The gender focus in Chile`s National Cyber Security Policy[1]

El enfoque de género en la Política Nacional de Ciberseguridad de Chile

Paloma Herrera Carpintero
Centro de Estudios en Derecho Informático
Facultad de Derecho, Universidad de Chile

Introduction

The increasing economic and social development of the States stems in great part from globalization and the constant evolution and development of Information and Communication Technologies (ICTs).

The physical borders stopped being obstacles for people to develop diverse areas in their lives thanks to communication, access and the spreading of knowledge that is produced in cyberspace.
However, this techno globalization also has negative consequences, since it offers a space for activities that threaten State security and its citizens (Castro Valdebenito & Monteverde Sánchez, 2018).

According to the Economic World Forum, security events and cyberattacks are within the main global risks that are envisaged in the next ten years, specifically attacks to critical infrastructure (banks, healthcare centers, and transportation among others) and information theft, e.g. phishing)

Cyberspace must be understood as a digital information area that goes beyond the internet and includes human interactions that take place in that area (Álvarez Valenzuela & Vera Hott, 2017: 40).

Therefore, it´s an area in which people project their freedom and development. Due to the pandemic of Covid-19 this has increased, it has caused people to be more dependent on ICTs. The importance of cyberspace has made it necessary to rethink the notion of human rights, with the objective of being respected, fulfilled and protected in cyberspace.

Cybersecurity should not only be understood as a phenomenon that manifests itself and is perceived in the set of actions that are developed, coordinated and implemented for the execution and minimization of risks in cyberspace, with the objective of protecting the

[1] This text was elaborated by Daniela Olivares Rojas, investigation assistent of Center for Studies in Computer Law, and corresponds to a summary of the article *The gender focus in Chile`s National Cyber Security Policy*, by Paloma Herrera Carpintero, published in the Chilean Law and technology magazine, Vol 9 Núm. 1. (2020), elaborated to be presented at the international event "Gender approaches to cyber security". Available at: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679

characteristics of the information (confidentiality, integrity and availability). It also needs to be considered from a warranty perspective since it needs to provide and assure the respect and promote human rights in cyberspace (Álvarez Valenzuela y Vera Hott, 2017: 53). To achieve this we must count on the collaboration of the public and private sector, the civil society and citizens in general.

Regarding cybersecurity matters one the biggest worries at world level is the lack of talent and specialized professionals. The Cybersecurity Work Force report of 2019[2] indicated that the global work force of technicians and professionals needs to grow with 145% and there is a double probability of cybersecurity professionals being male.

For historical and cultural reasons women are discriminated against for being such (Durack, 1997), a bias that has also been trespassed in the design and implementation of technology, which has not been nor is neutral. An example of this is the feminization of virtual assistants such as Siri, Alexa or Cortana.

Chile´s National Cybersecurity policies[3]

In the year 2015 the Inter-ministerial committee about Cybersecurity is created, an entity in charge of proposing National Cybersecurity policies and giving advice regarding the coordination of actions, plans and programs to different institutional actors.

In the beginning of 2017, the National Cybersecurity policies are created, with the objective of improving the security standards in cyberspace and, this way ensuring full enjoyment of fundamental rights of people in equal conditions. The mentioned policies state four general objectives: i) to guard the security of people in cyberspace; ii) to protect the nation´s security; iii) to promote the collaboration and coordination between institutions; iv) to manage the risks in cyberspace.

The policies established to look out for the respect and promotion of fundamental rights in cyberspace (page 12). It also indicated that, regarding fundamental rights, a «gender focus that will make visible and affront inequalities that different groups face in cyberspace» will be employed (page 15). The prior stated is relevant because on Latin-American level Chili has been the only country that explicitly disposed the need for a gender focus in matter of cybersecurity.

The promotion of fundamental human rights in cyberspace in politics, agrees with the Charter of Human Rights and Principles for the Internet[4], that disposes the importance to «increase the awareness about the Charter in the light of increasing national and international public worry about the protection and full enjoyment of fundamental rights both online as offline» (page 1) and the importance of the respect and non-discrimination in the access, use and governance on the internet recognizing gender equality and indicating that it needs to assure «full participation of women in all areas related to the internet development to guarantee gender equality» (page 14).

