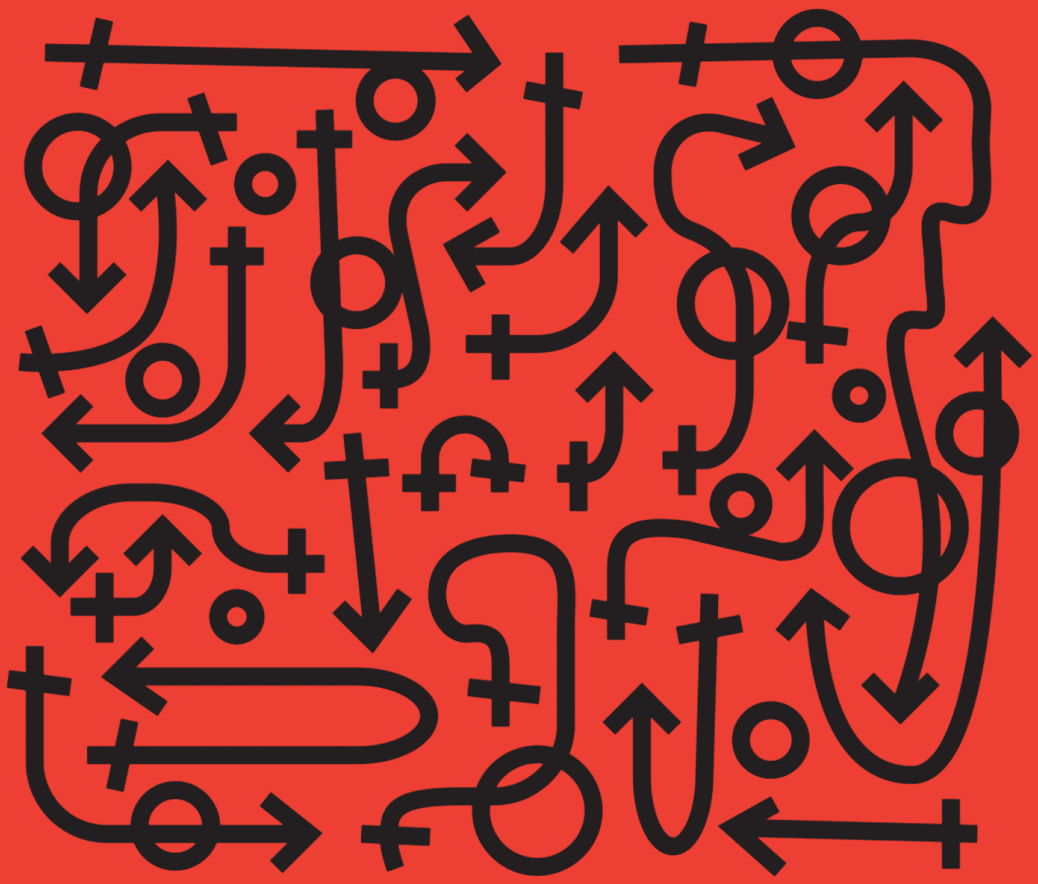
GLOBAL INFORMATION SOCIETY WATCH 2015

Sexual rights and the internet



Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch 2015
Sexual rights and the internet

Steering committee
Anriette Esterhuysen (APC)
Will Janssen (Hivos)

Coordinating committee
Monique Doppert (Hivos)
Valeria Betancourt (APC)
Mallory Knodel (APC)
Jac sm Kee (APC)
Nadine Moawad (APC)

Project coordinator
Roxana Bassi (APC)

Editor
Alan Finlay

Assistant editor, publication production
Lori Nordstrom (APC)

Proofreading
Valerie Dee
Stephanie Wildes

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Humanist Institute for Cooperation with Developing Countries (Hivos)

Hivos

APC and Hivos would like to thank the Swedish International Development Cooperation Agency (Sida) for its support for Global Information Society Watch 2015.

