Centre for International
Governance Innovation

Supporting a Safer Internet Paper No. 2

Non-Consensual Intimate Image Distribution

The Legal Landscape in Kenya, Chile and South Africa

Centre for International
Governance Innovation

Supporting a Safer Internet Paper No. 2

Non-Consensual Intimate Image Distribution

The Legal Landscape in Kenya, Chile and South Africa

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director & General Counsel Aaron Shull
Manager, Government Affairs and Partnerships Liliana Araujo
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Graphic Designer Abhilasha Dewan

For publications enquiries, please contact publications@cigionline.org.

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Project

Supporting a Safer Internet: Global Survey of Gender-Based Violence Online is a two-year research project, in partnership with the International Development Research Centre (IDRC) and Ipsos. This project explores the prevalence of online gender-based violence (OGBV) experienced by women and LGBTQ+ individuals in the Global South. From cyberstalking, impersonation and the non-consensual distribution of intimate images, to deliberate personal attacks on communications channels, OGBV is silencing the voices of women and LGBTQ+ individuals, causing digital exclusion and propagating systemic inequalities. To address these emerging challenges, the survey and papers produced under this research initiative will help to develop policy recommendations and navigate shared governance issues that are integral to designing responses to OGBV — whether that be through the regulation of online social media platforms, educational programming or legal recourse.

Acronyms and Abbreviations

AI	artificial intelligence
BAKE	Bloggers Association of Kenya
CIMA	Computer Misuse and Cybercrimes Act
KICA	Kenya Information and Communications Act
LGBTQ+	lesbian, gay, bisexual, transgender, queer or questioning and other sexualities
MPs	members of Parliament
NCII	non-consensual intimate images
NCIID	non-consensual intimate image distribution
OGBV	online gender-based violence
POPIA	Protection of Personal Information Act
TOS	terms of service

Executive Summary

This paper provides an overview of the state of the law, both existing and proposed, in three countries in the Global South as it relates to the non-consensual distribution of intimate images. It was prepared under the overall coordination of CIGI's Kailee Hilt and Emma Monteiro, who also wrote the introduction and conclusion. The three case studies were written by leading experts from Kenya, Chile and South Africa. The authors discuss current and proposed legislation in response to non-consensual intimate image distribution (NCIID), while also sharing recommendations for further action to address this growing form of gender-based violence within the digital sphere.

Introduction

NCIID, colloquially referred to as "revenge pornography" (Franks 2019)[1] or "image-based sexual abuse" (McGlynn and Rackley 2017) is an unforgiving reality that continues to plague the lives of many within the current digital landscape. It alludes to the non-consensual distribution of photos or videos depicting nudity, partial nudity or sexually explicit acts (Citron and Franks 2014). Evidence on the ground points to a growing problem[2] that has been enabled by a technological and cultural upheaval, which has placed a cellphone with a camera in every pocket and produced an audience for almost every post that makes its way into the digital world. Motives for these actions seem to vary, ranging from surreptitious actors seeking to wreak havoc on individuals' lives; ex-partners pursuing vengeance out of jealous rage; a form of entertainment, bonding, showing off or "fitting in" among peers (Hall and Hearn 2017); a mechanism for profit or entertainment (Henry et al. 2020); or an incidence of cyberbullying intended to embarrass or control, among others. Some victims are left feeling like their lives have been upended and their reputations irreparably damaged, inflicting considerable anxiety and/or a lasting scar (Citron and Franks 2014).

Incidents have driven perceptions of "slut shaming," the insidious message that once an individual has exposed themselves violating defined "sexual standards," they can be shamed repeatedly — especially as an example of deviant or promiscuous character (Chun and Friedland 2015). This logic can be degrading toward women's femininity or sexual attractiveness and can precipitate a loss of sexual autonomy in some cases (Citron 2018). Furthermore, incidents of NCIID have also been shown to impact personal relationships with family, friends and partners. Some individuals have experienced a loss of professional or educational opportunities (Citron and Franks 2014); have had to relocate; have risked further surveillance when personal information is included alongside photos (Uhl et al. 2018); have lost control over their identities, resulting in changing their names or altering their appearance (Kitchen 2015); and have experienced further provocation, such as fear that the image may resurface (Mori et al. 2020). For example, entire websites have been created for posting pictures of ex-intimates (Korenis and Billick 2014). Even when these sites are, in some cases, shut down, it can be challenging, if not impossible, to fully rid the web of copies of the image once it has been published, given the ease with which information can be shared within the digital world (Dunn and Petricone-Westwood 2018).

There is a temptation to fit NCIID within a single framing; however, such actions can have multiple meanings, intentions and contexts surrounding them. Arguably, claims of sexually exposed women as "ruined" are based on historical or cultural depictions asserting that women's sexual virtue must be protected and contained (Chun and Friedland 2015). The assertion that an image shared publicly is "catastrophic" or "inherently devastating" is not always the case for every victim, as some individuals remain unaffected or refuse to be embarrassed by having their nude and/or sexual image shared (Dodge, forthcoming

1 Use of the term "revenge pornography" is problematic as it implies retribution for some form of wrongdoing on the part of the victims, thereby contributing to victim blaming. Furthermore, the term "porn" implies that the subject of the image (photograph or video) consented to their image being shared, which is extremely misleading. Therefore, the term "non-consensual intimate image distribution," or NCIID, is preferred by many scholars and activists working in this space. However, the case studies included in this comparative analysis may refer to the concept by different terms, depending on norms in their respective country.

2 For example, a recent study conducted by the Australian Institute of Criminology on image-based sexual abuse in Australia, the United Kingdom and New Zealand (Henry, Flynn and Powell 2019) found that one in three people have been victims of this form of abuse. This was an increase from 2016 (where the report was one in five), but it is likely that the real number is even higher.

2021). Some scholars suggest that social and legal responses to NCIID should leave room for a future framework that embraces a sex-positive perspective. That is, one that maintains the view that there is no inherent shame to sexual expression, and instead fixates more on eliminating sexual coercion by discussing consent and the right to privacy (Livingstone et al. 2013).

Furthermore, while research within this sphere primarily focuses on women and girls, studies have demonstrated that men, LGBTQ+ (lesbian, gay, bisexual, transgender, queer or questioning and other sexualities), and people with disabilities are also known victims (Henry, Powell and Flynn 2017). Since incidents are so wide-ranging, they are situated at the intersection of some of the most difficult challenges of our time, addressing aspects of sexual trauma, victims' rights, internet privacy and freedom of expression. The barrage of striking stories that emphasizes incidents of extortion for explicit images, race-based sexual harassment, impersonation (also known as "cat-fishing") and retaliation make this statement stronger (Waldman 2017).

Take, for example, a woman from Nigeria who was fired from her job after being outed as a lesbian and having her private images uploaded to Facebook (African Feminism 2020). Or an openly gay man from the United States, whose ex-boyfriend stole and posted his intimate images, impersonated him on an app and allegedly sent hundreds of men to his home and workplace looking for sex (Goldberg 2019). The 2015 Miss Zimbabwe winner was stripped of her title when nude photos of her surfaced, demoralizing her character (Mutsaka 2015). A student from Mexico became a tabloid story in her hometown and soon made national headlines after private videos were circulated widely on WhatsApp (McLaughlin 2020). Explicit images stolen from the laptop of a Ugandan model and socialite were leaked after she did not pay US$3,000 in blackmail money (McCool 2018). A politician from Morocco became a victim of controversy when her private photos, which were arguably "fabricated," were exposed to defame and ruin her political career (Koundouno 2019). A social media influencer from Singapore received death threats after someone hacked into her ex-boyfriend's cloud storage space and revealed their sex videos online (Ng and Yuxin 2020). The list goes on and on.

In Canada, the cases of Rehtaeh Parsons and Amanda Todd — teens who experienced cyberbullying after photos exploiting them circulated online, and who died by suicide within six months of each other — were perhaps the first to bring national attention to this issue. Parsons was 15 years old when she was sexually assaulted while intoxicated at a party. The incident was photographed and shared with classmates, which was followed by slurs of "slut" and propositions for sex (Schein 2019). A 35-year-old man residing in the Netherlands convinced Todd to reveal her breasts to him on a webcam. He then created a Facebook page with the picture (Dean 2012).[3] Media coverage of both cases prompted an outpouring of public concern regarding cyberbullying, sparking legislative reform.

It should be highlighted, however, that a proper investigation was not launched until after the young women's deaths. Both had reported the harassment they experienced, but at the time, were told that there was not much that the police or social media companies could do to help them (Garossino 2014; White 2015). It is instances like these that demonstrate why many victims may be hesitant to report their experiences given the apprehension that they will not be taken seriously, igniting little to no investigation.

