Foundation for Media Alternatives

Lessons on Human Rights Advocacy and Cybercrime Policy

TABLE OF CONTENTS

INTRODUCTION

About the Cybercrime Prevention Act

The Cybercrime Prevention Act of the Philippines (Republic Act No. 10175) was passed and enacted in 2012. In the same year, the constitutionality of the law was questioned before the Supreme Court for provisions that violate human rights such as the freedom of speech, expression, and of the press; the right against unreasonable searches and seizures; the right to liberty; the right to privacy; and other fundamental freedoms.

While the Supreme Court struck down some of the law's provisions for being unconstitutional, other provisions—as well as the Act's implementing rules—continue to imperil human rights online. Online libel and cybersex remain as crimes under the law. Implementing rules authorize the collection of computer data, justifying overbroad real-time electronic surveillance without adequate limitations aside from a court order.

Today in 2020, the CPA remains to be the most powerful and overreaching law against digital freedoms, especially during a time where most people are confined to their homes and most essential activities were forced to shift online. However, as the bounds of the "digital" expands, so does the possibility for abuse of the law.

About the MHRC project

This paper serves as a culmination of a project called Mainstreaming Human Rights in Cybercrime and Cybersecurity Policymaking Processes, or MHRC. The project was formulated by Global Partners Digital, an advocacy organization based in the United Kingdom.

The overall objective of the project was to shape the outcome of the policymaking process around the amendment of the CPA to reflect international human rights and standards, based on the assessment that certain provisions of the law are violative of the fundamental human rights of free speech, free expression, and the right to privacy.

The project strategy was divided into two advocacy tracks: first is finding champions in the Senate and House of Representatives to introduce amendatory bills for the CPA; and second, influencing executive agencies (particularly the Department of Justice, Department of Interior and Local Government, and Cybercrime Investigation and Coordinating Center under the Department of ICT) to initiate the process of amending the implementing rules and regulations of the CPA.

The project started its full implementation in 2019 and is slated to wrap up in the last quarter of 2020.

The first phase of project implementation was the development of a policy brief. Within the first couple of months, a first draft was developed by the FMA project team, with some input from GPD's legal officers who have been doing research on cybercrime legislations all over the globe.

An updated version of the policy brief is currently available for viewing and download on the FMA website.[1]

The policy brief draft was then further developed through a series of stakeholder consultations from May to June 2019. It was then presented during a meeting with the Office of Cybercrime of the Department of Justice (DOJ-OOC).

Finally, the project team arranged meetings with identified lawmakers who might be interested in filing a proposal to amend the law based on the project's recommendations. In the House of Representatives, the team met with two legislators from the Makabayan bloc: Rep. Arlene Brosas of GABRIELA and Rep. Carlos Zarate of Bayan Muna. In the Senate, the team was only able to meet with the staff of Senator Leila de Lima.

As the project prepares to wrap up, it is important to look back on the past two years of implementation and reflect on its successes and failures to be able to inform similar future endeavors. This is particularly crucial now that the CPA is increasingly being used for new purposes such as cracking down on disinformation or "fake news," which was particularly significant in 2020 as the country dealt with public panic around the COVID-19 pandemic.

STAKEHOLDER CONSULTATIONS

Three stakeholder consultations were conducted in the course of the project in 2019: first on cyberlibel on May 24, on cybersex on June 7, and on real-time data collection on June 21.

In lieu of their attendance, the DOJ-OOC sent a letter containing their official response to the policy paper that FMA submitted prior to the consultation. The DOJ prefaces the letter by emphasizing that the CPA was patterned after the Budapest Convention on Cybercrime, and that some of the issues raised in the policy brief were already addressed in the landmark case of Disini v. The Secretary of Justice. In particular, the DOJ points to the fact that the paragraph allowing real-time collection of traffic data was stricken down by the Supreme Court for being unconstitutional. The letter also defers to the ruling of the Supreme Court as to the criminalization of cybersex, asserting that the provision is applicable only to cybersex as a commercial activity.

As to online libel, the DOJ pointed out that at the time it was one of the provisions sought to be amended by an amendatory bill that was identified as part of the priority legislative agenda of the Duterte administration. The DOJ-OOC in their letter named House Bill No. 6184 filed by Rep. Victor Yap as the version they endorse but in a separate meeting with them (after the stakeholder consultations were conducted), they shared that the office was in the process of looking for another champion in Congress to carry their preferred amendments.

On cyber libel

The discussion on cyber libel was attended mostly by journalists and media practitioners. The Department of Justice - Office of Cybercrime was invited as well but could not make it due to a scheduling conflict.

