“Cybercrime, Defamation and Democracy: An International Litigation Strategy”

Kasey Clarke and Julia Peoples

I. Introduction

The COVID-19 pandemic brought about a new era of our digital lives. Work, education, and socialization moved online, as did political protest. Many social movements temporarily stalled, but many others adapted, broadening their reach by organizing online.[1] Pandemics are often followed by periods of social and political unrest, and this pandemic is no exception.[2] Globally, authoritarianism and nationalism are on the rise.[3] The International Press Institute has found over 675 press freedom violations linked to the pandemic, in the form of legal action and verbal or physical harassment.[4] Increased reliance on technology post-pandemic makes digital rights an essential part of protecting global freedom of expression. But, as internet freedoms have declined for over a decade, and authoritarian leaders seize the opportunity to enforce new restrictions online, human rights are at risk.[5]

Governments seeking to consolidate power over their citizenry predictably “embraced [the pandemic as a] pretext to enhance censorship.”[6] The preferred method of increasing internet content control sees governments strengthen civil and criminal penalties of existing defamation laws, enact cyber libel laws, and pass cybercrime legislation with unassuming provisions used broadly to police online speech.[7] A recent and rapid “surge in cybercrime laws around the world,” has been accompanied by the use of cyber libel provisions and the like to prosecute journalists, media organizations, bloggers, lawyers, and

---

[1] Samantha Kiernan et al., *Pandemic Protests: When Unrest and Instability Go Viral*, Think Global Health (July 28, 2021), https://www.thinkglobalhealth.org/article/pandemic-protests-when-unrest-and-instability-go-viral.
[2] Kashmira Gander, *History Tells Us Epidemics Are Followed by Huge Civil Unrest for These Three Reasons*, Newsweek (Sept. 7, 2020, 8:14 AM), https://www.newsweek.com/history-epidemics-pandemic-civil-unrest-reasons-1530055.
[3] Sarah Repucci & Amy Slipowitz, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*, Freedom House (Feb. 2022).
[4] *IPI News and Data Hub*, International Press Institute (last visited Jul. 14, 2022), https://ipi.media/hub/?topic=covid-19&search=&language=0&country=0&years=0&.
[5] Press Release, Freedom House, Report: Global Internet Freedom Declines in Shadow of Pandemic (Oct. 14, 2020), https://freedomhouse.org/article/report-global-internet-freedom-declines-shadow-pandemic
[6] Mikhail Khordokovsky, *Russia’s great export: hostility to the free press*, 50 Index on Censorship 3, 82-3 (2021).
[7] *See, e.g.,* Claudia Ciobanu, *Poland’s Ruling Party Abuses Insult and Defamation Laws*, Reporting Democracy (Apr. 27, 2021, 7:11 AM), https://balkaninsight.com/2021/04/27/polands-ruling-party-abuses-insult-and-defamation laws/. Polish government increasingly punishing internet posters through assumed to be obsolete provisions of the penal code, with increased penalty for defamatory statements published in mass media; Jessie Yeung et al., *Japan makes ‘online insults’ punishable by one year in prison in wake of reality TV star’s death* , CNN (June 14, 2022, 1:24 AM), https://www.cnn.com/2022/06/14/asia/japan-cyberbullying-law-intl-hnk-scli/index.html. Japanese government criminalized “online insults,” punishable by imprisonment or heavy fine.; Simone Toussi, *New Mali Cybercrime Law Potentially Problematic to Digital Rights*, CIPESA (Feb. 21, 2020), https://cipesa.org/2020/02/new-mali cybercrime-law-potentially-problematic-to-digital-rights/. The government of Mali enacted a cybercrime law targeting illegal access, data interference, child pornography, and other legitimate aims of cybercrime legislation, with provisions punishing online insults by up to ten years in prison or a heavy fine.

political dissidents of all forms.[8] These mechanisms criminalize and silence political opposition, creating a chilling effect on political speech and endangering freedom of expression. This paper will present a powerful and effective countermeasure to the regime of repressive cyber libel laws and the prosecutions thereunder. Briefly stated, the countermeasure consists of a defense to the prosecution by arguing as follows:

- Article 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantees all citizens broad rights of freedom of expression.
- Article 10 of the European Convention on Human Rights (ECHR) also guarantees broad protection of the right of freedom of expression, in similar language to the ICCPR.
- The case law of the European Court of Human Rights (ECtHR) has issued over 1,000 judgments that affirmed and greatly expanded freedom of expression, including heighted protection for political speech.
- That case law represents statements of international norms protecting freedom of expression.
- The text of ICCPR Article 19 so mirrors the text of ECHR Article 10 that the case law of Article 10 and the statements of international norms protecting freedom of expression effectively interprets and applies ICCPR Article 19.
- In the name of freedom of expression, that case law bars prosecutions for criminal libel which threaten imprisonment and/or heavy fines. Prison/heavy fines are not "necessary in a democratic society" or "proportionate."[9]
- Country X ratified and is bound by ICCPR Article 19.
- If Country X threatens to punish a defendant for criminal libel with imprisonment and/or heavy fine, it will violate its treaty obligations under the ICCPR.
- The government must prove that such a law is necessary, in a democratic society, proportionate and the least intrusive limitation on freedom of expression.

This countermeasure strategy has proven successful in a number of cases in the Middle East and North Africa. The International Senior Lawyers Project (ISLP), a non-governmental organization has submitted amicus briefs following this strategy in freedom of expression cases regarding imprisoned journalists. In every case charges have been dropped and the defendant released.

II. Cyber Libel Laws

A. Criminalization at Odds With International Norms on Freedom of Expression

Increasingly broad defamation, cybercrime, and cyber libel provisions threaten freedom of expression by legitimizing judicial harassment of journalists, bloggers, media outlets, political dissidents, and citizens. Overinclusive cybercrime laws have empowered governments to stifle free speech and opposition. Media control through increased penalties for online defamation mirrors decades of autocratic efforts to evade international norms and "protect and entrench power when direct repression is not a viable option."[10] These regimes utilize vague and ambiguous language to grant broad authority to the government to

[8] Deborah Brown, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, Human Rights Watch (Aug. 13, 2021, 12:55 PM), https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.
[9] Handyside v. UK, 5493/72 Eur. Ct. H.R. (1976).
[10] Ozan O. Varol, *Stealth Authoritarianism*, 100 Iowa L. Rev 1673, 1678 (2015).

"curtail[...] the public's ability to monitor and sanction government policies" through perceptually justified mechanisms.[11] In recent years, the number of cybercrime laws enacted has increased dramatically. Lacking meaningful limits, these laws threaten freedom of expression and "open [...] the door to punishing and surveilling activists and protesters in many countries around the world."[12]

Worldwide, the definition and procedure of defamation varies, but international norms resoundingly disapprove of criminal penalties for defamation. International treaties reconcile the tension between a right to freedom of expression and protection of privacy and reputation through international defamation standards.[13] These treaties generally require that a defamatory statement be untrue, damages be recoverable through civil courts in reasonable amounts, and heightened scrutiny be applied for statements regarding politics, public figures, and government officials.[14] Human rights organizations and international courts, including the European Court of Human Rights, have "repeatedly found applications of criminal defamation laws to disproportionately restrict free expression."[15] The African Court of Human and Peoples' Rights has also ruled on the issue, holding that, absent "exceptional circumstances," criminal charges for libel "are disproportionate responses that therefore violate freedom of expression."[16] Civil remedies that are "excessively punitive" have also been found to violate international norms regarding freedom of expression.[17] Despite international law requiring limitations on restricting political speech, autocracies around the world have consistently abused existing defamation laws and increasingly enacted additional penalties for statements posted online.