Even though most social media companies do have terms of service (TOS) that include reporting and safety strategies, these procedures are often non-transparent and are written in such a way that most individuals rarely read or understand them.[4] Researchers have reported difficulty finding accurate data on how TOS are applied and what forms of abuse have been investigated, making it especially onerous for victims to know what types of complaints will be addressed.[5]

Additionally, "companies typically draft standard form TOS to define only vaguely the rules relating to content and to maximize the company's exclusive discretion to interpret and apply the rules contained in them. As a result, users most often have no way of holding social media companies legally accountable for failing to enforce them"

3 The accused in the Todd cyberbullying case was extradited to British Columbia, Canada, in December 2020 to face charges of extortion, criminal harassment, child luring and child pornography. Additionally, he was sentenced to 11 years in prison in the Netherlands in 2017 for fraud and blackmail for his role in cyberbullying dozens of other young girls and gay men (see Brend 2021).

4 See Dunn, Lalonde and Bailey (2017, 87).

5 See Young and Laidlaw (2020, 151–52).

(Dunn, Lalonde and Bailey 2017, 87). At a minimum, platforms should be required to implement clear parameters for swift removal of offensive content while providing meaningful assistance to those who have been victimized (ibid., 88).

In any case, it should also be recognized that law enforcement's deference to the TOS of social media companies is problematic and should not supersede applicable criminal or civil law procedures (ibid., 90). Such a response suggests that law enforcement officers may require further training and additional resources to be more proactive in applying appropriate measures.

To this end, the stark reality is that solutions to this growing phenomenon are challenging. Just as the motives are wide-ranging, there is no one-size-fits-all approach to combatting NCIID; however, its rise is triggering feminist resistance worldwide. For example, South Korean women have taken to the streets to demand a crackdown on "spy-cam pornography" (the online sharing of intimate photos and videos taken by secret cameras), which has become an epidemic in the country (BBC News 2018). Women's rights defenders in Zimbabwe have protested vigorously for relevant cyber laws to protect victims of "non-consensual pornography" (Chakamba 2017) and digital rights foundations in India are among the many activists who continue to challenge online gender-based violence (OGBV) in all its forms (Digital Rights Foundation 2017).

With cases of NCIID now reported in the media at a soaring pace, policy makers around the world are beginning to contemplate responses. In jurisdictions such as Australia, Canada, Israel, Japan, the Philippines, the United Kingdom and the United States, among others, the growing attention has resulted in specific criminal and civil law responses (Dodge 2019).

In countries where NCIID-specific legislation does not exist or is not yet in force, victims are utilizing existing laws related to privacy and data protection to obtain justice. However, one of the drawbacks to relying on these types of provisions is that they may not capture situations whereby the image was initially obtained with the consent of the subject, or by the subject themselves; rather, it was the sharing of the image that was not authorized. This gap in the law further serves to reinforce the notion of victim blaming, by insinuating that those who voluntarily provide intimate images to others are less deserving of justice when these images are further distributed without consent (Dunn and Petricone-Westwood 2018).

Other types of laws that have been applied to prosecute actions of NCIID include, but are certainly not limited to, voyeurism, extortion, criminal harassment, and laws related to the sexual abuse of minors or possession of child pornography — depending on the age of the victim. In some cases, copyright law has also served as an effective legal tool by raising important questions regarding authorship and notice-and-takedown procedures (ibid.).

The choice between developing new laws and frameworks for digital offences or working with existing laws is a dilemma faced in many countries, in particular within the Global South. To understand how diverse legal systems address NCIID, this analysis focuses on the state of the law in three countries in the Global South to provide an overview of the regulatory models that exist and to stimulate further action where improved solutions are needed. It relies on leading experts residing in Kenya, Chile and South Africa, who discuss current and proposed legislation, while sharing recommendations and possible road maps for further action within the existing landscape.

Case Studies

Kenya

Grace Mutung'u, Centre for Intellectual Property and Information Technology Law, Strathmore University

A judgment delivered in December 2017 criticized Kenyan police officers for their role in taking and circulating nude images of a female high-school student (referred to as "MWK") during the investigation of a crime.[6] The petitioner was among 37 high-school students travelling to Nairobi from Karatina using a public service vehicle. It was reported that the students were intoxicated, smoking bhang (cannabis) and engaging in sex in the vehicle, which was playing loud music. The vehicle was stopped at a police

6 *M W K v another v Attorney General & 3 others*, [2017] eKLR [*M W K*].

patrol base, where the police stripped MWK's blouse, lifted her skirt, and pulled her bra and underwear in search of the bhang. All of this was recorded by police officers on their phones and the search took place in the presence of male police officers. MWK was then taken to a police station where she was again recorded showing her intimate parts where the bhang had been found. The videos and pictures were widely circulated on social media as commentary on the decaying morals of young people. The court found that regardless of the alleged crime, the searching and photographing of MWK in the presence of male police officers, students and members of the public was a gross violation of her constitutional rights to dignity and privacy, and her right not to be subjected to degrading treatment. She was awarded KSh 4 million (approximately US$40,000) in damages.

The case illustrates many of the issues surrounding non-consensual distribution of intimate images in Kenya. There is a growing practice of sharing intimate images (Kadandara 2018). For example, there are private messaging app channels dedicated to the sharing of intimate images, and sometimes images are shared on the channels without the knowledge or consent of the subjects. The sharing of nude images is typically cast as a generational problem affecting youth and often linked to the "decaying moral fabric" (Chisala-Tempelhoff and Kirya 2016; Wandia 2018). Kenyan law employs language such as "immoral" and "obscene" to describe and outlaw sexual images. Policy makers shun the idea that sharing of intimate images can be part of healthy sexual development, and the issue of sexual education is controversial (Oginde 2018). Observation of the cases of non-consensual sharing of intimate images indicates that the issue is a gendered problem, disproportionately affecting women (Wanjiku 2018) and sexual minorities.[7]

As the MWK case was being heard in court, Kenya's national Parliament was debating the Computer Misuse and Cybercrimes Bill. The bill was a culmination of concerted advocacy by the information and communications technology industry and community for a comprehensive law to address threats to the growing cyberspace (ARTICLE 19 2014). Typical of many laws in the country, the bill borrowed from international initiatives such as the Convention on Cybercrime (the Budapest Convention) and the Commonwealth Model Law on Computer and Computer Related Crime. Advocacy groups faulted the law for failing to follow the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) (Kenyanito and Chima 2016). Notably, the conventions do not specifically provide for the offence of non-consensual distribution of intimate images. They generally provide for four groups of offences, following the International Telecommunication Union (2014) typology: offences against the confidentiality, integrity and availability of computer data and systems; copyright-related offences; content-related offences and computer-related offences. Non-consensual distribution of intimate images would fall under content-related crimes.

The Computer Misuse and Cybercrimes Act (CIMA) was enacted in May 2018. It does not specifically provide for non-consensual distribution of intimate images. It does, however, create the offences of cyber harassment (section 27), wrongful distribution of obscene or intimate images (section 37), false publication (section 22) and publication of false information (section 23).[8] Notably, these provisions, in particular section 37, criminalize sharing of all intimate images, a framing that could have the unintended effect of deterring victims from reporting cases of non-consensual distribution of intimate images.

Reading through the Hansard report on the debate on the bill, it appears that legislators who had experienced content-related threats were keen to criminalize pornography as a whole and not so much the non-consensual distribution of intimate images.[9] Events that occurred around the time of reading the bill influenced the debate. First, the bill was among the first pieces of legislation in the eleventh Parliament, instituted following contested 2017 general elections. A significant part of campaigning had taken place online, and the election had witnessed a surge in misinformation, with companies such as Cambridge Analytica retained by some political parties (Mutung'u 2018).

7 See, for example, the #WATETEZI stories recorded by LGBTQ+ activist Dennis Nzioka since 2014. They include blackmail threats to share intimate images of LGBTQ+ people.

8 *Computer Misuse and Cybercrimes Act, 2018*, No 5 of 2018 [CIMA], online: <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf>.

9 See www.parliament.go.ke/sites/default/files/2017-05/Hansard_Report_-_Wednesday_21st_March_2018P.pdf.

Photo: Juan Alberto Casado/Shutterstock

Legislators were therefore keen to regulate the spread of fake news. Second, religion had been a key factor in the campaigns, with legislators visiting places of worship and promising to support religious agendas (Baraka 2019). Third, and related to religious moral standards, there had been several incidences where intimate images of some female members of Parliament (MPs) had been leaked online (Nge'noh 2021). Other MPs, including the majority leader at the time, also alleged that they had persistently received unsolicited nude photos (Owino 2018).

In the case of the female legislators, the alleged perpetrator was charged with conspiracy to defraud under the Penal Code (Walter 2018). The aggrieved MPs asserted that the prosecution against the perpetrator had not been successful owing to the lack of well-defined offences with regard to this type of harassment. The debate on the bill therefore focused on the need to control a cyberspace where all sorts of computer crimes, including pornography, were taking place. The issue of non-consensual distribution of intimate images did not feature. Instead, legislators condemned pornography, especially among youth, terming it a "moral decadence." For example, the majority leader and others referred to the case of Saudi Arabia, where pornography in all its forms is strictly prohibited. In their remarks, several other members decried the increasing consumption of pornography by younger people.