[2] Available at: https://bit.ly/3f5NQ4k.
[3] «National Cybersecurity politics», Chilean government, 2017, p.12, available at: https://bit.ly/2Rgcipj.
[4] Available at: https://bit.ly/3g64UYD.

To achieve the previously indicated, the States must intensify its efforts to prevent and eliminate any violation, abuse, discrimination and violence against women and girls in the digital context.

It is necessary to show that in the policies the establishment of explicit parameters regarding what needs to be understood with gender focus and which are the primary indicators and measures we must consider in the context of gender and cybersecurity are omitted. Without these parameters it isn´t possible to verify if the statute of women has improved in the society.

One of the main measures to consider to achieve a substantial change is the generation of regular, national surveys by the State, which measure and analyze gender breach in cybersecurity and how this impacts social and economic development. Nevertheless, these practices are currently practically nonexistent.

In order to fulfill the proposed objectives in the National Cybersecurity policies in an efficient way, from a gender perspective, it´s necessary to create surveys and reports that show the relation of women with cyberspace and specifically with cybersecurity. At least, a work indicator should be considered (statistics about women in the work force and cybersecurity) and a social indicator (discrimination and gender violence online) to urge the debate between different stakeholders in this matter.

Gender focus

The international human rights system is based on two guiding principles: the equality of rights between men and women and the nondiscrimination between them, In consequence, the States must adopt the necessary measures to guarantee everyone, in equal conditions, the full enjoyment of fundamental rights. However, over the course of history women have been discriminated against and deprived of the participation in transcendental instances of social occurrences, what is present in a physical space can be intensified in a digital space.

To reduce discrimination against women, from the nineties the international community of human rights started to make an allusion to the gender focus and the importance of its mainstreaming. Gender mainstreaming is a term that originated in the Fourth World Women´s Conference celebrated in Beijing in 1995, and makes reference to the duty that the members have to «adopt measures that are necessary to eliminate all forms of discrimination against women and girls, and eliminate all obstacles in gender equality, advancement and strengthening of women´s roles»[5]. In general, the conference refers to the importance of collaboration between all the sectors and the implementation of political strategies and techniques that tend to achieve substantial equality between both genders.

The gender focus was defined in 1997 by the United Nations Economic and Social Council (ECOSOC) as:

> «The evaluation process of consequences for men and women of any planned activity, inclusive the laws, policiesand programs in all sectors and on all levels. It is a strategy destined to make the worries and experiences of women, as well as men, are integrated elements in the elaboration, application, supervision and evaluation

[5] «Report of the Fourth World Women´s Conference », United Nations, A/CONF.177/20/ Rev.1, 1996, p. 4, available at: https://bit.ly/3b1jyN0.

> of policiesand the programs in all political, economic and social fields with the objective that both men and women benefit equally and that continuous inequality is impeded. The final objective is to obtain a substantial equality between genders»[6].

UN Women has interpreted and complemented the previous definition, indicating the existing means-end relationship between the concepts of *gender equality and gender perspective* in the area of human rights. In this sense, it manifested gender equality is the general long-term development objective, while the incorporation of a gender perspective is the combination of specific focusses and strategies, as well as technical and institutional processes that are adopted to reach this objective.

The non-inclusion of women in different social corners affects us all equally. Not counting on thinking perspectives, abilities and talents coming from all social groups has as a main consequence the hindering of sustainable development and social welfare

From the ICT area and specifically from cybersecurity, the low participation and inclusion of women translates to the lack of human resources and the technical tools necessary to deal with the challenges and current risks in the digital space. On a global level cybersecurity hasn´t managed to meet the demand of professionals to work in this field, and women that decide to do so must face an industry marked by gender discrimination. A report, based on interviews with women who work in cybersecurity, showed that in their workspace it was common to hear discussions about their supposed natural inability to program or that colleagues were unmotivated to attend a talk on the subject if the speaker was a woman.

The gender breach in cybersecurity

By gender breach we mean the difference between the male and female rate in a variable category. The smaller the breach, the closer we are to equality.

The World Economic Forum (WEF) showed, in its report «The global gender gap report» of 2020, that on Latin-American level in spite of both women and men having the same access to computers and internet connection, when analyzing the use of technologies there is a digital breach, the percentage of women being lower than men. This demonstrates a lack of interest and a lack of information generating in this aspect a negative female stereotype regarding the ICT´s.

