CYBERCRIME & HUMAN RIGHTS

Justifications for amending the Philippines' Cybercrime Prevention Act

2019

Foundation for Media Alternatives

CYBERCRIME & HUMAN RIGHTS

Justifications for amending the Philippines' Cybercrime Prevention Act

This policy paper presents justifications and recommendations for the amendment of the Philippine Cybercrime Prevention Act of 2012, with regard to the provisions on online libel and cybersex, and law's implementing rules with regard to collection of computer data. The policy paper has three parts: 1) an introduction describing the context in which the law has been applied, its significance in combating cybercrime, and instances where its application violated human rights; 2) a review of the three specific provisions sought to be removed/repealed; and 3) concrete recommendations to make the law more adherent with human rights standards as mandated by the Constitution and international treaties.

This policy paper, drafted by the Foundation for Media Alternatives with support from Global Partners Digital, is informed by stakeholder consultations with Philippine civil society organizations and government agencies working on issues related to the implementation of the Cybercrime Prevention Act. The consultations were conducted from May to June 2019.

Introduction

A day shy of Valentines' Day in 2019, journalist Maria Ressa was arrested in the newsroom of Rappler, a social news network she co-founded in the Philippines. Ressa, one of President Duterte's fiercest critics, was served a warrant for committing online libel, designated as a crime under the Cybercrime Prevention Act of 2012 (Republic Act 10175). Journalists have called the arrest an assault on freedom of speech, expression, and the press, one that relies "on an extreme legal strategy that imperils everyone who posts online or on social media."[1]

Aside from Ressa, other journalists and activists have been subjected to online libel cases, in increased numbers from previous years.[2] For example, four members of the civil society network Philippine Misereor Partnership, Inc., were charged with online libel in 2016 for reporting on a corporation's mining operations in Eastern Samar.[3]

Recently, distributed denial of service (DDoS) attacks took down websites of alternative news networks Bulatlat, Kodao Productions, Pinoy Weekly, and Altermidya—attacks that have not stopped since December 2018. Websites of news organizations Arkibong Bayan, Manila Today, and the National Union of Journalists in the Philippines, as well as human rights groups Karapatan, Bagong Alyansang Makabayan, and Ibon Foundation were also attacked, in what has been described as "cyber warfare" that is "part and parcel of the ongoing assault by the administration on the media."[4]

All these have sparked a renewed interest in the Philippines' Cybercrime Prevention Act, reigniting strong calls for a repeal of its problematic provisions. The law, which had been under fire even before its passage in 2012, was contested before the Supreme Court for violating human rights, including the freedom of speech, expression, and the press; the right against unreasonable search and seizure; the right to liberty; the right to privacy; and other fundamental freedoms.[5]

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.

For various civil society groups, criminalizing online libel is a step backward in the movement to decriminalize libel altogether;[6] while the provision on cybersex, albeit well-intentioned, has been described as misinformed on "the real state of ICT-related violence against women," thus endangering women's rights.[7]

Cybersex and libel are not cybercrimes as outlined in the Budapest Convention on Cybercrime—which the Philippines ratified in 2018—and their inclusion as cybercrimes in the Philippines is inappropriate and does not represent international best practice.[8] Where the local law suffers from vagueness and overbreadth, such as the Philippine definition for cybersex, the language "needs to be very specific so that it is not vague or over criminalizes"[9] — assuming that cybersex, insofar as it does not clearly refer to abuse or exploitation, needs to be criminalized at all.

Meanwhile, the authorization to collect or record computer data effectively skirts around a previous court decision, which found the authorization to collect specific traffic data alone sweeping and without restraint.[10]

The importance of a Philippine anti-cybercrime law

It cannot be discounted that the Cybercrime Prevention Act is a landmark legislation in the fight against cybercrime, as it enhances security of individuals online. Many of the law's provisions are directly taken from the Budapest Convention, which binds States to adopt legislation and foster international cooperation to combat crimes committed via the internet and computer networks.

The Convention's preamble states that parties (including the Philippines) are "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights" under multiple treaties, "which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy."

The Cybercrime Prevention Act penalizes the following offenses outlined in the treaty:

- Offenses against the confidentiality, integrity, and availability of computer systems (illegal access, illegal interception, data interference, system interference, and misuse of devices);
- Computer related offenses (computer-related forgery and computer-related fraud);
- Content-related offenses (child pornography); and
- Offenses related to infringements of copyright and related rights.

The passage of the law in 2012 was significant for the Philippines. In 2011, the Philippine National Police stated that the country had become a "haven" for transnational cybercrime groups involved in cyber pornography, cybersex dens, illegal online gambling, credit card fraud and identity theft. Police decried weak laws and the lack of technical training by law enforcers to deal with cybercrime.[11] The passage of the law was a direct response to the growing threat of cybercrime not just in the Philippines, but all over the world.