The bill did not envisage situations where consenting adults could have intimate images and, conversely, it did not provide for specific situations where intimate images are distributed without the consent of the subjects. Although the issue personally affected MPs who had been involved in cases of leaked nude photos, it was viewed as cyberbullying, perhaps to avoid the suggestion that they could have been involved in situations involving intimate images. When the bill was enacted in May 2018, it was challenged in court by the Bloggers Association of Kenya (BAKE). Among the issues raised in the BAKE petition was the broadness of content offences, including the above-mentioned sections 27, 37, 22 and 23. In 2020, the High Court dismissed the petition in its entirety.[10]

Section 27 of CIMA criminalizes cyber harassment. It provides:

1. A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone

10 *Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties)*, [2020] eKLR.

known to that person, commits an offence, if they know or ought to know that their conduct —

a. is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or

b. detrimentally affects that person; or

c. is in whole or part, of an indecent or grossly offensive nature and affects the person.[11]

This section of the act targets threatening behaviour and states that a person committing such an offence may receive a fine of up to KSh 20 million (approximately US$186,000) or imprisonment for a term not exceeding 10 years, or both. The provision also envisages restraining orders that may be used to prevent further communication of the subject of the offence. This would provide relief for persons fearing that perpetrators have copies or other records of their intimate images. However, as shall be discussed below, Kenya has had previous experience with ambiguous laws. As was argued in the BAKE case, the terms "indecent" and "grossly offensive" are also likely to be applied to cases involving political expression, in which case the goal of deterring content crimes such as non-consensual distribution of intimate images would be diminished.

Section 37, on the other hand, provides that:

> A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person commits an offence and is liable, on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years, or to both. (ibid.)

This provision is a double-edged sword in cases involving non-consensual distribution of images. On the one hand, it criminalizes the making of intimate images, giving protection to people whose intimate images are taken without their consent. This is useful in cases involving young people who may take intimate images without full knowledge of the repercussions (Wandia 2018), as it may deter others who may have the images from distributing them. It can also be used to stop blackmailing as victims can report the blackmailers to the police for action. However, the same provision could equally remove protection as it criminalizes the very act of sharing intimate images, whether consensual or non-consensual. A likely effect of the provision is that it could discourage victims of non-consensual distribution of intimate images from reporting due to fears that they themselves will be criminalized.

Section 22 addresses "false publications" that, among other things, "negatively affects the rights or reputations of others." Similar to this is section 23, which criminalizes the "publication of false information" that may, among other things, "discredit the reputation of a person" (ibid.). These two sections have been criticized for decriminalizing defamation. Nevertheless, they provide a basis for prosecution where the non-consensual distribution of intimate images damage one's reputation. The offences attract fines of up to KSh 5 million (approximately US$47,000) or imprisonment for a term of up to two and 10 years, respectively.

Besides the CIMA provisions, legacy laws that can apply to non-consensual distribution of intimate images include section 66 of the Penal Code, which creates the misdemeanour of publication of alarming information, as well as section 84D of the Kenya Information and Communications Act (KICA), which outlaws the publication of obscene information. Prior to 2016, KICA also included the misdemeanour termed "improper use of system" that was nullified by the High Court.[12] The offence under section 29 outlawed the use of a licensed telecommunication system to send a message known to be "grossly offensive, indecent, obscene, menacing" or "false, for the purpose of causing annoyance, inconvenience and needless anxiety" to another person.[13] This provision had been used in prosecution of threatening phone messages. However, it was increasingly

11 *CIMA, supra* note 8.

12 *Kenya Information and Communications Act*, 2011, online: <https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf>.

13 *Ibid*.

used against bloggers and dissenters, due to its ambiguous wording, which created room for discretionary prosecutions (Freedom House 2016).

The ambiguity of the law was among the grounds raised in the petition against CIMA. Provisions for content offences under CIMA arguably leave room for prosecutors to debate on offences, and this was likely to lead to the object of the cybercrimes law not being achieved (Sugow and Satar 2020).

Civil law also provides avenues for prosecution of non-consensual distribution of intimate images. As seen from the case of MWK, a constitutional petition succeeded on the grounds of violation of privacy, dignity and the rights of the child.[14] Other cases include *Roshanara Ebrahim v. Ashleys Kenya Limited & 3 others*, where Roshanara Ebrahim was dethroned as Miss Kenya following the leak of nude photos by her former boyfriend. Although the court declined to restore her position and employment as Miss Kenya, her former boyfriend was ordered to pay her KSh 1 million (approximately US$9,000) as damages for breach of her privacy.[15] In a civil suit that was filed in 2008, prior to the promulgation of the current Constitution, the plaintiff successfully sued a newspaper for defamatory publication that included his images with younger women at a party.[16]

The success of petitions and civil suits in cases involving non-consensual distribution of intimate images shows that courts view the act as a violation of constitutional rights, such as dignity, privacy and, in the case of minors, their rights as children. However, the cases were instituted by people who are economically able or, in the case of MWK, with the help of a children's rights organization. Many people facing the threat of intimate images being distributed are confronted with the choice of either paying the person who is blackmailing them or waiting to be exposed to their family and community. The women's rights community has advocated for laws that would deter OGBV such as non-consensual distribution of intimate images (Grace, Victor and Alice 2013). The realities of a new generation of young adults who have more access to smart mobile devices and routinely share intimate images call for a law that specifically prohibits NCIID.

Chile

J. Carlos Lara and Michelle Bordachar, Derechos Digitales

Given that the digital world is but an extension of our physical reality, what is punishable in the physical world should also be punishable in the virtual world. However, when it comes to prosecuting crimes committed through digital means, one of the biggest obstacles to their punishment is the lack of adaptation of traditional crimes to new circumstances. There is no existing statute that punishes NCIID in Chile. At best, one could try recourse to other rules created not for gender-based violence but for other purposes. However, given the lack of specific laws that address the problem, several bills have been introduced in recent years, modifying existing laws or adding new penalized conduct. Although Chile urgently needs a law that provides women with the protection that they are lacking — in both the physical and the virtual world — so far, none of the bills have become law.

There are certain criminalized acts within existing statutes that can be used as a basis for prosecution of NCIID, albeit in an ill-fitting and incomplete manner. In 1995, law number 19423 introduced two new articles to the Penal Code: Article 161-A punishes various violations of privacy, which in general refers to the criminalization of the non-consensual capturing and distribution of conversations or communications, documents or instruments, images or events of a private nature that are produced, carried out, occur or exist in private enclosures, or places that are not freely accessible to the public. It also punishes the dissemination of those materials, to the extent that they are illicitly obtained as described.[17] Article 161-B, linked to the previous rule, contains a special offence of blackmail, punished as the demand to provide money, or carry out an act to prevent dissemination of material obtained as part of the definition of article 161-A. The penalties associated are imprisonment and a fine.

However, the legislative debate did not contemplate the possibility of criminalizing the

14 *M W K, supra* note 6.

15 *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others*, [2016] eKLR.

16 *James Gitau Singh v Headlink Publishers Limited & 3 others*, [2015] eKLR.

17 *Penal Code*, 1874, modified 3 February 2021, online: <www.bcn.cl/leychile/navegar?idNorma=1984>.

Photo: Vivian Morales C./Wikimedia

dissemination of images without the consent of the affected person by itself, when these images have been captured with the authorization of the victim, or by the victim themself. Consensually obtained private materials are not part of the definition, and their dissemination is therefore excluded from the provision. This is especially problematic, considering that the provision is likely to be more beneficial to victims of NCIID who provided their images or initially consented to the images being taken, as they would have knowledge of the material's existence, rather than victims whose images were illicitly obtained.

Therefore, article 161-A considers different criminal offences that protect against intrusion into private life, indiscretion or disloyalty in communications and private actions, as well as the dissemination of information obtained by means of an intrusion or indiscretion. Yet the law falls short: if the images or audiovisual materials eventually distributed had been sent voluntarily by their owner, or obtained privately but with consent, or if the images are captured or obtained in places of public access (for example, cases of photographs or videos taken under women's skirts to record their underwear, also known as "up skirting"), those acts will not be covered by the legal hypotheses as criminal offences. Because of this limitation, this has been one of the legal provisions whose reform is currently under debate in Congress.

Legislation relating to cybercrime is enshrined in law 19223 of 1993, which "typifies criminal offences relating to information technology" by establishing four criminal offences related to information systems and the data therein.[18]

Article 2 punishes unauthorized access to an information processing system with the purpose of taking over, using or knowing its information improperly, a somewhat vague definition that could apply to the hacking of intimate images but not to their dissemination. However, article 4 penalizes malicious disclosure or dissemination of the data contained in an information system. This is a broad definition that exceeds cybercrime and covers most ways in which dissemination can be conducted. Therefore, by means of an extensive application of article 4, some acts involved in NCIID could be prosecuted under this law, although it is unclear the same breadth could prevent its enforcement in court in the case of legally and consensually obtained images.