In cybersecurity, this digital breach is far more worrying if we consider there is already a huge deficiency in qualified personnel. Incentivizing and motivating women participation in this area requires a mayor social effort. The information technology company Kaspersky Lab, in its study about the reasons that impede women to access the cybersecurity field, got to the conclusion that the low percentage in female participation is due to lack of interest and lack of information about these topics, these originated mainly in instilled social prejudices at an early age[7].

[6] «Report of United Nations Economic and Social Council corresponding to 1997», United Nations, A/52/3/ Rev.1, 1997, p. 24, available at: https://bit.ly/2YxhycK.p.

[7] The study predicts that in the year 2020 the cybersecurity breach will reach 1.8 millions of people, which is exacerbated by the lack of female participation. «How to move forward?: A study about the reasons that impede women to access the cybersecurity area», Kaspersky Lab, 2017, available at: https://bit.ly/2Woz945.

Education on ICT topics is the main mechanism to achieve the destruction of *machismo* in this area and ending the abusive behavior towards women in cyberspace. For such purposes, education plans must start at an early age, so that women will be empowered, will have flexibility and the ability to develop a critical analysis free of prejudices and discrimination based on gender.

The right to a private life and the protection of personal data

The right to privacy and the right to personal data protection are especially affected in cyberspace. Just as in the physical world, discrimination stereotypes exist in the virtual world, women suffer more from online harassment compared to men, and going through online bullying and threats many times in the virtual world, generating negative effects in female victims of this behavior.

To comply with the policies, the analysis with gender perspective in the private life and the protection of personal data must understand the individual threats to which women are predisposed in cyberspace, to establish indicators, preventive measures and coercion in case of violation.

The lack of efficient mechanisms to protect topics related to the privacy and protection of personal data, such as the lack of classification of certain crimes related to technology have left women exposed to: i) focalized, uncontrolled and abusive surveillance; ii) abusive and indiscriminate treatment in the context of big data; iii) non-consensual pornography; among others.

i) Focalized, uncontrolled and abusive surveillance

The use of surveillance technologies such as drones or balloons can lead to a «indiscriminate, constant and permanent surveillance towards certain social or ethnic groups who are compelled to stop acting naturally by feeling observed and persecuted»[8].

Regardless whether this type of technology was implemented with the justification of protecting national security, in practice it has become a massive and highly intrusive surveillance policy.

Although this issue affects general public, the use of these technologies can violate women even more. In 2011 North-American NGO American Civil Liberties Union, warned that drones can be used to record sexual intimacy between couples in their homes with voyeuristic purposes[9]. This is already happening on a global level, there is an abundance of material on the internet obtained with drones, where women are the most affected, as they are exposed to sexual objectification.

ii) Abusive and indiscriminate treatment in the context of big data

In this text we understand big data as the ability to store, deal with and analyze big data bases using data mining technological tools, with the objective of inferring information and correlating it in a certain context.

[8] «The right to privacy», joint communication of Digital Rights, Intelligent Citizen, Pro Access Foundation and Privacy International, July 2018, available at: https://bit.ly/3giRlVB.
[9] Report available at: https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

The benefits that the use of big data bring to different areas of society are innumerable. The public domain is highlighted where big data has had a big impact on the design, implementation and evaluation of public policies, like incentivizing the use of public transportation or resolve unequal access to services and citizen security (Rodríguez, Palomino & Mondaca, 2017: 1).

Additionally, obtaining and analyzing data related to gender is essential to reduce inequality between men and women. To obtain this benefit, the actors that intervene in its development, implementation and analysis must consider a gender approach when executing their work since technology isn´t neutral and is historically and culturally biased by its developers and others involved. So big data can be transformed into an abusive and discriminatory mechanism that violates human rights, specifically women´s for being such.

Another important view is that discrimination against women is also present in the implementation of algorithms in the context of big data inside the data base. In fact, algorithms are created and formulated by human beings, who reproduce their biases in them, so counting on the participation of women and minorities in areas related to technology is essential for the development of technologies that respect and promote human rights.

