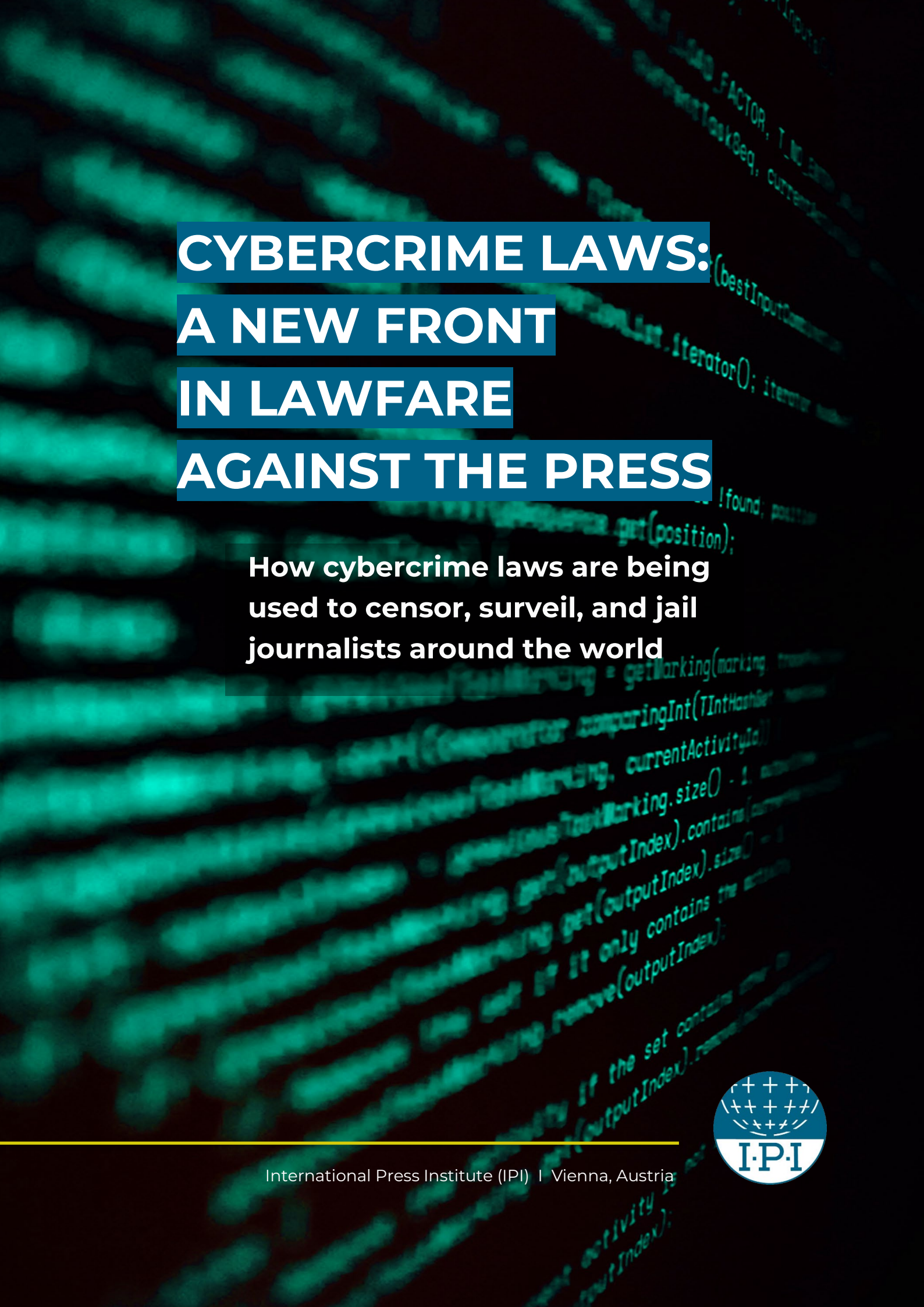

CYBERCRIME LAWS: A NEW FRONT IN LAWFARE AGAINST THE PRESS

How cybercrime laws are being used to censor, surveil, and jail journalists around the world

International Press Institute (IPI) I Vienna, Austria

ABOUT THIS REPORT

Around the world, repressive cybercrime laws are being used to target and punish journalists, advocates, and other public watchdogs and to restrict access to independent news and information. Often enacted under the guise of protecting national security or combating harmful speech such as disinformation and hate speech online, these laws in practice have become powerful tools to censor, surveil, and jail journalists and critics in many countries around the globe.
This report reflects more than a year of research and monitoring by IPI into the use of cybercrime laws by governments around the world to punish journalists and to censor independent news and information online. Our analysis draws on a review of 30 cybercrime laws in 30 countries – in Asia, Southeast Asia, Middle East, Africa, and Latin America – where the use of such laws against journalists has been increasing.

Authors: Amy Brouillette, Jamie Wiseman, Marystella Simiyu.

Background research: Rowan Humphries, Katherine Dailey, Colette Yamashita Holcomb, Samuel Kennedy, Nevena Krivokapić Martinović (SHARE Foundation), Tijana Stevanović (SHARE Foundation), Bojan Perkov (SHARE Foundation).

Acknowledgements:
We wish to thank legal expert Joan Barata for providing key input into this report, including developing the Recommendations.

ABOUT IPI

International Press Institute (IPI) is a global network of journalists, editors, and publishers who share a common dedication to quality, independent journalism. Together, we promote the conditions that allow journalism to fulfill its public function and to safeguard the media's ability to operate free from interference and without fear of retaliation. Our mission is to defend media freedom and the free flow of news wherever they are threatened.

International Press Institute

The production of this report was supported by a grant from:

Federal Ministry
Republic of Austria
European and International Affairs

VIENNA +30 OUR RIGHTS FUTURE

Photo credit: A.C. / Unsplash

Contents

Overview: Key trends and findings

Cybercrime laws with inadequate safeguards for human rights online are increasingly being weaponized by repressive governments across the globe to target journalists and muzzle dissent.[1] Often enacted under the guise of combating terrorism, disinformation, and harmful speech online – all legitimate policy challenges – these laws in practice have become much-abused catch-all offenses to target journalists and critics as part of a wider pattern of "lawfare" being waged by governments against the media and civil society.[2]

The increasing use and abuse of these laws pose real threats to journalists and journalism in many parts of the world – and is significantly eroding the rights to expression, information, and privacy on which the media relies in order to carry out their work freely, independently, and safely.

For this report, IPI reviewed cybercrime legislation in 30 countries – in Asia, Southeast Asia, the Middle East, Africa, and Latin America – where the use of such laws against journalists has been increasing, according to IPI's research and monitoring. While not an exhaustive assessment of all cybercrime laws globally, this analysis reflects broader trends about cybercrime laws and their impact on journalists and independent media in many countries around the world.