There are also other statutes that may be part of the prosecution or the prevention of NCIID or some of its effects, while not addressing the full range of issues involved in NCIID. These rules include:

18 *Law 19223 – Tipifica Figuras Penales Relativas a la Informática,* 1993, online: <www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223>.

- The aforementioned article 161-B of the Penal Code, which contemplates the crime of extortion or blackmail, would potentially be applicable to extortive conduct involving the threat of disseminating images captured with the consent of the affected person. There is at least one judicial decision that evaluates the applicability of the type of extortion or blackmail described. Although limited to the circumstance of "sextortion," it would cover some ground related to NCIID.

- Articles 296 and 297 of the Penal Code penalize serious and credible threats to cause harm such as coercion to engage in acts that can include those that are part of NCIID.[19]

- Article 366 Quáter of the Penal Code criminalizes improper or indirect sexual abuse or exposure of minors to sexually significant acts, as well as requests to "deliver or display images or recordings of him or herself or another person under 14 years of age, with sexual significance" (author's translation).[20] The article seeks to penalize child grooming and sexting with minors, including through the use of electronic means, and it aims to cover situations where intimate images are obtained under the apparent consent of the victim.

- Article 20 of the Constitution allows for remedy from the courts, without the need for legal assistance, in case of disturbance on the exercise of fundamental rights. Actions of NCIID may affect psychic integrity, privacy and the sanctity of communications (article 19, numbers 1, 4 and 5, respectively). As the most rapid action in the legal system, it is the first tool for a victim of NCIID to remove images and prevent further dissemination. However, it is still insufficient to address the problem, and its efficacy to stop the spread is questionable. It also does not create penalties for engaging in NCIID.

- Law 20066 on domestic violence does not expressly define NCIID. Article 14 of the law contains the crime of habitual abuse, understood as the habitual exercise of physical or psychological violence against the spouse, cohabitant or relative of the victim. The dissemination of intimate images could be qualified as an act affecting psychic integrity under this broad definition, although it would create the need to connect NCIID with this form of violence and is still limited to people who are or have been in a relationship.

- Law 17336 on intellectual property allows for the removal of content from internet platforms, as well as fines and eventual financial compensation, but only if the victim is the copyright holder over the material, and only after undergoing legal action in civil courts.[21]

Furthermore, between July 2018 and January 2019, two draft bills were introduced in Congress, bills number 11923 and number 12164-07. Both sought to amend the Penal Code to punish NCIID.

The first of these bills (bill number 11923-25) proposed adding a new paragraph to article 161-A of the Penal Code, in order to establish a penalty of imprisonment for anyone who disseminates or publishes, through the internet or any other electronic means, images of sexual content or connotation that have been obtained during the private life of a couple and without the consent of one of the individuals. It also punished the administrators of the site where these images are hosted if they do not remove them. The definition only referred to images obtained during the private life of a couple, therefore requiring a relationship, and only sanctioned their dissemination or publication to the extent that they were made through electronic media.

Bill number 12164-07 was composed of two articles, the first of which proposed a new article 161-C to criminalize the distribution of a person's image focusing on their sexuality, in circumstances when the person did not consent to and could be humiliated or degraded by the publication. The bill also sought to modify article 296 of the Penal Code, to establish that threats of the crime established in the proposed article 161-C (as a form of sextortion) would be an aggravating circumstance. Other aggravating circumstances included that the conduct is carried out in the context of a relationship (between spouses, cohabitants or as intimate partners without cohabitation), and that the distribution is done with the intention of

19 *Law 20066 – Establece Ley de Violencia Intrafamiliar*, 2005, online: <www.bcn.cl/leychile/navegar?idNorma=242648>.

20 *Penal Code*, *supra* note 17.

21 *Law 17336 – Propiedad Intelectual*, 1970, online: <www.bcn.cl/leychile/navegar?idNorma=28933>.

making a profit. Finally, the proposal established a special protection that considers various circumstances when the offence involves minors.

A proposal was made in Congress to merge these bills. The merged proposal attempts to modify the Penal Code, creating a new article 161-A bis, and a new article 161-C. The proposed article 161-A bis punishes (with imprisonment and a fine) the person: "who, having captured, recorded or obtained images, audio recordings or audiovisual recordings, real or simulated, with sexual content or connotation, which have been produced in private premises or in places where there is a reasonable expectation of privacy and with the consent of those who are found in such records, disseminates them by any means without having previously requested and obtained their consent" (author's translation).[22] An intimate relationship with the victim is an aggravating circumstance. Exemptions are provided when the conduct is already covered by crimes involving minors, and when it is carried out by legally or judicially authorized persons. The merged proposal no longer limited the definition to private enclosures but included the problematic idea of a reasonable expectation of privacy. The newly proposed article 161-C, in turn, punishes the administrator of an internet site who, having been notified of a court order to cease the publication of images, audio recordings or audiovisual records, does not comply within the term conferred by the respective resolution.

The merged bill was voted on favourably and sent to the Senate for review on January 10, 2019. No further movement or progress has occurred since then.

After the merged bill stopped moving in Congress, and after arduous drafting work, which involved the creation of a working group with activists and representatives from several civil society organizations at the behest of a freshman member of Congress, on December 1, 2020, a new draft bill was introduced to Congress: bill number 13928-07, which outlaws, criminalizes and punishes digital violence in its various forms and provides protection to the victims. Among the conduct that the bill seeks to criminalize is the non-consensual distribution of intimate content, but unlike the previous bill, this is part of a much broader effort, focused on digital violence in general.

This bill explicitly declares a gender-sensitive approach to both its rules and their interpretation, with special attention to the context in which digital violence presents itself. The bill aims to create a new law on the matter, penalizing NCIID, as well as doxing, impersonation through digital means, delivery or exhibition of unsolicited violent or sexual content (cyber flashing), and harassment or cyberstalking, all with fines as penalties instead of imprisonment. In the case of NCIID, the criminal conduct is defined as disseminating, by any means, an image or video containing total or partial nudity, either sexually explicit or with sexual connotation. The bill includes a list of aggravating circumstances.

This bill entered Congress in December 2020 and has not yet been put to a vote.

The bill on computer crimes (number 12192-25) also seeks to adapt national law to the provisions of the Council of Europe's Convention on Cybercrime (the Budapest Convention). The law would replace law number 19223, creating new criminal offences for cybercrimes and adapting some offences defined in the Budapest Convention. These include, more importantly, the felonies of unauthorized access, as well as dissemination of information obtained through unauthorized access, which would apply, with limitations, to the distribution of images obtained through hacking. It also penalizes receiving personal data. The bill has been in Congress since 2018 and has gone through several changes with active participation from different stakeholders; however, it has not been considered through a gendered perspective.

It is reasonable to conclude that Chilean legislation is not only missing specific legislation to address instances of NCIID but is also unable to apply current definitions of crimes to many acts involved in NCIID. Similarly, it appears that current criminal law does not consider a gendered perspective when enacting crimes that disproportionately affect women's rights in cyberspace. Consequently, in the last period, efforts to update the current regulations have been accelerated by means of different bills. Taking into consideration what has been exposed in this work, it is essential to provide this type of conduct with a legal treatment from a gendered perspective that allows it to be understood as a form of gender violence.

22 See www.camara.cl/verDoc.aspx?prmID=24191&prmTIPO=OFICIOPLEY.

South Africa

Nonhlanhla Chanza, Law Society of South Africa

The Constitution of the Republic of South Africa provides legal protections for NCIID-related rights,[23] namely the right to human dignity,[24] privacy,[25] freedom and security of the person,[26] equality and non-discrimination,[27] and bodily and psychological integrity.[28] In 2019, South Africa joined a growing list of countries that have enacted offences that criminalize NCIID when President Cyril Ramaphosa signed into law the Films and Publications Amendment Act 11 of 2019.[29] However, the act has not yet come into effect pending the finalization of the regulations (Pickworth 2020). NCIID will be further regulated and criminalized through the Cybercrimes Bill (B 6D—2017),[30] which is currently awaiting the president's signature. Until these two pieces of legislation come into effect, and in the absence of a law that explicitly outlaws NCIID, victims of this crime have to make use of other legal avenues that are available under South African law.