Within the use of certain services, like e-mail, videogame platforms or user profiles created on the internet, people assume that provided data is private and provide information without verifying the purposes of data processing or the robustness of the security system, which makes them susceptible to attacks on cybersecurity. An example is the Celebgate case, in which intimate photographs of various actresses were leaked from the Apple iCloud platform, these images were obtained through phishing, remote access, forcing the password reset and using social engineering to access their email accounts to spread the images afterwards. The leak affected solely women, and the ones spreading the images were men (Marwick, 2017: 187).

iii) Non-consensual pornography

Non-consensual pornography involves the recording and spreading of erotic or explicitly sexual graphic audiovisual material without the consent of any of the people portrayed and without any legitimate purpose[10].

Women are the main victims in these practices and who commit these types of actions are usually men, by which non-consensual pornography is recognised as a type of gender violence[11].

Worldwide, countries that have legislated against non-consensual pornography, classifying it as a crime in their domestic law, are the exception[12].

[10] The definition was elaborated by the Latin-American Online Harassment Project, which was created in response to the gender violence through the non-consensual publication of images and sexual or erotic videos. «¿Porno vengeance?», Online harassment, available at: https://bit.ly/3cTvwdg.

[11] See «Cyber violence against women and girls», The European Institute for Gender Equality, 2017, available at: https://bit.ly/2QKIUoZ

[12] In Israel, The Philippines, France and Germany it is a crime.

This is due to: the lack of comprehension of the seriousness, reach and dynamic of the problem; historical indifference and hostility towards women´s autonomy; and overall the lack of comprehension in the notion of privacy (Keats & Frank, 2014: 347).

The European Institute for Gender Equality (EIGE) indicates that the perpetrators of these acts are frequently ex partners who have obtained the images or videos over the course of a previous relationship, and it´s main purpose is to publicly embarrass and humiliate the victim. However, the objective can also be profit, entertainment or voyeurism.

There are many websites dedicated to non-consensual pornography, and the users share a large quantity of photographic and audiovisual material, in some cases included with personal and sensitive data of the victim (contact number, home address among others). This can cause them to be harassed, extorted, judged, and denigrated (Hearn y Hall, 2018), which is also a transgression of their intimacy and general dignity, attends against their psychological and physical integrity: «According to the study effectuated by Cyber Civil Right Initiative, more than 80% of the victims of non-consensual pornography experience severe emotional anxiety, leading some to the extreme of suicide» (Keats y Franks, 2014: 351).

In Chili, the scarce statistics make visibility of this problem difficult. However, according to the report
«Online gender violence in Chili» the Protected Data foundation, in which women and persons of the LGTBQ+ community were surveyed, 88.1% of the respondents declare having suffered some type of violence on the internet, 66.1% indicated to have suffered (sexual) harassment, 13,6% suffered the spreading of intimate images without their consent, and 10,2% suffered extortion on the network (Matus, Rayman & Vargas, 2018: 14).

Recommendations

Through the Inter-ministerial committee about Cybersecurity the State must define what is understood by the focus on gender in the context of respect and promotion of fundamental rights and cybersecurity. Only this way guidelines can be established to face the threats and challenges in cyberspace. To achieve the previously stated, the State must start by identifying, through studies and surveys, the main risks, threats and scams that women face developing and using cyberspace.

To identify the origin of the lack of women dedicated to cybersecurity in Chili, it´s necessary to:

- Identify the number of women who study or work in any field related to cybersecurity and their motivations.
- Interview women dedicated to cybersecurity and consult whether they have suffered any type of discrimination or gender violence while performing their work tasks.
- Elaborate surveys for adolescents and girls to measure the knowledge and interest they have in technologies and specifically cybersecurity.

After that, in order to understand the discrimination and gender violence Chilean women suffer in cyberspace, it is suggested to:

- Identify, by age and ethnic group, women who use the internet and with what purpose.

- Consult those women who use the internet if they have been victims of gender violence online and if they know their rights when facing threat or transgression.

Only to the extent that the State, in collaboration with the private sector, the academic area and the society can collect and analyze this information, will they work in guidelines and advices directed to different social actors.

The State must impede that the argument for national security will be an excuse for state and municipal authorities to take disproportional security measures that will be harmful to fundamental citizen rights and specifically those of women. For such purposes, the State must coordinate, between its agents and municipals, workshops in cybersecurity topics and gender, with the objective of having public workers understand the importance of gender perspective in the execution of their duties from a regulatory and ethical scope.

