Access Now and Fundación Vía Libre Joint Submission to the United Nations Human Rights Council on the Universal Periodic Review 42nd Session Fourth Review Cycle

13 July 2022

About Access Now and Fundación Vía Libre

Access Now is an international organization that works to defend and extend the digital rights of users at risk around the world. Through representation worldwide, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. 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. As an ECOSOC accredited organization, Access Now routinely engages with the United Nations in support of our mission to extend and defend human rights in the digital age.[1]

Fundación Vía Libre is a non-profit civil organization born in the city of Córdoba, Argentina, in the year 2000. Initially focused on Free Software public policies for the dissemination of knowledge and sustainable development, Via Libre focused its mission on broader social, economic and cultural rights and civil and political rights in environments mediated by digital technologies. Our mission is to promote and defend fundamental rights in environments mediated by information and communication technologies, with special emphasis on the monitoring and development of public policies, public awareness of issues on our agenda, capacity building and promotion of debates on issues linked to technologies that have an impact on the exercise of Human Rights.

I. Introduction

1. The Universal Periodic Review (UPR) is an important United Nations (U.N.) mechanism aimed at addressing human rights issues across the globe. Access Now and Fundación Vía Libre welcome the opportunity to contribute to Argentina's fourth review cycle.

[1] Access Now (2021) About Us, Available at , https://www.accessnow.org/.

2. This submission examines the right to freedom of expression, access to information, data protection, and the right to privacy. Specifically, this submission raises concerns regarding the persecution of the information security community, the relevance of their work to protect individual's rights, the lack of policies to protect their work, and the use of the criminal legal system to silence them.

II. Follow up from previous review[2]

3. During the third UPR cycle, Argentina received 188 recommendations, out of which 175 were supported and 13 noted. The supported recommendations related to legal and general framework of implementation, universal and cross-cutting issues, civil and political rights, economic, social, and cultural rights, women's rights, and rights of other vulnerable groups and persons. It did not include recommendations related to the right to privacy.[3]

4. The third UPR cycle included recommendations on access to public information, including recommendations on the continued adoption of measures aimed at ensuring the effective regulation and implementation of the Law on Access to Public Information in All Branches of the State.[4]

5. A recommendation on freedom of opinion and expression focused on the intensification of efforts to consolidate a broad national multisectoral strategy to combat structural discrimination, including verbal expressions, against indigenous peoples, Afro-descendants and other vulnerable groups, considering their specific needs and capacities, through the empowerment of their rights and fair reparation mechanisms.[5]

6. Since the adoption of the Working Group report of Argentina in November 2017, Argentina has made some progress in the implementation of the voluntary commitments. Argentina's National Plan on Human Rights (2017-2020) defined the Government priorities in the field of human rights in accordance with the Sustainable Development Goals and the recommendations from the UPR, treaty bodies and special

[2] United Nations General Assembly (2017, December), Report of the Working Group on the Universal Periodic Review: Argentina. Available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/367/18/PDF/G1736718.pdf?OpenElement

[3] OHCHR (2017, November). Argentina The Universal Periodic Review. Available at https://www.ohchr.org/sites/default/files/lib-docs/HRBodies/UPR/Documents/Session28/AR/ARGENTINA_Infographic_28th.pdf

[4] OHCHR (2017, November). Universal Periodic Review - Argentina. Matrix of Recommendations (Page 16). Available at https://www.ohchr.org/en/hr-bodies/upr/ar-index

[5] OHCHR (2017, November). Universal Periodic Review - Argentina. Matrix of Recommendations (Page 6). Available at https://www.ohchr.org/en/hr-bodies/upr/ar-index

procedures mandate holders.[6]

7. Argentina has advanced in the implementation of the National Mechanism for the Prevention of Torture, by completing the appointment of its members and establishing Local Mechanisms for the Prevention of Torture in eight provinces. Finally, the delegation emphasized that the President of the Republic had promoted that a wide and open debate be held in the Argentine Parliament on the decriminalization of abortion and the universalization of sexual education.[7]

III. International, regional, and domestic human rights obligations

8. As of 19 February 1968, Argentina is a state party to the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[8]

9. As of 14 August 1984, Argentina is signatory to the American Convention on Human Rights or "Pact of San José de Costa Rica".[9]

10. Article 14 of the National Constitution of Argentina guarantees the right to "publish their [people] ideas through the press without prior censorship" and to "teach and learn".[10] Article 75, numeral 22 declares the constitutional rank of international and regional treaties.[11]

11. Jurisprudentially, both at local and regional levels, the limitations on freedom of expression are analyzed in light of the tripartite test: (1) they must be established by law, precisely in its terms; (2) they have to pursue a legitimate objective; and (3) they must meet the requirements of necessity in a democratic society and proportionality. The Supreme Court of Justice of the Nation still maintains that the limitations to freedom of expression must be interpreted restrictively.[12]

---

[6] Human Rights Council (2018, June). A/HRC/37/2: Report of the Human Rights Council on its thirty-seventh session (Page 79). Available at Report of the Human Rights Council on its 34th sessionhttps://www.ohchr.org › Documents › A_HRC_37_2

[7] Human Rights Council (2018, June). A/HRC/37/2: Report of the Human Rights Council on its thirty-seventh session (Page 79). Available at Report of the Human Rights Council on its 34th sessionhttps://www.ohchr.org › Documents › A_HRC_37_2

[8] OHCHR, UN Treaty Body Database, Available at https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN.

[9] United Nations Treaty Collection, Available at https://treaties.un.org/pages/showdetails.aspx?objid=08000002800f10e1

[10] Argentinian National Constitution, Available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

[11] Id.