Sida

Published by APC and Hivos
2015

Printed in USA

ISBN 978-92-95102-41-5
APC-201510-CIPP-R-EN-P-232

BOLIVIA

DIGITAL VIOLENCE: MULTI-SECTORAL ANSWERS TO CHILD SEXUAL ABUSE ONLINE

Fundación Redes para el Desarrollo Sostenible (REDES Foundation)
J. Eduardo Rojas
eduardo@fundacionredes.org

Introduction

In June 2013, a national campaign to prevent digital violence, No Caigas en la Red ("Don't Fall into the Web"),[1] was implemented by the Bolivian government, represented by the Telecommunications and Transportation Authority (ATT). The campaign formalised the state's concern regarding the violation of human rights online, emphasising the protection of women and children.

Reports produced by the REDES Foundation's programme ENREDOMINO (2010-2015) confirm that the most common cases of digital violence amongst secondary school students have to do with hacking, grooming, harassment, impersonation and identity theft, threats, extortion, blackmail, the consumption of violent content and pornography, and threats that are the result of the use of social media for illicit ends (by organised crime, and for crimes such as sexual commerce, selling drugs and human trafficking).[2]

A form of digital violence that is increasing exponentially is the production, distribution, circulation and consumption of online material containing child sexual abuse. This is a real concern for stakeholders in the educational community, such as parents, students and teachers, as well as police officials and local and national authorities.

At the beginning of 2015 a working group against child sexual abuse material on the internet was formed. Organisations participating in the working group were the REDES Foundation, a task force in charge of fighting against violence in Cochabamba (FELCV, for its acronym in Spanish), the TICBolivia Network[3] and the Internet Society[4] chapter in Bolivia. This is the first effort in combating the problem, and the working group, alongside 45 countries in the world, aims to create a telephone hotline to report these acts.

Legislative context

The production of online content containing child sexual abuse requires a complex legal response involving different legislation dealing with, for instance, technology-related crime on one hand and sexual abuse and the protection of children on the other. It implies legislating on the digital storage, reproduction and circulation of content, as well as the trade and exchange of material among people and networks worldwide. It involves both organised crime and individuals acting independently.

In Bolivia, Article 60 of the Constitution, Article 7 of the Child and Adolescent Code, and Article 5, Clause 4 of Law 263 Against Human Trade and Trafficking all establish that the state holds the "highest responsibility for children and adolescents." Additionally, Articles 130 and 131 of the Constitution provide for the Protection of Privacy Act (*Habeas Data*), which allows for the "protection of personal data retained by any physical, electronic, magnetic or computerised means in public or private archives or databases."[5] Notably, the Protection of Privacy Act is only applied once an individual's rights are infringed upon.

Apart from these legislative tools, there are no explicit references for child protection on the internet. Few public and private institutions know about –and research – this issue in any depth. In September 2014 the REDES Foundation trained 40 members of FELCV to be able to deal with cases of digital violence. This was in response to an increase in the number of reports regarding the use of information and communications technologies (ICTs) in the violation of citizen rights. The REDES Foundation contributes by providing technical tools that help to strengthen legal action, widening the protection of rights to all people in cyberspace, not just children.[6]

1 www.nocaigasenlared.bo

2 www.teprotejo.org/index.php/es, www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=1222, new.safernet.org.br, www.inhope.org/gns/home.aspx, https://www.unodc.org/documents/wdr2014/V1403603_spanish.pdf

3 www.ticbolivia.net

4 www.isoc.org

5 www.silep.gob.bo/silep/inicio

6 www.nocaigasenlared.bo, www.enredomino.fundacionredes.org, www.fundacionredes.org/index.php/home/7-noticias/154-2015-03-04-02-03-24

The need to take action

Between 2012 and 2015, through an alliance that involved inter-institutional cooperation,[7] the REDES Foundation trained 17,837 secondary students on the topic of preventing digital violence. This took place in La Paz, Cochabamba, Santa Cruz and Tarija. During these workshops, the training team became aware of many cases such as the theft of computer chips and portable memory devices (i.e. an invasion of privacy), the theft of passwords, impersonation or identity theft, and harassment. More alarming cases included cyber extortion, violent digital content gone viral in educational communities, sexual abuse using ICTs as the main tool of contact, and – the main theme of this article – the production of online material containing child sexual abuse.