B. Laws and Provisions

Cyber libel laws take several forms. Some countries have enacted laws directly penalizing cyber libel, while others have used broader cybercrime legislation to give existing defamation laws new applications online. Increased libel legislation has been accompanied by a widespread increase in the use of intimidation lawsuits to silence activists and NGOs.[18] Wealthy and powerful individuals have employed Strategic Lawsuits Against Public Participation, known as SLAPPs, to intimidate and exhaust the resources of their critics. When used transnationally, SLAPPs allow forum shopping for the most plaintiff-friendly defamation laws.[19] Media freedoms are also impacted by disinformation laws, which compliment cyber libel laws by offering alternate routes to prosecute online communications and justify internet shutdowns. Disinformation laws have been used to detain journalists whose reports conflict with

---

[11] *Id.* at 1684.
[12] Clément Nyaletsossi Voule (Special Rapporteur on the rights to freedom of peaceful assembly and of association), *Rep. on the rights to freedom of peaceful assembly and of association*, 2, U.N. Doc. A/HRC/41/41(July 12, 2019).
[13] *See*, International Covenant on Civil and Political Rights (ICCPR) art. 19, art. 17, Dec. 16, 1966, T.I.A.S. 92-908, 999 U.N.T.S. 171; European Convention on Human Rights (ECHR) art. 10, Nov. 4, 1950, E.T.S. No. 005.
[14] Gen. Comment no. 34 on Art. 19, UN Hum. Rts. Comm., U.N. Doc. CCPR/C/GC/34, at 12 (Sept. 12, 2011).
[15] Sarah Shirazyan et al., *How to Reconcile International Human Rights Law and Criminalization of Online Speech: Violent Extremism, Misinformation, Defamation, and Cyberharassment*, Stan. L. Sch. L. and Pol'y Lab, 29 (2020).
[16] *Id.* at 221; Lohé Issa Konaté v. Burk. Faso, App. No. 004/2013, Decision, African Court on Human and Peoples' Rights [Afr. Ct. H.P.R.] ¶¶ 158-164 (Dec. 5, 2014), https://www.african-court.org/en/images/Cases/Judgment/Judgment%20Appl.004-2013%20Lohe%20Issa%20Konate%20v%20Burkina%20Faso%20-English.pdf.
[17] Gen. Comment no. 34, *supra* note 14 at 14.
[18] Annalisa Ciampi, (Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association), *Information Note: SLAPPs and FoAA rights*, https://www.ohchr.org/Documents/Issues/FAssociation/InfoNote SLAPPsFoAA.docx (last visited Jul. 15, 2022).
[19] Emeric Prévost, *Liability and jurisdictional issues in online defamation cases*, Eur. Consult. Ass. 6, Doc. No. DGI(2019)04 (2019).

official government statements, restricting freedom of speech under the guise of curbing fake news.[20] The following section surveys some popular mechanisms that enable cyber libel prosecutions.

1. Recent Cybercrime and Defamation Laws

Online insult laws often share a common framework. These laws loosely define offenses, giving the government discretion to punish speech that could undermine public order or offend moral values.[21] They tend to be part of a larger defamation scheme with special provisions for insulting religion or government leaders, or are buried in more general cybercrime legislation that carries increased prison terms or daunting fines.[22] But they are most united by a common effect – their use by authorities to punish dissidents, chill criticism, and remove information from public forums.

The Ugandan Computer Misuse Act was enacted in 2011 to provide for "the safety and security of electronic transactions and information systems," but select provisions have become powerful political tools to silence government critics. Section 25 criminalizes "offensive communications," encompassing any "electronic communication to disturb the peace, quiet, or right of privacy of any person."[23] The penalty is imprisonment for up to one year, a heavy fine, or both. Section 25 is a paradigmatic cyber libel law: broad, vague, and ambiguous. Authorities in Uganda have successfully deployed Section 25 to charge, convict, and imprison, and fine countless journalists, bloggers, and other online dissenters who posted criticism of those authorities.[24]

Russia, a vocal proponent of expanding global cybercrime agreements, punishes cyber libel with imprisonment. One law passed in 2019 subjects those found guilty of spreading fake news or disrespecting the government to substantial fines.[25] Repeat offenders face heightened fines, or up to 15 days in prison. In the first six months following the law's enactment, 45 government insult cases were opened, the majority of which prosecuted social media posts.[26] The following year, amendments to Article 128.1 of Russia's criminal code criminalized "slander in public speech, on the Internet and in the

---

[20] *See*, Daniel Funke & Daniela Flamini, *A guide to anti-misinformation actions around the world*, Poynter, https://www.poynter.org/ifcn/anti-misinformation-actions/ (last visited Jul. 15, 2022). Arrests of journalists and citizens in Bangladesh, Egypt, Indonesia, Myanmar, Rwanda and Thailand under disinformation statutes. In Bangladesh, a photographer was arrested under an anti-propaganda and fake news statute after a protest.

[21] *See, e.g.,* Anti-Cyber Crime Law, Art. 6 (Saudi Arabia).

[22] *See,* Scott Griffen, Int'l Press Inst. (IPI), Defamation and Insult Laws in the OSCE Region: A Comparative Study 6-8 (Barbara Trionfi ed., 2017); Hum. Rts. Watch, *Morocco: Crackdown on Social Media Critics*, (Feb, 5, 2020, 12:00 AM), https://www.hrw.org/news/2020/02/05/morocco-crackdown-social-media-critics; Comm. to Protect Journalists, *Pakistan expands prison terms for online defamation to 5 years*, (Feb. 22, 2022, 3:59 PM), https://cpj.org/2022/02/pakistan-expands-prison-terms-for-online-defamation-to-5-years/.

[23] Computer Misuse Act art. 25, (Uganda).

[24] *See, e.g.,* Unwanted Witness, *Uganda's Internet is increasingly getting controlled and criminalized; Over 25 Internet users are on trial for online expression*, (Jan. 18, 2018), https://www.unwantedwitness.org/ugandas-internet-is-increasingly-getting-controlled-and-criminalized-over-25-internet-users-are-on-trial-for-online-expression/; Hum. Rts. Watch, *Uganda: Ensure Justice for Detained, Tortured Author, Human Rights Watch* (Feb. 11, 2022, 12:00 AM), https://www.hrw.org/news/2022/02/11/uganda-ensure-justice-detained-tortured-author; Hum. Rts. Watch, Trial Observation Report: Uganda vs. Stella Nyanzi 19 (Feb. 16, 2020).

[25] Федеральный закон № 90-ФЗ [Federal Law No. 90-FZ], Официальный интернет-портал правовой информации [Official Internet portal of legal information], 2019, 0001201905010025 (Russ.).

[26] Meduza, *How Russia's law against insulting the government online has been enforced in its first half year*, (Sept. 30 2019, 8:57AM), https://meduza.io/en/short/2019/09/30/how-russia-s-law-against-insulting-the-government-online-has-been-enforced-in-its-first-half-year.

media," with fines and imprisonment and raised the allowable sentence to two years.[27] These laws are instrumental to Russia's efforts to create a sovereign internet under government control.[28]

In the Philippines, the Cybercrime Prevention Act of 2012 was an effective tool to former president Rodrigo Duterte, who used the law to convict vocal critic and Nobel peace laureate Maria Ressa of cyber libel in 2020.[29] The act revised the definition of criminal libel to include libel committed through a computer, and granted broad discretion to Filipino authorities to monitor the internet.[30] The law exemplifies how existing libel laws can be supplemented by cybercrime legislation to expand their scope in online applications. Concerningly, in Ressa's case, charges were brought for statements made before the cybercrime law had passed, because the article had been updated after the legislation took effect.[31] In July 2022, the Court of Appeals upheld the charges against Ressa, the CEO of news website Rappler, and Reynaldo Santos, Jr, the article's author, and lengthened the maximum jail sentence to six years.[32] As Rappler warns, the decision to "extend the shelf life or prescription period of cyber libel to 15 years" would give the government additional discretion to bring claims against its enemies.[33] The potential for the law to apply retroactively to republished content could prove especially chilling to the speech of Filipino citizens, and could set a worrying global trend.