The following is a summary of the main takeaways and trends, based on our review:

Legal justification. The introduction of new or expansion of existing cybercrime laws are often justified by governments on grounds of legitimate policy issues – including for the **protection of national security, and/or countering disinformation, hateful, and toxic speech online**. Yet the measures introduced in cybercrime legislation typically go far beyond addressing these types of policy challenges and

[1] Weaponizing the Law: Attacks on Media Freedom
[2] IPI General Assembly Resolution: State and non-state actors must cease 'lawfare' against the press (IPI)

instead provide legal grounds for expanding online censorship and surveillance of journalists and civil society. Expansive cybercrime laws can often include criminal bans on a wide range of legitimate speech – from hateful speech to disinformation. While such speech can be harmful, it is often not expressly illegal, and in many cases is protected under domestic and international human rights laws and case law.

Expansive scope. Cybercrime laws often reach far beyond core, "cyber dependent" crimes – i.e., crimes that can only be carried out with the use of a computer or digital technologies, such as hacking or DDoS attacks – to include "cyber enabled" crimes. Cyber enabled crimes are "traditional" crimes, such as fraud, piracy, forgery, as well as harassment or bullying that can be carried out without the use of a computer but that can also be facilitated or enabled by the internet and digital technologies. The expansion of cybercrime laws to include cyber-enabled crimes has opened the door to the criminalization of a wide range of expression and content that can impose undue restrictions on protected speech.

Extension of traditional "offline" offences deemed inconsistent with international law. Many cybercrime laws criminalise certain types of expression online – such as defamation, libel, sedition, and blasphemy – which in the "offline" context are widely regarded as incompatible with international law and principles.

Lack of legal certainty. Cybercrime laws often contain vague, poorly defined, or undefined terms – for instance, prohibiting content or expression that upsets 'public order', 'public morality', or 'peace and tranquillity'– which leave these crimes prone to misinterpretation or abuse by authorities. Such vague and overbroad terms violate the principle of legal certainty – a fundamental element of the rule of law – that requires laws to be formulated clearly so that their application is foreseeable.

Demands on private companies to block websites, remove content, or restrict access to information. In some cases, cybercrime laws give authorities unchecked powers to order

private companies – Internet Services Providers (ISPs) and social media platforms – to block or remove online content, without proper judicial oversight or remedy.

Enabling expansive, warrantless surveillance. Cybercrime laws often hand authorities sweeping investigatory and surveillance powers that include accessing users' mobile and internet communications and activities in real time, as well as communications data collected and stored by ISPs and telecommunications companies, with weak or absent human rights safeguards. This typically imposes onerous data collection and retention policies on private ISPs and telecommunications companies, together with requirements to hand over user information without strong judicial intervention or oversight or notice of such demands to affected users.

Banning anonymity online. Many cybercrime laws also include provisions banning or weakening encryption, or requirements to provide authorities "backdoor" access to systems, as well as prohibiting the use of Virtual Private Networks (VPNs). The right to communicate anonymously online, including through the use of encrypted communications, is regarded as essential to the exercise of other human rights – including rights to expression, information, and privacy.

Disproportionate, exaggerated criminal penalties. Cybercrime laws can impose unnecessary and disproportionate penalties – extending in some cases to life imprisonment and crippling fines. Cybercrime laws also often introduce aggravated or specific penalties for "cyber-enabled" crimes based exclusively on the fact that they are committed through the use of information technologies.

*See our **recommendations** for developing cybercrime laws that respect and protect human rights at the end of this report.*

Introduction

In June 2020, journalist Maria Ressa was found guilty of "cyber libel" by a Manila court.[3] The charge stemmed from a 2012 article published by Rappler, the online media outlet co-founded by Ressa, that alleged links between a Filipino businessman and a Supreme Court judge.

The court ruling capped years of harassment by government authorities, who targeted Rappler for the outlet's critical reporting that often exposed corruption involving public officials, including former President Rodrigo Duterte's inner circle.

Ressa is one of numerous journalists globally to be targeted and charged with draconian cybercrime laws – in some cases for merely sharing information on social media.[4] Around the world, repressive cybercrime laws are being used to target and punish journalists, advocates, and other public watchdogs and to restrict access to independent news and information.

More than 150 countries have enacted some form of cybercrime law.[5] Often enacted under the guise of addressing legitimate policy challenges – such as combating actual cybercrime, protecting national security, or combating harmful speech like disinformation and hate speech online – in too many cases these laws in practice have become powerful tools to censor, surveil, and jail journalists and critics in many countries around the globe.

The proliferation of repressive cybercrime laws puts a spotlight on the broader and dangerous escalation of legal harassment and attacks by governments against journalists and independent media on a global level. Governments are increasingly deploying restrictive criminal laws to prosecute

[3] People of the Philippines v. Santos, Ressa and Rappler - Global Freedom of Expression.
[4] IPI condemns convictions of two journalists in Niger, International Press Institute, 2021.
[5] Cybercrime Legislation Worldwide | UN Trade and Development (UNCTAD)

and imprison journalists,[6] as part of a wider pattern of so-called "lawfare" being waged by governments against the press. This includes the use of draconian criminal defamation and sedition laws as well as national security laws and so-called "fake news" laws, to silence journalists for reporting stories exposing public corruption and abuses of power.

Cybercrime laws have become the latest front in this "lawfare" against the press, particularly as governments seek to tighten control over online spaces – often the last pockets of independent information in many countries and regions of the world.

Across South Asia, Africa, the Middle East, and Latin America, these laws are being used to justify the expansion of digital surveillance and online censorship, and restrict the flow of independent news and information. As noted above, authorities in these cases often use legitimate concerns about the impacts of disinformation, hateful, and discriminatory speech to justify the criminalisation of a broad range of online content.[7]

In addition to criminalizing a wide range of expression that is in many cases permissible under international human rights law, domestic cybercrime laws also often grant authorities powers to block websites, shutdown internet and mobile services – restricting the access to critical news and information online – as well as to weaken encryption, and restrict the use of VPNs and other essential privacy tools that enable journalists and civil society to protect their sources and whistleblowers and to communicate and navigate safely and anonymously online.

The increasing use of cybercrime laws to stifle the press is adding to the mounting pressure on journalists and independent media in many countries and regions around the

[6] Weaponizing the Law: Attacks on Media Freedom, by Joel Simon, Carlos Lauría and Ona Flores. Thomson Reuters Foundation and Tow Center for Digital Journalism at Columbia Journalism School. April 2023.
[7] Human rights impacts of new technologies on civic space in South-East Asia,

world, at a time when strong accountability journalism is needed more than ever. The abuse of such laws is chipping away at the foundations and frameworks of press freedom and human rights on which journalists rely to carry out their work freely, safely, and without fear of reprisal.