Latest data from the Department of Justice – Office for Cybercrime[12] show that in 2016, Philippine law enforcement agencies received 3,951 complaints for cybercrime and related offenses, which is 53.92 percent higher from 2015. These cases comprise of the following:

- 322 complaints regarding offenses against the confidentiality, integrity, and availability of computer data and systems;
- 830 complaints on computer-related fraud and forgery;
- 640 content-related complaints—cybersex, child pornography, and online libel—with cases of online libel as the most-complained offense; and
- 1,578 complaints on cyber-enabled offenses, or conventional crimes committed via ICT.

The need for a cybercrime law is clear—but while the courts have already struck down several of its overreaching provisions, it failed to align the provisions on online libel and cybersex with international and national human rights law, including the Constitution and international treaties and resolutions. Also worrisome is how a repealed provision (on real-time collection of traffic data) has been resurrected and expanded to encompass computer data in the law's implementing rules, not only bypassing the court's decision in this regard but also opening up the floodgates of abuse in computer data collection.

Both legislators and enforcement officers must therefore urgently consider amending the law and its implementing rules to conform to international and national human rights frameworks. In light of the Philippines' recent accession to the Budapest Convention on Cybercrime,[13] it subjects itself even further to a global regime that makes imperative the need to adequately balance anti-cybercrime efforts with respect for fundamental freedoms.

Reviewing the Cybercrime Prevention Act

Online libel

Libel is an old crime; it is one of the crimes listed in the Revised Penal Code of 1930, which is lined up for repeal by Congress in view of a new draft criminal code.[14]

Online libel, a content-related offense in the cybercrime law,[15] takes from the definition in the archaic penal code: "a public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance tending to cause the dishonor, discredit, or contempt of a natural or juridical person, or to blacken the memory of one who is dead."[16] The penalty for online libel in the cybercrime law is one degree higher than libel in the penal code.[17]

The law makes it clear that whether online or print, libelous imputations are automatically assumed malicious, unless they qualify as 1) private communications made out of duty, or 2) a fair and true report made out of good faith.[18] While writers, journalists, and editors online may find reassurance in the second clause, it is not a defense against libel, but rather only a rebuttal against the presumption of malice.

A close scrutiny of online libel under the cybercrime law will reveal that it is a harsher crime than libel in the penal code:

	Libel (Revised Penal Code)	Online libel (Cybercrime Prevention Act)	Effect
Penalty of imprisonment	4 years	4 to 8 years	Penalty for online libel offenders is harsher
Availability of probation	Yes	Depends, if prison term does not exceed 6 years	Probation may not be available for online libel offenders
Prescriptive period	1 year	12 or 15 years, in the context of "continuing publication"	Online libel offenders may be filed cases several years after the offending piece was published; "continuing publication" may render the crime without a prescriptive period
Venue of filing	Place of publication or where publication is made available	Anywhere where elements of the crime occurred	While potential for abuse already exists in the libel provision for venue, the venue for online libel makes it more possible to file libel complaints in inconvenient venues

The dramatic disparity between libel and online libel, among others, led various groups and stakeholders to challenge the law before the Supreme Court. By a vote of seven justices, the Supreme Court upheld the constitutionality of online libel in a landmark case in 2014. Considering the nature of the internet, the Supreme Court decision provided that liability for online libel is limited to the original author of the post, and does not include those who merely "like," comment, or share an article.[19]

Still, the decision is incompatible with international human rights standards on freedom of expression as codified in numerous instruments, such as Art. 19 of the International Convention on Civil and Political Rights (ICCPR), to which the Philippines is a State party. Art. 19 provides:

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

    (a) For respect of the rights or reputations of others;

    (a) For the protection of national security or of public order (ordre public), or of public health or morals.

The United Nations Human Rights Committee (UNHRC), in 2012, had the opportunity to directly comment on the Philippines' imposition of imprisonment as a penalty for libel. Based on a complaint filed by a Davao radio broadcaster who served his sentence for the crime, the committee stated that "...the sanction of imprisonment imposed on the author was incompatible with article 19, paragraph 3, of the Covenant," and the facts "...disclose a violation" of Art. 19 of the ICCPR, among others.[20]

While the ICCPR allows for restrictions to freedom expression, the criminalization of libel and the imposition of imprisonment does not comply with the requisites in Art. 19, most notably the requirements of necessity and proportionality. "States parties should consider the decriminalisation of defamation," the UNHRC stated, "and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."[21] The Budapest Convention does not contain a provision on online libel; nor do any other related instruments suggest its inclusion. Thus, including an online libel provision in the local cybercrime law is inconsistent with the treaty after which the cybercrime law is modeled.

Libel has been repeatedly utilized in practice as a weapon to harass journalists or stifle dissent in the Philippines.[22] Ressa's recent arrest is a concrete example of how online libel may be abused. In her case, the National Bureau of Investigation (NBI)

floated the idea of "continuing publication" in the internet as basis to persecute individuals who may have written stories even before the passage of the cybercrime law,[23] violating the principle of non-retroactivity of criminal laws.