In Poland, officials have revived existing defamation laws as "part of a systemic approach since 2015 to stifle criticism of the government and create a chilling effect on freedom of expression."[34] The government has increased its use of criminal defamation laws to prosecute journalists, activists and dissenters.[35] In a group of cases under *Kurłowicz v. Poland*, the European Court of Human Rights ruled that criminal convictions for defamation violate Article 10 of the European Convention on Human Rights, but Poland has been slow to implement the case decisions, and Article 212 of the Polish Criminal Code, which punishes defamation with up to one year in prison, remains unrevised.[36] Instead, the government is in the process of enacting more problematic legislation, including a draft law that would give the government control over websites content regulation choices.[37]

2. Strategic Litigation Against Public Participation

Cyber libel laws have the potential for abuse not only by local governments, but also by the wealthy and powerful to stifle dissent. SLAPPs have increased exponentially in recent years, primarily due to suits

---

[27] Reuters, *Russian lawmakers vote for jail penalties for online slander* (Dec. 23, 2020, 9:38 AM), https://www.reuters.com/article/us-russia-politics-law-defamation/russian-lawmakers-vote-for-jail-penalties-for-online-slander-id USKBN28X1RX.
[28] Sean S. Costigan, *Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty*, 20 Connections: Q. J. 9, 10 (2021); *See infra* part III.B.
[29] People of the Phil. v. Santos, Ressa and Rappler, Criminal Case, No. R-MNL-19-01141-CR, (June 15, 2020).
[30] Cybercrime Prevention Act, Rep. Act No. 10175 (2012) (Phil.).
[31] People of the Phil. v. Santos, Ressa and Rappler, *supra* note 29.
[32] Barnaby Lo, *Maria Ressa and Reynaldo Santos' convictions of cyber libel upheld by Court of Appeals*, CBS News, (July 8, 2022, 11:12 AM).
[33] Lian Buan, *When CA Upheld Ressa's Conviction, It Extended Cyber Libel Shelf Life To 15 Years*, Rappler, (July 12, 2022, 4:43 PM).
[34] Ciobanu, *supra* note 7.
[35] Helsinki Found. for Hum. Rts., *Rule 9 Submission* (Feb, 11, 2020) https://www.hfhr.pl/wp-content/uploads/2020/02/1714_001.pdf?fbclid=IwAR0IeM84g-4U0oA1ULasoQXJHx7eY6ZloyTwy-tvnIafd781vnG9GNyABBU.
[36] *Id.* at 2.
[37] Magdalena Gad-Nowak & Marcin S. Wnukowski, *Polish government to pass law that will allow it more control over the Internet content and legitimize blocking access to certain websites*, National Law Review (Feb. 12, 2021).

related to internet speech[38] Distinguishable from legitimate uses of defamation laws, SLAPPs aim to force journalists to engage in self-censorship and involve speech of substantial public interest.[39] SLAPPs are typically filed without an expectation of winning a defamation claim, but instead are used "to stifle scrutiny and public debate on issues such as corruption, mismanagement of public resources."[40] Increasingly, lawsuits of this nature push media organizations to engage in excessive self-censorship to avoid threats of "expensive, long-lasting, and complicated" litigation.[41] SLAPPs are primarily on the rise in Europe, but the cross-border nature of internet speech and cyber libel regimes suggests a global threat.

SLAPPs are particularly prevalent in the UK, which has become "infamous for legislating the largest number of SLAPP cases, both domestically and transnationally."[42] Even without additional cyber libel laws, the country has seen a surge in SLAPPs, often for online speech, due to procedural mechanisms that overwhelmingly favor plaintiffs in defamation cases. Defendants face disproportionate barriers in retaining legal counsel, risk paying the claimant's legal fees, and are only able to recover a portion of their own legal fees if the suit is dismissed.[43] U.K. courts have also "allowed claimants to bring cases when there is only the merest link to the country, for example on the grounds that the claimant had property or some business interests there."[44] This has resulted in such cases as *Tony Robbins v. BuzzFeed UK Ltd*, where an American sued Dublin-based Buzzfeed UK for an article posted by an American journalist working for the American outlet, Buzzfeed Inc.[45] Despite the fact that Buzzfeed UK did not publish the article, the suit was allowed to continue in Ireland because "the articles were viewed as many as 13,382 times by users geo-located in Ireland."[46] This sets a dangerous precedent for future online speech SLAPPs. The UK's claimant-friendly and cross-border accessible defamation regime applied to internet speech presents a clear threat to freedom of expression as powerful people worldwide use SLAPPs to silence journalists, bloggers, and even citizens.

Similar trends have emerged in Thailand and the Philippines. In Thailand, the broad Computer Crimes Act was used for 21% of the 33 clearly identifiable SLAPPs in the past 25 years.[47] In the Philippines, wealthy plaintiffs have successfully employed SLAPPs for defamation and cyber libel through Cybercrime Prevention Act.[48] The Hinatuan Mining Corporation used the Act in 2016 to file "criminal 'cyber-libel' charges against members of the Philippine Misereor Partnership," a collection of social advocacy groups.[49] Mining companies in the Philippines have used defamation SLAPPs to intimidate and harass journalists for two decades, and the addition of cyber libel has provided a new tool for them to do so.[50] Broad, vague, and ambiguous cybercrime and defamation laws provide an attractive mechanism for powerful businessmen, politicians, and corporations to strategically force media outlets to engage in

---

[38] Rebecca Bonello Ghio & Dalia Nasreddin, *Shutting Out Criticism: How SLAPPs Threaten European Democracy*, The Coalition Against SLAPPs Eur., (March 2022).
[39] *Id*. at 11.
[40] Article 19, *SLAPPs against journalists across Europe*, (March 2022), https://www.article19.org/wp-content/uploads/2022/03/A19-SLAPPs-against-journalists-across-Europe-Regional-Report.pdf.
[41] Bonello Ghio & Nasreddin, *supra* note 38 at 49.
[42] Article 19, *supra* note 40 at 63.
[43] *Id.* at 63.
[44] Bonello Ghio & Nasreddin, *supra* note 38 at 34.
[45] *Id.* at 37.
[46] Tim Healy, *Buzzfeed fails to prevent millionaire American self-help guru Tony Robbins suing it for defamation in the High Court here*, Independent Ireland (June 4, 2021, 6:29 PM).
[47] Nikhil Dutta, Int'l Center for Not-For-Profit L., *Protecting Activists from Abusive Litigation*, 17 (July 2020).
[48] *See* discussion *supra* Part II.B.2.
[49] Dutta, *supra* note 47 at 12.
[50] *Id.* at 12.

self-censorship while draining their resources. Eliminating overinclusive cyber libel laws and abuses of traditional defamation laws to punish online speech can prevent additional abuse of the legal system.[51] Many cybercrime laws have additional provisions that lend way to punishing online speech, functionally parallel to but legally distinguishable from cyber libel. Claimants in SLAPPs will increasingly seek to use these provisions as another route for judicial harassment.

3. Disinformation Laws[52]

Disinformation claims provide another vehicle for authoritarian leaders to attack opponents. Former U.S. President Donald Trump's frequent and unsubstantiated accusations of "fake news" used to discredit media institutions he personally disliked is a leading example of this strategy.[53] These culturally pervasive attacks have become a popular tool of politicians worldwide, used to "influence elections and other political processes, control the narrative of public debates or curb protests against and criticisms of Governments."[54] Simultaneously, governments have rushed to pass laws to control the spread of disinformation regarding treatment and infection of COVID-19, in what has been called an "infodemic" within the pandemic.[55] These laws seek to address a serious public health risk, but terms with "vague definition and broad scope mean[] that they can be easily manipulated to censor critical reporting."[56] Bypassing alternatives such as public media literacy campaigns or government fact checking websites, autocratic regimes have sanctioned the spread of misinformation, making journalists vulnerable to lawsuits or arrest for publishing information government leaders disapprove of.[57]

In the last five years, laws establishing prison sentences for the spread of misinformation have taken effect in several countries: Algeria, Bangladesh, Burkina Faso, Cambodia, China, Egypt, Kenya, Malaysia, Myanmar, and Singapore.[58] Within a year of its passage, The Protection from Online Falsehoods and Manipulation Act, Singapore's disinformation bill, was "invoked[] more than 50 times, primarily against content critical of the government or its policies."[59] In Bangladesh, the controversial Digital Securities Act criminalizes transmission or publication of "offensive, false or threatening" information with up to three years in prison.[60] The act gives the government a "carte blanche" to collect

---

[51] *Id.* at 36.

[52] As this section points out, disinformation and related terms such as fake news are often misnomers, given to statements that are not actually false. This section uses the term disinformation as an umbrella term covering misinformation and malinformation. As noted by the UN report on Disinformation And Freedom of Opinion and Expression, "[a]cademics have developed a taxonomy of an information disorder in which "disinformation" is described as false information that is knowingly shared with the intention to cause harm, "misinformation" as the unintentional dissemination of false information and "malinformation" as genuine information shared with the intention to cause harm." Here, "disinformation" is used in relation to laws targeting these categories of information, and is not always intended to mean information that is untrue. Irene Khan (Rapporteur for Freedom of Opinion and Expression), *Disinformation and freedom of opinion and expression*, 3, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021).

[53] *Id.* at 5.

[54] *Id.* at 10.