This experience is in line with cases registered by the Bolivian judicial system: in 2011 the national police registered a total of 574 accusations of tampering with a computer in eight out of the nine capital cities in the country.[8] On the other hand, the Magistrate Council in the city of La Paz confirms that between 2002 and 2012, the same crime was involved in 255 criminal trials in the city. According to the director of FELCV, Captain Mauricio Méndez, over the last 10 years "there has been an increase of 890% in cases of computer manipulation in the country. Police officials must be prepared to include digital evidence in all their investigations. In 2014 we began training police officials to manage these cases and, at the start of 2015, we installed computing equipment for computer forensic analysis; however there is still a lot for us to do."

We are facing a global phenomenon with alarming statistics. The UN Special Rapporteur on the sale of children, child prostitution and child pornography, Najat Maalla M'jid, reported to the UN General Assembly on 24 December 2012: "It is estimated that child sexual exploitation affects up to two million children each year around the world. The real magnitude of this phenomenon is unknown, given the lack of investigations and data available about the victims and the perpetrators. The criminal nature of this activity and the fear of the negative repercussions that its revelation may have, block the accessibility to information. Indubitably, the great majority of cases never get reported. The number of images of child sexual abuse has quadrupled between 2003 and 2007."[9]

Setting up the hotline

According to REDES Foundation reports, the formation of a multi-sectoral national system for the prevention of digital violence is needed.[10] This system would involve the collaboration of multiple stakeholders that share the responsibility for the collection of "digital evidence" to be used in criminal cases involving human rights violations online.

Partly in response to these needs, since 2014, the REDES Foundation has been developing an initiative in collaboration with the International Association of Internet Hotlines (INHOPE). The main objective is to set up a hotline to report and eliminate child sexual abuse content online. The hotline will be part of a global network, and will have the support of Interpol.

The initiative works through an international database coordinated by Interpol. Anonymous complaints can be made to the hotline of online child sexual abuse content. Hotline operators then remove the content, once it has been confirmed that it violates human rights. In Latin America the hotline operates in three countries: Brazil, Colombia and Peru. At present, Bolivia and Paraguay are considering implementing the service.[11]

On 9 March 2015, in the city of Cochabamba, the REDES Foundation convened a meeting with more than 30 institutions with the aim of discussing the potential of setting up the hotline.

Those who participated in this meeting included representatives of local and national governments, national police officials, the Ombudsman's Office of Bolivia and ATT functionaries. Members of the TICBolivia Network and ISOC Bolivia, civil society organisations, and academics from public and private universities were also present. The event resulted in the creation of a working group, which committed itself to standing up against the production of online child sexual abuse content.

Months later, the working group presented a paper titled *Diagnosis of institutional capabilities to mitigate and deal with the production, consumption and circulation of online child sexual abuse*

7 CREPUM Foundation, Municipal Council of La Paz, Municipal Council of Santa Cruz, CONEXIÓN Fondo de Emancipación, Ombudsman's Office of Bolivia, VIVA Foundation, TICBolivia Network, Telecommunications and Transportation Authority (ATT).

8 This data shows an increase in cases of computer tampering for which the maximum penalty is eight years in prison, according to the gravity of the crime. The relevance of this finding is that the focus is on tampering and therefore the defence of a capital asset, rather than the defence of the legal interests of the person owning the property.

9 www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session22/A-HRC-22-54_sp.pdf

10 www.fundacionredes.org/index.php/home/7-noticias/152-reporte-giswatch-vigilancia-de-internet-en-bolivia

11 www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA_InhopebrochureWEB_2014.pdf

content.[12] The internal document states: "The institutional and professional capacity to deal with cases of digital violence in Bolivia is precarious. All professionals recognise situations of digital violence in their daily lives, where potential threat is suspected, but they have yet to explore the possibilities of how their own work could contribute to an emerging professional field."

