Freedom of Information and expression needed for protecting human rights from social violence (사회적 폭력으로부터 인권을 보호하기 위한 정보자유와 언론자유)

Kyung Sin ("KS") Park, Open Net/Korea University

May 16, 2023

Goal 16. Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

Target 16.10: Ensure public access to information and protect fundamental freedoms

The full text of Target 16.10: "Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements."

The target has two indicators:

- Indicator 16.10.1 Number of verified cases of killing, kidnapping, enforced disappearance, arbitrary detention and torture of journalists, associated media personnel, trade unionists and human rights advocates in the previous 12 months.
- Indicator 16.10.2 Number of countries that adopt and implement constitutional, statutory and/or policy guarantees for public access to information.

There are three important topics I would like to discuss today:

1. Access to Information
    1.1 FOIA laws and Korea case
    1.2 Open government data and Korea case
    1.3 New threats to FOIA: National Critical Technologies and other national security-based exceptions
2. Persecution of Journalists
    2.1 Criminalization of speech and journalists
    2.2 Legal strategies for protecting journalists
3. Internet freedom
    3.1 Value of internet as seen through prism of internet shutdowns
    3.2 Emerging threats to internet freedom in Korea and other parts of Asia – 4 layers of data governance

---

1.1 FOIA laws and Korea case

Freedom of Information (FOI) laws are a crucial element of democratic governance, as they ensure transparency and grant citizens the right to access information held by public authorities. Over the years, more countries have recognized the importance of these laws and have adopted them in varying degrees.

Number of Countries with FOI Laws:
As of September 2021, more than 130 countries around the world have enacted Freedom of Information laws. This number has grown significantly since the first FOI law was adopted in Sweden in 1766, indicating a global trend toward increased transparency in governance.

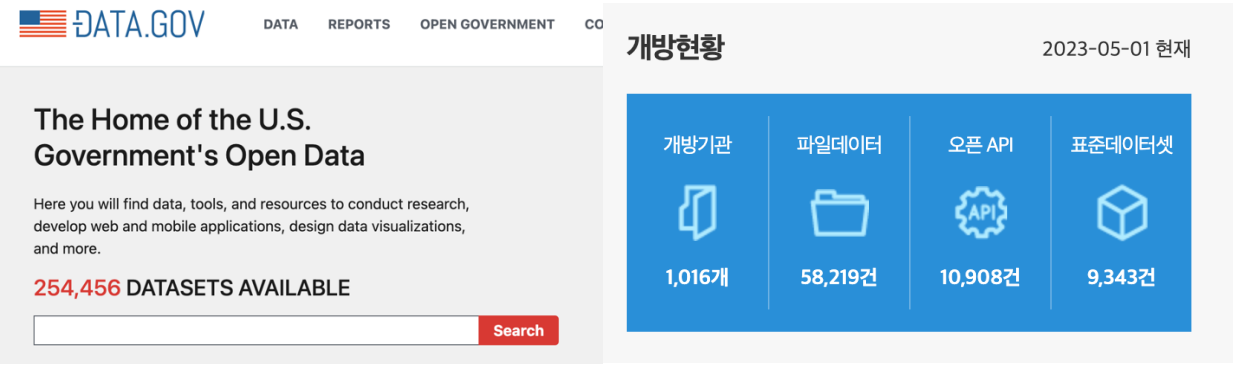
Korean FOIA law allows regulations to provide for exceptions from disclosure obligations while American FOIA allows only statutes to do so. This allows many minister-level departments and agencies to change their regulations so that the information they hold can be exempt from disclosure. Although these regulations are called “Presidential Decrees”, they are never like American ‘Executive Orders’ which are controlled closely by the White House itself.