[55] Jamie Wiseman, *Rush To Pass 'fake News' Laws During Covid-19 Intensifying Global Media Freedom Challenges*, Int'l Press Institute (Oct. 3, 2020).

[56] *Id*.

[57] *See* Funke and Flamini, *supra* note 20.

[58] *Id.*

[59] Hum. Rts. Watch, *World Report 2021: Singapore*, https://www.hrw.org/world-report/2021/country-chapters/singapore.

[60] Digital Security Act, S.R.O. NO. 310-Law/2019 (2018), Art. 25 (Bangl.).

and preserve data on its citizens via "several definitions [that] are too vague and overbroad."[61] In 2021 writer and government critic Mushtaq Ahmed died in pre-trial detention after being charged with violating the act.[62] In Algeria, where ISLP has previously employed its brief strategy, recent amendments to the penal code criminalizes false news that "harms national unity."[63] The bill gives the Algerian Government power to arbitrarily censor "news reports, social media, or other media" by threatening "prison terms of two to five years."[64] Many countries justify the passage of these laws by arguing they are necessary to combat misinformation that could be injurious to public health, but recent trends indicate new provisions are used to undermine democracy and stifle discourse.[65]

Proposed laws are currently pending in several more countries, including Brazil, where a looming bill threatens digital freedoms.[66] The bill "puts every user under suspicion of malicious activities," allows monitoring of private messaging, increases criminal defamation penalties, and mandates identification requirements that many Brazilians can not fulfill.[67] It also severely undermines the media's watchdog role by providing parliamentary immunity online.[68] Should it pass, Brazilians would be subject to a tightly controlled internet, where privacy and freedom of expression are significantly reduced. In April of 2022, the bill, heavily criticized by NGOs and human right organizations, failed to pass the fast-tracked path, and is now being rerouted through congress.[69] This narrow failure opens the door to potential renegotiations of controversial provisions, giving CSO's a chance to intervene.

State responses to disinformation also compromise access to information, with some jurisdictions stopping the flow of information altogether rather than trying to censor or sanction it. In India, internet shutdowns are a commonplace response to stop the spread of false information.[70] Experts warn these shutdowns are arbitrary, harmful to the economy, and highlight the need for "better checks on [government], greater transparency and better maintenance of records of internet shutdowns."[71]

Shutdowns can be initiated to stop an emergency or threat to public safety, two terms which are undefined under Section 5(2) of the Indian Telegraph Act.[72] Ambiguous terms are a common feature of

---

[61] Article 19, *Bangladesh: analysis of the Digital Security Act* (Nov. 12, 2019), https://www.article19.org/resources/bangladesh-analysis-of-the-digital-security-act/.
[62] New Age Bangl., *Writer Mushtaq detained under DSA dies in jail*, (Feb. 25, 2021, 11:35 PM), https://www.newagebd.net/article/131159/writer-mushtaq-detained-under-dsa-dies-in-jail.
[63] Comm. to Protect Journalists, *Algeria blocks 3 news websites and criminalizes false news*, (Apr. 22, 2020, 1:39 PM), https://cpj.org/2020/04/algeria-blocks-3-news-websites-and-criminalizes-fa/.
[64] *Id*.
[65] Molly Quell, *More Countries Pass 'Fake News' Laws in Pandemic Era*, Courthouse News Service, (June 5, 2020) https://www.courthousenews.com/more-countries-pass-fake-news-laws-in-pandemic-era/.
[66] *See* Funke and Flamini, *supra* note 20.
[67] Freedom House, *Joint Statement: Brazil Disinformation Bill Threatens Freedom of Expression and Privacy Online* (June 29, 2020).
[68] Coalizão Direitos na Rede [Rights on the Network Coalition], Alerta de organizações da sociedade civil sobre o Projeto de Lei 2630/2020 [Alert from civil society organizations about Bill 2630/2020], (Apr. 6, 2022), https://direitosnarede.org.br/2022.
[69] Júlio Lubianco, *Fake News bill gets stuck in Brazilian Congress and it's unlikely to be voted on before the elections*, LatAm Journalism Rev., (Apr. 12, 2022) https://latamjournalismreview.org/articles/fake-news-brazil-payment-journalism/.
[70] Jayshree Bajoria, *India Internet Clampdown Will Not Stop Misinformation*, Nikkei Asian Rev., (Apr. 24, 2019, 2:13 PM), https://asia.nikkei.com/Opinion/India-internet-clampdown-will-not-stop-misinformation.
[71] Mehab Qureshi, *Decoding India's dubious distinction as world's 'internet shutdown capital'*, Indian Express, (Dec. 4, 2021, 8:59 PM) https://indianexpress.com/article/technology/tech-news-technology/india-ranks-highest-in internet-suspensions-7654773/.
[72] *Id*.

cybercrime laws targeting false information, leading to "excessive discretion" and "arbitrary decision making" which may violate Article 19(3) of the ICCPR.[73] Protecting online freedom of expression requires more than the halting or revision of problematic bills, it requires the passage of safeguards to prevent governments from basing major restrictions on simple, undefined justifications.

It is important to note that misinformation laws are not libel laws. Misinformation laws are not designed to protect an individual's reputation, aiming instead to reduce the spread of false or misleading information that jeopardizes public health, national security, or public order. However, so-called "fake news" policies have taken the shape of libel cases under a different name. Indefinite legislation passed in haste, accelerated by the pandemic, and targeted at such general offenses as "social disturbance" gives officials and oligarchs power to protect their desired reputation without revising defamation laws.[74] Even where defamation laws are enforced through only proportionate remedies, disinformation laws can create a legal loophole, weakening freedom of speech protections.

III. Why These Laws Are a Threat

A. New Attacks: Surveillance and Online Harassment

Intimidation of journalists did not begin with the popularization of the internet nor the emergence of the COVID-19 pandemic, but these factors exacerbated the fragile state of digital rights globally. Cyber libel and online disinformation laws in the wake of the pandemic allow governments and powerful individuals to use national health and safety as a justification for increasingly harsh restrictions on freedom of expression.[75] New surveillance technologies have also contributed to the harassment of the media, as software like Pegasus and Circles allows governments access to private information on the phones of journalists, human rights defenders, lawyers, political opposition, and ordinary citizens.[76] Expanded defamation laws and cybercrime regimes compounded with intrusive surveillance "negatively affects not only the personal privacy of the individuals but threatens to pose the harm to their inner and outer circle, compromise their dignity and reputation, and expose them, their family members and beneficiaries to the greater risks of threats, aggression and violence."[77] At least 180 journalists have had their information targeted by the intrusive software, putting their sources at risk for further harassment and even incarceration, and likely countless others that have not been detected or reported.[78]

International

The Israeli cyber-arms company, NSO Group, developed Pegasus before acquiring Circles in 2014. Circles has been deployed in at least 25 countries and poses a very real threat to freedom of expression worldwide because phones tracked through the software show no signs of the software's intrusion on

---

[73] Khan, *supra* note 52 at 8.

[74] Ralph Jennings, *In the name of 'fake news,' Asian governments tighten control on social media* , L.A. Times, (Feb. 8, 2019, 12:01 PM); *See,* Jane E. Kirtley, *Getting to the Truth: Fake News, Libel Laws, and "Enemies of the American People,"* 43 Hum. Rts. Mag.

[75] *See* Brown, *supra* note 8; Wiseman, *supra* note 55.

[76] Amnesty Int'l, *Scale of secretive cyber surveillance 'an international human rights crisis' in which NSO Group is complicit* (July 23, 2021), https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/.