The consultation featured two guest speakers: Raymund Villanueva from the National Union of Journalists in the Philippines (NUJP) and Atty. Oliver Reyes, who was also part of the Philippine Internet Freedom Alliance. Villanueva stressed that NUJP has long campaigned for the decriminalization of libel and noted that recent events highlight the need to review Philippine libel

laws, which are excessive, outdated, and prone to abuse. During the dictatorial regime of former president Ferdinand Marcos, libel was used to stifle press freedom; until now, criminal libel remains a sword over the heads of the Philippine press, made sharper by the CPA by making the offense punishable with harsher penalties. Villanueva asserted that the cybercrime law is a weapon against press freedom and freedom of expression.

Responding to the DOJ's official letter-statement, Reyes noted that the specific House Bill that contained the Department's preferred amendments did not particularly eliminate the crime of cyber libel. Hence, the bill would have no practical effect as the disparity of penalty vis-a-vis offline libel would remain. Apart from the higher degree of penalty, Reyes raised other significant features of the CPA. For one, a person guilty of cyber libel is at risk of not being entitled to probation. The law also extended the prescriptive period to 12 or 15 years, as opposed to one year in the Revised Penal Code. The CPA also drastically changed the rule on venue, in that a case may be filed anywhere where elements of the crime occured, making it possible to file libel complaints in inconvenient venues. Contrary to the MHRC project's policy brief, however, Reyes maintained that amending the CPA is not the ideal solution as it would not ultimately decriminalize libel. Rather, the solution should be to assault libel under the Revised Penal Code and the longstanding criminal justice framework. An insight that Reyes offered as to possible advocacy strategies is that to date, assault through the judiciary has not met success. In the Disini case, the only Supreme Court Justice who was mostly sympathetic was Justice Leonen. Ultimately, Reyes suggested that even simply emphasizing the disparity between online and offline libel may actually lead somewhere.

On cybersex

The consultation on the provision that criminalizes cybersex was attended mostly by women's rights and children's rights advocates, as the provision also closely intersects with issues of human and sexual trafficking.

The consultation featured two resource persons: Christina Lopez of FMA's Gender and ICT program and Jelen Paclarin of the Women's Legal and Human Rights Bureau. Lopez provided a summary of FMA's position on the criminalization of cybersex: that it endangers women's rights and perpetuates violence against women.

Paclarin then delivered an overview of the campaign against the provision ever since it was passed into law. WLB believes that although online and offline VAW can be traced back to the same roots (i.e., unequal power relations between women and men), ICT-related VAW is a distinct phenomenon because of the following features: borderlessness, anonymity, intractability, fluidity of online identity, and absence of physicality. She stressed that the main problem with Sec. 4(c)1 is the lack of clear definitions for the terms it uses. For example, the title itself uses the word sex, which is something consensual. Paclarin argued that cybersex is something positive and therefore shouldn't be

criminalized, and that the intent of the law is to legislate activities like trafficking and pornography, which are not accurately represented by the term “cybersex.”

On real-time data collection

The last stakeholder consultation was on provisions relating to the collection of computer data. Data protection and digital security specialists were invited to this discussion.

The resource person for the third round of consultations was Atty. Jamael Jacob, Privacy Program Manager at FMA and former Director of the Privacy Policy Office of the National Privacy Commission. Jacob distinguished between traffic data, content data, and computer data under the CPA and its implementing rules and regulations (IRR). While the Supreme Court in the Disini case did strike down the collection of “traffic data,” Jacob pointed out that the revival of the term “computer data” in the implementing rules, which also sanctioned the collection of computer data, disregards the case law in Disini and may open the floodgates to abuse. Indeed, data privacy practitioners who attended the consultation expressed their concerns on how to deal with instances where this rule may be enforced by authorities, vis-a-vis their duty to protect personal and sensitive information (classifications of information which are still within the scope of “computer data”).

It became clear that the CPA’s implementing rules cannot go beyond the express declaration of the Supreme Court. Atty. Reyes, who also attended this stakeholder consultation, offered valuable insight on how to construct the IRR vis-a-vis rules that the Supreme Court issued itself to limit discretion on computer data collection. The Supreme Court’s Rule on Cybercrime Warrants, as explained by Reyes, may have already tempered the overbreadth and overreach of the CPA IRR, as it provides for four (4) different kind of warrants that all law enforcement authorities must first seek from the courts before proceeding with any kind of action relating to data collection. While the proper timing for the amendment of the IRR may not be availing under the circumstances, the Supreme Court’s cyber warrants rule provides for available remedies against possibilities of abuse.