As it is, the Philippines is the most dangerous country for journalists in Asia.[24] The 2018 Freedom on the Net Report describes the country as "partly free" (scoring 31/100) in terms of internet freedom, obstacles to access, content limits, and violations of users' rights.[25] While freedom of speech, expression, and the press is protected in the Bill of Rights[26] and international instruments to which the Philippines is a party,[27] State practice and unilateral declarations—especially by a sitting president hostile to the press[28]—have promoted a chilling effect among journalists all over the country,[29] no doubt exacerbated by the now-higher penalty for libel committed online.

These recent events highlighted the need to review libel laws, viewed by journalists to be excessive, outdated, and prone to abuse.[30] However, while journalists have lobbied for decades for the decriminalization of libel, they have been generally ignored by Congress.[31] Even now, efforts to amend the cybercrime law are not the priority for legislators, and decriminalizing libel has never been mentioned in the president's State of the Nation Address.[32] The most significant development thus far is UNHRC's communication in 2012 that the criminal sanction for libel is too excessive, violating the Philippines' obligations under Art. 19 of the ICCPR.[33]

Related to online libel is the rule on cyberwarrants, which is applicable to all cybercrime cases. Content posted online may easily be gathered as evidence without a cyberwarrant if these are posted without a "reasonable expectation of privacy"[34]—as stated by the Supreme Court—thus facilitating evidence-gathering for online libel cases.[35] Be that as it may, only a small portion of online libel cases reach the courts, because of the difficulty of attributing identities of offenders who post anonymously online.[36]
To emphasize, this is not to say that libel should go unpunished, but only that the penalty of imprisonment is excessive.

A dissenting Supreme Court justice has stated that a review of the "history and actual use of criminal libel"—perhaps implying its role in the harassment of individuals— should result in a declaration of its unconstitutionality, both in the Revised Penal Code and the cybercrime law:

> "We have to acknowledge the real uses of criminal libel if we are to be consistent to protect speech made to make public officers and government accountable. Criminal libel has an in terrorem effect that is inconsistent with the contemporary protection of the primordial and necessary right of expression enshrined in our Constitution."[37]

Cybersex

Cybersex is a content-related offense under the cybercrime law. It's defined as "[t]he willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration."[38] The same definition appears in the implementing rules.

The government justifies the provision as a way to address cyber prostitution, white slave trade, and pornography for consideration.[39] Even as various agencies, both local and transnational, battle these crimes, the country has been described as the "epicenter" and "regional hub" of cybersex trafficking rings, with 80 percent of victims being minors.[40]

After advocates challenged the law in 2014, the Supreme Court upheld the cybersex provision "where it stands a construction that makes it apply only to persons engaged in the business of maintaining, controlling, or operating, directly or indirectly, the lascivious exhibition of sexual organs or sexual activity with the aid of a computer system as Congress has intended." To come up with this statement, however, the Court heavily relied on the bicameral committee deliberations to clarify what cybersex supposedly covers, despite the definition's plain meaning.

A straightforward reading of the cybersex definition in the law reveals vagueness and overbreadth—for one, the word 'willful' may not consider that persons involved in cybersex are most often unwilling victims of exploitation.[41] It fails to define "lascivious exhibition," "sexual organ," or "sexual activity," and fails to clarify whether works of art may fall under the category of cybersex.[42] The wording, according to a dissenting Supreme Court justice, may "empower law enforcers to pass off their very personal standards of their own morality."[43]

The majority decision also too readily invoked the State's power to regulate pornographic materials, without considering possible violations of free speech not

only under international standards, but more so in the Philippine Constitution. Previous court decisions had laid out a "strict scrutiny" test for content-based restrictions like cybersex, a matter that the Supreme Court did not even discuss.

Outside of the Supreme Court's decision, concerned groups stated that the provision endangers women's rights as it perpetuates violence against women.[44] A 2015 study also found that legislating cybersex as a crime fails to answer questions of consent and nuance, as when cybersex turns into a meaningful relationship, or when workers use cybersex to provide for their economic needs.[45]

Cybersex has been described as "affective labor," one that may be read "as a symptom of the ineffectiveness of ICT-driven development."[46] The study further states that "[i]n casting cybersex as cybercrime, the State seems to evade the more fundamental problem of social exclusion that has brought about the informal economy of cybersex in the first place."[47]

Criminalizing cybersex also fails to account for existing legislation regarding online sexual trafficking, prostitution, and anti-voyeurism, and how such legislation may aggravate the effects of the cybercrime provision against women. Cybersex as a crime overlaps with that of online trafficking and prostitution, and in this respect may even be redundant. With regard to anti-voyeurism, women who file a case against voyeurism may unwittingly admit to committing cybersex.[48]