Cybercrimes: Definitions and scope

Lawmakers often point to the proliferation of cyber attacks as grounds for introducing or expanding existing cybercrime laws. Indeed, cybercrimes – such as hacking, spyware, and distributed denial-of-service (DDoS) attacks aimed at crashing media website's servers – are on the rise globally and are increasing in scale and complexity.[8] Meanwhile, some types of cybercrime, such as DDoS attacks, can also require less technical sophistication and resources to carry out than are required to trace or defend against them – creating an advantage for malicious actors.

In recent years, journalists and media outlets themselves have also become targets of cyber attacks, including DDoS attacks aimed at crashing media website's servers and preventing access to certain stories, as well as malicious hacking, and theft of private content.[9]

Hence, there is a legitimate need for robust domestic legal and policy frameworks for investigating and defending against illegal cyber attacks – but in a way that does not undermine human rights online. Human rights experts widely agree that this can be achieved with narrowly scoped cybercrime laws that focus on addressing so-called "cyber-dependent" crimes – or crimes that can only be carried out with the use of a computer or digital technologies, such as hacking, spreading malware, ransomware, and DDoS attacks.

[8] Lumen Q3 DDoS research reveals increases in quantity, size and complexity of attacks
[9] New surge of DDoS attacks threatens media freedom in Europe (IPI), 2024.

However, in recent years, governments and policy makers have pushed for the inclusion of a wider scope of so-called "cyber enabled" crimes. These are "traditional" crimes – such as fraud, piracy, forgery, as well as harassment and bullying, as well as certain types of extreme, illegal content – that can be carried out without the use of a computer but are facilitated or enabled by the internet and digital technologies.

Oftentimes, activities and content that can be regarded as "cyber-enabled" crimes are already prohibited in existing criminal codes. However, cybercrime laws often introduce aggravated or increased penalties for "cyber-enabled" crimes based exclusively on the fact that they are committed through the use of information technologies.

For instance, in **Tunisia**, Decree-Law No. 54 states that harsher punishments are permissible for cybercrimes than for similar offences under the country's Penal Code, Code of Criminal Procedure, and Code of Military Procedures and Penalties.[10] This type of increased penalties for crimes committed online – for the same crime committed offline – give authorities greater opportunities to impose strict controls over the internet and digital platforms, and to punish journalists and civil society.

Human rights experts warn that the inclusion of this wider scope of "cyber-enabled" offences within cybercrime laws can also lead to the criminalization of legitimate content and expression that is protected under international human rights law. For instance, "cyber-enabled" offences can include cyber-bullying, trolling, and virtual mobbing, and cyber-enabled violence against women and girls ('VAWG').[11] These activities are harmful and, in some cases, may even be illegal – depending on the context and jurisdiction – but human rights experts say that including these activities within the scope of cybercrime legislation can open the door to overreach and abuse.

[10] Tunisia: Cybercrime law investigations expose new threats to freedom of expression - Amnesty International
[11] Cyberviolence against women, Council of Europe.

For example, cybercrime laws with "cyberstalking" or cyber-bullying" offences are common across Africa, where such provisions have been used to punish journalists who report on political figures or public authorities. In **Nigeria**, Article 24 of the 2015 Cybercrimes Prohibition and Prevention Act, which prohibits "cyberstalking," has been used repeatedly to harass, arrest, and prosecute journalists,[12] human rights defenders, and social media users for sharing content online critical of public officials. Similar "cyberstalking" provisions also appear in the cybercrime law in **Uganda**, where the Computer Misuse Act has been repeatedly abused by the authorities to target journalists and critics, including arresting nine members of an online broadcaster and charging two for "cyberstalking" the president.[13]

Legal justifications: Protecting state security; combatting disinformation and harmful online content

Governments around the world also often cite the protection of national security, and/or countering disinformation, as well as hateful, toxic speech online – also legitimate policy concerns – as justifications for the development of new or expansion of existing cybercrime laws. However, rather than actually protecting state security or minimising the spread of harmful content online, these laws in practice are often powerful tools for censoring independent news and information online and for surveilling and investigating critics and journalists.

3.1 Protecting state security

The rampant use of national security laws and justifications to silence and punish journalists is a well-documented trend that has driven steady declines in press freedom at both state and global levels for the last two decades.[14] This trend is linked to

[12] Nigeria: Journalists targeted again under cybercrime law (IPI)
[13] Uganda: Two journalists held on charges of 'cyber stalking' the president (IPI)
[14] Crackdown on journalists: State security vs human rights | Al Jazeera

the alarming upsurge of national security legislation introduced by democratic and non-democratic states post 9/11. According to a 2012 report by Human Rights Watch, in the decade after September 11, a vast majority of countries – 144 of the world's 195 countries – had passed new counter-terrorism laws.[15] That analysis showed that a majority of those laws contained sweeping and overbroad provisions against crimes such as disrupting "public order," along with broad powers for warrantless searches, surveillance and detentions – in ways that are incompatible with international human rights laws and standards.

As more journalists and civil society have gone online and turned to digital tools and technologies to disseminate news and information, governments have transposed already problematic "anti-terrorism" measures present in their criminal codes to their cybercrime laws. In the group of cybercrime laws we reviewed, all contained deeply dangerous and problematic measures prohibiting "cyberterrorism" – the definitions of which are often lacking or absent.

Such vague "cyberterrorism" provisions are especially common in cybercrime laws across the MENA region, where governments impose stringent controls over online speech. **Egypt's** 2018 *Anti-Cyber and Information Technology Crimes Law*, for example, gives authorities power to order the blocking of websites with content deemed to undermine state security – violations for which can result in steep fines and prison.[16] Similar "cyberterrorism" provisions exist in cybercrime laws in Qatar, Jordan, UAE and Saudi Arabia, giving authorities an additional tool to crack down on the media and censor online content.

[15] Global: 140 Countries Pass Counterterror Laws since 9/11 | Human Rights Watch
[16] Anti-Cyber and Information Technology Crimes Law "EGYPT" Law No. 175 of 2018

Restricting press freedom on national security grounds

While press freedom and freedom of expression are protected by international human rights laws and instruments, these rights may be restricted in narrow circumstances, including on grounds of national security. In these case, the state must show that the restriction meets the so-called three part test:

1) it must be clearly defined in the law;

2) it must genuinely be f**or the purpose of protecting national security**, and must have the demonstrable effect of protecting that aim. (Restrictions that are aimed at stifling journalistic reporting do not meet this test).

3) it must be necessary, meaning the restricted expression is a serious threat to national security and limiting the expression is the least restrictive way of addressing this threat.

➔ *Read more at: The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*

Across the globe, authorities use sweeping and vague "cyberterrorism" measures within cybercrime laws to punish media and journalists for reporting stories that can be deemed critical of government policies, or that expose corruption, crime, or human rights violations and abuses.