By June 2015, the initiative had achieved the following:

- The formation of a national inter-institutional working group.
- The publishing of the *Diagnosis of institutional capabilities* report, which includes public policy recommendations.
- The formation of a high-level government team to work on state policy to support the initiative.[13]
- A commitment from the vice-presidency of the Senate Chamber, represented by Senator Nélida Sifuentes, to support a bill for the prevention of digital violence (including the fight against online child abuse).
- The formation of a public-private team of computer forensics and forensic psychology experts in Cochabamba.[14]
- The TICBolivia Network confirmed its administrative and institutional support while ISOC Bolivia confirmed its technical and technological assistance for setting up and running the hotline.
- Using their own money, FELCV installed computers in Cochabamba to contribute towards the management and research of cases of digital violence. For the third year in a row, ATT carried out the national campaign Don't Fall into the Web, which includes the fight against online child sexual abuse content.
- Agreements of technical support and collaboration from solid international allies were achieved.[15]

What has been described is a working multistakeholder model that aims to have a national impact, and with a clear vision of the active and participatory role of civil society actors. A collective effort involving local, national and international actors is being made that offers answers to a specific type of digital violence using the hotline. The main finding of the initiative so far is that a law on the prevention of digital violence that includes input from all stakeholders needs to be created, to protect people online.

Action steps

Initiatives that aim to defend human rights online are more substantial when they are backed up by evidence, especially research based on experience. It is a priority to design an online system that is sustainable and multidimensional.

The formulation of a long-term plan of action is recommended; this could include the design of policies, strategies, programmes, plans and projects that have to do with the prevention and eradication of online child abuse.

It is important to promote specialised, inter-institutional cooperation when dealing with cases of digital violence. This should include sharing specialised experiences, research, and the development of capacity for a transnational response to the challenge of online child abuse.

12 REDES Foundation. (2015). *Diagnosis of institutional capabilities to mitigate and deal with the production, consumption and circulation of online child sexual abuse content.* La Paz: REDES Foundation. This paper is considered a confidential internal document and is not linked here.

13 Such as the need for a "Law on the Prevention of Digital Violence".

14 Computer forensics is dedicated to generating evidence in criminal cases related to computer crimes or violation of rights using digital technology. Forensic psychology is the application of the science and profession of psychology to questions and issues relating to law and the legal system.

15 Such as with INHOPE, Interpol and the TICBolivia Network.

GLOBAL INFORMATION SOCIETY WATCH 2015

Sexual rights and the internet

The theme for this edition of Global Information Society Watch (GISWatch) is sexual rights and the online world. The eight thematic reports introduce the theme from different perspectives, including the global policy landscape for sexual rights and the internet, the privatisation of spaces for free expression and engagement, the need to create a feminist internet, how to think about children and their vulnerabilities online, and consent and pornography online.

These thematic reports frame the 57 country reports that follow. The topics of the country reports are diverse, ranging from the challenges and possibilities that the internet offers lesbian, gay, bisexual, transgender and queer (LBGTQ) communities, to the active role of religious, cultural and patriarchal establishments in suppressing sexual rights, such as same-sex marriage and the right to legal abortion, to the rights of sex workers, violence against women online, and sex education in schools. Each country report includes a list of action steps for future advocacy.

The timing of this publication is critical: many across the globe are denied their sexual rights, some facing direct persecution for their sexuality (in several countries, homosexuality is a crime). While these reports seem to indicate that the internet does help in the expression and defence of sexual rights, they also show that in some contexts this potential is under threat – whether through the active use of the internet by conservative and reactionary groups, or through threats of harassment and violence.

The reports suggest that a radical revisiting of policy, legislation and practice is needed in many contexts to protect and promote the possibilities of the internet for ensuring that sexual rights are realised all over the world.

GLOBAL INFORMATION SOCIETY WATCH
2015 Report
www.GISWatch.org

APC Hivos

ISBN 978-92-95102-07-1