If one thinks about it, the ordinary meaning of cybersex is sexual activity mediated via a computer system. Based on a layman's definition, cybersex then should not be referred to as a crime, as it may cover intimate relationships between consenting individuals. Criminalizing cybersex is tantamount to legislating sexual behavior,[49] one that throws us back as a society into the dark ages.[50]

The Supreme Court's clarification that the crime of cybersex is only applicable to "persons engaged in business" does not provide ample reassurance against misinterpretations and misuses of the law, especially for ordinary citizens. The provision does not speak for itself, and therefore may be subject to abuse.[51]

The provision also fails to consider issues of anonymity, affirmation, and the fluidity of online identity in the modern world—how technology allows people to move beyond usual social markers of class, ethnicity, gender, and age, among others, and how technology fulfils a need to express oneself online, as an alternative to

oppressive offline spaces. This is true especially for marginalized peoples such as members of the LGBTQIA+ sector, or persons with disabilities. [52]

Collection of computer data

In 2014, the Supreme Court nullified the cybercrime law's provision on real-time collection of traffic data. The provision previously authorized law enforcement agencies to collect traffic data with due cause, referring to traffic data as those that "refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities." The repealed provision provided that other kinds of data require a warrant.[53]

According to the Supreme Court:

> "The authority that Section 12 gives law enforcement agencies is too sweeping and lacks restraint. While it says that traffic data collection should not disclose identities or content data, such restraint is but an illusion. Admittedly, nothing can prevent law enforcement agencies holding these data in their hands from looking into the identity of their sender or receiver and what the data contains. This will unnecessarily expose the citizenry to leaked information or, worse, to extortion from certain bad elements in these agencies."[54]

However, the issuance of the implementing rules in 2015 carried with it a new and more dangerous provision, one that could not have been challenged by critics in 2012 or ruled upon by the Supreme Court in 2014 because it was never there to begin with.[55] Sec. 13 of the implementing rules now states that law enforcement authorities are authorized, upon the issuance of a court warrant, to collect or record "computer data that are associated with specific communications transmitted by means of a computer system." Service providers are mandated to cooperate in such collection or recording.[56]

"Computer data" in the implementing rules is an overbroad term that encompasses all sorts of data, as seen in the comparisons of definitions below:

Traffic data	Content data	Computer data
Cybercrime Prevention Act: "Any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service."	Implementing rules: "Refers to the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data."	Cybercrime Prevention Act: "Any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online."

In the context of these three types of data—computer, content, and traffic data—the provision in the implementing rules is problematic and sweepingly intrudes on the privacy of persons without clear limitations.

First, allowing the collection of "computer data" in the implementing rules despite the silence of the law on that specific term violates the Constitution. Implementing rules are only effective in so far as they do not contravene or add to the law implemented; the spring cannot rise higher than the source. In essence, while Sec. 13 did provide the requirement of a court order before authorizing computer data collection, it unduly expanded on its object by referring not to "traffic data" or "content data," but anything that might come within the scope of "computer data," an all-encompassing-term with a high potential for abuse.

This implementing rule on collection of computer data also multiplies exponentially the crimes that may now be subject to government surveillance, beyond existing laws. The Anti-Wiretapping Law (Republic Act 4200) and the Human Security Act (Republic Act 9372), for example, provide exceptions to the prohibition against communications surveillance, in cases of crimes against national security. But the rules now make government surveillance applicable virtually to all crimes in the Revised Penal Code and in the cybercrime law.[57]

Allowing computer data collection under Sec. 13 of the implementing rules—notwithstanding its apparent unconstitutionality— may also raise questions on the application of the Data Privacy Act (Republic Act 10173), which was already effec-

tive a few years before the implementing rules were drafted.

Data privacy and human resource officers, for example, grapple with the obligation to protect personal and sensitive information under the Data Privacy Act, along with the duty to comply with requests for information from law enforcement authorities investigating a suspected criminal.[58]

It is not clear whether personal, sensitive, proprietary, or other kinds of information are exceptions to collection of computer data, even though a reading of the Data Privacy Act should lead to that conclusion. Computer data may even include both traffic data or content data, both of which, by themselves, may disclose the identities of individuals in violation of the Data Privacy Act.

Further, the power of computer data collection, granted to law enforcement agencies by a mere implementing rule, does not bode well for the lack of accountability mechanisms in intelligence agencies in the Philippines. Several bills have been filed in 2010 and 2013 to oversee their mandate and activities, but were never passed into law.[59] There are no clear monitoring mechanisms or bodies outlined in the cybercrime law or the rules.

The Supreme Court's Rule on Cybercrime Warrants,[60] which took effect on Aug. 2018, provided a procedure for the handling of "computer data" in the implementing rules. The rule on cyberwarrants enumerated four distinct types of cyberwarrants, each limiting specific actions related to data collection, thus:

1. Preservation warrant, for the preservation of computer data usually while authorities secure a disclosure warrant
2. Disclosure warrant, for the disclosure of a subscriber's data, including network and traffic data
3. Interception warrant, for activities such listening recording, monitoring, and surveillance of computer data
4. Search, seizure, and examination warrant, for the search, seizure, and examination of computer data

Among many others, the rule on cyberwarrants delineated the purposes of each warrant, their prerequisites, the periods of their validity, as well as provisions for data return. The rule also provided a process for the destruction of data.