[12] Exemplary rulings: "Rodríguez, María Belén c. Google Inc. s/ daños y perjuicios", "Sujarchuk, Ariel Bernardo c. Warley, Jorge Alberto s/ daños y perjuicios", "Roviralta, Huberto c. Editorial Tres Puntos S.A. s/ daños y perjuicios", "Ponceti de Balbín, Indalia c. Editorial Atlántida S.A. s/ daños y perjuicios"

12. Article 19 of the National Constitution of Argentina guarantees the right to privacy by establishing that "the private actions of men that in no way offend public order and morals, or harm a third party, are only reserved to God and exempt from the authority of magistrates. No inhabitant of the Nation will be forced to do what the law does not mandate, nor deprived of what it does not prohibit". Article 18 declares that "the place of residence is inviolable, as are epistolary correspondence and private papers; and a law will determine in what cases and with what justifications their search and occupation may be carried out."

IV. Freedom of expression, access to information and the information security community

13. In August 2021, Access Now in collaboration with the Harvard Law School Cyberlaw Clinic based at the Berkman Klein Center for Internet & Society and Fundación Via Libre, published the report, "The persecution of the information security community in Latin America"[13]. As explained in the report, digital security researchers are being persecuted for their work in many countries of Latin America, one of them being Argentina.

14. "Digital security researchers," refers to 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.

15. 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.

16. 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.

V. Laws to persecute information security community in Argentina

[13] Access Now (2021, August) "The persecution of the information security community in Latin America", Available at https://www.accessnow.org/cms/assets/uploads/2021/08/persecution-infosec-latam-report.pdf

17. "Persecute" generally refers to 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 take many forms, including criminal prosecution, civil legal action, regulatory or administrative sanctions, physical harassment, surveillance, and other extralegal means of intimidation.

18. 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.

19. 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 therefore by definition, infringe, sections of copyrighted code.

20. Argentinean law enforcement has invoked cybercrime laws against digital security researchers for conducting vulnerability research. Under Article 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.[14] Although "alter" could be interpreted very broadly, "destroy" and "disable" suggest that there must be some type of damage done to violate this article.[15]

21. Article 157 bis of the criminal code could also be used to criminalize the work of digital security researchers. Article 157 bis (in relevant part) punishes anyone who knowingly and illegitimately, or in violation of confidentiality and security systems, accesses, in any

[14] 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."

[15] 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.

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.[16] Depending on what is considered to be "knowingly" and "illegitimately" under Article 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."

22. Article 153 bis of the criminal code also has broad language that could be used to criminalize digital security research. Article 153 bis punishes anyone who knowingly logs in, without authorization or exceeding the authorization they possess, to an information system with restricted access.[17] Once again, the intent requirement of Article 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 Article 153 bis also raises questions about what constitutes authorization and who gives authorization for lawful access to such systems.

23. 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.[18] 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.

---

[16] 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 coubanco 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."

[17] 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."

[18] 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; ...

24. Additionally, copyright infringement in Argentina can also be punished by criminal sanctions. Per Article 71 of the intellectual property regime, any "fraud" against the intellectual property rights of another can result in the criminal penalties specified in Article 172 of the criminal code, which includes up to six years in prison.[19] 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.[20]

VI. Cases of persecution

25. Article 183 of the Código Penal was used to question the activities of software developer **Joaquín Sorianello** in 2015. After warning the company MSA of a vulnerability in the electronic ballots system that was going to be used in the Autonomous City of Buenos Aires, his home was raided.[21]

26. Judicial interpretation of the 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.

27. In October 2019, Argentinian police detained **Javier 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."[22] 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.

---

[19] 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."

[20] 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."

[21] See "Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica," La Nación (2016, August) Available at https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088/.

[22] 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

28. 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. 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.

29. 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.[23] 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.

30. In 2019, **Gaspar Ariel 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.[24] Ortmann then attempted to disclose this vulnerability to security officials at the bank, reaching out to them via email, LinkedIn, and WhatsApp. Aer 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.

[23] 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/

[24] Sebastián Gamen (2020, December). "Caso Gaspar Ariel Ortmann, otra sentencia a favor del hacking ético." Perfil.Available at https://www.perfil.com/noticias/opinion/sebastian-gamen-caso-gaspar-ariel-ortmann-otra-sentencia

31. 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.[25] 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.

VII. Recommendations

32. The persecution of digital security researchers and trainees threatens the exercise of fundamental rights all over the world, especially in Argentina where no safeguards for their work are in place. 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.

33. Many of the laws relevant to digital security researchers that we have identified previously 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:

34. **Review and amend information technology and cybersecurity laws to ensure robust protection of fundamental human rights.**

35. **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

[25] Ibid.

should include digital security research that is carried out for public benefit.

36. **Identify and amend existing laws that penalize vaguely defined acts** like "accessing computer systems" and "avoiding security mechanisms."

37. **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.

38. **Amend existing laws to require a heightened intent requirement**, beyond mere knowledge in cases of unauthorized access to computer systems or databases.

39. **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.

40. We also recommend the following public policies and administrative reforms:

41. **The federal government must seek to promote vulnerability disclosure in the public and private sectors** as a key cybersecurity policy goal. It must implement **a vulnerabilities equities process** (VEP) for their own operations as well as a **vulnerability reporting policy** for government-provided services and own institutions. The government 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.

42. **National and local 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.

43. **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.

44. 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.

45. **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.

46. The UPR is an important U.N. process aimed to address human rights issues worldwide. Access Now and Fundación Vía Libre are grateful to make this submission.

For more information, please contact: un@accessnow.org & info@vialibre.org.ar