2020 DEVELOPMENTS

So much has happened since the policy paper was produced and the stakeholder consultations were conducted. Shortly after Metro Manila and other major cities were placed in quarantine due to the COVID-19 pandemic, the Philippine Congress enacted the Bayanihan To Heal As One (BHAO) Act. One of its provisions, hastily added to the law, criminalized the creation, perpetration, and dissemination of "false information," which was undefined. Not only did this additionally provide justifications for law enforcement authorities to arrest ordinary citizens speaking up against bad governance during the pandemic, it also led to a sudden spike in the publicly reported cases of cyber libel.

While the BHAO law expired in June 2020, at the time of writing, "fake news" or misinformation cases are still being prosecuted using the CPA.[2] Because of the "catch-all provision" in Section 6 of the CPA, which places all crimes under the Revised Penal Code (RPC) under the coverage of the CPA if committed with the use of ICTs, fake news cases have been treated as various offenses. Some examples of RPC offenses that have been used in conjunction with the CPA for cases of disinformation are "unlawful use of means of publication and unlawful utterances" and "alarms and scandals"

Maria Ressa/Rappler decision

The most high-profile case since the CPA was passed in 2012 is arguably that against online news outfit Rappler, its editor-in-chief Maria Ressa, and former researcher-writer Reynaldo Santos, Jr. On June 15, 2020, a mid-level court judge issued the first decision on this case, and ruled that the online libel complaint against Ressa, et al, filed on February 5, 2019, has not prescribed even as the article was originally published a few months before the cybercrime law took effect. Citing a law promulgated in 1926, the judge ruled the prescriptive period for online libel was 12 years, and the reckoning point was from Rappler's "re-publication," when it updated the article in 2014. Owing to the nature of the internet, issues of publication online will continue to significantly affect prosecutions of online libel.

Weaponization of the cybercrime law

Although our perception may be skewed by the ratio of reported and unreported cases, it appears from media reports that cyber libel cases spiked during the COVID-19 lockdown, along with the government's self-proclaimed crackdown on "fake news." While online libel is still mainly invoked whenever there is an opportunity to question the truth of any statement (including valid criticism), law enforcement personnel have also used the catch-all provision of the CPA to convert into a cybercrime the crime of inciting to sedition. Among others, on this basis, police have arrested without a warrant (and made an example of) a teacher who posted online that 'people were going hungry because of the coronavirus and should raid the local gym where goods are stocked.' Police have also arrested another teacher who tweeted that he will offer a bounty of 50 million pesos for anyone to kill the president.

Cybercrime during the COVID-19 lockdown

At the same time, the prolonged quarantine and forced shift to digital platforms also meant that there were higher risks of cyber incidents such as hacking, phishing, and other forms of computer fraud.

As early as April 2020, the Philippine National Police (PNP) warned the public about the "100% increase" of cybercrime incidence in the country, the most common of which is phishing, or disguising one's identity as to appear legitimate, to lure someone into sharing personal information, such as bank account numbers. The PNP also warned against donation scams (luring unsuspecting individuals to donate to fake causes), online shopping scams (dubious transactions where prices of products are lowered to entice buyers), and sales of ATM cards for fraud (to use as deposit accounts for stolen money).[3]

From March to May 2020, banks reported losses in the amount of Php 60.6 million on account of the spike in cybercrime cases, which comprised approximately 59% of total bank losses during the two-month period.[4]

In May 2020, the PNP also reported that cases of online child sex abuse tripled during the pandemic. It was also reported that from March 1 to May 24, there were 279,166 cases of online child sex abuse in the Philippines – during the same timeframe in 2019, in comparison, there were only 76,561 cases.[5]

In July, the PNP stated that phishing is the most prevalent crime during the lockdown, with cases reported increasing to 200%.[6]

the reach of ordinary citizens," with posting for bail becoming increasingly difficult, cases being delayed, with online initiatives to aid disadvantaged litigants hampered by poor internet connections.[7]

The Anti-Terror Law and cybercrime

In July 2020, the controversial Anti-Terrorism Law (ATL) was railroaded in the House of Representatives despite overwhelming opposition from the public. Before the law was passed, critics repeatedly called Congress to remove provisions therein punishing, among others, crimes such as "inciting to terrorism," defined too broadly and widely as to capture legitimate acts of dissent. In the law, government officials may also deem themselves the arbiter of what acts constitute terrorism or inciting to commit terrorism, affecting the safety and security of many journalists in a country already tagged as one of the most dangerous places in the world for journalists. Indeed, one month into the law's passage, the chief of the Armed Forces of the Philippines has already proposed to include social media regulation in the implementing rules and regulations of the law, backtracking only after drawing criticism online.