For instance, in **Pakistan,** a journalist with Dunya News, Shahzeb Jillani, was charged in 2019 with "cyberterrorism" under Section 10 of the country's Prevention of Electronic Crimes Act (PECA) for her reporting on a series of enforced

disappearances.[17] Scores of journalists have been arrested on charges of violating this law, which contains vague and overbroad provisions, including bans on online speech that brings the armed forces, judiciary, or intelligence agencies into "disrepute". Section 10 of the PECA imposes criminal penalties for content that "coerces, intimidates, creates fear, panic, or insecurity in the government, the public or society."[18] The offence is punishable with a fine or imprisonment of up to 14 years, or both.

Likewise, in **India**, journalist Rajesh Kundu, the owner of Indian news portal Ink, was arrested and charged with "cyberterrorism" in 2021 for one of his social media posts,[19] drawing strong criticism from journalists groups. The journalist had been covering protests by farmers in the state of Haryana against new farming laws. Kundu was charged under various sections of the Indian Penal Code and the Information Technology (IT) Act, including Section 66F, which criminalizes cyberterrorism as any act committed "with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people".[20] Punishment can include life imprisonment.

3.2 Countering disinformation, harmful content online

Governments also point to the swell of disinformation and other types of harmful speech online as grounds for expanding or developing new cybercrime laws. The rampant spread of misinformation and disinformation is indeed a legitimate policy concern – as these types of harmful content have a deeply corrosive effect on our news and information environments, and weaken trust in the media and other democratic institutions.[21] Likewise, the flood of hateful, racist,

[17] Pakistan extends bail for journalist accused of 'cyberterrorism' | Media News | Al Jazeera.
[18] The Prevention of Electronic Crimes Act, 2016
[19] Haryana: Journalist Booked For 'Cyber-Terrorism' Over Social Media Post
[20] Section 66F
[21] Disinformation is a threat to our trust ecosystem. Experts explain how to curb it |

abusive speech online can lead to real world violence, and can have a deeply damaging effect on public discourse, as well as perpetuate and entrench discrimination and other types of human rights harms toward individuals and groups, both on and offline.

Journalists themselves can be and often are targets of such harmful content – women journalists in particular – including targeted disinformation campaigns and online abuse, harassment, bullying, and threats.[22] A notable case is journalist Rana Ayyub, a prominent investigative reporter in India and Washington Post columnist and frequent critic of the current government, who has been the target of a relentless campaign of online harassment on an industrial scale.[23]

Despite the obvious harms caused by the proliferation of such harmful content, platforms have consistently failed to put effective policies and practices in place to control the spread of harmful content at the systemic and sustained levels, even when such content violates their own policies and terms. Policymakers have also failed to respond to these challenges in ways that adequately address these issues at their root – the surveillance capitalism-based business model[24] – and in ways that protect expression and access to information rights.

Instead, many governments around the world have leveraged and exploited the legitimate problem of disinformation and harmful content online and disinformation to impose new restrictions on online spaces and crack down on critics and journalists.

World Economic Forum

[22] The Issue - On The Line, International Press Institute.

[23] Rana Ayyub is targeted online every 14 seconds, says an ICFJ study; Rany Ayyub: Targeted online violence at the intersection of misogyny and Islamophobia.

[24] It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy - Ranking Digital Rights

Disinformation: Harmful, but not illegal

Numerous international bodies, as well as regional and domestic courts have found laws aimed at prohibiting disinformation, or so called "false news" laws, to be a disproportionate restriction of freedom of expression. This is primarily because definitions of "false news" provided for in such laws are missing, or are vague and ambiguous – which itself is regarded as incompatible with legitimate restrictions on freedom of expression rights under international law. The basis of this is the 'three-part test', which says that states may only impose restrictions on the right to freedom of expression in the narrowest of circumstances, and on the condition that the state can demonstration that such limitations are clearly provided for by law; serve a legitimate interest; and are necessary and proportionate to protect that interest.

➔ *See: Joint Declaration on Freedom of Expression and "Fake News", Disinformation And Propaganda, OSCE.*

Prior to the pandemic, a growing number of governments were using so-called "fake news" laws to crack down on journalists and to drive distrust in critical media – a trend that had emerged as a major threat to press freedom globally.[25] During the pandemic, governments around the world used concerns about the spread of misinformation and disinformation relating to the COVID-19 to justify the expansion of restrictions and to criminalize a broad range of speech that could be deemed critical of state responses to the crisis.

IPI's COVID-19 Media Freedom Monitoring tool tracked and documented the remarkable spread of new restrictions and

[25] Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally

emergency decrees prohibiting "false news" at the outset of the pandemic.[26] These measures outlawed all forms of online disinformation, with vaguely defined provisions allowing prosecutors to charge or fine journalists for publishing any information about the pandemic that could be regarded as critical of the state.

The pandemic saw a new wave of such measures, rushed through parliaments with little resistance or debate – with the intention of rolling back these emergency measures once the pandemic passed.[27] However, as IPI's global monitoring has shown, in some countries the "fake news" measures passed during COVID were quickly transposed permanently into domestic criminal codes – including, often, in domestic cybercrime laws.[28]

In **Kenya**, numerous bloggers in 2021 were arrested for publishing "false information" during COVID under the country's 2018 Computer Misuse and Cybercrimes Act – which was revised in 2021 to include new provisions banning 'false news'.[29] Among them was blogger Robert Alai, who was arrested for publishing 'false news' about COVID-19 on his social media, charged under Sections 22 and 23 of the Cybercrimes Act.[30] He had questioned the government's reported case numbers and was charged with spreading false information on Twitter before being released on bail. Sections 22 and 23 criminalize "false publications" which "intentionally publish false, misleading or fictitious data" and "knowingly publish false information that leads to panic, chaos or unrest".

Vague and overbroad prohibitions against so-called 'false news' are a common feature in all of the 30 cybercrime laws we reviewed for this study. These provisions are especially

[26] COVID-19 Media Freedom Monitoring - International Press Institute
[27] Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges, International Press Institute
[28] COVID-19 Media Freedom Monitoring - International Press Institute
[29] State opposes LSK case against arrest of bloggers
[30] Attacks against journalists in Eastern and Southern Africa, ARTICLE 19

concerning in countries where media and online news are already tightly controlled.

In **Iran**, for example, Chapter 5 of the Computer Crimes Law of 2010[31], which criminalizes the "dissemination of lies" published online, was used in 2020 to charge Majid Motalebzadeh, a journalist and media consultant for the Voice of Reforms newspaper.[32] He was charged by the Computer Crimes Prosecutor's Office with "spreading false news through computerized devices" and "insulting government officials". Chapter 5 criminalizes the publication of information online with the intent to "cause damage to another person or distress the public mind or official authorities". The charges were brought by the Cyber Police Unit (FATA), which was founded in 2011 to counter alleged Internet crimes. The law has been criticized as a central part of the regime's censorship apparatus. The journalist was sentenced to one year in prison.[33]

In **Zimbabwe**, numerous journalists have been arrested and charged for publishing falsehoods under the 2021 *Cyber and Data Protection Act*.[34] In 2022, journalists Wisdom Mdzungairi and Desmond Chingarande of media company Alpha Media Holdings were charged under this Act for transmitting "false data intending to cause harm" over an article they had published about a local cemetery.