Section 18F of the Films and Publications Amendment Act 11 of 2019[31] explicitly outlaws the non-consensual distribution of another person's private sexual photograph or film with the intention of causing that individual harm.[32] A photograph or film is defined as "'private' if, judging from the context in which the photograph or film is taken or made, it was not intended by any individual in the photograph or film to be seen by others."[33] It is "'sexual' if...(a) it shows all or part of an individual's exposed female breasts, anus, genitals or pubic area; (b) it shows something that a reasonable person would consider to be sexual because of its nature; or (c) its content, taken as a whole, is such that a reasonable person would consider it to be sexual."[34]

The act provides for defences[35] and compels internet service providers to provide the Film and Publications Board or the South African Police with the details about the identity of the perpetrator. The available penalties for the offence vary depending on whether the person(s) depicted in the image or film can be identified or not. The penalties are captured under section 24E(1)[36] and section 24E(2) of the act.[37] In instances where the depicted person(s) in the image or film is identifiable, the penalty increases to a fine not exceeding R 300,000 (approximately US$21,000) or to imprisonment for a period not exceeding four years or a combination of both a fine and imprisonment.

While the introduction of the new criminal offence is a positive development, it has inherent weaknesses, including the intent to harm requirements, narrow scope of the images covered by the offence and problematic definitions of "private" and "sexual," that critics argue will render it ineffective and limit the protections and legal remedies available to victims (Brook and Sloane 2020). There is also a strong view that such an offence should have been covered by the Sexual Offences and Related Matters Act.[38] Critics argue that NCIID is a sexual crime and its inclusion in the Sexual Offences

23 *Constitution of the Republic of South Africa, 1996*, No 108 of 1996, online: <www.gov.za/sites/default/files/images/a108-96.pdf>.

24 *Ibid*, s 10.

25 *Ibid*, s 14.

26 *Ibid*, s 12.

27 *Ibid*, s 9.

28 *Ibid*, s 12(2).

29 *Films and Publications Amendment Act, 2019*, No 11 of 2019, online: <www.saflii.org.za/za/legis/num_act/fapaa201911o2019g42743352.pdf>.

30 B 6D–2017, *Cybercrimes Bill* (S Afr), 2017, online: <https://pmg.org.za/bill/684/>.

31 *Films and Publications Amendment Act, 2019, supra* note 29.

32 *Ibid*.

33 *Ibid*, s 18F.

34 *Ibid*.

35 It is a defence under this law if the person charged with the offence can prove that they reasonably believed that the disclosure was necessary for the purposes of preventing, detecting or investigating crime. A person's prior consent to the creation of the material is not an available defence.

36 Section 24E(1) of the act states that "any person who knowingly distributes private sexual photographs and films, in any medium including the internet and social media, without prior consent of the individual or individuals in the said sexual photographs and films with the intention to cause the said individual harm shall be guilty of an offence and liable upon conviction, to a fine not exceeding R 150 000 or to imprisonment for a period not exceeding two years or to both a fine and such imprisonment."

37 Section 24 E(2) of the act states that "any person who knowingly distributes private sexual photographs and films in any medium including through the internet, without prior consent of the individual or individuals and where the individual or individuals in the photographs or films is identified or identifiable in the said photographs and films, shall be guilty of an offence and liable upon conviction, to a fine not exceeding R 300 000 or to imprisonment for a period not exceeding four years or to both a fine and such imprisonment."

38 *Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007*, No 32 of 2007, online: <www.gov.za/sites/default/files/gcis_document/201409/a32-070.pdf>.

Photo: Alexandros Michailidis/Shutterstock

Act would have provided victims with better protections, including automatic anonymity during criminal proceedings (Parliamentary Monitoring Group 2017a). That the act has not yet come into force is problematic as well.

NCIID will also be regulated by the Cybercrimes Bill (B 6D—2017),[39] which deals with crimes that have a bearing on cybercrime (Parliamentary Monitoring Group 2017b). Section 16 criminalizes the disclosure of "a data message of an intimate image." Section 16(1) provides that "any person ('A') who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person ('B'), without the consent of B, is guilty of an offence." Section 16(2) provides a comprehensive definition of "person B" and "intimate image."[40] Any person found guilty of this offence is liable on conviction to a fine or up to three years' imprisonment or a combination of both a fine and imprisonment.[41]

While it is widely believed that section 16(1) is aimed at addressing the problem of "revenge pornography," drafters of the bill maintain that

40 Section 16(2) states that:

> for purposes of subsection (1)– (a) 'B' means– (i) the person who can be identified as being displayed in the data message; (ii) any person who is described as being displayed in the data message, irrespective of the fact that the person cannot be identified as being displayed in the data message; or (iii) any person who can be identified from other information as being displayed in the data message; and (b) 'intimate image' means a depiction of a person– (i) real or simulated, and made by any means in which – (aa) B is nude, or the genital organs or anal region of B is displayed, or if B is a female person, transgender person or intersex person, their breasts, are displayed; or (bb) the covered genital or anal region of B, or if B is a female person, transgender person or intersex person, their covered breasts, are displayed; and (ii) in respect of which B so displayed retains a reasonable expectation of privacy at the time that the data message was made in a manner that– (aa) violates or offends the sexual integrity or dignity of B; or (bb) amounts to sexual exploitation.

39 *Cybercrimes Bill, supra* note 30.

41 *Cybercrimes Bill, supra* note 30.

this conduct will be comprehensively addressed by amendments that the Cybercrimes Bill makes to the Sexual Offences and Related Matters Act (Parliamentary Monitoring Group 2017c). Section 11A to be added to the Sexual Offences and Related Matters Act creates an offence of harmful disclosure of pornography.[42] It criminalizes the intentional and harmful distribution of adult pornography without the consent of persons depicted in the images. It allows victims to seek a court order pending the finalization of criminal proceedings that prohibits any further distribution of the images and orders electronic communication service providers to block access to and delete the images. Courts can also order the destruction of images by the perpetrator after the finalization of the trial. Threats to disclose the images and sextortion are also criminalized. The Cybercrimes Bill has been with the president since December 2020 and awaits his signature. It also has weaknesses, including the intent to harm requirements. The framing of the offence as pornographic material is also problematic.

There are several existing legal remedies under South African law that are available to NCIID victims until the Films and Publications Amendment Act comes into effect or the Cybercrimes Bill is signed into law. However, these legal options have their own drawbacks, such as legal costs; some have also proven to be more effective than others. Under criminal law, an offender can be charged with *crimen injuria*, criminal defamation or even extortion (South African Law Reform Commission 2019). NCIID victims continue to open *crimen injuria* cases but, to date, there have been no reports of any perpetrator who has been criminally prosecuted and convicted (Craig 2019). Greta Potgieter's criminal case, which was opened after her ordeal in 2008, never fully took off and appears to remain unresolved to this day. Her lawyer once reported that prosecutors had struggled during the criminal investigation to pin a crime to the perpetrator, even after Potgieter had won a lawsuit (*Mail & Guardian* 2017).

NCIID victims can also pursue several legal avenues under civil law. They can apply for an interdictory (injunctive relief) court order prohibiting, among other things, the distribution of their images on online platforms (BusinessTech 2018). South African courts have, in recent years, granted progressive and victim-centred orders that strongly upheld victims' constitutional rights to privacy, dignity and integrity. While the cases have been few and far between, there have been successes. For example, in 2018, a Western Cape high court granted an urgent application in a divorce matter where the husband had threatened to disclose his estranged wife's explicit material if she did not accede to his demands. He was ordered to refrain from distributing the material, to destroy the material in his possession, to pay the victim's legal costs and to provide the court with the contact details and addresses of the people with whom he had shared the material. He also had to file — within 72 hours of the court order — an affidavit confirming his compliance with the order (Mngadi 2018).

Victims have also pursued civil litigation cases at the high courts. In 2018, a victim successfully sued for defamation and breach of her rights to dignity and privacy. She also argued that there had been a breach of contract or, alternatively, breach of fiduciary duty and was awarded a landmark damage amount for the various harms she suffered. She was awarded general damages, costs for past medical expenses and the court added a 10 percent interest rate until final payment. In a move to protect the victim, she was granted full anonymity in media reports and the defendant was also ordered to take reasonable steps to ensure removal of all material from online platforms.[43] Although Potgieter was reportedly left with a R 250,000 (approximately US$18,000) legal bill following a successful civil suit, some courts have ordered defendants to pay the victim's legal costs in successful civil suits (*Mail & Guardian* 2017).[44]

NCIID victims can avoid prohibitive legal costs by using a cheap civil remedy available under the Protection from Harassment Act 17 of 2011.[45] Section 2 of the act allows victims of online harassment to apply for a protection order at the Magistrate Court. It is a criminal offence to contravene the terms of the criminal order. However, there are no reported cases yet on the use of this legal recourse for NCIID. But it is promising that in February 2021, a

42 See schedule to the *Cybercrimes Bill*, *supra* note 30.

43 In order to comply with the court order for ensuring anonymity for the victim, this case is referred to as Adv Foden order, case No 25457/17 at the High Court of South Africa, Gauteng Division, Pretoria.

44 *Ibid*.

45 *Protection from Harassment Act, 2010,* No 17 of 2011, online: <www.gov.za/sites/default/files/gcis_document/201409/a172011.pdf>.

cyberbully who harassed his neighbour was criminally convicted of attempted extortion in a landmark judgement (Naidoo 2021).