WHAT HAPPENS NEXT?

Relevant bills in Congress

At the time of writing, there are four bills in the House of Representatives proposing amendments to the CPA: House Bill No. 359 by Rep. Victor Yap, House Bill No. 1707 by Rep. Luis Raymund Villafuerte, Jr., House Bill No. 5672 by the Makabayan bloc,[8] and House Bill No. 7010 by Rep. Rufus Rodriguez. Proposed amendments vary across the different bills. As of this writing, the Makabayan bill is the closest to the MHRC project's model bill, with provisions repealing the cyber libel offense in Section 4(c)4, the catch-all provision in Section 6, and Section 19, which allows the DOJ to issue an order to restrict or block access to computer data when such data is prima facie found to be in violation of the law. It also amends Section 12 to add the requirement of a court warrant for law enforcement authorities to be authorized to conduct real-time collection of traffic data. The Villafuerte bill likewise repeals the same provisions, and adds a clause that explicitly provides that dealing with offenses against the confidentiality, integrity, and availability of computer data and systems must be consistent with the Data Privacy Act.

Interestingly, the Yap bill allows law enforcement authorities, upon securing a court warrant, to conduct interception and collection of traffic and content data that are held and maintained by a cloud computing service provider situated outside the Philippines. The bill also adds to the duties and functions of the PNP Anti-Cybercrime Group and the NBI Cybercrime Division the following, among others:

1. to investigate the prohibited acts under Chapter II and to support investigations where computer systems are involved including the search, seizure, evidence preservation, forensic recovery of data from crime scenes and systems used in crimes; and
2. to conduct data recovery and forensic analysis on computer systems and other electronic evidence seized as provided under Chapter IV of [the CPA].

The Rodriguez bill, which was filed after the Regional Trial Court's judgement of the Rappler case, adds a prescription period of three (3) years from the commission of the offense, except for Sec. 4(c)4 Libel, which is given the prescription period of one (1) year from date of publication.

Initiatives responding to the CPA and other laws that threaten free speech

On 20 August 2020, FMA conducted an online discussion titled What's Next for the FOE Advocacy? The discussion served as a sharing session among representatives from various fronts of civil society (human rights defenders, journalists, legal practitioners, progressive lawmakers) on the challenges they're facing in advocating for free speech in the time of the Anti-Terror Law, as well as the future of the advocacy.

During the discussion, Nonoy Espina from NUJP mentioned the United Nations Human Rights Council (UN HRC) resolution calling for the decriminalization of libel in the Philippines. The guests also mentioned the need to continuously monitor and respond to legislation that could significantly impact free expression, such as the proposed anti-fake news bills.

Other possible venues of advocacy

Despite the diversity of these strategies, there are still avenues of advocacy that remain unexplored. International and regional mechanisms are particularly underutilized. As early as 2011 even before the passage of the CPA, the UN HRC already issued a statement calling for decriminalization of libel in the Philippines.

One key recommendation that surfaced during the stakeholder consultations under this project was the need to anchor the cybercrime advocacy work on a broader campaign for the decriminalization of libel. As Atty. Reyes shared, even removing Sec. 4(c)4 would not completely do away with the criminal libel, as long as libel is a crime under the Revised Penal Code.

Key learnings and recommendations from the MHRC project

Since its inception, the Philippines' cybercrime law has already been closely intertwined with efforts by civil society to ensure that it is consistent with human rights standards. The fight persists to this day and is now informed by numerous actual cases and real-life experiences - and the point of this report is precisely to document this long history of victories and losses, with the hope of encouraging more stakeholders to take on the mantle of pushing for the necessary changes to the law. The following are just some of the key elements that the MHRC project identified as being essential to sustain the advocacy.

Cooperation and coordination among civil society

At the onset, the MHRC project was designed in such a manner that is heavily dependent on working with other CSOs. This importance became even more evident as the project went on and especially when the pandemic started. With mobility restricted in most parts of the country, physical meetings and events were impossible and the project therefore had to rely on online activities.

More substantially, having to deal with the pandemic meant that the Congress had to inevitably shift their priorities. It was therefore crucial to reformulate an advocacy strategy that would tie the project's original goals with the newer and more pressing concerns, such as criminalization of "fake news" under the BHAO law and opposing the Anti-Terrorism Law. Input from various sectors within civil society was also instrumental in the development of both the policy brief and the model bill. For instance, hearing about the actual experiences of media practitioners during the consultation on cyber libel grounded our legal analysis on how the issue of prescription presents real danger for media practitioners.