In **Guinea**, *Law No. L/2016/037/AN on Cybersecurity and Personal Data Protection Law of 2016* regarding "false publications" was used in 2019 to charge the director of Lynx Radio, Boubacar Algassimou Diallo, and its founder, Souleymane Diallo, with spreading "false" information and complicity in an attempt to undermine the internal security of the state over the publication of comments by an activist which critical of the government.[35]

---

[31] Iran, Computer Crimes Law, 2010
[32] Majid Motalebzadeh arrested, charged with cybercrimes for economic reporting - Committee to Protect Journalists
[33] Islamic Republic of Iran: Computer Crimes Law, ARTICLE 19
[34] Journalist arrested and charged for publishing falsehoods | MISA Zimbabwe
[35] Guinea, Law No. L/2016/037/AN on Cybersecurity and Personal Data Protection Law of 2016

In **Pakistan**, lawmakers in 2022 agreed to amend the existing 2016 cybercrime law (PECA) to criminalize any "fake news" or the "ridiculing of a person" — which includes any government body — on television.[36] And in early 2025, lawmakers in Pakistan replaced the 2016 law with a new version, which was passed quickly[37] without input from key stakeholders and media organisations, sparking widespread protests by journalists and civil society.[38] While the stated aim of the cybercrime legislation was to more clearly define and address existing provisions on hate speech and disinformation, the new provisions are equally vague and overbroad, opening the door to further overreach and abuse.

Of particular concern is Section 26A, which punishes the "intentional dissemination, exhibition or transmission of information through any information system, that the sender knows or believes to be false or fake and likely to cause or create a sense of public fear, panic, disorder or unrest." A person convicted under section 26A may face an imprisonment term of up to three years or a fine of up to two million rupees (approximately USD 7,000) or both.

Legal uncertainty allows for arbitrary implementation, abuse

Along with their expansive scope, cybercrime laws often contain vague, poorly defined, or undefined terms – such as banning content or expression that incites 'public disorder', violates 'public morality', upsets 'peace and tranquillity', or 'undermines the state or the constitution' – as well as sweeping bans on the publication or dissemination of 'false news', examined above.

[36] Why Electronic Crime Prevention Ordinance has Pakistan journalists fuming and Opposition outraged – Firstpost
[37] Pakistan Cracks Down On Free Speech Online
[38] Nationwide Protests Against Pakistan's PECA Amendment - The Pinnacle Gazette

From a legal standpoint, such vague and overbroad terms can mean these offences are open to arbitrary interpretation or abuse by authorities. This type of arbitrary application and interpretation of criminal law violates the principle of legal certainty – a fundamental element of the rule of law – that requires laws to be formulated clearly so that their application is foreseeable.[39] The European Court of Human Rights (ECtHR) has, for instance, repeatedly stated that laws must be "formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct".[40]

For instance, in **Bangladesh** Cybersecurity Act (2023) prohibits expression that 'hurts religious sentiments' (Section 28) or 'deteriorates law and order' by 'disrupting communal harmony' (Section 31).[41] The CSA carries over these speech-related offenses from the previous cybersecurity law, 2018 Digital Security Act,[42] which was used to arrest hundreds of journalists in Bangladesh. The DSA was a remarkably powerful weapon for silencing journalists and critics in Bangladesh, casting a chill across the media and human rights communities.[43] The new Cybersecurity Act has already been used to crack down on civic space and human rights.[44]

In **Nicaragua**, the Special Cybercrime Law has become part of a growing tangle of laws used by authoritarian president Daniel Ortega to widen an existing crackdown on independent journalism.[45] The law — known as the "gag law"— was passed in 2020 by the governing Sandinista National Liberation Party and is one of the most problematic in Latin America.[46] It

---

39 Compilation of Venice Commission Opinions and Reports Concerning Legal Certainty
40 Compilation of Venice Commission Opinions and Reports Concerning Legal Certainty
41 Repackaging Repression: The cyber security act and the continuing lawfare against dissent in Bangladesh - Amnesty International
42 How Bangladesh's Digital Security Act Is Creating a Culture of Fear | Carnegie Endowment for International Peace
43 How Bangladesh's Digital Security Act Is Creating a Culture of Fear | Carnegie Endowment for International Peace
44 Restore freedom of expression in Bangladesh & repeal Cyber Security Act
45 Ley Especial de Ciberdelitos
46 Nicaragua's proposed 'cyber security' laws threaten press freedom - ipi.media

contains sweeping provisions that threaten journalists' rights, and has faced strong criticism from press freedom organizations over its broad scope and discriminatory application.[47]

Article 30, for instance, imposes harsh penalties for the publication or dissemination of false information that causes "alarm, fear, or anxiety in the population", a crime carrying between three to five years in prison, or a fine of three hundred to five hundred days' wages.[48] It is also possible that the law could be applied to journalists in exile, as the government may bring them to trial in absentia.

Likewise, vague and overbroad cybercrime laws are prevalent across the Middle East. In **Jordan**, thousands of journalists, writers, and activists were arrested under the country's former cybercrime law, which gave authorities sweeping powers to censor online speech.[49] The country's new 2023 cybercrime law – which criminalises a wide range of online expression activity, including defaming, insulting, or criticising public bodies and officials – has been used repeatedly to arrest journalists who covered Jordan's role in the Israel-Gaza war.[50]

In **Tunisia**, six journalists were arrested[51] in 2024 under the country's draconian cybercrime law,[52] which grants authorities extensive surveillance powers and carries prison sentences for the publication of "rumors" and "false news", among other vague and overbroad categories.[53]

Across Africa, cybercrime laws with vague and overbroad speech related offenses are commonly used to stifle the press. For example, **Niger**'s 2019 cybercrime law has been used to target critical online media and journalists, including Samira

47 Nicaragua's proposed 'cyber security' laws threaten press freedom - ipi.media
48 Nicaragua's regime expands repression to exiled journalists through sweeping cybercrime legislation - LatAm Journalism Review by the Knight Center
49 Jordan: Journalists calling out corruption muzzled by cybercrime laws | Middle East Eye
50 Jordanian journalist arrested under cybercrime law
51 Tunisia: IPI demands an end to repressive use of cybercrime law against journalists
52 Decree-law No. 2022-54 of 13 September 2022
53 Tunisia: Decree-law No 54 of 2022 - ARTICLE 19

Sabou and Moussa Aksar, who were convicted in 2022 of defamation by electronic means and disseminating data to "disturb public order" for sharing on Facebook a report on the alleged illegal acquisition of drugs from traffickers by the Niger authorities.[54] **Mali**'s 2019 Law on the Suppression of Cybercrime criminalizes online threats and insults with punishments of up to 10 years in prison.