NCIID victims in an existing domestic relationship can access remedies available under the Domestic Violence Act.[46] The case of *KS v. AM*[47] demonstrates that the courts are willing to provide victims of this crime with the fullest protections available under the act. Under this act, victims can apply for relief under section 7(1) and 7(2). In 2015, a Magistrate Court granted a prohibitive order under section 7(1) of the act after finding that the posting of the victim's sexual material on her Facebook account amounted to an act of domestic violence. It granted a prohibitive order that effectively interdicted the distribution of the victim's intimate images and videos on online spaces or to any third party.[48]

However, the Magistrate Court's decision to deny the victim relief sought under section 7(2)[49] of the act was taken on review and successfully set aside by the High Court. The victim had asked the Magistrate Court to use its discretionary powers under section 7(2) and order the possession of the perpetrator's digital devices so they could be checked by a digital expert who would permanently delete material depicting the victim. The High Court hearing the appeal matter ordered the respondent "to handover and place in the temporary custody of the Sheriff of this Court all digital devices under his control in order for a forensic expert appointed by the applicant's attorneys to identify and permanently remove from any such devices any photograph, video, audio and or records relating to the Applicant."[50] The court further agreed with the victim's lawyers that the continued possession of the victim's material by the respondent was an infringement of her constitutional rights to dignity, privacy and integrity. It maintained that victims of domestic violence must be granted full protections under the act.

There are other remedies that are reported to be available and possible under South Africa's Copyright Act[51] and the Protection of Personal Information Act (POPIA).[52] Their effectiveness remains unclear as both pieces of legislation do not appear to have been tested yet on NCIID cases. Also, varying views exist on their applicability, especially that of the data protection law. Nevertheless, it has been argued that victims who have taken their own photos can use the Copyright Act to apply for an interdictory (injunctive relief) and demand the removal of their images from online platforms (BusinessTech 2018). Victims have also been advised to use section 99(1) of the POPIA to initiate a civil claim for non-patrimonial damages for unlawful processing of their personal information (Gabriel 2020).

The criminalization of NCIID in South Africa is a welcome and important legislative intervention in the fight against the problem. However, until the new criminal offence comes into effect, victims will have to continue to make use of existing legal remedies.

46 *Domestic Violence Act*, Act 116 of 1998, online: <www.saflii.org/za/legis/consol_act/dva1998178.pdf>.

47 *KS v AM*, [2017] ZAGPJHC 297, [2018] 1 SACR 240 GJ.

48 *Ibid*.

49 Section 7(2) of the act provides: "The court may impose any additional conditions which it deems reasonably necessary to protect and provide for the safety, health or wellbeing of the complainant, including an order– (a) to seize any arm or dangerous weapon in the possession or under the control of the respondent, as contemplated in section 9; and (b) that a peace officer must accompany the complainant to a specified place as assist with arrangements regarding the collection of personal property."

50 The court held that "the respondent's possession of the material constitutes a continuous violation of the appellant's rights to dignity, privacy and bodily and psychological integrity. The special order sought by the appellant, which the court below declined, is the only remedy capable of effectively protecting and providing for the well-being of the appellant, and thus is reasonably necessary in terms of s 7(2) of the Act to order the respondent to hand over the material for forensic audit to be done on the equipment used and for the same to be removed and destroyed."

51 *Copyright Act, 1978*, No 98 of 1978 (as amended), online: <www.gov.za/sites/default/files/gcis_document/201504/act-98-1978.pdf>.

52 *Protection of Personal Information Act, 2013*, No 4 of 2013, online: <www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf>.

Conclusion

This analysis set out to survey the legal landscape as it pertains to three countries in the Global South. It made clear that the current legal remedies for addressing NCIID can be insufficient in protecting victims or punishing perpetrators. In countries such as Kenya, Chile and South Africa, where NCIID-specific legislation is not yet in force, victims have resorted to accessing justice through legislation prohibiting cyber harassment, defamation, extortion, improper use of information technology and domestic violence, among other provisions. In some instances, domestic laws within this space have been shown to be plagued with a variety of caveats that make prosecution for NCIID extremely difficult, posing challenges for victims in pursuit of justice.

While there are legal remedies directed at perpetrators that can be effective, it is important to note that both civil and criminal procedures can also be limiting. This is particularly true for those who may not have the financial means to pursue these options due to the high costs involved (Suzor, Seignior and Singleton 2017). Similarly, the remedies available to civil litigants might not adequately compensate victims in cases where perpetrators do not have ample financial resources to do so. Given the slow and complex nature of the justice system, such actions can also be unattractive to those who just want to rapidly minimize the damage, by getting the image(s) taken down to stop the spread (Henry and Powell 2016). The time-consuming process stands to exacerbate the suffering already experienced by the victim due to repercussions such as unwanted attention and the potential unlikelihood of fully ridding the internet of the explicit content (Dunn and Petricone-Westwood 2018). Lastly, given the transnational nature of this type of abuse, pursuing legal measures is challenging; this challenge is exacerbated in cases where the photos and/or videos were obtained by anonymous perpetrators, such as hackers (Suzor, Seignior and Singleton 2017).

It is also worth mentioning that researchers have supported the possibility that many young women and girls have lost faith in reporting to law enforcement agencies because criminal law sanctions are too often intermittently applied (Bailey 2015). Consequently, "not believing that law enforcement will take the complaint seriously is cited as one reason why gender-based crimes are underreported" (Dunn, Lalonde and Bailey 2017). Additional resources need to be provided to law enforcement to ensure proactive human rights-based approaches. Cyberviolence needs to be communicated to the public with seriousness to better enforce that the police are committed to ending cyberviolence against women and girls, while also respecting expressive and equality rights to fully engage online (Bailey 2016).

Beyond legislative measures, there is also value in developing and implementing educational programs and campaigns to truly convey the moral and legal boundaries of NCIID. Research shows that educational responses, primarily within the context of youth cases, are far more appropriate than punitive responses. This has been further supported by policy makers, criminal justice personnel and educators (Dodge and Spencer 2018). With the growing anxieties surrounding new technologies and youth sexual expression, educational efforts should focus on facilitating a better understanding of the repercussions of sexual violence, harassment, bullying and related acts. School curricula promoting cybersafety could be a starting point to effectively reduce inappropriate and harmful behaviours that could result from misuse of digital technology in this regard (Ringrose et al. 2012).

On a larger scale, community education campaigns should also "meet the information and support needs of victims; encourage 'witnesses' or 'bystanders' to take action to support a victim and/or challenge the perpetrator; [as well as] challenge the culture of victim-blaming that both excuses perpetrator behaviour and prevents victims from seeking assistance." (Henry, Powell and Flynn 2017, 9). On the notion of victim blaming, in particular, there needs to be greater drive to educate individuals to avoid sharing photos that an intimate partner has trusted them with. There is a risk when it comes to education that messages may fixate on the impulse that the victim may have consented to the photos being taken, therefore the victim is responsible for any harm that may result. This only heightens the gender inequities of such offences and amplifies existing and/or outdated cultural norms that blame victims who experience this type of gender-based violence. As a result, efforts must challenge these common perceptions and the associated stigma that may persist (Salter and Crofts 2015).

Notifying an intermediary can also be a practical tool for victims when a photo or video has been shared without consent via a social media platform (Young and Laidlaw 2020, 150). The unfortunate reality, of course, is that this may not be feasible for the less reputable platforms or websites that share photos, given that not all websites will have a reporting feature and/or visible contact information to make a complaint (Suzor, Seignior and Singleton 2017). Complaints-based systems also tend to be global by default for some platforms, and some intermediaries may be reluctant to expand the resources required to proactively monitor complaints as well as content submitted by users. In any case, "a policy that relies on victims to complain only addresses the symptom of the problem, not its cause" (ibid., 38).

However, despite the known struggles of major platforms to monitor and contain inappropriate content on their sites, there has been some positive movement in this regard. Facebook, for example, recently started using artificial intelligence (AI) to make it easier to find, flag and remove intimate photos that might have been posted without the subject's consent. The technology was trained to recognize "nearly nude" photos coupled with "derogatory or shaming text that would suggest someone uploaded the photo to embarrass or seek revenge on someone else" (CBC News 2019). While the technology may have its flaws, this expansion of content moderation is a step forward in capturing inappropriate posts. The willingness of some platforms to act also reflects the fact that these growing policy challenges are pushing the boundaries, forcing platforms to be more proactive in finding ways to combat abuse. However, more work still needs to be done to provide transparent and effective reporting systems that address cyberviolence in a more meaningful manner (Dunn, Lalonde and Bailey 2017).