Additionally, from the field of public procurement of a technological nature we suggest agents to consider the evaluation criteria and its awards, the points given for fulfillment of the gender quota by the suppliers of technological services and products, with the aim of encouraging the hiring and training of women in technology.

The State and society in general must direct their efforts in incentivizing girls and adolescents in studying careers related to cyber security. Besides, it is important to empower professionals through workshops and offer training specialization scholarships.

Finally, the organization in charge of personal data protection must consider gender focus when they issue their reports, guidelines and decisions. Consequently, the supervisory body must have the necessary powers of coercion to demand compliance with high standards in terms of data protection.

Conclusions

Cybersecurity must be understood from a human rights perspective that gives its assurance, promotion and respect to cyberspace. Taking this into consideration, the main objective of the National Cybersecurity policies is to improve the security standard in cyberspace to assure the full enjoyment of fundamental rights for people in equal conditions.

To achieve this objective, multisector collaboration and cooperation is essential. Cyber-attacks affect everyone equally, there for the prevention and incident management should be dealt with by all actors of society.

The importance of considering a gender focus in respecting and promoting human rights has been emphasized by different international organizations, since there is an agreement that as long as there are prejudices, discriminations and arbitrariness to the detriment of the rights of certain groups, as occurs with women, equality in human rights will continue to be only an idyllic concept.

For this reason, mainstreaming the gender approach is essential to tackle this inequality. To the extent that all sectors of society collaborate in the implementation of political and technical strategies that are inclusive with the female gender, we will be one step closer to achieving substantial equality in this matter.

In cybersecurity, this gap is certainly worrying. On the one hand, it manifests itself in the lack of training and female inclusion in the area; on the other, in the particular risks suffered by women in cyberspace due to being such, like the threat and violation of their right to privacy and protection of their personal data.

The lack of specialists in cybersecurity issues is alarming. New and creative ways in which cyberattacks are carried out emerge every day. Consequently, encouraging and generating new talents that come from all sectors of society is of vital importance to maintain a robust and resilient IT system.

To the extent that guidelines are not adopted to encourage women from an early age to train in ICT issues, the shortage of talents in areas related to cybersecurity will only increase. We believe that this will have as its main consequence the maintenance of gender biases in the development and use of technologies that are not neutral, but rather project the stereotypes and cultural patterns of those who intervene in them.

Only to the extent that we ensure and encourage broad female participation in cybersecurity, can we achieve a free, open, safe, resilient and equal cyberspace.

References

ÁLVAREZ VALENZUELA, Daniel & Francisco Vera Hott (2017). «Ciberseguridad y derechos humanos en América Latina». En Agustina del Campo (compiladora), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Buenos Aires: Universidad de Palermo. Available at:https://bit.ly/2Lo8IvW.

CASTRO VALDEBENITO, Hugo & Alessandro Monteverde (2018) «Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito». *Espacios,* 39 (39) Available at:https://bit.ly/3fgD3V5.

DURACK, Katherine T. (1997). «Gender, technology, and the history of technical communication», *Technical Communication Quarterly Journal,*6 (3): 249-260. DOI: 10.1207/s15427625tcq0603_2.

HEARN, Jeff y Matthew Hall (2018). «This is my cheating ex: Gender and sexuality in revenge porn». *Sexualities,* 22 (5-6): 1-23. DOI: 10.1177/1363460718779965.

KEATS, Danielle & Mary Anne Frank (2014). «Criminalizing revenge porn». *Wake Forest Law Review*, 49: 345-391. Available at:https://bit.ly/2KZ88i5.

MARWICK, Alice E. (2017) «Scandal or sex crime? Gendered privacy and the celebrity nude photo leaks». *Ethics and Information Technology,* 19: 177-191. DOI: 10.1007/ s10676-017-9431-7.

MATUS, Jessica, Danny Rayman & Rodrigo Vargas (2018). *Violencia de género en internet en Chile*. Santiago: Datos Protegidos. Available at:https://bit.ly/2KZ8xRD.

RODRÍGUEZ, Patricio, Norma Palomino & Javier Mondaca (2017). «El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el caribe». Available at:https://bit.ly/2Sv2Pve.