While the rule above delineated a clear process by which to handle computer data, it remains that "computer data" is still the term used to refer to the data collected. Nonetheless, in determining what safeguards should be available and what changes should be made to the law's implementing rules, the rule on cyberwarrants and the judiciary's own rule-making power are relevant, since such procedural rule was issued following the effectivity of the Act and the implementing rules.[61]

Policy recommendations

Striking a balance between fighting criminal activity and respecting human rights is a continuing goal of the global regime on cybercrime—a goal that takes on a more significant meaning since the Council of Europe, which adopted the Budapest Convention on Cybercrime, is an active promoter of human rights.[62]

Notably, the Budapest Convention contains in its Art. 15 conditions and safeguards in the implementation of measures against cybercrime. These are:

- Respect for human rights,
- The principle of proportionality,
- Judicial or other independent supervision,
- Grounds justifying application,
- Limitation of the scope and the duration of such power or procedure, and
- The impact on rights, responsibilities and legitimate interests of third parties.

In this context, the following recommendations are made to legislators, enforcement agencies, and other policy officers in the Philippines, as well as to the groups advocating for amendments to the cybercrime law:

On online libel

1. Decriminalize libel, rendering offenders only liable for damages under civil law.

The cybercrime law has a catch-all provision that makes all crimes in the Revised Penal Code a "cybercrime" if committed through a computer

system. Thus, amending the cybercrime law to delete the online libel provision is not enough; libel itself in the penal code must be decriminalized.

This does not mean libel must go unpunished and that the rights of individuals cannot be balanced with press freedom—only that imprisonment should not be a penalty. Since "imprisonment is never an appropriate penalty" for libel, offenders should be made liable only for damages, which should also be subject to "reasonable limits."[63]

While lobbying for the decriminalization of libel does not seem feasible for the apparent lack of allies in the Philippine Congress, it may still be worth it to bring the matter to a legislator to raise and sustain awareness on the issue. There were pending bills to decriminalize libel in the previous Congress—the way forward may be to raise awareness on these previous efforts and rejuvenate public interest on decriminalization.

2. Strengthen legal mechanisms to protect journalists, writers, and editors from harassment due to libel suits.

Truth should be an absolute defense in libel, and not merely a condition to lift the presumption of malice on the offender. Public interest should also be considered a defense.[64] The lack of defenses available for journalists, writers, and editors unduly tilt the balance of power in favor of individuals with resources to litigate, and who, under the present legal framework and existing political context, use libel suits as weapons in silencing critics.

3. Explore the potential of litigation to develop a consensus that libel should not be penalized.

While shaping policymaking processes should be directed to legislators and executive officials, court decisions by the judiciary also influence law and policy. "Low profile" libel cases filed in court may hold potential at shaping the legal framework of online libel, as opposed to high-profile cases, such as the Maria Ressa case. Since "low profile" libel cases are less politically sensitive, this gives more opportunity for the courts to hand down decisions that are protective of civil liberties.

Legislators and policymakers may be persuaded, for example, by the Supreme Court's "Guidelines in the Observance of a Rule of Preference in the Imposition of Penalties in Libel Cases,"[65] issued in 2008 by former Chief Justice Reynato Puno. The circular, while recognizing the penalty of imprisonment for libel, cites several cases where courts opted to impose only a fine for persons convicted of the crime. In no uncertain terms, the Supreme Court recognized that "the foregoing cases indicate an emergent rule of preference for the imposition of fine only rather than imprisonment in libel cases under the circumstances therein specified."

4. Expand discussions on libel beyond highly politicized cases and the media community.

Popular libel cases in the Philippines usually involve journalists and newsrooms, which means discussions about it are usually limited to the media community and related groups. However, libel may be committed by anyone; especially in a country crazy about posting on social media, everyone is put at higher risk. It is in this context that public awareness on the criminalization of libel should start. Such discussions should be inclusive and go beyond the media and academic community, consider the viewpoint of ordinary individuals about libel, and emphasize the harshness of its criminalization vis-à-vis the gravity of harm done to the public.

On cybersex

1. Repeal the provision on cybersex in the law, and remove it from the implementing rules.

The reasons for including cybersex as a crime in the Cybercrime Prevention Act are not compelling enough to warrant its criminalization. Current laws already punish the business of sexual trafficking.

Further, existing data on the number of cases prosecuted and filed as cybersex under the Cybercrime Prevention Act also seem to be non-existent, as these cases are considered as trafficking in persons cases monitored by the Inter-Agency Council Against Trafficking.[66] This implies that the provision on cybersex is a useless appendage to the cybercrime law.

