENDATIONS TO IMPROVE THE ECOSYSTEM FOR SECURITY RESEARCHERS

The persecution of digital security researchers and trainees is a serious issue all over the world. Building an environment where they can carry out their activity without fear of being criminally prosecuted is a complex endeavor and implies many changes in legal frameworks, public policy, official narratives, media coverage, among other areas. The following recommendations are an initial glimpse of what this path of protection should look like.

RECOMMENDATIONS FOR LEGAL REFORMS:

Many of the laws relevant to digital security researchers that we have identified in this report include broad, ill-defined terms and phrases, such as "unauthorized" and "illegitimate" "access," and "alteration" or "modification" to the functioning mechanism, that fail to adequately consider the intent of the actor and whether the access actually resulted in some type of damage or harm. Although many criminal offenses do not incorporate intent, this element might also be complicated for security researchers to demonstrate. They often do not have a real purpose while investigating; accessing a system could lead them to discover new networks, access one institution after the other, and identify new infrastructures. To address these issues, we recommend that legislators consider the following at minimum when dealing with proposals or existing laws at a federal level in a country which impact security researchers:

1. **Amend existing laws that could be used to punish digital security researchers** to define activities that constitute "illegitimate" or "unauthorized" "access" to a computer system, or alternatively, define certain "legitimate" types of unauthorized access that would not be punishable under the law. This type of legitimate unauthorized access should include digital security research that is carried out for public benefit.
2. **Identify and amend existing laws that penalize vaguely defined acts** like "accessing computer systems" and "avoiding security mechanisms."
3. **Incorporate a good faith approach to vulnerability disclosures, or alternatively create an affirmative defense of conducting digital security research**, so that individuals informing authorities or private entities of vulnerabilities and threats are ensured of protection.
4. **Amend existing laws to require a heightened intent requirement**, beyond mere knowledge in cases of unauthorized access to computer systems or databases.
5. **Review existing cybercrime provisions to ensure that the cost of reasonable security measures are not used to cast liability on researchers** who reveal their absence using responsible vulnerability reporting practices**.**

RECOMMENDATIONS FOR PUBLIC POLICY AND ADMINISTRATIVE REFORMS:

1. **Governments must seek to promote vulnerability disclosure in the public *and* private sectors** as a key cybersecurity policy goal. Governments must implement **a vulnerabilities equities process** for their own operations as well as a **vulnerability reporting policy** for government-provided services and own institutions. Governments must promote and support the development of **coordinated vulnerability policies** for all entities operating in its jurisdictions, making sure that it promotes and protects a culture of cybersecurity research and community cooperation. They must not only have a vulnerability disclosure process for when they find or become aware of technology flaws in government systems, but also ensure that the whole-of-government facilitates coordinated vulnerability disclosure (CVD) for industry.
2. **Governments must work collaboratively with the infosec community** and **develop a transparency mechanism to disclose the number of suggestions/recommendations concerning security vulnerabilities in public sector systems** made each year, the kind of report, and whether the recommendation was implemented.
3. **Authorities must not create hostile environments for those who speak up with concerns about information security**; specifically, they must seek to not persecute, discredit, or defame individuals who express their concerns about computer systems, security mechanisms, databases, and other related tools.
4. Government authorities, using mechanisms appropriate to their domestic constitutional structure and legal tradition, **should issue guidelines to prosecutors concerning information security-related cases discouraging initiation of prosecution or providing prosecutorial leeway** to avoid persecution, harassment, and criminalization of responsible security research.
5. **Ensure that policymaking and legislative processes are open to** academics, information security researchers, social sector entities, and the public so they can participate actively and be heard.

For more information:

Gaspar Pisanu
(gaspar@accessnow.org)

Raman Jit Singh Chima
(raman@accessnow.org)

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.