[77] Tamar Kaldani and Zeev Prokopets, *Pegasus spyware and its implications on human rights*, Council of Europe, 18 (June 2022), https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

[78] Amnesty Int'l, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally* (June 19, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/.

their privacy.[79] This new frontier of threats to freedom of expression emerges at a time media outlets are an increased risk of financial intimidation and judicial harassment through cyber libel laws, disinformation laws, and SLAPPs, forcing struggling "news outlets and civil society organizations [to] compete with an ever more sophisticated surveillance industry that continues to flourish."[80]

The governments of European nations and others "have been targeted, and implicated, in NSO Group's Pegasus scandal."[81] NSO Group and governments using the service have threatened to sue several news outlets in the wake of articles exposing the extent of surveillance occurring with their software, alleging that the articles are incomplete and defamatory.[82] Like cyber libel laws, enhanced surveillance software is not only used by authoritarian governments, wealthy individuals, and powerful corporations to increase intimidation of political dissidents, but is also increasingly and worryingly present in democratic nations, who provide substantial financial support to NSO Group and the spyware industry.[83]

B. Shrinking Digital Rights as a Threat to Democracy

Authoritarian regimes seek to completely control the flow of information reaching their citizens on the internet, and cybercrime laws have provided them the perfect tool, domestically and internationally. Cybercrime has become a particularly prevalent risk as internet use has exploded globally, and the pandemic only heightened the urgency felt by governments to protect national security through regulation. As governments have sought solutions to the cybercrime issue, "two radically different visions of cyberspace" have emerged.[84] The first model, maintained by democratic states and the United Nations, seeks to create an "open, free and accessible Internet," with the primary focus on increased information flowing securely and available globally.[85] On the other hand, authoritarian governments have pushed for international norms to support their vision of "the so-called 'sovereign model,' where the primary focus is state control over information and, ultimately, people."[86]

Because international law currently provides rigorous protections for freedom of expression, these regimes have sought to instill authoritarian values and create sovereign internets using two strategies. First, by enhancing domestic cybercrime laws into vague and broad cyber libel provisions and using other mechanisms to increase punishment for online speech, autocrats "silenc[e] dissidents through harassment and violence" at home.[87] Second, they seek to influence international politics and law, using the justification of national security concerns posed by increased cybercrime, to loosen international

---

[79] Bill Marczak and John Scott-Railton, *Running in Circles*, The Citizen Lab (Dec. 1, 2020), https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
[80] Samuel Woodhams, *Spyware: An Unregulated and Escalating Threat to Independent Media*, Center for Int'l Media Assistance (August 25, 2021), https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/
[81] James Lynch, *Iron net: Digital repression in the Middle East and North Africa*, European Council on Foreign Relations (June 29, 2022) https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/.
[82] *See, e.g.,* Ronen Bergman & Patrick Kingsley, *Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses*, N.Y. Times (Nov. 8, 2021); Reuters, *Morocco to sue NGOs behind Pegasus spyware allegations* (July 22, 2021, 2:18 PM).
[83] Bergman & Kingsley *supra* note 82.
[84] Costigan, *supra* note 28 at 10.
[85] *Id.* at 10.
[86] *Id.* at 10.
[87] Varol, *supra* note 10 at 1678; *see also*, discussion *supra* Part II.B.1.

protections for online expression.[88] Both of these strategies have been vigorously, and often successfully, utilized by authoritarian countries in the wake of the pandemic, contributing to the increase in cyber libel laws and their abuses on a global scale, to the detriment of a democratic, open internet model.
A primary consequence of vague cybercrime laws is the "chilling effect," whereby states use legal action against dissenters, "pre-emptively dissuading them from exercising their rights" by instilling fear of "sanctions or informal consequences such as threats, attacks or smear campaigns."[89]

This new frontier of threats to freedom of expression at a time when media outlets are at an increased risk of financial intimidation and judicial harassment through cyber libel laws, disinformation laws, and SLAPPs, is forcing struggling "news outlets and civil society organizations [to] norms agree that criminal penalties and "excessively punitive" civil penalties for defamation have a chilling effect.[90] The European Court of Human Rights has noted that legal regimes which impose a chilling effect not only impact on individual speakers, but also cause "the detriment [] to 'society as a whole,' as the public is denied information of a public interest."[91]

Cybercrime laws chill public debate in two ways: 1) targeting a journalist, media organization, or other individual to discourage criticism, or 2) targeting social media companies through regulations that force them to overregulate their platforms. India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules provide an example of the latter mechanism, exposing social media companies to criminal liability if they do not comply with requests from the government to take down content, "curb[ing] companies' willingness to push back against state censorship requests that do not meet international human rights standard."[92] Threats of these lawsuits under increasingly repressive media law regimes contribute to the chilling effect and self-censorship online, silencing criticism before public officials ever hear it. Autocratic governments have utilized these tactics for decades, but with more urgency and support in recent years than ever before.

Traditional defamation, cyber libel and disinformation laws have a common element that has caused many legal debates: falsity. Combatting false speech online by law often means that either "platforms, as private actors, or governments, as state authority" become "arbiter[s] of free speech."[93] Platforms have regulatory methods to combat false information and the detrimental effect it could have on democratic governance, but without some regulation, the legitimacy of speech would be determined by its profit margin.[94] Additionally, as illustrated by the curtailment of press rights throughout history, "unilateral government regulation of public communication tends to sit in tension with freedom of speech."[95] Cyber libel laws may even go further than unilateral government regulation, however, as they are often vague and broad enough to allow government officials to control the flow of information.[96] Protecting internet users and internet service providers from undue restrictions on internet speech requires increased "oversight of

[88] Varol, *supra* note 10 at 1679.
[89] Laurent Pech, Open Society Founds., *The Concept of the Chilling Effect*, 4 (March 2021).
[90] *See supra* Part II.A
[91] Ronan Ó Fathaigh, Article 10 and the Chilling Effect, 210 (2019) (Ph.D. dissertation, Ghent University), http://hdl.handle.net/1854/LU-8620369.
[92] Adrian Shahbaz & Allie Funk, *Freedom on the Net 2021*, Freedom House, 13.
[93] Judit Bayer et al., *Commission Study on the Fight Against Disinformation and the Right to Free Expression*, European Union, 63 (2021).
[94] Natali Helberger et al., *Governing online platforms: From Contested to Cooperative Responsibility*, 34 Info. Soc'y 1, 8 (2017).
[95] *Id.* at 8.
[96] *See supra* Part II.B.1.

independent judicial authorities" and active collaboration with civil society, which regimes abusing cyber libel and other enhanced defamation laws often lack.[97]

Authoritarian media control through cyber libel and other mechanisms designed to chill online speech seek to undermine public participation for the advancement of further autocratic control. The right to freedom of expression is a core value that "is central to the protection of democracy."[98] Without media freedom, there is no democratic participation and no democratic governance, as public oversight is impossible.[99] Autocrats seeking to minimize public debate silence critics, while "aggressively impos[ing] their own narratives to shape public perceptions."[100] This has led autocrats to champion the sovereign internet model, whereby they can "squelch open debate, pursue dissidents, and compromise rules-based institutions beyond their borders."[101] In the modern age, digital rights are crucial to maintaining democracy, as the internet provides the globe's main source of communication. Cybercrime laws and other enhancements of defamation laws have been touted as preventing bad actors from disrupting democracy, but they have been used as weapons against journalists worldwide to silence public debate. This problem compounds upon itself, as "erosion of press freedom is both a symptom of and a contributor to the breakdown of other democratic institutions and principles."[102] Simply put, democratic control relies upon public debate, and autocratic control of the internet endangers democracy worldwide.

IV. Application of International Norms to Enforce Media Freedoms

ISLP has fought authoritarian suppression of online speech by utilizing international law in local courts. The litigation strategy pursued by ISLP involves filing amicus curiae briefs arguing that protection of free expression is required by international law, both online and off.[103] Relying on the European Convention on Human Rights and the International Covenant on Civil and Political Rights, ISLP has successfully utilized the international norms litigation strategy to defend digital rights and freedoms in multiple jurisdictions.[104]

A. International Norms on Freedom of Expression

International treaties and norms support broad protections for freedom of expression, both online and off. One of the major provisions of the European Convention on Human Rights (ECHR), Article 10, states that "everyone has the right to freedom of expression," including the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority."[105] Article 10 and its case law, developed by the European Court of Human Rights (ECtHR) over 60 years and 1,000 cases, are

[97] David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report on the promotion and protection of the right to freedom of opinion and expression*, 4, U.N. Doc A/HRC/38/35 (Apr. 6, 2018); Bayer et al., supra note 93 at 65.
[98] Michelle Bachelet (U.N. High Comm'r for Hum. Rts.), *Human Rights and Democracy in the Digital Age* (Apr. 25, 2022), https://www.ohchr.org/en/statements/2022/04/human-rights-and-democracy-digital-age.
[99] Freedom House, *Media Freedom*, https://freedomhouse.org/issues/media-freedom (last visited Jul. 21, 2022).
[100] Lynch, *supra* note 81 at 6.
[101] Michael J. Abramowitz, *Democracy in Crisis*, Freedom House (2018) https://freedomhouse.org/report/freedom-world/2018/democracy-crisis.
[102] Sarah Repucci, *Media Freedom: A Downward Spiral*, Freedom House (2019), https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral.
[103] Int'l Senior Laws. Project, *UNESCO recognizes ISLP* (Oct. 12, 2021) https://islp.org/unesco-recognizes-islp/.
[104] *See* strategy *supra* Part I.
[105] ECHR, *supra* note 13 at art. 10.