2. Improve implementation of already existing laws protecting women from exploitation on the internet, and continue lobbying for progressive laws protecting women.

Laws already exist to address violence against women in the Philippines, extending to violence perpetuated online. Relevantly, all crimes under the penal code and special laws, when committed via ICT, are already covered by the catch-all provision in the cybercrime law.

These include the Anti-Violence in Women and Children Act (Republic Act 9262); Anti-Trafficking in Persons Act (Republic Act 9208); Anti-Photo and Video Voyeurism Act (Republic Act 9995); and the Anti-Child Pornography Act (Republic Act 9775), among others. The challenge lies with implementation. Bodies tasked to monitor the implementation of these laws, such as the Inter-Agency Council on Human Trafficking, need to fulfill their mandate more effectively when it comes to the violations of these laws via a computer system.

In this respect, members of Congress have also recently filed two key laws that need sustained support: one about electronic violence against women and children (House Bill 479), and another on amendments to the anti-rape law (House Bill 480), which will enhance prosecution of cases of online gender-based violence.

At the same time, there is also a need to revisit laws that discriminate on women in the Revised Penal Code. One of them is the provision that limits prostitution only to women.[67] Another is the disparity between adultery and concubinage, which is prejudicial against women.

3. Intensify efforts to educate women, children, and other marginalized communities on laws and policies that protect them against exploitation, and prioritize economic empowerment to lessen reliance on sex work.

Whether cybersex is decriminalized or not, educational and economic empowerment efforts directed to sectors most prone to gender-based violence should be emphasized and sustained. More members of margin-

alized communities must be made aware of the risks of exploitation and legal remedies available against online trafficking or child pornography. Underlying this is the need to cut through the problem of poverty and the need for a stable source of income outside of sex work, as it should not be the only option, or an option at all, for women and members of the LGBTQIA+ sector in the absence of other economic opportunities.

4. Explore the possibility of clarifying the definition of cybersex in the implementing rules.

In the event that lobbying for the repeal of cybersex is not feasible, another option is to engage executive officials on the possibility of amending the implementing rules to clarify the definition and scope of cybersex in the law. However, caution should be taken in this approach, so as not to further confuse the definition or cause a revision that still does not work for the benefit of women and other marginalized sectors.

On real-time collection of computer data

1. Remove or clarify Sec. 13 of the implementing rules and regulations regarding real-time collection of computer data.

Sec. 13 of the implementing rules, authorizing the collection and recording of computer data, never existed in the law. An implementing rule cannot go beyond the law it supposedly implements—thus, Sec. 13 is null and void at the outset, and must be removed or at least revised as to comply with the law and harmonize with the judiciary's rule on cyberwarrants. Further, the Department of Justice must exert efforts to issue new rules that do not go beyond what the cybercrime law prescribes. Consistent with the Budapest Convention, any new rules issued must be sufficiently limited in scope and duration and provide reasonable grounds for application, aside from providing judicial supervision.

2. Strengthen monitoring mechanisms of the cybercrime law to guard against abuse.

Both the law and the implementing rules do not contain detailed mechanisms for monitoring the implementation of the law, but merely assign

monitoring responsibilities to the Cybercrime Investigation and Coordinating Center (CICC) and the DOJ. The CICC is merely tasked to monitor cybercrime cases handled by participating law enforcement and prosecution agencies, while the DOJ receives "timely and regular reports on pre-operation, post-operation, and investigation results," as well as other documents from the PNP and the NBI.

There needs to be clearer, more definite, and separate accountability bodies, mechanisms, and standards by which individuals can assess and check for abuses in the implementation of the cybercrime law, defined and outlined in the rules. Monitoring should go beyond reporting the number or incidence of cybercrime complaints or activities performed, but must also include insight on successes and roadblocks in implementation, specific outcomes, lessons and mistakes made, adaptive measures used to address constraints, and concrete efforts undertaken to balance anti-cybercrime operations with respect for human rights. Meanwhile, bodies formed to monitor the implementation of the cybercrime law must have clearly-delineated responsibilities to avoid gaps in accountability.

3. Prioritize a rights-based approach in discussing the implications of data collection under the implementing rules.

Protecting data collected under Sec. 13 of the implementing rules is everyone's concern, and not just of privacy rights advocates. From cellphone signal blocking to unwarranted disclosure of employee information, anyone is at risk of abuses of authority when data is illegally collected. A rights-based approach—emphasizing what individuals can do or what remedy they have in specific cases when their data is not secured or handled properly—can be more productive in terms of simplifying the implications of Sec. 13 of the implementing rules.

4. Explore the possibility of acceding to an international treaty on data privacy and protection, such as the Council of Europe's Convention 108+ (Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data).