Defamation, libel, sedition, and blasphemy: Extension of offline offences deemed inconsistent with international law

Many cybercrime laws criminalise certain types of expression online – such as defamation, libel, sedition, and blasphemy – which in the "offline" context are widely regarded as incompatible with international law and principles.[55]

According to such standards, journalists must be free to report and investigate stories of public interest without fear of criminal punishment. Any limits to these rights must be narrowly defined, clearly prescribed by law, and be necessary and proportionate. Although still present in many countries, criminal punishments for journalists on the basis of criminal defamation, sedition, and blasphemy laws have been consistently found to be incompatible with these principles.[56]

In practice, criminal defamation and libel laws can and often are used to limit and punish reporting on political figures and business elites – thereby undermining the media's role and right to report on matters of public interest. While all individuals have the right to privacy and the right to protect their reputations from intentional harm, public figures – i.e., political and business elites – should be exposed to higher

[54] IPI condemns convictions of two journalists in Niger (IPI)
[55] Defamation and Freedom of Expression: A summary - ARTICLE 19
[56] Out of Balance: Defamation Law in the EU (IPI)

levels of public scrutiny given the impact of their policies, decisions, and practices on society, the economy, and environment.

Likewise, criminal blasphemy laws – which are especially prevalent across South Asia and the Middle East – are likewise often deployed by authorities to reinforce dominant religious orthodoxies and to limit ideas and information that encourages human rights reforms.[57] Anti-blasphemy laws across the Middle East – for instance in Iran, Qatar, and Saudi Arabia – include harsh restrictions on any content that can be deemed to undermine Islam. While punishments vary widely, sentences can include life in prison or death.

In the online context, we are now seeing a proliferation of crimes such as "cyber libel", as well as online defamation, blasphemy and sedition within domestic cybercrime legislation. This poses new challenges, as there is a great deal of legal uncertainty, including questions of jurisdiction, when applying offline offences to the online realm. In any case, the inclusion of such offences within the scope of cybercrime laws has further entrenched problematic legal provisions within domestic criminal codes, and in many cases amplifying them, with cyber counterparts often carrying enhanced punishments in comparison to their 'offline' counterparts, as noted in the first section of this report.

[57] On Religious Freedom and Discontent: Report on International Standards and Blasphemy Laws, High Level Panel of Legal Experts on Media Freedom, Media Freedom Coalition, May 2023.

Offline and Online Rights

"[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights."

➔ *See: The promotion, protection and enjoyment of human rights on the Internet: Resolution adopted by the Human Rights Council on July 13, 2021*

Such is the case in the **Philippines**, where the country's Cybercrime Prevention Act of 2012[58] introduced significantly increased penalties for computer-related libel – doubling the punishment from six to 12 years in prison for cyber libel as compared to standard libel.

The Cybercrime Prevention Act covers a range of vaguely defined offenses, including "cybersquatting" and "cyber libel." Immediately after it was adopted, the Supreme Court issued a temporary pause on the law while reviewing its constitutionality.[59] However, the court upheld a majority of provisions, including the controversial cyberlibel offence, which has been widely criticized for violating international freedom of expression standards.[60] Since passing the law, authorities have charged multiple journalists with cyberlibel, including Maria Ressa.

[58] Republic Act No. 10175
[59] SC issues 120-day TRO on cyber law | Philstar.com
[60] www.hrw.org/news/2012/09/28/philippines-new-cybercrime-law-will-harm-free-speech

Expansive investigatory and surveillance powers

Cybercrime laws also often give authorities sweeping, unchecked surveillance and investigatory powers, along with other powers that threaten and undermine the journalists' right to privacy and security. Such powers are incompatible with international human rights law, case law, and investigatory procedures.[61]

Well-crafted cybercrime laws should be grounded in respect for human rights, including the fundamental right to privacy, and comply with existing data protection frameworks that dictate law enforcement powers and procedures in criminal investigations and prosecutions.

Such frameworks establish that any infringements to privacy must be narrowly drawn and for specific purposes clearly defined in law. At the minimum, principles of legality, fairness, subject consent, transparency, purpose specification, proportionality, data minimization and security should underpin the formulation and enforcement of cybercrime procedural law.

However, in many countries, cybercrime laws lack such effective oversight and procedural safeguards to protect against overreach and abuse. For instance, the 2023 Cyber Security Act in **Bangladesh** gives authorities sweeping powers to search, arrest and detain individuals and seize their devices without providing adequate safeguards.[62]

Tanzania's Cybercrime Act of 2015 – widely used to crack down on journalists, bloggers, and activists[63] – enables extensive surveillance and monitoring in the investigation of cybercrimes.[64] Part IV of the Act gives authorities broad

[61] Government surveillance | Media Defence - eReader
[62] Restore freedom of expression in Bangladesh & repeal Cyber Security Act
[63] internews.org/wp-content/uploads/2023/11/ARISA-IEA-CHAPTER-16-Tanzania.pdf
[64] Tanzania: The Cybercrimes Act 2015, Reporters Without Borders.

search-and-seizure powers, as well as the authority to issue orders for evidence preservation, and traffic and content data disclosure and collection without prior judicial authorization. Efforts to challenge some of these provisions at the Tanzanian High Court have been unsuccessful.[65]

Similarly, section 38 of **Nigeria's** Cybercrimes Act requires mobile and internet service providers to give law enforcement access to real-time communications and data without a prior judicial order or oversight.[66] Privacy risks are further compounded by the absence of a clearly defined criminal scope of the data retained by service providers.

Governments also have exploited cybercrime laws to restrict the use of privacy-enabling technologies, such as Virtual Private Networks (VPNs) and other tools to encrypt online activities and communications. For example, Article 12 of **Jordan**'s 2023 Cybercrime Law prohibits the use of IP-masking tools to commit or conceal a crime, an offense carrying up to six months in prison.[67]

These trends reflect wider efforts by lawmakers globally to weaken online anonymity and encryption – often justified on national security grounds. Such efforts are evident in many countries – from more repressive regimes, like Cuba and China, to democratic countries, like the UK and Australia.
The UK's Online Safety Bill,[68] which became law in 2023, drew major criticism from digital rights groups over measures which would essentially break end-to-end encryption on digital platforms. The criticism centred on the so-called "Spy Clause", Clause 122, which granted the regulator Ofcom powers to force tech companies and messaging service providers to deploy software to scan people's messages in the name of identifying child abuse content, which critics said would fundamentally

[65] www.mediadefence.org/resource-hub/wp-content/uploads/sites/3/2021/04/Jamii-Media-v-the-Attorney-General-of-Tanzania-and-Other-2017.pdf
[66] Cybercrimes (Prohibition, Prevention, etc) Act, 2015
[67] Jordan, Cybercrime Law of 2023
[68] Online Safety Act: explainer - GOV.UK

undermine user security and privacy.[69] The Act was passed without addressing key concerns, though implementation has been limited.[70] This came after the 2016 Investigatory Powers Act in the UK which broadened the electronic surveillance powers of intelligence agencies and police and granted them greater access to encrypted information.