highly protective of political criticism, adding procedural and substantive requirements to any restrictions on expression.[106] The right of freedom of expression is not absolute, however, but Article 10 allows restrictions on the right only where they a) are "prescribed by law,"[107] b) advance a "legitimate aim,"[108] and c) are "necessary in a democratic society."[109] The Court does not distinguish between statements made online or offline, instead applying these limitations to all restrictions on freedom of expression, and unanimously holding that freedom of expression applies online, "regardless of frontiers."[110]

The International Covenant on Civil and Political Rights (ICCPR), which binds 173 countries, mirrors the ECHR in its protection for free expression. Article 19 of the ICCPR has nearly identical language for free speech as the norms established by Article 10 of the ECHR and its ECtHR case law, stating that "everyone shall have the right to freedom of expression."[111] Article 19 also "include[s] freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers" and irrespective of media choice.[112] The Human Rights Committee has stated that the freedoms contained within Article 19 "are indispensable conditions for the full development of a person" and "constitute the foundation stone for every free and democratic society."[113] Like Article 10, Article 19 requires that restrictions on the right of freedom of expression be "provided by law," and "conform to the strict tests of necessity and proportionality."[114] Legitimate aims of regulation are limited to "respect for the rights or reputations of others" and "the protection of national security or of public order [], or of public health or morals."[115] Article 10 of the ECHR and Article 19 of the ICCPR represent comprehensive, analogous statements on the international norms of freedom of expression.

The African Court on Human and Peoples' Rights (AfCHPR), which binds 26 African Union member states, reiterated the international condemnation of criminal defamation statutes in *Lohé Issa Konaté v The Republic of Burkina Faso*. In *Konaté*, the AfCHPR held that Burkina Faso's laws imposing criminal penalties for defamation were incompatible with Article 9 of the African Charter on Human and Peoples' Rights and Article 19 of the ICCPR. Journalist Lohé Issa Konaté was imprisoned and fined for defamation after publishing articles accusing a state prosecutor of corruption.[116] The Court determined that criminal

---

[106] Jeremy McBride, *The Doctrines and Methodology of Interpretation of the European Convention on Human Rights by the European Court of Human Rights,* Eur. Consult. Ass. 9 (2021), https://rm.coe.int/echr-eng-the doctrines-and-methodology-of-interpretation-of-the-europe/1680a20aee. Stating explicitly that "there is little scope under Article 10 §2 for restrictions on debates on questions of public interest."

[107] *See* ECHR, *supra* note 13 at art. 10 §2; Sunday Times v. UK, 13166/87 Eur. Ct. H.R. (1979). The Court held that limitations on fundamental rights must be "prescribed by law," and "formulated with sufficient precision to enable the citizen to regulate his conduct."

[108] *See* ECHR, *supra* note 13 at art. 10 §2. The Convention requires that restrictions on freedom of expression occur "in the interest of national security, territorial disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."; Bayev & Others v. Russia, 67667/09, 44092/12, 56717/12 Eur. Ct. H.R. (2017). The European Court of Human Rights struck down Russian limitations on expression that failed to earnestly pursue legitimate aims.

[109] *See* ECHR, *supra* note 13 at art. 10 §2; Handyside v. UK, *supra* note 9. The Court held that, to consider a restriction 'necessary,' it must (a) correspond to a "pressing social need," that is "convincingly established," (b) is proportionate and, (c) is the least restrictive means of achieving said goal.

[110] *See* ICCPR, *supra* note 13 at art. 19, art. 17; Yildirim v. Turkey, 3111/10 Eur. Ct. H.R. (2012).

[111] ICCPR *supra* note 13 art. 19.

[112] *Id.*

[113] Gen. Comment no. 34, *supra* note 14 at 1.

[114] *Id.*

[115] ICCPR *supra* note 13 art. 19 §3.

[116] Lohé Issa Konaté v. The Republic of Burkina Faso, *supra* note 16 at 3.

penalties for defamation go further than necessary to achieve the legitimate objective of protecting the reputation of others.[117] It additionally held that fines imposed on Mr. Konaté, totaling $12,000 USD, and the 6 month suspension of the news outlet were disproportionate punishments.[118] The Court ordered Burkina Faso to amend its laws to remove "custodial sentences for acts of defamation; and to adapt its legislation to ensure that other sanctions for defamation meet the test of necessity and proportionality."[119] *Konaté v Burkina Faso* provides important precedent for the African continent regarding the use of custodial sentences for acts of defamation. ISLP employs the analogous relationship between Article 19 and Article 10 in its litigation strategy by using ECtHR case law on criminal and civil defamation to demonstrate how Article 19's guaranteed freedom of expression protects individuals from excessive sanctions on online speech. ISLP's approach has been cited with approval by the "UNESCO Guide for *Amicus Curiae* Interventions in Freedom of Expression Cases."[120]

B. Challenges

One can speculate that courts may be unwilling to subject the national government to violating its treaty obligations under the ICCPR. However, while decisions by the ECtHR are influential and persuasive, they are not binding to non-members of the Council of Europe. Both the ECHR and the ICCPR apply to online speech indirectly through declarations that international human rights law applies in cyberspace, but there is a lack of specific resolutions addressing potential problems with adapting to digital contexts.[121] It will likely require more experience using this argument in other regions to determine its full potential. As matters now stand, however, the prospect looks encouraging.

C. Case Studies: Successful Uses of ISLP's Strategy

ISLP has used the brief argument in cases in the Middle East and North Africa where defendant critics were facing trial or had been convicted under the nation's cybercrime laws. The amicus curiae interventions succeeded in each case. The court dismissed all charges, and acquitted and set free all defendants. In no case where ISLP intervened has the court failed to dismiss the criminal charge.

In Iraq, the Al Muthanna Provincial Council charged defendant Baseem Khashan with violating Article 226 of Iraq's penal code, which criminalizes public insult of a government body.[122] The defendant was sentenced to three years in prison for a post on his Facebook page that read: "the provincial council is between corrupt and coward or marginalized and useless."[123] ISLP filed an amicus brief arguing that government bodies are barred from bringing defamation claims against an individual. The brief noted that the Parliamentary Assembly of the Council of Europe adopted a report prepared by the Parliamentary Assembly's Monitoring Committee advocating for a "clear ban on [the ability of] public bodies to institute

---

[117] *Id*. at 44.
[118] *Id*. at 46.
[119] Colum. Glob. Freedom of Expression, *Lohé Issa Konaté v. The Republic of Burkina Faso*, https://globalfreedomofexpression.columbia.edu/cases/lohe-issa-konate-v-the-republic-of-burkina-faso/ (last visited Jul. 21, 2022).
[120] UNESCO, *Guide for Amicus Curiae Interventions in Freedom of Expression Cases*, 6, UNESCO Doc. CI-2021/FEJ/G-1, (2021) at 6. https://unesdoc.unesco.org/ark:/48223/pf0000379020.
[121] Duncan Hollis, *A Brief Primer on International Law and Cyberspace*, Carnegie Endowment for Int'l Peace (June 14, 2021), https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.
[122] Hum. Rts. Watch, *"We Might Call You in at Any Time"* (June 15, 2020) https://www.hrw.org/report/2020/06/15/we-might-call-you-any-time/free-speech-under-threat-iraq.
[123] *Id.*

civil proceedings in order to protect their 'reputation.'"[124] The ECtHR has found violations of the right to freedom of expression where local government councils have brought civil and criminal actions against individual critics.[125] The brief finds that courts in India and the United States have also held that instituting prison sentences for government criticism violates Article 19. In March 2022, the ECtHRs reaffirmed that a "legal entity that exercises public power may not, as a general rule, be regarded to be in pursuance of the legitimate aim of 'the protection of the reputation ... of others' under Article 10 § 2 of the Convention," providing continued support to ISLP's argument that reputational protections of defamation laws do not extend to public authorities.[126]