Neither the cybercrime law nor its implementing rules adopted the human rights safeguards of the Budapest Convention. Aside from engaging

policy officials and implementing officers to include such safeguards in the actual law and rules, it is also worth suggesting that the Philippines should be a party to the Council of Europe's Convention 108+, which mandates countries to provide additional safeguards for personal data protection. As of now, the Philippines is only an observer to the Convention.

Endnotes

1 John Nery. "Assault on Press Freedom? Q &A," Inquirer.net, Feb. 19, 2019, https://opinion.inquirer.net/119650/assault-on-press-freedom-q-and-a#ixzz5idD2todQ
2 "Freedom on the Net 2018: Philippines," Freedom House, https://freedomhouse.org/report/freedom-net/2018/ philippines
3 "Dev't network facing e-libel raps files bail," Philippine Misereor Partnership, Inc., June 13, 2016, http://www.pmpi.org.ph/projects/anti-mining-campaign/298-pmpi-4-e-libel-case-update-2
4 "Pooled editorial | Overcome cyber martial law," Bulatlat, Mar. 12, 2019, https://www.bulatlat.com/2019/03/12/pooled-editorial-overcome-cyber-martial-law/
5 Tetch Torres, "Bayan files petition vs anti-cybercrime law," Inquirer.net, Oct. 1, 2012, https://technology.inquirer.net/17596/bayan-files-petition-vs-anti-cybercrime-law
6 "Journalists reiterate call to decriminalize libel," PhilStar.com, Feb. 18, 2019, https://www.philstar.com/headlines/2019/02/18/ 1894716/journalists-reiterate-call-decriminalize-libel
7 Kateřina Fialová, "Philippines: The Problematic Cybercrime Prevention Law of 2012," GenderIT.org, Oct. 8, 2012, https://www.genderit.org/articles/philippines-problematic-cybercrime-prevention-law-2012
8 Zahid Jamil, "Cybercrime Model Laws: A discussion paper presented for the Cybercrime Convention Committee," Project Cybercrime @Octopus, Council of Europe, Dec. 9, 2014, https://rm.coe.int/1680303ee1
9 Ibid.
10 Jamael Jacob, "Commentary: The IRR of RA 10175," Foundation for Media Alternatives, June 16, 2016, https://www.fma.ph/ 2016/06/16/commentary-the-irr-of-ra-10175/
11 Dona Z. Pazzibugan, "Philippines now haven for transnational cybercrime groups – police," Inquirer.net, Oct. 23, 2011, https://globalnation.inquirer.net/16203/philippines-now-haven-for-transnational-cyber-crime-groups
12 "2016-2017: Philippine Cybercrime Report," Department of Justice Office of Cybercrime, May 2017, https://doj.gov.ph//files/OOC/ooc_report_corrected.pdf
13 "Philippines joins the Budapest Convention," Council of Europe, Apr. 6, 2018, https://www.coe.int/en/web/cybercrime/-/philippines-joins-the-budapest-convention
14 "New Criminal Code of the Philippines," Senate of the Philippines: 17th Congress, filed Oct. 27, 2016, https://www.senate.gov.ph/lis/bill_res.aspx?congress=17&q=SBN-1227
15 Sec. 4(c)[4], Republic Act 10175, An Act Defining Cybercrime, Providing for the Prevention, Investigation, and Suppression and Imposition of Penalties Therefor and Other Purposes [RA 10175].
16 Art. 353, Revised Penal Code of the Philippines [RPC].
17 Sec. 6, RA 10175.
18 Art. 353, RPC.
19 Disini v. Secretary of Justice, G.R. No. 203335, Feb. 18, 2014, http://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/56650
20 Alexander Adonis v. The Philippines, Communication No. 1815/2008, U.N. Doc. CCPR/C/103/D/1815/2008/Rev.1 (2012), http://hrlibrary.umn.edu/undocs/1815-2008.html
21 UN Human Rights Committee, General Comment No. 34 to Art. 19 of the ICCPR, Sept. 12, 2011, https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf
22 "Criminal Libel Suits Against Journalists," Center for Media Freedom and Responsibility, Apr. 10, 2016, https://cmfr-phil.org/press-freedom-protection/press-freedom/criminal-libel-suits-against-journalists/
23 "FAQs: What you need to know about Rappler's cyber libel case," Rappler, updated Feb. 19, 2019, https://www.rappler.com/about-rappler/about-us/223545-frequently-asked-questions-cyber-libel-case
24 Raul Dancel, "Philippines: Most dangerous place for journalists in Asia," The Straits Times, Nov. 2, 2018, https://www.straitstimes.com/asia/se-asia/most-dangerous-place-for-journalists-in-asia
25 "Freedom on the Net 2018: Philippines," supra note 2.
26 Sec. 4, Art. III, 1987 Constitution of the Philippines.
27 See, e.g., Art. 19 of the International Convention on Civil and Political Rights [ICCPR], Art. 19 of the UN Declaration on Human Rights [UNDHR].
28 Florence Peschke, "Journalists still under pressure in Duterte's Philippines," International Press Institute, Feb. 10, 2017, https://ipi.media/journalists-still-under-pressure-in-dutertes-philippines/
29 "STATEMENT | NUJP condemns Duterte's red-tagging of journalists," Interaksyon, Dec. 24, 2017, http://www.interaksyon.com/breaking-news/2017/12/24/114467/statement-nujp-condemns-dutertes-red-tagging-of-journalists/
30 Foundation for Media Alternatives [FMA] stakeholder consultation on online libel, 24 May 2019.
31 "Persecution of Rappler underscores need to decriminalize libel NOW," National Union of Journalists in the Philippines, Feb. 18, 2019, https://nujp.org/statement/persecution-of-rappler-underscores-need-to-decriminalize-libel-now/
32 FMA stakeholder consultation on online libel, 24 May 2019.