A year of social isolation in 2020–2021 due to the COVID-19 pandemic has driven many people to engage with their partners online over virtual communication platforms — there is a high likelihood that incidents of NCIID have grown in the past year alone.[53] Improved policy efforts will, in turn, need to focus on ensuring that victims are aware of the available support services that exist or are needed. The initiative implemented by the Australian Government's eSafety Commissioner is a credible effort in this regard and could serve as a model for other nations. The dedicated image-based abuse site contains a wide assortment of resources on applicable laws, reporting mechanisms and counselling services, as well as general information on reducing tech-facilitated abuse.[54] Similarly, the UK government has supported the launch of a helpline to "provide a safe, non-judgemental first point of contact for victims." It also liaises with law enforcement to remove content and offers free legal advice.[55]

At the very least, it is imperative that victims are aware of their options and existing legal rights to pursue offenders or platforms that are hosting their intimate content. Policy makers, legislatures and civil society groups alike have an obligation to ensure victims are familiar with the necessary tools and supportive resources available to them.

The digital era has ignited new avenues for the propagation of sexual violence, as it diffuses reprehensible tactics to manipulate and harass. The growing manifestation of such digital harms could potentially continue to multiply as new tactics — such as pornographic deepfakes,[56] a next-generation tactic of NCIID — are on the rise. This will shift the borders of this discussion, especially within the context of privacy and reputation. From this view, the tragic consequences associated with some cases of NCIID are not to be taken lightly. Given the variable contexts and levels of harm associated with NCIID, developing responses will not be a simple task. The continuance of multi-pronged approaches should be stressed in order to truly address this rising form of gender-based violence.

53 For example, reports of image-based sexual abuse to Australia's eSafety Commissioner increased by 200 percent, on average, from March to May 2020. See Long (2020).

54 See www.esafety.gov.au/key-issues/image-based-abuse.

55 See https://revengepornhelpline.org.uk/.

56 For example, recently it was discovered that a deepfake pornography bot operating on the message app Telegram was being weaponized at an alarming scale to abuse thousands of women. Specifically, still images of nude women were generated by an AI that removed items of clothing from a non-nude photo, without the victim's knowledge. Unlike non-consensual explicit deepfake videos, these types of photo apps do not require a high-level of technical skill, given that the process is as simple as uploading an image. See Burgess (2020).

Works Cited

African Feminism. 2020. "Silencing Women: Nonconsensual Distribution of Intimate Images As Gender-based Violence in Nigeria." June 24. https://africanfeminism.com/silencing-women-nonconsensual-distribution-of-intimate-images-as-gender-based-violence-in-nigeria-part-i/.

ARTICLE 19. 2014. "Kenya: Cybercrime and Computer Related Crimes Bill." www.article19.org/wp-content/uploads/2018/02/Kenya-Cybercrime-Bill-129072014-BB.pdf.

Bailey, Jane. 2015. "A Perfect Storm: How the Online Environment, Social Norms and Law Shape Girls' Lives." Ottawa Faculty of Law Working Paper No. 2015-40. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605468.

———. 2016. "Canadian Legal Approaches to 'Cyberbullying' and Cyberviolence: An Overview." Ottawa Faculty of Law Working Paper No. 2016-37. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841413.

Baraka, Carey. 2019. "Religion and Politics: The Devil Is in the Details." The Elephant, May 10.

BBC News. 2018. "South Korean women protest in Seoul over hidden sex cameras." BBC News, July 7. www.bbc.com/news/world-asia-44751327.

Brend, Yvette. 2021. "Dutch man charged in Amanda Todd cyberbullying case was extradited to Canada in early December." CBC News, February 5. www.cbc.ca/news/canada/british-columbia/extradited-aydin-coban-2017-trial-appeal-amanda-todd-1.5902918.

Brook, Megan and Justin Sloane. 2020. "South Africa Cracks Down on Revenge Porn." Schindlers, August 27. www.schindlers.co.za/2020/south-africa-cracks-down-on-revenge-porn/.

Burgess, Matt. 2020. "A deepfake porn bot is being used to abuse thousands of women." *Wired UK*, October 20. www.wired.co.uk/article/telegram-deepfakes-deepnude-ai.

BusinessTech. 2018. "What you need to know about revenge porn laws in SA." BusinessTech, May 19. https://businesstech.co.za/news/technology/245525/what-you-need-to-know-about-revenge-porn-laws-in-sa/.

CBC News. 2019. "Facebook launches AI to find and remove 'revenge porn.'" CBC News, March 15. www.cbc.ca/news/science/facebook-ai-revenge-porn-1.5057817.

Chakamba, Rumbi. 2017. "Zimbabwean Activists Call for Specific Laws to Fight Revenge Porn." *The New Humanitarian*, June 28. https://deeply.thenewhumanitarian.org/womenandgirls/articles/2017/06/28/zimbabwean-activists-call-for-specific-laws-to-fight-revenge-porn.

Chisala-Tempelhoff, Sarai and Monica Twesiime Kirya. 2016. "Gender, law and revenge porn in Sub-Saharan Africa: a review of Malawi and Uganda." *Palgrave Communications* 2 (16069). www.nature.com/articles/palcomms201669.

Chun, Wendy Hui Kyong and Sarah Friedland. 2015. "Habits of Leaking: Of Sluts and Network Cards." *Differences: A Journal of Feminist Cultural Studies* 26 (2): 1–28.

Citron, Danielle Keats. 2018. "Sexual Privacy." *The Yale Law Journal* 128 (7): 1–70.

Citron, Danielle Keats and Mary Anne Franks. 2014. "Criminalizing revenge porn." *Wake Forest Law Review* 49: 345–91.

Craig, Nathan. 2019. "KZN woman in 'revenge porn' video opens crimen injuria case." IOL, October 11. www.iol.co.za/thepost/community-news/kzn-woman-in-revenge-porn-video-opens-crimen-injuria-case-34681771.

Dean, Michelle. 2012. "The Story of Amanda Todd." *The New Yorker*, October 18. www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd.

Digital Rights Foundation. 2017. "Measuring Pakistan Women's Experiences of Online Violence." https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

Dodge, Alexa. 2019. "Nudes are Forever: Judicial Interpretations of Digital Technology's Impact on 'Revenge Porn.'" *Canadian Journal of Law and Society* 34 (1): 121–43.

———. Forthcoming 2021. "'Try Not to be Embarrassed': A Sex Positive Analysis of Nonconsensual Pornography Case Law." *Feminist Legal Studies* 29 (1): 23–41.

Dodge, Alexa and Dale C. Spencer. 2018. "Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth." *Social & Legal Studies* 27 (5): 636–57.

Dunn, Suzanne, Julie S. Lalonde and Jane Bailey. 2017. "Terms of Silence: Weaknesses in Corporate and Law Enforcement Responses to Cyberviolence against Girls." *Girlhood Studies* 10 (2): 80–96.

Dunn, Suzie and Alessia Petricone-Westwood. 2018. "More than 'Revenge Porn' Civil Remedies for the Non-consensual Distribution of Intimate Images." 38th Annual Civil Litigation Conference 16, CanLIIDocs 10789. https://canlii.ca/t/sqtc.

Franks, Mary Anne. 2019. "The Crime of 'Revenge Porn.'" In *The Palgrave Handbook of Applied Ethics and Criminal Law*, edited by Larry Alexander and Kimberly Kessler Ferzan, 661–92. Cham, Switzerland: Springer International Publishing.

Freedom House. 2016. "Freedom on the Net 2016: Kenya." https://freedomhouse.org/country/kenya/freedom-net/2016.

Gabriel, Paula. 2020. "Can victims of revenge pornography rely on POPI's protection?" De Rebus, April 1. www.derebus.org.za/can-victims-of-revenge-pornography-rely-on-popis-protection/.

Garossino, Sandy. 2014. "Did Police Miss Chance To Protect Amanda Todd From Blackmailer?" Huffington Post, April 27. www.huffingtonpost.ca/sandy-garossino/amanda-todd-canada-police-online-sex-extortion_b_5219705.html.

Goldberg, Carrie. 2019. *Nobody's Victim: Fighting Psychos, Stalkers, Pervs, and Trolls*. New York, NY: Penguin Random House.

Grace, Githaiga, Kapiyo Victor and Munyuna Alice. 2013. *Women and Cybercrime: The Dark Side of ICTs*. Kenya ICT Action Network.

Hall, Matthew and Jeff Hearn. 2017. "Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts." *Journal of Gender Studies* 28 (2): 158–70.

Henry, Nicola and Anastasia Powell. 2016. "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law." *Social & Legal Studies* 25 (4): 397–418. https://journals.sagepub.com/doi/abs/10.1177/0964663915624273?journalCode=slsa.

Henry, Nicola, Asher Flynn and Anastasia Powell. 2019. "Image-based sexual abuse: Victims and perpetrators." Trends & issues in crime and criminal justice series no. 572. Australian Institute of Criminology.

Henry, Nicola, Anastasia Powell and Asher Flynn. 2017. "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse." May. Melbourne, Australia: Gendered Violence and Abuse Research Alliance, Centre for Global Research and Centre for Applied Social Research.

Henry, Nicola, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott. 2020. *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery*. New York, NY: Routledge.