ISLP has twice employed its brief strategy in Palestine. In the first matter, the defendant, high profile activist Issa Amro, was charged with disturbing the public order and insulting authorities under Palestine's Cybercrime Law for his Facebook comments criticizing actions of public officials.[127] ISLP's brief "cited authorities in the European Court of Human Rights (ECtHR), France, Egypt and elsewhere in the Arab world."[128] ISLP argued that neither insult or hate speech laws apply to unnamed government officials because criminal defamation statutes are disproportionate to government criticism and public officials do not represent a different sect to be protected under anti-hate speech laws. Also in Palestine, ISLP submitted a brief opposing Cybercrime Law Articles 20 and 22, which was used against six bloggers who criticized public officials.[129] The brief reviewed the law in light of international norms to show that Palestine's criminalization of non-violent, truthful speech breached the country's treaty obligations under the ICCPR.[130] Additionally, ISLP analyzed speech and media protections within provisions of Palestine's Basic Law to evince that savings clauses within the law subordinated the provisions to the Cybercrime Law and inadequately protected freedom of expression. Local counsel reported that "the trial judge cited and relied on the ISLP brief, acquitted all six defendants, and announced that he will keep the brief for future reference."[131]

In Tunisia, defendant Wajdi Mahouechi was arrested for criticizing a local public prosecutor on his blog. The defendant was convicted under Article 86 of the Telecommunications Code of 2001, which criminalizes insult "through public telecommunications network" and Article 125 of Chapter Four of Tunisia's Penal Code, which criminalizes defamation of public servants.[132] Mahouechir received a two year prison sentence for comments on the public prosecutor's alleged failure to arrest and investigate an imam accused of promoting violence.[133] In April 2021, ISLP filed an amicus curiae brief arguing that

---

[124] Eur. Consult. Ass., *Honouring of obligations and commitments by the Russian Federation*, ¶ 393, Doc. No. 10568 (2005).
[125] *See* discussion *supra* Part II.A.
[126] OOO Memo v. Russia, 2840/10 Eur. Ct. H.R. (2022).
[127] Amnesty Int'l, *Palestine: Authorities must drop charges against human rights defender Issa Amro for peaceful criticism* (Mar. 27, 2019) https://www.amnesty.org/en/latest/press-release/2019/03/palestine-authorities-must-drop-charges-against-human-rights-defender-issa-amro-for-peaceful-criticism/.
[128] Int'l Senior Laws. Project, *ISLP Defends Facebook Blogger in Palestine* (Dec. 20, 2018), https://islp.org/islp defends-facebook-blogger-in-palestine/.
[129] Int'l Senior Laws. Project, *One Amicus Curiae Brief, Six Free Speech Acquittals* (Sept. 25, 2019), https://islp.org/one-amicus-curiae-brief-six-free-speech-acquittals/.
[130] Hum. Rts. Watch, *Palestine: Reform Restrictive Cybercrime Law* (Dec. 20, 2017, 12:00 AM), https://www.hrw.org/news/2017/12/20/palestine-reform-restrictive-cybercrime-law.
[131] *Id*.
[132] Hum. Rts. Watch, *Tunisia: Harsh Sentence Against Blogger* (Nov. 24, 2020, 12:00 AM), https://www.hrw.org/news/2020/11/24/tunisia-harsh-sentence-against-blogger.
[133] *Id.*

Mahouechi's punishment violated ICCPR treaty obligations and disregarded international norms.[134] ISLP also argued that as a blogger, Mahouechi should be afforded the protections of a traditional journalist. On January 20, 2022, Mahouechi was freed, having had his sentence reduced to 16 months in prison.[135]
In Algeria, defendant Saïd Boudour was charged with publishing criticism of public officials on the internet, a violation of the Cybercrime Law, for his "Facebook post criticizing military leaders, the army, and a pro-government news executive."[136] Articles 144-147 of Algeria's penal code authorize varying prison terms for defamation of government and military personnel, the president, and religion.[137] Article 296 defines defamation as "attacks [...] against the reputation or dignity [...] or when something improper is attributed [....] This article applies even if names […] are not directly mentioned but can be inferred…."[138] ISLP filed an amicus curiae brief, which used international norms to explain how punishing defamation with imprisonment violates Algeria's treaty obligations and provisions of Alegria's constitution, which guarantees the freedom of the press.[139] ISLP used international agreements and human rights court decisions to support the proposition that Algeria's criminal code conflicted directly with its constitutional and international guarantees.[140] On appeal, Boudoir's defense presented arguments contained in ISLP's brief, and his sentence was reduced "to a 2-months suspended sentence," shortly after which he was freed and all charges were dropped.[141]

D. Adapting the Strategy to Defend Against Cyber Libel Laws

International cybercrime law is still in its infancy. General consensus reasons that existing international law applies online, but questions remain as to how duties, rights, and regulations operate in cyberspace, and what mechanisms may ensure accountability.[142] Few guidelines for international cyberspace rules exist. Most prominently, the Budapest Convention provides for cooperation and common policy among its 66 signatories.[143] Additionally, the African Union Convention on Cyber Security and Personal Data Protection was adopted in 2014, but has only been ratified by 5 of the 15 countries necessary for the agreement to take effect.[144] For the past decade, autocracies have pushed for a new cybercrime agreement, and their most recent resolution challenging the authority of the Budapest Convention garnered eighty-eight votes in support and only fifty-eight votes in opposition.[145] The Russian Federation has submitted a complete draft proposal for this treaty, which would place content-based restrictions on a myriad of online communications.[146] The draft has widespread autocratic support, but democratic

---

[134] Int'l Senior Laws. Project, *ISLP Continues to Defend the Right to Freedom of Expression: Updates from Tunisia and Algeria* (March 9, 2022), https://islp.org/islp-continues-to-defend-the-right-to-freedom-of-expression/.
[135] *Id.*
[136] *Id.*
[137] Int'l Ctr. for Not-for-Profit L., *Algerian Penal Code Excerpts*, https://www.icnl.org/wp-content/uploads/Algeria_crimenselection.pdf.
[138] Code Penal [Penal Code] art. 296 (Alg.).
[139] Alg. Const. Nov. 1, 2020, art. 54. Stating "this freedom shall not be exploited to infringe upon the dignity, liberties and rights of others," and "press offenses shall not incur a custodial sentence."
[140] Int'l Senior Laws. Project, *supra* note 134.
[141] *Id.*
[142] Hollis, *supra* note 121.
[143] Eur. Consult. Ass., *The Budapest Convention (ETS No. 185) and its Protocols*, https://www.coe.int/en/web/cybercrime/the-budapest-convention, (last visited July 21, 2022).
[144] Coop. Cyber Def. Ctr. of Excellence (CCDCOE), *African Union*, https://ccdcoe.org/organisations/au/, (last visited July 21, 2022).
[145] Brown, *supra* note 8.
[146] Article 19, *Russia: Proposed UN Cybercrime Convention must uphold free speech* (Feb. 17, 2022), https://www.article19.org/resources/russia-proposed-un-cybercrime-convention-must-uphold-free-speech/.

coalitions vary widely in their conception of the necessary scope of a cybercrime treaty, the human rights concerns inherent therein, and the appropriate level of civil society involvement in the drafting process.[147] As support increases for a more comprehensive international agreement regarding cybercrime, democracies must remain vigilant to not provide ambiguity that autocratic regimes can take advantage of to justify restrictions on freedom of expression.[148]

ISLP has successfully applied the international norm strategy to cybercrime laws criminalizing online speech in a variety of jurisdictions, without much adaptation as compared to the strategy's potential application to offline defamation.[149] The ECtHR has held that Article 10 protects freedom of expression online as well as offline, acknowledging that "its accessibility and its capacity to store and communicate vast amounts of information" has positioned the internet as a key facilitator of news and information.[150] Criminal cyber libel laws present a threat to the free flow of information online and are often abused by authoritarian governments to silence political opposition. International norms dictate the necessity of broad protections for political speech, as democratic governance requires that "the actions or omissions of the government must be placed under the watchful scrutiny of the press and public opinion."[151] By limiting journalists, bloggers, and even citizen's ability to express "discontent or political aggression as a means for democratic citizenship in cyberspace," criminal cyber libel laws are fundamentally incompatible with the protections of free speech contained within the ECHR and ICCPR.[152]