33 "Decriminalizing libel: UN declares PH libel law 'excessive,'" Center for Media Freedom and Responsibility, Feb. 7, 2012, https://cmfr-phil.org/press-freedom-protection/press-freedom/decriminalizing-libel-un-declares-ph-libel-law-excessive/
34 Vivares v. St. Theresa's College, G.R. No. 202666, 29 September 2014, http://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/57754
35 FMA stakeholder consultation on online libel, 24 May 2019.
36 Ibid.
37 Disini v. Secretary of Justice, G.R. No. 203335, Feb. 18, 2014, Dissenting and Concurring Opinion (Leonen, J.), http://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/56650
38 Sec. 4(c)[1], RA 10175.
39 "Disini v. Secretary of Justice, supra note 19.
40 "Cybersex ops still prevalent on PH; 80 pct of victims are minors," ABS-CBN News, Feb. 22, 2019, https://news.abs-cbn.com/spotlight/02/22/19/cybersex-ops-still-prevalent-in-ph-80-pct-of-victims-are-minors
41 Liat Clark, "Philippines passes law that criminalises cybersex," Wired, Sept. 20, 2012, https://www.wired.co.uk/article/philippines-cyber-crimes-act
42 Foundation for Media Alternatives, "Human Rights and the Philippine Digital Environment: Joint Submission to the Universal Periodic Review of the Philippines," Association for Progressive Communications, Sept. 2016, https://www.apc.org/sites/default/files/UPR_FMA.pdf
43 Disini v. Secretary of Justice, supra note 19.
44 Women's Legal and Human Rights Bureau, "Delete, Undo, Retrieve: Statement on the Cybercrime Prevention Act of 2012," GenderIT.org, Oct. 10, 2012, https://www.genderit.org/feminist-talk/delete-undo-retrieve-statement-cybercrime-prevention-act-2012
45 E.M Cruz & T.J. Sajo (2015) "Cybersex as Affective Labour: Critical Interrogations of the Philippine ICT Framework and the Cybercrime Prevention Act of 2012." In: Chib A., May J., Barrantes R. (eds.), Impact of Information Society Research in the Global South. Springer, Singapore.
46 Ibid.
47 Ibid.
48 FMA stakeholder consultation on cybersex, 7 June 2019.
49 Ibid.
50 Disini v. Secretary of Justice (Dissenting and Concurring Opinion), Leonen, J. supra note 37.
51 FMA stakeholder consultation on cybersex, 7 June 2019.
52 Ibid.
53 Sec. 12, RA 10175.
54 Disini v. Secretary of Justice, supra note 19.
55 Jamael Jacob, supra note 10.
56 Sec. 13, Implementing Rules and Regulations, RA 10175.
57 Jamael Jacob, supra note 10.
58 FMA stakeholder consultation on collection of computer data, 21 June 2019.
59 Foundation for Media Alternatives, supra note 42.
60 Rule on Cybercrime Warrants, Supreme Court of the Philippines, http://sc.judiciary.gov.ph/1420/
61 FMA stakeholder consultation on collection of computer data, 21 June 2019.
62 Jovan Kurbalija, An Introduction to Internet Governance, 6th ed., DipLo Foundation (2014), p. 103.
63 UN Human Rights Committee, supra note 21.
64 Ibid.
65 Administrative Circular No. 08-2008, "Guidelines in the Observance of a Rule of Preference in the Imposition of Penalties in Libel Cases," Supreme Court, https://www.lawphil.net/courts/supreme/ac/ac_8_2008.html
66 "The number of cases filed and prosecuted under cybersex and child pornography offenses," eFOI request by Elinor May Cruz to the Department of Justice, 10 June 2019, https://www.foi.gov.ph/requests/aglzfmVmb-2ktcGhyHQsSBoNvbnRlbnQiEERPSioyOTgxODA4MzIxMjAM
67 FMA stakeholder consultation on online libel, 21 June 2019.

Foundation for Media Alternatives

Foundation for Media Alternatives
Unit 203 CRM Building III, 106 Kamias Road, East Kamias
1102, Quezon City
T. (632) 7753 5584
E. info@fma.ph