Champions in Congress

At the outset, it seems that repealing or even amending the current cybercrime law is impossible given the dominance of Duterte-allied lawmakers in both chambers of the Philippine Congress. However, the much-publicized fight against the Anti-Terrorism Law was an illustration of how important it is to have progressive voices in Congress, however few they are. The tireless opposition of a few representatives were key in sustaining public fervor, which eventually led to a significant number of lawmakers attempting to withdraw their votes in favor of the law. Such victory, as well as the continued interest and willingness of some lawmakers to push for CPA amendments show that not all hope is lost in the legislative front. What the ATL experience teaches us, however, is that legislative advocacy could always benefit from clamorous public support and even global attention.

As long as technology shifts and advances, so will the cybercrime law.

The COVID-19 pandemic and the long quarantine period that resulted from it have forced businesses and even government agencies to speed up digital transformation. This may call for the review of several internet governance laws (such as the cybercrime law), whose current versions may be insufficient to address legal gaps brought about by such rapid transformation. For instance, more entities are now adopting digital payment systems, making transactions more vulnerable to possibly new forms of cyber attacks. It is therefore expected that the cybercrime law would be put to the test against these new and emerging cyber threats.

The CPA needs to be understood in conjunction with other related laws.

Rather than focusing on the CPA itself, more efforts should be given to understanding the bigger landscape of cyber-legislation in the Philippines - this includes all laws that relate to the governance of internet and computer-related activities. Additionally, one of the most common sentiments among journalists and free speech advocates is that decriminalizing online libel is not enough; the push to eliminate the crime of online libel under the CPA should also feed into the longstanding fight to decriminalize libel under the Revised Penal Code.

Monitoring the implementation of the law is as important as amending it

Admittedly, the project fell short in its attempt to engage with the executive agencies involved in the implementation of the CPA, namely, the Department of Justice, Department of Interior and Local Government, and the Department of Information and Communications Technology.This is partly due to the realization that it is challenging, if not completely impossible and contradictory, to tackle the implementation of the law without first addressing its flaws from the policy level; and what we learned was that there isn't much going on in these agencies with regards to updating cybercrime policy. Nevertheless, the continued increase in cybercrime-related cases necessitates that civil society also pay attention to how law enforcement actors implement the law, and respond to any human rights violation in such implementation

As the MHRC project comes to an end, the project team hopes that the lessons learned during the project and the gains it accomplished will serve as a driving force for other groups or individuals who might want to take on the advocacy in the near future.

ENDNOTES

[1] "Cybercrime & Human Rights: Justifications for amending the Philippines' Cybercrime Prevention Act," Foundation for Media Alternatives, https://www.fma.ph/cybercrimepaper2019/

[2] "Netizen who spread fake news about physical distancing after sex faces raps," ABS-CBN News, Sept. 7, 2020, https://news.abs-cbn.com/news/09/07/20/netizen-who-spread-fake-news-about-physical-distancing-after-sex-faces-raps

[3] Kristel Limpot, "NBI warns of prevalence of cybercrimes as cases doubled during lockdown," CNN Philippines, Apr. 27, 2020, https://cnnphilippines.com/news/2020/4/27/NBI-cybercrime-cases-double-covid-lockdown.html

[4] Bianca Cuaresma, "Banks lost P60.6 million to cybercrime in initial quarantines–BSP report," BusinessMirror, Nov. 5, 2020, https://businessmirror.com.ph/2020/11/05/banks-lost-p60-6-million-to-cybercrime-in-initial-quarantines-bsp-report/

[5] Nanchanok Wongsamuth, "Online child sex abuse cases triple under lockdown in Philippines," ABS-CBN News, May 29, 2020, https://news.abs-cbn.com/news/05/29/20/online-child-sex-abuse-cases-triple-under-lockdown-in-philippines

[6] "Phishing is top PH cybercrime during pandemic – authorities," Rappler.com, Jul. 12, 2020, https://www.rappler.com/nation/phishing-top-philippines-cybercrime-during-pandemic

[7] Angelica Carballo Pago, "Access to PH Justice System Suffers Amid the Lockdown," Philippine Center for Investigative Journalism, May 22, 2020, https://www.rappler.com/nation/phishing-top-philippines-cybercrime-during-pandemic

[8] The bloc is composed of Rep. France Castro of ACT Teachers Party-List, Rep. Carlos Isagani Zarate, Rep. Ferdinand Gaite, and Rep. Eufemia Cullamat of BAYAN MUNA Party-List, and Rep. Sarah Jane Elago of KABATAAN Party-List.

Foundation for Media Alternatives

Unit 203 CRM Building III, 106 Kamias Road, East Kamias 1102, Quezon City

info@fma.ph

https://www.fma.ph

(632) 7753 5584