VI. Conclusion

The full impacts of cyber libel laws have yet to be seen, and additional research and tracking should be done. Some regional analyses have been compiled, but global analyses must be conducted because the typical cyber defamation law reaches beyond its country's borders.[153] Emerging surveillance technologies give authoritarian regimes "an astonishing array of tools [...] they can use [...] with little concern that they will be held accountable for doing so."[154] Without international consensus and safeguards, authoritarians can exploit new technologies to exert control over the digital information landscape. As subjective attitudes in media are in flux, it is important for digital laws to preserve and promote the free flow of information, rather than increasing government control.[155] Civil society plays an important role in monitoring and demanding accountability for the effects of cyber crime laws.[156] Additionally, civil

[147] Kumar et al., *The UN's Cybercrime Treaty: Where Do Things Stand?*, Glob. Partners Digit. (Nov. 24, 2021), https://www.gp-digital.org/the-uns-cybercrime-treaty-where-do-things-stand/.
[148] Madeline Earp, *Why the UN's Push for a Cybercrime Treaty Could Imperil Journalists Simply for Using the Internet*, Comm. to Protect Journalists (Jan. 18, 2022, 12:19 PM), https://cpj.org/2022/01/why-the-uns-push-for-a cybercrime-treaty-could-imperil-journalists-simply-for-using-the-internet/.
[149] *See* discussion *supra* Part IV.D.
[150] Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2), 3002/03, 23676/03 Eur. Ct. H.R. §27 (2009).
[151] Eur. Consult. Ass., *Internet: case-law of the European Court of Human Rights*, 18 (2015), https://www.echr.coe .int/documents/research_report_internet_eng.pdf.
[152] Birgit Mitterlehner, *Cyber-Democracy and Cybercrime: Two Sides of the Same Coin*, Cyber Dev., Cyber Democracy and Cyber-Def. 207, 209 (2014).
[153] *See e.g,* Shweta Chhetri, *The Defamation in the Internet Age: Cyber Defamation*, 4 Int'l J. L. Mgmt. & Humans. 1981, 1991 (2021); Voule, *supra* note 12.
[154] Lynch, *supra* note 81 at 2.
[155] Benjamin Toff et al., *Overcoming indifference: what attitudes towards news tell us about building trust*, Reuters Institute (Sept. 9, 2021), https://reutersinstitute.politics.ox.ac.uk/overcoming-indifference-what-attitudes-towards -news-tell-us-about-building-trust.

[156] Bayer et al., *supra* note 93 at 65.

society campaigns against disinformation and hate speech promote self-regulation, reducing the need for government intervention in online spaces.[157]

A very real, but immeasurable consequence of a government's surveillance of the web and its prosecution and incarceration of journalists is the climate of fear it produces.[158] Self-censorship is the inevitable consequence, as would-be critics must avoid the internet "while the exuberance that has characterized internet communication [] decline[s] into conformity and acquiescence."[159] The cost to individual journalists, news organizations, and society as a whole are unfathomable. Also immeasurable are the news stories reporting official crimes and corruption which journalists never write. Indifference and delay in regards to the threat posed by vague and overinclusive cybercrime laws have created these unacceptable costs and left journalists, bloggers, human rights defenders, lawyers, and media organizations to pay.[160]

Defamation laws have been used by authoritarian governments for decades to suppress free expression, and cyber libel laws have provided them yet another tool. Media freedom necessitates the "repeal [of] any law criminalizing defamation, online or offline."[161] In addition, all defamation regimes must meet international standards, including "clearly and narrowly defin[ing]" all restrictions premised upon national security.[162] These laws must "limit the discretion of executive authorities," granting remedies through independent authorities instead.[163] Governments must also ensure that remedies for violations of freedom of expression are "accessible, affordable, adequate, and timely."[164] Governments, civil society organizations, and international bodies must act in tandem to support policies promoting transparency and media freedom, online and off.[165]

Notwithstanding freedom of expression concerns inherently present in criminal and overly punitive defamation regimes, cyber libel regimes themselves are fundamentally incompatible with international human rights law. Unless and until cyber libel laws are finally repealed, journalists, bloggers and dissenters will continue to be sent to prison for criticizing politicians online. In order to achieve wholesale repeal, the following recommendations are offered:

A. Recommendations for Governments:

- The most impactful strategy requires the repeal of all cyber libel laws, along with "revising and amending cybercrime, surveillance and antiterrorism laws" to comply "with international human rights norms and standards governing the right to privacy, the right to freedom of opinion and expression, the right to freedom of peaceful assembly and the right to freedom of association."[166]

---

[157] *Id*. at 63.
[158] David Robie & D.M. Abcede, *Cybercrime, criminal libel and the media: From 'e-martial law to the Magna Carta in the Philippines*, 21 Pac. Journalism Rev. 211, 222 (2015).
[159] *Id.* at 222.
[160] *See* Brown *supra* note 8.
[161] Kaye *supra* note 97 at ¶ 65.
[162] Voule *supra* note 12 at ¶ 69.
[163] David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression), *Report on the promotion and protection of the right to freedom of opinion and expression*, ¶ 57, U.N. Doc. A/71/373 (Sept. 6, 2016).
[164] Voule *supra* note 12 at ¶ 72.
[165] Bayer et al., *supra* note 88 at 65.
[166] Voule, *supra* note 12 at ¶ 73(c).

- In the meantime, national courts should give priority to cases which allege that these laws violate the national constitution and international norms of freedom of expression.
- Furthermore, all branches of governments should "refrain from imposing disproportionate sanctions," on individuals and ICT companies.[167]
- Democratic member states of international organizations should resist autocratic efforts to redefine international cybercrime agreements.
- Finally, governments must "renew their commitments to a multi-stakeholder approach as a cornerstone of Internet governance processes."[168]

B. Recommendations for Civil society Organizations, Media, and Advocates

- Civil society organizations, the media, and human rights defenders must campaign to convince national legislatures to repeal cyber libel laws and revise other threats to free expression online.
- In addition, advocates should aggressively fund and "utilize strategic litigation," such as the ISLP international norm strategy, to fight violations of digital rights and freedoms.[169]
- Civil society organizations should advocate for a multistakeholder approach to digital policy making, engaging government and online platform providers where possible to "increase participation of underrepresented voices in the online environment."[170]
- To assist these ends, civil society organizations should "expand and improve data collection on – and documentation of digital threats to" human rights online, "shar[ing] knowledge, promot[ing] standards for data collection, and collaborat[ing] with other stakeholders in these efforts."[171]

C. Recommendations for International Bodies

- Organs of the United Nations should take measures to convince member nations to repeal these laws.[172]
- Other international organizations such as the Council of Europe and the African Union should adopt policies to convince member nations to repeal these laws.[173]
- The United Nations and other international organizations should remain wary of autocratic attempts to suppress free expression through international cybercrime agreements.
- International human rights courts, such as the European Court of Human Rights, The African Court of Human and People's Rights, and the inter-American Court of Human Rights, should give priority to cases alleging violations of freedom of expression norms.
- The Human Rights Committee, UN Special Rapporteurs, and other international human rights

[167] Kaye, *supra* note 97 at ¶ 66.
[168] Voule, *supra* note 12 at ¶ 81.
[169] Freedom House, *Policy Recommendations: Internet Freedoms*, https://freedomhouse.org/policy recommendations/internet-freedom, (last visited July 21, 2022).
[170] Bayer et al., *supra* note 93 at 65.
[171] Voule, *supra* note 12 at ¶ 94.
[172] *See Id.* at ¶ 96; Hum. Rts. Watch, *Submission to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes* (Apr. 28, 2022, 10:19 PM), https://www.hrw.org/news/2022/04/28/submission-human-rights -watch-united-nations-ad-hoc-committee-elaborate.
[173] *See, e.g.,* Marija Pejčinović Burić, *State of Democracy Human Rights and the Rule of Law*, Eur. Consult. Ass., 30 (2021), https://rm.coe.int/annual-report-sg-2021/1680a264a2.

> authorities should continue and escalate investigations and criticisms of overinclusive cybercrime laws, and call for their repeal.[174]

The complexity of implementing these recommendations represents the arduous path forward that the future of free expression requires. The alternative, however, is preserving the *status quo* out of indifference, which can only encourage more authoritarian governments to adopt these laws and accelerate prosecuting, imprisoning, and silencing their online critics.

[174] Article 19, *Response to the consultations of the UN Special Rapporteur on Freedom of Expression on her report on disinformation* (Feb. 2021), https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/disinformation/2-Civil-society-organizations/ARTICLE19.pdf.