In Australia, the Telecommunications (Assistance and Access) Act[71] passed in 2018 also drew criticism from digital rights groups for provisions which would force tech companies to give access to end-to-end encrypted messages to police and security agencies. The law allowed police to compel messaging app providers to create a technical function that would grant that access to encrypted messages of suspected criminals without the user's knowledge. As in the UK, this coercive clause has not since been used.[72]

The right to communicate anonymously online, including through the use of encrypted communications, is regarded as essential to the exercise of other human rights – including the right to privacy, the right to expression, the right to access information, and right to hold opinions.[73] As summarized by David Kaye, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: “Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference.”

Restrictions on anonymity not only curtail the ability of journalists to freely carry out sensitive investigative work and protect their own security and that of their sources, they also impede on journalists' right to freely share information.[74]

---

69 UK: 'Spy clause' in Online Safety Bill could lead to mass surveillance
70 Online dangers of UK government assault on encryption | openDemocracy
71 The Assistance and Access Act 2018
72 Australia’s big encryption-busting laws have done little more than give authorities the power to ask nicely | Paul Karp | The Guardian
73 https://documents.un.org/doc/undoc/gen/g15/095/85/pdf/g1509585.pdf
74 https://documents.un.org/doc/undoc/gen/g15/095/85/pdf/g1509585.pdf

Access restrictions: Shutdowns, website and platform blocking, filtering and content removals

Cybercrime laws are increasingly imposing obligations on internet intermediaries such as social media platforms, search engines and ISPs to restrict access to information deemed as illegal, harmful or objectionable, or to protect public order and national security. Orders include blocking blacklisted websites or services, limiting or removing access to certain information or shutting down internet access entirely. The necessity and proportionality of these actions are highly disputable, alongside concerns that some administrations front legitimate aims to conceal more sinister motivations of information control and suppression of critical expression and dissent.

Access restrictions often contradict international laws and standards on freedom of expression. The Joint Declaration on Freedom of Expression and the Internet clearly provides that 'Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.'

Often, internet intermediaries are forced to comply with questionable laws and directives that may conflict with international laws to protect their local business interests. In cases where laws vaguely define content moderation obligations, overregulation by private actors seeking to comply with local laws risks restricting legitimate content and stifling expression. When adherence to national laws lies in opposition to their international law duty to respect human rights, international law should take precedence. The duty to respect human rights includes taking clear steps to identify potential violations and abuses, through human rights due diligence and risk assessment, and then addressing adverse human

rights impacts arising from activities, products or services of internet intermediaries.[75]

States have a greater responsibility to not only respect but also to protect and promote human rights and must ensure that cybercrime laws that restrict access to and dissemination of information strictly comply with international human rights law. The existence of vaguely couched provisions with little or no judicial oversight or adequate procedural safeguards elicits concerns of human rights infringements.

For example, section 69A of **India**'s Information Technology Act, 2000 grants the government broad content-blocking powers for the interests of India's sovereignty, integrity, defence, security, foreign relations, public order or prevention of a related offence. The safeguards outlined by the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 exclude prior judicial oversight.[76] Together with the Telegraph Act, 1885 and the Code of Criminal Procedure, the legal basis for India's unmatched occurrence of internet shutdowns is codified. In 2024 alone, India implemented 84 shutdowns and over 1o shutdowns have been reported in 2025 with significant human rights and economic costs.[77]

Article 33 of **Jordan**'s cybercrime law empowers a competent public prosecutor or court to order for content removal or the blocking of information systems, social media platforms, or websites that host illegal content. The legislation lacks clear legal procedures to curb its abuse. As of 2023, Jordan has reportedly blocked over 300 websites as well as social media platforms and VPNs for varied reasons ranging from licensing violations, 'platform misuse' or poor content moderation. At times, the decisions are not justified, but the government's attempt to control information flow is evident. In 2021, the website of the International Consortium of Investigative

[75] UN Guiding Principles on Business and Human Rights
[76] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 — Centre for Internet and Society
[77] Lives on hold: internet shutdowns in 2024

Journalists (ICIJ) was blocked ahead of the publication of the Pandora Papers, which implicated Jordan's King Abdullah II; in the same year Clubhouse, a popular platform for political discussion, was blocked amid the COVID pandemic; and TikTok in 2022 during a demonstration about high fuel prices.[78]

Regional and global cybercrime frameworks

Beyond national legislation, there are two main regional frameworks addressing cybercrime: the Council of Europe's Budapest Convention, which applies to Council of Europe states but has been adopted by many more,[79] and the African Union's Convention on Cyber Security and Personal Data Protection. Recently, a global convention on cybercrime was adopted, despite robust objections from civil society and industry of weak human rights safeguards. The new UN treaty is not yet in force.

While regional frameworks such as the Budapest Convention have been in force since 2004, the development and implementation of problematic national cybercrime laws has largely outpaced or persisted despite these frameworks. State obligations under the treaties hold varying implications on freedom of expression and privacy rights that may be subject to abuse in regimes with weak human rights standards. Critics have generally called for stronger human rights safeguards under the frameworks discussed below.[80]

[78] Freedom of the net 2024: Jordan
[79] About the Convention - Cybercrime
[80] Comparative analysis: the Budapest Convention vs the UN Convention Against Cybercrime

8.1 The Convention on Cybercrime

The Convention on Cybercrime (Budapest Convention)81 was the pioneer regional legal framework on cybercrime and has widely influenced subsequent regional and national frameworks on cybercrime. The Convention was negotiated and adopted by the Council of Europe in 2004 and has been ratified by 78 states including Council of Europe members and non-members. The offences defined in the Convention are largely cyber-dependent crimes with a narrow range of cyber-enabled crimes on computer-related forgery, fraud and child pornography. The Budapest Convention has an extraterritorial application and provides a framework for international cooperation in the investigation and prosecution of criminal offences related to computer systems and data, or collection of electronic evidence for criminal offences. Although the Convention has a general human rights clause and recalls human rights obligations in other provisions, protections for privacy and freedom of expression could be stronger in the framing of specific offences, and during investigations and prosecutions.82

8.2 African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention,[83] is a binding regional standard-setting document. It mandates member states to develop or strengthen legal frameworks on electronic transactions, personal data protection, and cybersecurity and cybercrime. The Malabo Convention entered into force in June 2023, nine years after its adoption, after Mauritania became the 15th ratifying state. While more States

[81] Budapest Convention on Cybercrime
[82] ARTICLE 19's briefing: The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol
[83] Malabo Convention

are called to ratify the Convention, it can also benefit from additional guidelines and protocols to align it with the operational context and address substantive gaps.[84] For example, the omnibus nature of the instrument in covering three themes broadened the scope of policy issues requiring state endorsement and sacrificed detailed provisions on the three thematic areas. The Convention also lacks definitions for key terms such as electronic data and physical data. The instrument has a general human rights clause requiring that cybersecurity measures and legislation should not infringe on human rights. The concerning inclusion of content-related offences largely focuses on child sexual abuse material – the combatting of which has notably been used in other jurisdictions to justify attempts to weaken encryption – while also including offences such as the creation and dissemination of xenophobic or racist information in the absence of exceptions such as for journalistic or research purposes, threatening human rights. The Malabo Convention also fails to designate a regional monitoring body. Positively, the treaty is largely compatible with the Budapest Convention, easing member state compliance with international cooperation provisions.

8.3 United Nations Convention against Cybercrime

The UN Convention against Cybercrime (UNCC) is the first global multilateral treaty on cybercrime. The instrument aims to enhance international cooperation to combat crimes committed through Information and Communication Technology (ICT) systems and facilitate electronic evidence sharing for serious crimes. Adopted in December 2024 by the UN General Assembly, the treaty will enter into force 90 days after its ratification by 40 member states. The final draft of the UNCC has been widely criticised by various stakeholders. It failed to adequately consider concerns raised by civil society

[84] The Malabo roadmap: Approaches to promote data protection and data governance in Africa

organizations and industry on the human rights implications of the treaty that threaten free expression, media freedom and privacy rights.[85] Shortcomings include vague definitions, overcriminalization of offences beyond core [86]cybercrimes, expansive evidence sharing provisions that may facilitate transnational repression, and weak human rights safeguards. The UNCC largely confers states with the discretion to implement national human rights protections in discharging their treaty obligations. The extension of optional rather than mandatory human rights mandates to guide State action is especially detrimental in authoritarian regimes. The flaws in the substantive norms of the UNCC make it an inadequate international framework to guide cybercrime regulation.

Developing cybercrime laws that respect and protect human rights: Recommendations for states

The following recommendations can guide states and policy makers to develop cybercrime laws that respect fundamental rights and safeguard the rights of journalists to carry out their work freely and without undue interference.

Cybercrime laws should be based on the fundamental principle that human rights, and particularly the right to freedom of expression, freedom of information, and the right to privacy, apply equally online and offline. Cybercrime laws therefore must not be used as a general instrument to establish and prosecute criminal activities related to online media and expression, electronic communications, or to regulate online platforms.

Cybercrime laws should be narrow in scope to focus on conduct and activity that can only be committed using

[85] Joint Statement on the Proposed Cybercrime Treaty Ahead of the Concluding Session, January 23, 2024
[86] The UN General Assembly and the Fight Against the Cybercrime Treaty

information and communication technologies ("cyber-dependent" crimes). Cybercrime legislation must therefore avoid establishing and including in their scope "cyber-enabled" crimes, i.e., "traditional" crimes are already covered by general criminal legislation, even when these crimes have increased their impact, scale, or modalities through the use of information and communication technologies.

Cybercrime laws should be subject, before their adoption, to a wide and meaningful consultation process involving industry, civil society, experts/academia, independent technical experts and other affected stakeholders. The specific nature of cybercrime does not justify secretive approaches to legislative drafting and approval processes. The preparation and discussion of cybercrime laws must be preceded by a proper, independent technical assessment of the existing threats and criminal activities affecting the use of information and communication technologies.

Cybercrime laws should not be used to introduce aggravated or specific penalties for "cyber-enabled" crimes based exclusively on the fact that they are committed through the use of information technologies.

Cybercrime laws must be based on fundamental principles of criminal law and respect for international human rights laws and standards as established by universal and regional instruments. This includes the principle of legality, necessity and proportionality, fair labeling, presumption of innocence, due process, minimum criminalization, *mens rea*, and dual criminality, among others. Cybercrime law must not include measures that do not meet the three-part test (unambiguous law, pursuance of a legitimate purpose, and respect for the principles of necessity and proportionality).

Cybercrime laws should not put illegitimate restrictions on the right to freedom of expression and privacy according to international human rights law. This includes permitting internet shutdowns; wholesale blocking of services applications, encryption/VPNs or content; criminal defamation

provisions, or general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news", "non-objective information" , "false, deceptive, misleading or inaccurate content", "obscene content", "corruption of morals", "causing emotional distress", "threatening social peace and harmony."

As a general principle, cybercrime laws must require that offenses be committed intentionally and without any legitimate purpose or justification.

Cybercrime laws must include clear exceptions for journalists, whistleblowers, public watchdogs, researchers, or any person who uses or discloses information such as misconduct, wrongdoing, fraud, illegal activity, human rights violations – for the purpose of protecting a general public interest. There must also be clear public-interest exceptions in areas such as privileged information, and the protection of confidentiality of journalist sources.

Cybercrime laws must include robust safeguards and oversight regarding data sharing and communications surveillance by authorities. Measures established for the purpose of specific criminal investigations and proceedings must incorporate robust human rights safeguards to prevent unnecessary and disproportionate interferences. This includes, at minimum, requirements for prior independent (judicial) authorization of surveillance measures and monitoring throughout their application; adequate notification of the individuals concerned once it no longer jeopardizes investigations; and transparency obligations such as regular reports, including statistical data on the use of such measures.

Cybercrime laws must establish adequate safeguards to prevent political interference and arbitrary control. In cases where the enforcement of legal and regulatory provisions has an impact on the exercise and effective protection of fundamental rights, decisions must be taken by an independent regulatory body or agency (subject to judicial oversight) or a judge/court.

Human rights institutions and bodies must be granted specific oversight and reporting powers regarding the implementation of cybercrime laws. All authorities identified or designated to monitor, enforce, or develop provisions included in cybercrime law must count on adequate resources, tools, and technical capacities to perform their tasks.

International cooperation provisions contemplated in national legislation on cybercrime must be narrowly defined in scope and incorporate limitations and safeguards to guarantee the respect for the already mentioned fundamental principles of criminal law and human rights standards.

International cooperation provisions contemplated in national legislation on cybercrime must only apply to “cyber-dependent” crimes directly contemplated by these laws.

The sharing of data and surveillance across jurisdictions requires strong safeguards, such as prior judicial authorization and data protection oversight, as well as effective remedy, transparency, and user notification, in line with applicable legislation and international human rights standards.