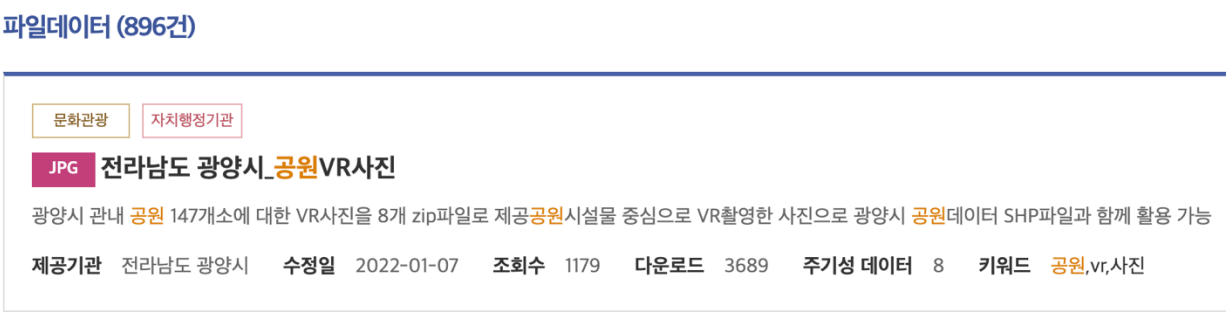
Korea’s Freedom of Information Act Article 9 Paragraph 1 Item 1 exempts from disclosure obligations the information ‘designated as confidential by other statute or regulation authorized by such statute’. According to this provision, courts reviewing non-disclosure cases have engaged in only formal review of whether such statute or regulation exists but not in any substantive review of whether such designation is constitutionally proper. Furthermore, there remains a controversy on whether only those laws and regulations specifically referring to the confidential information qualify under the provision or also those laws and regulations abstractly defining the types of the confidential information qualify, which grant discretion to the interpreting authorities. Finally, some courts do not even review de novo whether the discretionary non-disclosure decision by the interpreting authority is proper within the meaning of the relevant ‘other law and regulation’.

FOIA is supposed to guarantee the constitutional ‘right to know’ which predates the statute and should not be arbitrarily excised by the legislature, the regulator, or the interpreting authority, and the courts should play a role in making sure such result, and if it is difficult, we need to make legislative changes, based on comparative-legal analysis, to restore the constitutional status of the right to know.
First of all, courts must substantively review whether each ‘confidentiality’ designation by statute and regulation constitutes a proper limitation on the right to know to make sure that the legislative or the executive do not excessively restrict that right. Also, the ‘confidentiality’ designation should be done specifically on the subject data not by abstractly defining it using criteria that grant too wide discretion to the interpreting authority. Courts must recognize only the specific laws and regulations as ‘other laws and regulations’ qualified under Article 9(1)[1] of FOIA, or FOIA must be amended to ensure such result. Finally, courts at least must substantively check whether confidentiality designation has been properly made even within the meanings of the relevant ‘other laws and regulations’.

1.2 open data and Korea case

There are continuing instances of government agencies claiming exclusive ownership and access to otherwise publicly valuable data such as the train arrival time data. Korea’s success vis-à-vis open data belies weaknesses such as the fact that the country’s OGP efforts is still mono-ministerial as represented by the dearth of nation-wide data sets in the country’s main open data portal (data.go.kr) dominated by granular local-wide data sets submitted by local governments under the influence of the Public Administration and Safety Ministry. These are just some of the issues we need to confront as OGP enters its next decade.





<Comparison of U.S. and Korea on FOIA 2.0>

1.3 National Critical Technologies exception

Korea passed law in 2019 that made information about "national critical technologies" secret and therefore exempted from FOIA disclosure obligations. The immediate impact was that many workplace health advocates were immediately banned access to the valuable workplace hazard information that were mandatorily registered with the government agencies by the workplaces handling hazardous material, such as Samsung's semiconductor and LCD panel factories. In some cases, the workers' compensation lawsuit could not go forward because the workers do not have information about what toxic material they were required to handle work.

"National critical technologies" are the concepts originating from the 1980s when the U.S. and Japan decided to keep **ownership and practice** of certain technologies at home for national security purposes. It was not intended to keep **information** about those technologies. Some of NCT are patented and therefore already publicly available information and most of NCT do not even constitute trade secret. NCT regulations were simply designed to make sure NCT is owned and practiced by domestic personnel no matter how much information NCT is shared with others.

This is just one example of the new set of laws that are threatening the effectiveness of FOIA by making amorphous national-interest-based exceptions. The pre-existing national security exception to FOIA disclosure obligations is usually narrowly defined around military and diplomacy. The new "national interest" based exceptions within or outside FOIA should be resisted.

2.1 Persecution of journalists

The freedom of the press is a fundamental pillar of democratic societies, as it allows for the dissemination of information and the holding of power to account. However, journalists around the world continue to face persecution for fulfilling their roles. This report provides an overview of the state of persecution of journalists globally, highlighting key trends and concerns.

In recent years, persecution of journalists has increased in various forms, including harassment, threats, imprisonment, and even murder. Authoritarian regimes, extremist groups, and criminal organizations often target journalists who investigate or report on sensitive issues, such as corruption, human rights abuses, and organized crime. In 2022, according to the Committee to Protect Journalists (CPJ), a record number of journalists were imprisoned globally, with the majority being held in China, Turkey, Egypt, and Saudi Arabia. These imprisonments often occur under the pretext of national security, cybercrime, or defamation charges. Journalists have faced an increased risk of targeted killings and physical attacks in recent years. Countries such as Mexico, Afghanistan, Syria, and the Philippines have been particularly dangerous for journalists due to ongoing conflicts, drug cartel activities, and weak rule of law. The rise of social media and the digital era have given way to new forms of harassment against journalists. Online threats, doxxing, and targeted disinformation campaigns have become increasingly common, often with the intention of discrediting or silencing reporters. Many governments have used legal measures to restrict press freedom, such as implementing restrictive media laws, shutting down news outlets, and **blocking websites.** These measures are often framed as necessary for national security or public order but can ultimately serve to suppress critical reporting.

The lack of accountability for crimes against journalists remains a significant concern. According to Reporters Without Borders (RSF), in 9 out of 10 cases of murdered journalists, the perpetrators are never brought to justice. This impunity perpetuates a cycle of violence and fear, effectively silencing the press. The increased persecution of journalists has contributed to a decline in press freedom globally. According to the 2021 World Press Freedom Index, journalism is fully or partly blocked in 73% of the 180 countries surveyed. The persecution of journalists has serious implications for democracy, as it undermines and causes profound chilling effects on the role of the press in holding power to account and informing the public. This can lead to a decline in democratic values, increased corruption, and reduced transparency.

2.2 Criminalization of speech and strategies to fight them

Criminalization of speech refers to the use of legal means by governments or authorities to penalize certain forms of speech or expression, often under the pretext of preserving public order, national security, or protecting social values. This phenomenon can have a significant impact on the persecution of journalists, as it may be utilized to stifle dissent, limit press freedom, and suppress critical reporting.

Legal Measures to Silence Journalists:
Governments may employ a variety of legal measures to criminalize speech and target journalists, including:

a. Defamation Laws: Defamation laws, which protect individuals or entities from false statements that harm their reputation, can be abused to silence journalists who report on controversial or critical issues. Journalists may face costly lawsuits, fines, or even imprisonment for alleged defamation.

b. Blasphemy Laws: In some countries, blasphemy laws are used to target journalists who are perceived as criticizing religious beliefs or institutions. These laws can be exploited to suppress dissenting voices and limit freedom of expression.

c. Anti-Terrorism and National Security Laws: Governments may use broad and vaguely defined anti-terrorism or national security laws to prosecute journalists who report on sensitive topics or criticize the government. Such laws often grant authorities wide powers to surveil, detain, and charge individuals with little oversight.

d. “False news” crimes: _____

Chilling Effect on Press Freedom:
The criminalization of speech contributes to a chilling effect on press freedom, as journalists may self-censor or avoid reporting on certain issues due to fear of legal repercussions. This can result in less critical journalism, reduced transparency, and an erosion of democratic values.

Implications for Journalists' Safety:
Criminalizing speech can also increase the risk of physical harm to journalists. When governments or authorities label journalists as criminals or enemies of the state, it can encourage violence against them or legitimize their persecution. In some cases, this can lead to targeted attacks, abductions, or even murder.

Discrediting Journalists and Media Outlets:
The criminalization of speech can be used to discredit journalists and media outlets, undermining their credibility and authority in the eyes of the public. By painting critical journalists as lawbreakers, governments can turn public opinion against them, further hindering their ability to report on important issues.

2.3 Strategies to fight some of the Criminalizations

To address this issue, we proposed the following four **legal strategies** in terms of establishing press freedom and protecting journalists.

Firstly, criminal defamation has been condemned by international human rights bodies for being abused by not so democratic rulers as pretexts for oppressing the opponents, especially using prosecutorial resources for free. So, countries with safely democratic governments, say, European countries where criminal defamation originated from, refused to get rid of criminal defamation laws since their prosecutors are supposedly more independent and will not be commandeered to suppressing speech critical of the incumbent governments.

I don’t care about what ruminations, meditations, reflections, you European countries have about criminal defamation laws. Please remove the laws, if you are not using them, for god’s sake. As long as the laws are there, they are used to justify the existence of criminal defamation laws in other countries that look “up to” Europe, and in those countries, unlike Europe, it is actually used to send people into incarceration. There was one 20 month period back in 2005-2007 when about 200 people were punished to incarceration for defamation, another 40 or so people in Korea were punished that way, accounting for 28% of all people.

We should now make a straightforward argument against criminal defamation, not an argument based on the possibility of abuse because that argument is apparently not convincing European countries to actually abolish the law. The European Court of Human Rights has overturned many guilty criminal defamation judgments on various grounds and I cite them to show our country international repulsion against criminal defamation but none of them is fully satisfactory because none of them is categorically condemning the law.

Criminal defamation is usually justified by emphasizing the value of reputation and its importance to dignity. Lord Lester at MLRC yesterday said that reputation is on par with free speech. I do not believe so. Reputation is what other people think of you. Reputation is in other people's heads and under their control. Reputation doesn't belong to you as your limbs belong to you or as your private information belongs to you. You cannot control or assume what other people think of you before the supposedly defamatory remark has been made. No matter how well you behaved, people may have not thought nicely of you anyway for other reasons. Having said that, shall we really apply criminal law against an injury, the existence of which is not as certain as an injury, say, to your limbs?

To illustrate my point by comparison, let me tell you that I fully agree with criminal prosecution of privacy breach. People illegally wiretapping others whether they are police officers or not should be criminally punished for taking away what clearly belongs to others. Reputation on the other hand does not belong to you the same way.

If outright abolition is difficult, add at least a provision that officials cannot claim for criminal libel for statements on what they did at work. Why? Because such criminal libel prosecution ends up becoming a service done by prosecutors to their fellow officials, throwing their fairness in doubt. Susan at Google just mentioned that these days Korea is one of the 5 counties from which user data requests come supported by warrants. Well, a lot of times, prosecutors are really making data requests on behalf of fellow officials who filed a police report complaining of criminal libel.

The case in point, back in March 2009, a documentary done by Number 2 station's producers, PD Notes : Mad Cow Disease, in the country was criminally prosecuted for calling American beef dangerous when the agricultural minister declared the beef safe. The crime charged? Defamation. Wait a minute, for calling American cows dangerous? Whose reputation was harmed? The cows? Well, the prosecutors in the classically abusive case forewarned by international human rights bodies concocted an argument that defaming cows actually defames the agricultural minister who thought the cows were okay. Yes, the prosecutors were found not guilty through all three stages of the court. But the fact of prosecution alone chilled all other broadcasters and television producers into silence for close to 5 years since then and till now. No longer do we see television programs healthily critiquing government polices. Abolishing criminal defamation at least as to the statements about public officials will have prevented such tragic series of events.

Secondly, the other important strategy we should pursue is to abolish truth defamation, i.e., a system whereby liability attaches even to a true statement. People always talk about sex videos to support existence of truth defamation. Yes, we need a law criminally prosecuting a despicable ex-boyfriend for releasing a sex video with his girlfriend who now wants to leave him. We can make a special law about that. In Korea, sex video recorded or disclosed against the sex partner's will is subject to liability. Now, is that really a defamation law or a privacy law? It is privacy law because your reputation is not lowered by the people coming to knowledge that you are having sex. It is not your reputation hurt but your privacy. As I said before, I don't have a problem with criminal privacy law, so I will even approve criminal punishment of such video. Also, as many countries are adopting data protection laws under which privacy breaches are policed, abolition of truth defamation does not hurt.

A huge problem with truth defamation is that its existence distorts the burden of proof in favor of the prosecutor/plaintiff in falsity defamation cases, the staple of defamation litigation around the world. If you will be held liable regardless of whether your statement is true or not, judges will be naturally not so strict about the plaintiff's or prosecutors of burden of proving that what you said is false. This leniency is problematic because in most defamation cases it is usually the supposedly defamed party that has overwhelmingly more resources than the speaker/defendant in proving truth/falsity of a statement about him/herself. Therefore, the defamed party or the prosecutors can easily prevail on truth/falsity over the

speaker/defendant (This problem was further compounded in Korea by the recent Supreme Court precedent that imposed something like a burden of production on the defendant on the truth/falsity), who then has to establish a reasonable basis for having the supposedly false belief, a difficult task for a person who just wants to raise a doubt on another's secretly conducted behavior.

A case in point is that of Chung Bong-Ju, a politician who alleged that another politician Lee Myung Bak was involved in stock price manipulation of a company called BBK, who later became the President. Once in power, his prosecutors indicted him for election-related criminal defamation. Throughout the case, the court did not inquire into the truth of the statement and instead interrogated upon whether Jung had sufficient basis to say what he said. Jung, who merely wanted to cast doubt over Lee Myung Bak's financial deals, was not prepared to produce a basis that the judge now equipped with the benefit of hindsight will find sufficient.

I suspect that this will be a problem for all countries that have truth defamation in their books. It will corrupt the judicial process for falsity defamation cases. Actually, it is still mindboggling that many of the European countries place the onus of proving truth on the speaker in falsity defamation cases. But, I now suspect that it is the natural result of recognizing truth defamation: the presence of truth defamation tilts the burden of proof against the speaker.

Thirdly, if you are from countries with false news provisions, please do not give up even if the speech you want to defend contains clear falsity. There are a slew of international human rights law behind you that can back you up. I want to introduce this case of Minerva in Korea who was not only acquitted of all the charges but also the false news law was struck down as unconstitutional.

Minerva was a then anonymous economic pundit whose blog obtained a huge following of hundreds of thousands of daily visitors in a pre-SNS age by, for instance, correctly predicting the downfall of Lehman. He also criticized the government's exchange rate policy manipulated to give advantage of large cellphone and auto exporters such as Hyundai and Samsung at the expense of small to midsize companies, of course, to the wrath of the conservative politicians, who then called for a criminal investigation, for what crimes, only God knows. Our creative prosecution forces did come up with a provision that in the days of Morse code criminalized assumption of false identity over electric(not electronic, I guess) communication , and turned it into the false news provision.

How we won? There were many but among them was that we made a strong constitutional argument. We received the help not directly from Article 19 but from the case that Article 19 argued in Zimbabwe, also sadly but inevitabley the Canadian case of Zundel, the Holocaust denier. Especially helpful was the Zundel decision that said even clearly false statements need be protected because no one knows ex ante what is clearly false. Rainforest activists should be allowed to oppose deforestation without fearing that they will be thrown into jail in the event that the effect of deforestation on global warming turns out to be false. We built upon that argument and argued that, what is important is usually important on account of the fact that there is not much information available upon it. Since there is not much information on that subject matter, people should be allowed to say things that later turn out to be false. It will be different if someone's reputation is immediately at stake but when there is no one being directly hurt by the speech, the full free market of free ideas should be allowed to function. Again, I want to emphasize the importance of international human rights cases. Even if there is a false news provision, don't ever give up on making an argument that the law itself is void under human rights.

3.1 Internet freedom as seen through internet shutdowns

The extremely distributed architecture of the Internet has a civilizational significance of having given all powerless individuals an agency in mass communication previously available only to newspapers and broadcasting or other powerful individuals and entities hoarding their attention, and also has given them power of knowledge previously available only to governments and businesses. It has become tools for political equality and democracy for many around the world. In the words of one highest court, "[The] Internet, rapidly spreading and reciprocal, allows people to overcome the economic or political hierarchy off-line and therefore to form public opinions free from class, social status, age, and gender distinctions, which make governance more reflective of the opinions of people from diverse classes and thereby further promotes democracy. Therefore, anonymous speech in the Internet, though fraught with harmful side-effects, should be strongly protected in view of its constitutional values."[1]

Given its relationship to democracy and human rights, it is only dialectically befitting that the first major Internet shutdown threatening democratization movements also took place during the Egypt uprising in 2011.[2] Increasingly, successive regimes have resorted to Internet shutdowns or blockage of major social media platforms, from 75 in 2016, 106 in 2017, 196 in 2018,[3] and 213 in 2019[4] a majority of which has been enacted for the actual purpose of most of them for suppressing communications during political protest or instability, military actions, or elections.[5]

Their impact is beyond political. "People routinely depend on the Internet to stay in touch with family and friends, create local communities of interest, report public information, hold institutions accountable, and access and share knowledge".[6] Also economies suffer greatly: Brookings Institute estimated the impact on the combined GDP of 19 countries practicing Internet shutdowns to be 2.4 billion USD between June 2015 and June 2016, working back from the countries of GDP figures and the estimated percentage of contribution from Internet, mobile, and major apps.[7] The impact on social, cultural, and educational rights are far-reaching.[8]

---

[1] Korean Constitutional Court, 2010 Hun-ma 47, August 2012.

[2] http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html

[3] https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/

[4] TARGETED, CUT OFF, AND LEFT IN THE DARK, The #KeepItOn report on internet shutdowns in 2019 available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

[5] Id., and The State of Internet Shutdowns around the World: The 2018 #KeepItOn Report available at https://www.accessnow.org/cms/assets/uploads/2019/06/KIO-Report-final.pdf

[6] Internet Society, Internet Shutdowns: An Internet Society Public Policy Briefing, December 2019.

[7] Brookings Institute, "Internet Shutdowns Cost 2.4 Billions Last Year", October 2016 https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf ; See also CIPESA, Economic Impact of Internet Disruptions in Sub-Saharan Africa, September 2017 (employing similar methods as the Brookings Institute for 10 African countries), https://cipesa.org/2017/09/economic-impact-of-internet-disruptions-in-sub-saharan-africa; Deloitte, The economic impact of disruptions to Internet connectivity, October 2016, https://globalnetworkinitiative.org/wp-content/uploads/2016/10/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf (using similar methods as Brookings but granulating for different levels of connectivity); EXX Africa, Special Report: The Cost of Internet Shutdowns in Africa, https://www.exxafrica.com/special-report-the-cost-of-internet-shutdowns-in-africa;

[8] Disconnected: A Human Rights-Based Approach to Network Disruptions. Global Network Initiative. June 2018. https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf

These shutdowns of Internet or blocking of interactive social media platforms present unique *systematic* hurdles for media freedom as they interfere with "journalistic activities" by all *indiscriminately* - including those of professional journalists and "citizen journalists" and simple exchange of information and opinion among "netizens".

3.2 Lesser restrictions on internet freedom

It is easy to say that digital authoritarianism and digital populism are the two sides of the same coin – authoritarian governments often use private trolls or bots to spread the propaganda that justifies or incites public/private persecution of journalists -- but people often forget that such statement is ironic because populism requires support of the masses no matter how transient and misinformed it may be and authoritarianism at its core suppresses the will of the masses by force and pre-existing institutions. What makes possible this irony is the state's ability to conduct surveillance and censorship on people – an ability to identify and orient and selectively promote judicial and social attacks toward dissident activists and journalists.

There are four layers of state laws that affect the state's surveillance capacity. The first layer consists of **data availability**. Mandatory data retention laws fall under this category. Also, mandatory data localization laws also enhance data availability to the state by obviating the need for going through MLAT process for accessing foreign-based data.

The second layer consists of **data identification**. Mandatory identity verification laws fall under this category. Also the laws allowing warrantless "unmasking" of data significantly enhance the state ability to target dissidents.

The third layer consists of **data acquisition**. The laws allowing access to private data without judicial approval violate international standards of privacy or lower the bar of judicial approval to the extent that it is meaningless. In this presentation, I will discuss the laws and proposed laws of Indonesia, Myanmar, Viet Nam, and South Korea against the three-layer framework.

The fourth layer consists of **data restriction.** The laws criminalizing speech without clear external harms , which we talked about earlier,demonstrated fall under this category. Also, the administrative censorship laws imposing criminal/civil liability on authors and intermediaries for failure to take down noticed contents immediately or in unrealistic timeframes will constitute the most aggressive method by which governments restrict internet freedom in the ways that directly impact democracy.

If we survey Southeast Asian countries, Open Net's priority region, several of the countries which we identify have some or all of these elements, e.g, Indonesia' MR5, Viet Nam's Cybersecurity Law, Myanmar's Cybersecurity bill, (even Timor Leste's Cybercrime bill). Although we believe administrative censorship will be the most likely issue that we will work on for the regional report, measuring the size of the threat to internet freedom, we would like to keep monitoring the legal and extralegal situations in the region,.

Indonesia

- Data availability – "In order to prove the truth, the use of telecommunications facilities at the request by users of telecommunications services, the providers are obliged to record the use of telecommunications facilities used by the users, and to record the information in accordance with laws and regulations." (Article 41, Telecommunications Law" – mandatory data retention
- Data identification – mandatory registration of "electronic system operators" (Article 2 MR5) – any web/app mediating communication among ppl "to provide, manage, and/or operate

communications services including but not limited to short messages, voice call, video call, electronic mail, and conversation in network in the form of digital platform, network services and social media;" – no anonymity for intermediaries

- "Private Sector ESO provides access to Traffic Data and Electronic Systems User Information (Subscriber Information) requested by Law Enforcement Authorities in the event that the request is officially submitted to the Private Sector ESO Contact Person.(Article 36, MR5) – no anonymity for users

- Data acquisition – "For the purposes of the criminal justice process, telecommunication service providers may record the information sent and/or received by telecommunication service providers and provide the information as needed, by: (1) Written request from General Attorney and/or the Chief of Indonesian Police for specific criminal acts; (2) Request from investigators for specific criminal acts in accordance with applicable law." (Article 42, Telecommunications Law) – warrantless interception, also Article 36 warrantless acquisition of traffic data
- Data restriction – government demand "urgent" 4 hrs/non-urgent 24 hours takedown (Article 15, MR5) – "prohibited content" – definition "a. in violation of the law and regulation; b. causing public unrest and disturbance of public order; and c. providing information on the method or providing access to prohibited Electronic Information and/or Electronic Document." – but meaningless because once Minister finds it prohibited, ESOs have absolute duty to take down.

Myanmar

- 2022 Myanmar Cybersecurity Bill: ban use of virtual private networks (VPNs), abolish the need for certain evidentiary proof at trial, and require online service providers to block or remove online criticism of junta leaders.
- Data acquisition: Article 75 of the 2013 Telecommunications Law 391 grants unspecified government agents the authority *"to direct the organisation concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law"*. Although the clause adds this should be undertaken without impacting the fundamental rights of citizens, there are no further details on the process or privacy protections.
- Data restriction: Requires Digital Platform Service providers to block or remove content about which there is a "legitimate complaint" that the content "damages a person's social standing and livelihood." It would not require the information to be false or require a court order. - "misinformation and disinformation," information "causing hate, disrupting the unity, stabilization and peace," and statements "against any existing law."
- Prevalent use of Western-originated surveillance technlogies

Viet Nam

- Data availability and data acquisition: Decree 53 of the aforementioned Cybersecurity Law came into effect on October 1 2022, clarifying the rules that mandate all domestic companies and many foreign companies, including social media platforms, telecommunications services, payment providers, and gaming platforms, to store user data information locally and provide it to authorities upon request. (subscriber identifying information, for 24 months upon request)
- Data Restriction: Article 26 *Guarantees relating to information security in cyberspace* - Any domestic or foreign enterprise which provides services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [*cyberspace service provider*] has the following responsibilities: To prevent the sharing of information and to delete information with the contents prescribed in clauses 1 to 5 inclusive of article 16 of this Law on services or information systems directly managed by any agency or organization no later than twenty four (24) hours after the time of a request from the CTF under the Ministry of Public Security or from a competent agency under the Ministry of Information and Communications, and to save/maintain system logs in order to serve investigation of and dealing with breaches of the law

on cybersecurity within a [specified] period [to be] stipulated by the Government (2018 Cybersecurity Law) Information deemed particularly sensitive may be taken down within three hours.

- Article 16 *Prevention of and dealing with information in cyberspace with contents being propaganda against the Socialist Republic of Vietnam; information contents which incite riots, disrupt security or cause public disorder; which cause embarrassment or are slanderous; or which violate economic management order*
- Article 17 *Prevention of and combatting cyberespionage; and protection of information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace*
- Prevalent use of Western-originated surveillance technologies

Korea

- comprehensive online administrative censorship that is blocking many informative websites on such topics as North Korea, medical abortion (womenonweb.org), etc.;
- criminal defamation law applicable event to truthful statements, that has chilled much online whistleblowing such as #MeToo revelations or postings critical of the incumbents (US State has mentioned this in its annual human rights report);
- the sender pay interconnection rule that is causing fragmentation of South Korea from the rest of the world;
- mandatory notice-and-takedown that is together with truth defamation law and insult law incentivizing platforms to take down many clearly lawful contents such as consumer evaluations;
- warrantless user identification practice that has resulted in the unmasking of as many as 6-7 million users each year and therefore assisted suspicionless mass surveillance (warned to be struck down recently in the constitutional court but no legislative amendment forthcoming yet);
- the platform registration requirement that has been used by the government for collateral pressure on platforms ;
- the mandatory prior filtering for pretext of filtering out CSAM and revenge porno, that is putting all video uploads on major platforms through comparison against the government-pre-curated DNA fingerprint database.

Summary

- Germany's NetzDG – a response to disinformation – inspired administrative censorship regimes in Southeast Asia
- Data sovereignty and data localization in other parts of the world buttressed data availability initiatives in Southeast Asia
- Online safety bills in UK, Canada, Australia may end up justifying anonymity-restrictions in Southeast Asia
- Sale of 'dual-use' technologies by advanced countries should be regulated.
- Substance is of course more important, however, form should be always used with care.