International Telecommunication Union. 2014. *Understanding Cybercrime: Phenomena, Challenge and Legal Response*. November. www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf.

Kadandara, Nyasha. 2018. "Sex and the Sugar Daddy." BBC News. www.bbc.co.uk/news/resources/idt-sh/sex_and_the_sugar_daddy.

Kenyanito, Ephraim Percy and Raman Jit Singh Chima. 2016. "Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa." December. Access Now.

Kitchen, Adrienne. 2015. "The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment." *Chicago-Kent Law Review* 90 (1): 247–99.

Korenis, Panagiota and Stephen Bates Billick. 2014. "Forensic implications: Adolescent sexting and cyberbullying." *Psychiatric Quarterly* 85 (1): 97–101.

Koundouno, Tamba François. 2019. "Moroccans Should Focus on MP Maelainine's Politics, Not Her Clothes." Morocco World News, January 7. www.moroccoworldnews.com/2019/01/262586/morocco-maelainine-politics-pjd/.

Livingstone, Sonia, Rosalind Gill, Laura Harvey and Jessica Ringrose. 2013. "Teen girls, sexual double standards, and 'sexting': Gendered value in digital image exchange. *Feminist Theory* 14 (3): 305–23.

Long, Claudia. 2020. "Coronavirus shutdown prompts spike in reports of sextortion to eSafety Commissioner." ABC News, June 2. www.abc.net.au/news/2020-06-03/spike-reports-esafety-commissioner-coronavirus-shutdown/12314442.

Mail & Guardian. 2017. "Snap of shame: The rough road to stamping out 'revenge porn.'" *Mail & Guardian*, August 18. https://mg.co.za/article/2017-08-18-00-snap-of-shame-the-rough-road-to-stamping-out-revenge-porn/.

McCool, Alice. 2018. "When her naked selfies were posted online, she thought life couldn't get worse. Then she was arrested." CNN, November 10. www.cnn.com/2018/11/10/africa/uganda-pornography-revenge-porn-asequals-africa-intl/index.html.

McGlynn, Clare and Erika Rackley. 2017. "Image-based sexual abuse." *Oxford Journal of Legal Studies* 37 (3): 534–61.

McLaughlin, Molly. 2020. "Mexican Feminists Win Legal Protections against Revenge Porn." Latin America News Dispatch, March 17. https://latindispatch.com/2020/03/17/olimpia-law/.

Mngadi, Mxolisi. 2018. "Cape Town man ordered to remove all pornographic material which his wife is part of from digital devices." News24, August 11. www.news24.com/news24/SouthAfrica/News/cape-town-man-ordered-to-remove-all-pornographic-material-which-his-wife-is-part-of-from-his-digital-devices-20180811.

Mori, Camille, Jessica E. Cooke, Jeff R. Temple, Anh Ly, Yu Lu, Nina Anderson, Christina Rash and Sheri Madigan. 2020. "The Prevalence of Sexting Behaviors Among Emerging Adults: A Meta-Analysis." *Archives of Sexual Behavior* 49: 1103–19.

Mutsaka, Farai. 2015. "Miss Zimbabwe winner is stripped of title over nude photos." CTV News, June 11.

Mutung'u, Grace. 2018. "The Influence Industry: Data and Digital Election Campaigning in Kenya." Our Data Our Selves project. Tactical Tech. June. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf.

Naidoo, Mervyn. 2021. "Durban cyberbully who harassed neighbours convicted in landmark judgment." IOL, February 14. www.iol.co.za/sunday-tribune/news/durban-cyberbully-who-harassed-neighbours-convicted-in-landmark-judgment-60f54996-75e6-4e59-96a9-2650db67e995.

Ng, Desmond and Peh Yuxin. 2020. "The rise of non-consensual porn in Singapore and the battle to stem its spread." Channel News Asia, April 26. www.channelnewsasia.com/news/cnainsider/the-rise-of-non-consensual-porn-singapore-battle-stem-its-spread-12677446.

Nge'noh, Pkemoi. 2021. "Who leaked compromising photos of EALA Member of Parliament?" *The Nairobian*, March 26. www.standardmedia.co.ke/thenairobian/scandals/2001407532/who-leaked-compromising-photos-of-eala-member-of-parliament?amp.

Oginde, David. 2018. "Why the church opposes bid to introduce sex education." *The Standard*, January 21. www.standardmedia.co.ke/david-oginde/article/2001266642/why-the-church-opposes-bid-to-introduce-sex-education.

Owino, Samwel. 2018. "MPs reveal how woman has been sending them nude photos, ruining marriages." *Nairobi News*, March 14. https://nairobinews.nation.co.ke/news/mps-reveal-woman-sending-nude-photos-ruining-marriages.

Parliamentary Monitoring Group. 2017a. "Cybercrimes and Cybersecurity Bill: public hearings day 1." September 13. https://pmg.org.za/committee-meeting/25008/.

———. 2017b. "Cybersecurity and Cybercrime Bill: briefing, with Deputy Minister." May 30. https://pmg.org.za/committee-meeting/24496/.

———. 2017c. "Cybercrimes and Cybersecurity Bill — Chapters 1 to 9 of Bill: Summary of Written Submissions and Responses." November 7. https://pmg.org.za/committee-meeting/25424/.

Pickworth, Evan. 2020. "How the 'Internet Censorship' Act tramples constitutional rights," October 8, in *Business Law Focus* podcast, 19:54. www.businesslive.co.za/bd/business-and-economy/2020-10-08-podcast-what-sas-new-digital-content-censorship-will-mean-for-your-business/.

Ringrose, Jessica, Rosalind Gill, Sonia Livingstone and Laura Harvey. 2012. *A qualitative study of children, young people and 'sexting': a report prepared for the NSPCC*. London, UK: National Society for the Prevention of Cruelty to Children.

Salter, Michael and Thomas Crofts. 2015. "Responding to Revenge Porn: Challenges to Online Legal Impunity." In *New Views on Pornography: Sexuality, Politics and the Law*, edited by Lynn Comella and Shira Tarrant, 233–54. Santa Barbara, CA: Praeger.

Schein, Ava. 2019. "When Sharing is Not Caring: Creating an Effective Criminal Framework Free from Specific Intent Provisions to Better Achieve Justice for Victims of Revenge Pornography." *Cardozo Law Review* 40: 1953–99.

South African Law Reform Commission. 2019. "Project 107 — Sexual Offences: Pornography and Children." Discussion Paper 149. April. www.ellipsis.co.za/wp-content/uploads/2015/11/dp149-prj107-SexualOffences-PornographyChildren2019.pdf.

Sugow, Abdulmalik and Jaaziyah Satar. 2020. "The Computer Misuse and Cybercrimes Act Judgment: A Digest." Centre for Intellectual Property and Information Technology Law, March 26. https://cipit.strathmore.edu/the-computer-misuse-and-cybercrimes-act-judgment-a-digest/.

Suzor, Nicolas, Bryony Seignior and Jennifer Singleton. 2017. "Non-Consensual Porn and the Responsibilities of Online Intermediaries." *Melbourne University Law Review* 40 (3): 1–41. https://law.unimelb.edu.au/__data/assets/pdf_file/0007/2329396/Suzor-403-Advance.pdf.

Uhl, Carolyn A., Kaitlin J. Rhyner, Cheryl A. Terrance and Noël R. Lugo. 2018. "An examination of nonconsensual pornography websites." *Feminism & Psychology* 28 (1): 50–68.

Waldman, Ari Ezra. 2017. "A Breach of Trust: Fighting Nonconsensual Pornography." *Iowa Law Review* 102: 709–33.

Walter, Dzuya. 2018. "Wazir Chacha freed on Ksh.1M cash bail." *Citizen Digital*, April 25. https://citizentv.co.ke/news/wazir-chacha-man-accused-of-conning-mps-freed-on-ksh-1m-cash-bail-198307/.

Wandia, Tess. 2018. "In the Aftermath of Ifikie Wazazi: Social Media, Safety and Consent." *Wandia* (blog), May 7. https://tnwandia.com/2018/05/07/in-the-aftermath-of-ifikie-wazazi-social-media-safety-and-consent/.

Wanjiku, Evelyne. 2018. "Policy Initiatives to address Non Consensual Pornography on the Social Media Platform in Kenya." SSRN Electronic Journal, January. www.researchgate.net/publication/329198643_Policy_Initiatives_to_Address_Non_Consensual_Pornography_on_the_Social_Media_Platform_in_Kenya.

White, Patrick. 2015. "Rehtaeh Parsons Investigation Delayed by Crown Mistakes, Review Finds." *The Globe and Mail*, October 8. www.theglobeandmail.com/news/national/review-says-crown-decision-in-rehtaeh-parsons-case-was-reasonable/article26715933/.

Young, Hilary and Emily Laidlaw. 2020. "Creating a Revenge Porn Tort for Canada." *Supreme Court Law Review* 96 (2): 147–87.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline