Centre for International
Governance Innovation

Policy Brief No. 182 — January 2024

Digital Authoritarianism: The Role of Legislation and Regulation

Marie Lamensch

Key Points

- A unique relationship has emerged between states and private companies as they attempt to manage harmful speech within an ever-evolving information ecosystem.
- A growing number of illiberal and authoritarian regimes are deploying legislation and regulation as tools of digital authoritarianism; legislative and regulatory practices are also emerging among democracies, which complicates the discussion.
- International human rights law and initiatives can serve as a normative framework to confront digital authoritarianism. But the paucity of enforcement mechanisms, as well as tech companies' unique attributes, have limited their reach.
- Democratic governments, independent researchers and subject matter experts, as well as civil society groups, should collaborate to confront digital authoritarianism, including by working within multilateral bodies and emerging global tech initiatives.

Introduction

The utopian vision that the internet and social media would propel profound progressive change and weaken autocratic regimes is long gone. As information has moved online in the twenty-first century, so have repression and information manipulation, targeted and arbitrary surveillance, threats, and disinformation. Illiberal and autocratic state and non-state actors have learned to use digital technologies to manipulate the information space and shape it to their needs, both to suppress freedom of speech, and to monitor and control citizens.

The objectives of authoritarian information manipulation are not new — Adolf Hitler and Joseph Stalin had powerful and malignant propaganda and surveillance capacities, as have despots throughout history — but the modern tools are new. In 2023, the digital authoritarian tool box comprises a panoply of technologies, including social media platforms, artificial intelligence, spyware and surveillance cameras. Globally, we have seen a rapid convergence of such technologies and the application of legislation and regulation to shape the information ecosystem and control speech. This brings a significant erosion of fundamental freedoms and human rights, and of individuals' rights both on- and offline. As a consequence, democracy itself is undermined.

This policy brief will define digital authoritarianism and its practices, then cite case studies as an

About the Author

Marie Lamensch is the project coordinator at the Montreal Institute for Genocide and Human Rights Studies at Concordia University. Born in Belgium, Marie has lived in Germany, France, Canada and the United Kingdom. After completing a bachelor's degree in history (specialization in genocide studies) at Montreal's Concordia University, Marie volunteered in Ghana and Rwanda for several months where she also conducted research on reconciliation. She has a master's degree in conflict, security and development from the Department of War Studies at King's College London. She specialized in complex political emergencies, post-conflict reconciliation and women's roles during conflicts.

exploration of the relationship between national regulations and digital authoritarian practices. It will also examine the applicability and limitations of existing human rights norms, laws and initiatives to resist digital authoritarianism.

Defining Digital Authoritarianism

Erol Yayboke, director and senior fellow at the Center for Strategic and International Studies, based in Washington, DC, and Samuel Brannen, deputy assistant secretary of defense for plans and posture in the US Office of the Under Secretary of Defense for Policy, have defined digital authoritarianism as "the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties" (Yayboke and Brannen 2020). The authors place the focus on authoritarian leaders and regimes.

But one could expand their definition by applying Marlies Glasius and Marcus Michaelsen's twin concepts of "digital illiberal and authoritarian practices" in the digital sphere. Glasius, a professor of international relations at the University of Amsterdam, and Michaelsen, a senior researcher at Toronto-based Citizen Lab, argue that democratic states such as the United States, Germany and India may employ illiberal practices that impinge on or violate the rights of citizens, including arbitrary surveillance, disinformation and violation of freedom of speech (Glasius and Michaelsen 2018). The distinction between illiberal and authoritarian practices lies in the type and degree of harm and its political impact, these authors argue. While illiberal practices "infringe on the autonomy and dignity of the person," authoritarian practices "sabotage accountability and thereby threaten democratic processes" (ibid.).

Digital Authoritarian Practices through Laws and Regulations

The twenty-first century has seen the evolution of a new relationship between governments and private technology companies that provide communications infrastructure. The American legal scholar Jack M. Balkin (2018) envisions this as a triangle, formed by the nation-state, social media and internet infrastructure companies, and the user. The nation-state is capable, through regulations, for example, to coerce or co-opt private tech companies to limit freedom of speech or demand storage and access to user data, Balkin argues. As a consequence, he maintains, private tech companies have assumed a "state function of speech regulation and surveillance" (ibid.).

Meanwhile, social media and internet companies, which provide unprecedented access to worldwide information and communication, but also facilitate digital surveillance, have become the target of regulations governing speech, as well as the sharing of data (ibid.). This has led to a new public-private cooperation and co-opting between governments and private-infrastructure owners, Balkin believes, to the detriment of users and fundamental freedoms (ibid.).

One can speak here of cooperation, and not necessarily co-opting, because tech companies are interested primarily in profit. They are, therefore, typically willing to abide by national laws and regulations, especially if infractions can result in their being banned from a country or a market. Meta's decision to block news links in Canada in 2023 in response to the passing of Bill C-18, the Online News Act, is a notable exception.

As Balkin argues, "infrastructure providers are usually easier to locate, and most have good reasons to be receptive to state pressure. They want to make money, and they want to expand their markets to reach customers within the nation-state's jurisdiction. Even if infrastructure companies strongly believe in civil liberties and would rather not abridge the speech of their customers and end users, they may nevertheless conclude that cooperating with nation-states better furthers their profit-making goals" (ibid.).

As noted later in this brief, X (formerly Twitter) CEO Elon Musk has been willing to take down content at the request of the Turkish government ahead of that country's national elections to avoid his platform being blocked (BBC 2023). Similarly, the "Facebook Files," a collection of stories and internal documents leaked in 2021 to *The Wall Street Journal*, revealed that Facebook CEO Mark Zuckerberg had, in 2020, approved a decision to censor individuals and groups critical of the Vietnamese government, after that government threatened to block the social media platform from the country. As the information released on the personal websites of whistleblower Frances Haugen states, Haugen became concerned that the company was "prioritizing their own profits over public safety, putting people's lives at risk" (Wade 2021).

But Balkin's triangular model can be applied to both democratic and authoritarian states. Indeed, big tech companies such as Google, Meta, Alphabet and X themselves now admit that some form of speech and information regulation is needed. The European Union and Germany have passed laws to regulate online content and data access, including Europe's Digital Services Act, passed in 2023, and Germany's Network Enforcement Act (NetzDG), which came into effect in 2021.

Germany's NetzDG law has been widely debated and criticized. Passed by the German government to curb online hate speech, NetzDG imposes intermediary liability for large-scale social media networks and obliges platforms to take down what is considered illegal content — including hate speech, personal threats, defamation and antisemitism. But the law has been criticized by the international rights agency Human Rights Watch for being too vague and for turning private companies "into overzealous censors to avoid steep fines, leaving users with no judicial oversight or right to appeal" (Human Rights Watch 2018).

As argued by Daphne Keller, director of intermediary liability at Stanford's Center for Internet Society, the fear of legal responsibility can lead to over-implementation of content takedown (quoted in Mchangama and Fiss 2019, 5). Furthermore, as demonstrated by Jacob Mchangama, director at Justitia, and Joelle Fiss, human rights researcher and analyst consultant at the US Commission on International Religious Freedom, legislation such as NetzDG can accidentally become a model for use by flawed democracies and authoritarian states

(Mchangama and Fiss 2019), thereby contributing to the global erosion of internet freedom.

In the early days of the internet and social media, in the first decade of this century, autocratic leaders lost control of their message as communication and information went online and transborder. A government's power to legislate gives it an advantage over transnational companies such as Meta, X and Google. Legal and administrative actions are also useful for countries that, unlike China, do not have the capacity to build their own internet infrastructure.

Based on the findings of Freedom House's annual *Freedom on the Net* reports, there has been a steady growth of cyber laws, policies and regulations to curb user anonymity, limit access to information sources and increase surveillance and censorship. In 2019, 31 such regulations were passed worldwide (Shahbaz and Funk 2019, 28) followed by a staggering 69 in 2021 (Shahbaz and Funk 2021, 24). The year 2021 saw an outburst of regulations as norms "shifted dramatically toward greater government intervention in the digital sphere" (ibid., 2). This trend is also reflected in Twitter's July–December 2021 transparency report, which states that the company saw a "steady increase in actions taken" (Twitter 2021) against journalists and news outlets, particularly from India and Turkey, and a record of nearly 50,000 legal takedown demands to remove content.

David Kaye, who was UN Special Rapporteur on the promotion and protection of freedom of opinion and expression from 2014 to 2020, noted in his 2018 report to the Human Rights Council the growing trend by certain states to impose obligations on tech companies to restrict content: "obligations to monitor and rapidly remove content have also increased globally, establishing punitive frameworks likely to undermine freedom of expression even in democratic societies" (UN General Assembly 2018, para. 16). The Special Rapporteur acknowledged that companies face "pressure to comply with State laws that criminalize content that is said to be, for instance, blasphemous, critical of the State, defamatory of public officials or false" (ibid., para. 23).

Case Studies

In its 2021 *Freedom on the Net* report, Freedom House identified three types of national legislative or administrative actions aimed at regulating tech companies: online content laws; legal and administrative rules related to user data; and competition policies (Shahbaz and Funk 2021, 13–21). As noted, democracies can implement practices regarded as illiberal or authoritarian, or that may inspire rights abuses, using techniques similar to those of authoritarian states. Thus, case studies such as India and Turkey fall into the category of what Glasius and Michaelsen (2018) define as illiberal and authoritarian practices used by state actors, although both are democracies.

Saudi Arabia

Saudi Arabia's 2007 Anti-Cyber Crime Law criminalizes the "production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, or privacy, through an information network or computer."[1] According to Freedom House's 2022 Saudi Arabia *Freedom on the Net* report, Saudi dissidents and activists who criticize the government have seen their content removed and accounts blocked by platforms such as Facebook and Twitter.[2] According to a 2022 report by the Arab Center Washington DC, Saudi Arabia has the second-highest number of account removals by Twitter after China.[3] In November 2021, the Saudi Communication and Information Technology Commission (CITC) introduced the first draft of the Digital Content Platform Regulations aimed at regulating digital content, including audio and video. It includes requirements for social media platforms to obtain a registration certificate from the CITC and data protection authority, have a physical presence in the Kingdom, and to "comply with the regulations, acts, decisions, and instructions related to content regulations in force in the Kingdom."

1 *Anti-Cyber Crime Law*, Royal Decree No. M/17, 8 Rabi 1 1428, 2007, art 6, online: <www.dataguidance.com/legal-research/anti-cyber-crime-law-2007-royal-decree-no-m17>.

2 See https://freedomhouse.org/country/saudi-arabia/freedom-net/2022.

3 Ibid.

In 2021, Saudi Arabian authorities also published the Kingdom's first Personal Data Protection Law, which regulates the collection and storing of personal data, as well as the transfer of personal data out of Saudi Arabia. While this provides some protections to users, the law allows telecommunication companies to "retain and intercept customer data for use by law enforcement agencies and state authorities."[4] Indeed, the law states that "processing of Personal Data shall not be subject to the consent referred to in Paragraph (1) of Article (5) herein....If the Controller is a Public Entity and the Processing is required for security purposes or to satisfy judicial requirements."[5] The term "security purposes" can, therefore, lead to abusive access to users' personal data by state authorities.

Myanmar

Myanmar stands out as an example of how authoritarian forces can rapidly impose a digital dictatorship to quash democratic transitions. When the military junta staged a coup in February 2021, internet and mobile access were rapidly curtailed to prevent the mobilization of anti-military protests. After taking over the telecommunications department responsible for regulating telecom companies, the junta seized control of three of the country's four mobile service providers, including Norway-based Telenor, which sold its Myanmar operations following a military order to activate surveillance technology (Access Now 2022). The impact of the coup on internet and social media usage in Myanmar has been dramatic. Indeed, in the few years between the fall of the previous military rule in 2016 and the 2021 coup, Facebook had become a primary source of news for the Burmese population to the extent that users "confuse the Silicon Valley social media platform with the internet" (Mozur 2018).

In January 2022, Myanmar's military government introduced the second draft of a cybersecurity law that would require platforms to remove content such as "verbal statements against any existing law," "expressions that damage an individual's social standing and livelihood" or "disturb "stability" (Free Expression Myanmar 2022). The vagueness of the language means that digital companies may be held criminally responsible for hosting content critical of the government. The draft law also criminalizes the use of virtual private networks, thereby preventing users from communicating anonymously, giving the military government access to private data, and forcing online service providers to store data locally, which arguably makes it more susceptible to state control (ibid.).

In March 2023, Myanmar's Central Committee for Counter Terrorism introduced amendments and new bylaws that force providers to block access to a wide range of websites, mobile apps and social networks. The changes amended the Broadcasting Law and updated the Electronic Transaction Law to criminalize social media platforms for content deemed "fake news" or "unacceptable" (Sivaprakasam, Myant and Maguire 2023). The amendments also allow the committee to order the "'interception, blocking, and restriction' of mobile and electronic communications" (ibid.). Today, the people of Myanmar are limited to visiting just 1,200 government-approved websites, with access to Facebook, WhatsApp, X and Instagram heavily restricted (Shahbaz, Funk and Vesteinsson 2022, 6). In summary, Myanmar's military regime has created what a UN group of experts calls a "digital dictatorship" (UN Office of the High Commissioner for Human Rights 2022).

India

India's internet environment is assessed as only "partly free" by Freedom House. For several years now, the country has been counted among those that regularly shut down the internet and demand that social media platforms remove content deemed offensive to the government, according to reports from organizations such as Access Now and Freedom House as well as data from Twitter/X and Facebook.

Indeed, according to Twitter's July–December 2021 transparency report, the Indian government is the platform's largest requester of content removal, including on 114 accounts belonging to verified journalists and news outlets (Twitter 2021). This focus on restricting media content is emblematic of India's eroding democracy. Indeed, civil liberties, including freedom of expression and freedom of the press, have declined under Prime Minister Narendra Modi's leadership. According to the Freedom House 2023 country report, harassment, death threats and physical violence against journalists have

4 Ibid.

5 *Personal Data Protection Law*, Royal Decree No. M/19 and M/148, 2023, art 6, online: <https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal Data English V2-23April2023- Reviewed-.pdf>.

increased, leading to self-censorship.[6] Similarly, Paris-based Reporters Without Borders now ranks India 161 out of 180 in its Press Freedom Index and states "defamation, sedition, contempt of court and endangering national security are increasingly used against journalists critical of the government."[7] The erosion of freedom of expression and media freedom is clearly also happening online.

In 2000, the Government of India introduced the Information Technology Act (IT Act), which deals with cyber offences and electronic commerce in the country.[8] To adapt to the internet and social media era, the government has since passed a number of amendments to the IT Act and additional laws used by Indian authorities to censor political and religious speech, including criticism of the government.

The Information Technology Rules (IT Rules) enacted in February 2021 enshrined operational requirements on social media companies and digital news media. This has considerably limited access to online content in India. Under rule 16, for example, the Ministry of Information and Broadcasting has emergency powers to order content to be taken down. In January 2023, the IT Rules were used to block access to a BBC documentary investigating Prime Minister Modi's treatment of India's Muslim minority (Sharwood 2023). Under the new rules, intermediaries have "no less than thirty-six hours from the receipt of the court order or on being notified by the Appropriate Government or its agency" to remove content regarded as defamatory, threatening the security of the State, undermining public order, decency, or morality (Ministry of Electronics and Information Technology 2021).

In April 2023, the government also announced Amendments to the IT Rules, which propose the setting up of a self-regulatory "fact-checking unit" by the central government. The state-run unit would have the power to label information related to the government as "fake, false or misleading" and "make it obligatory on the intermediaries to not to publish, share or host fake, false or misleading information in respect of any business of the Central Government (Ministry of Electronics and Information Technology 2023, annexure 5). In view of the fragile freedom of expression and civil situation in India, the amendments raise further concerns.

Turkey

Turkish authorities have a track record of cutting off access to social media amid criticism, protests and elections (Buyuk 2023; Kagubare and Klar 2023). According to the Freedom of Expression Association's EngelliWeb initiative, 349,763 websites were banned in Turkey between 2016 and 2020, as well as 7,500 Twitter accounts, 50,000 tweets, 12,000 YouTube videos and 8,000 Facebook posts (Stockholm Centre for Freedom 2021).

Turkey's response in 2023 to the earthquake in February and May elections is an example of the Turkish government's control over the country's information space. In the aftermath of the earthquake on February 6, the Turkish government temporarily blocked access to X, even though the platform was being used by people looking for family members trapped in the rubble. Turkish authorities claimed that some accounts had been spreading "untrue claims, slander, insults and posts with fraudulent purposes" (Butler and Coskun 2023). The country's deputy infrastructure minister, Omer Fatih Sayan, said the takedown was due to the spread of disinformation (Ray 2023). However, the Turkish government's response to the earthquake had been heavily criticized on social media (ibid.). Indeed, following the earthquake, Turkish authorities arrested 78 people for creating fear by sharing "provocative posts," including four journalists (Atanesian and Kalle 2023).

With the re-election of President Recep Tayyip Erdogan in May 2023, the situation is unlikely to improve for social media companies. In 2021, the Turkish leader described social media as one of the main threats to democracy (Al Jazeera 2021).

Big Tech and Human Rights

Since the mid-2000s, private tech companies such as Facebook/Meta, Twitter/X and Google have amassed great influence, not simply financially, but in terms of collection and retention of user

6 See https://freedomhouse.org/country/india/freedom-world/2023.

7 See https://rsf.org/en/country/india.

8 *Information Technology Act* (India), 2000 (No. 21 of 2000), online: <https://eprocure.gov.in/cppp/rulesandprocs>.

data and the ability to shape what millions of people around the world see, say or can access online. As Jeffrey Rosen, a law professor at George Washington University, said of Facebook in 2010, "[The company] has more power in determining who can speak and who can be heard around the globe than any Supreme Court justice, any king or any president" (Helft 2010). This power has enormous implications for the fundamental rights of individuals, media freedom and democracy in general. At the same time, these private tech companies are not governed by any specific international norms or rules. That led UN Special Rapporteur David Kaye to state that these "companies perform public functions without the oversight of courts and other accountability mechanisms" (UN General Assembly 2018, para. 20).

As governments seek to pressure digital companies to regulate content and/or provide access to user data, how should these firms respond? Can international law or other instruments provide solutions to the new "free speech triangle," the public-private cooperation and co-option described by Balkin (2018)? Can and should tech companies be held accountable for their impacts on society and human rights? The following section will explore the applicability and limitations of existing human rights law and mechanisms in the digital sphere and the tech sector.

International Human Rights Law

International human rights law is, first and foremost, addressed to states. It is important to note that article 19 of the International Covenant on Civil and Political Rights guarantees freedom of expression and the right to access to information, including online. Per article 19, states that seek to restrict freedom of expression may only do so for the purpose of protecting national security, public order or the rights and reputations of others (legitimacy) (UN Human Rights Committee 2011, para. 32). Furthermore, restrictions must be "provided by law" (legality) and "must conform to the strict tests of necessity and proportionality" (ibid., para. 12 and para. 15).

In his landmark 2018 report, UN Special Rapporteur Kaye used international human rights law as a basis for addressing the regulation of user-generated online content. Outlining the obligations of states and companies, the report underlines that "human rights law gives companies the tools to articulate their positions in ways that respect democratic norms and counter authoritarian demands" (UN General Assembly 2018, 1). Kaye reiterates that the principles of necessity, proportionality, legality and legitimacy mentioned above should be incorporated in the terms of service and community standards of the companies.

The UN Guiding Principles on Human Rights

The UN Guiding Principles on Human Rights were adopted in 2011 in an attempt to hold businesses accountable for their human rights impact. The principles outline a state duty to protect under human rights law, the corporate responsibility to protect, as well as the need to ensure remedies to victims of human rights violations.

In his report, Kaye cites the UN Guiding Principles on Business and Human Rights as a framework for the rights and obligations of internet companies. The principles state that "business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved" (UN Office of the High Commissioner for Human Rights 2011, 13). The UN Guiding Principles on Business and Human Rights may serve as guidelines to social media and internet companies when faced with government requests for content takedown and data access.

The Global Network Initiative

In recent decades, social media and internet companies have become increasingly willing to adopt human rights language in their operational rules. This is perhaps best exemplified by the launch in 2008 of the Global Network Initiative (GNI), a voluntary movement to deal with requests received by companies to "censor content, restrict access to communications services, or provide access to user data."[9] Companies such as Meta, Google, Microsoft and Telenor, along with academics and civil society groups, are members of the GNI. Notably absent is X. As part of the initiative, participating companies are "independently assessed every two or three years in their progress in implementing the GNI principles."[10]

9 See https://globalnetworkinitiative.org/about-gni/.

10 See https://globalnetworkinitiative.org/company-assessments/.

The GNI principles outline that "participating companies will respect and work to protect the freedom of expression rights of users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to communications, ideas and information in a manner inconsistent with internationally recognized laws and standards" (GNI 2017a, 3).

Furthermore, the GNI Implementation Guidelines for the Principles on Freedom of Expression and Privacy state:

> 3.3 When faced with a government restriction or demand that appears overbroad, unlawful, or otherwise inconsistent with domestic laws or procedures or international human rights laws and standards on freedom of expression or privacy, participating companies will in appropriate cases and circumstances:
>
> a. Seek clarification or modification from authorized officials of such requests;
>
> b. Seek the assistance, as needed, of relevant government authorities, international human rights bodies, or non-governmental organizations; and
>
> c. Challenge the government in domestic courts. (GNI 2017b, 10)

The principles outline important steps that companies could take to counter state overreach. Whether they are willing to do so or whether this human rights language is only used to improve the image of social media companies remains to be seen.

The Limits of Human Rights Norms and Laws

In practice, there are limits to the applicability of the global human rights norms, guidelines and principles explored above. In an article in the *UC Irvine Journal of International, Transnational and Comparative Law*, Evelyn Douek, currently an assistant professor at Stanford Law School, explores the applicability of international human rights laws for content moderation and regulation. While Douek acknowledges that international human rights law provides a normative framework, she also presents its limitations, many of which are specific to the nature of social media and internet companies (Douek 2021).

As transnational private corporations, large social media and internet companies are unique. First, they operate across different socio-political and legal environments. Second, in the absence of concrete global regulations or a regulatory body, they rely on self-governance, community standards and moderation rules, many of which are applied with inadequate transparency or consistency. As Special Rapporteur Kaye noted in the report cited above, "the United Nations, regional organizations and treaty bodies have affirmed that offline rights apply equally online, but it is not always clear that the companies protect the rights of their users or that States give companies legal incentives to do so" (UN General Assembly 2018, 3). While other large-scale transnational companies lack transparency, the tech industry is particularly non-transparent as "even basic facts about the industry remain a mystery" and "the details of moderation practices are routinely hidden from public view, siloed within companies and treated as trade secrets when it comes to users and the public" (Buni and Chemaly 2016).

Guidelines such as the UN Guiding Principles and the GNI have no enforcement mechanism. For example, while the member companies of the GNI must undergo an assessment, the process is confidential, and the aim is "to determine whether each member company is making good-faith efforts to implement the GNI Principles with improvement over time."[11] Once again, there is a lack of transparency even within an initiative that is intended to provide comprehensive guidance. Moreover, companies cannot be forced to implement the policies and procedures outlined in the GNI. Instead, one must rely on their "good-faith efforts."

Since tech companies are primarily interested in profit, relying on their good faith is not sufficient. As Douek (2021) shows, GNI assessment mechanisms failed to reveal the extent of data gathering and sharing by many members of the GNI as part of the US National Security Agency's mass surveillance program. Furthermore, as of December 2023, the 2021–2022 company assessments are yet to be released. One could

11 See https://globalnetworkinitiative.org/company-assessments/.

argue that 15 years after its establishment as a voluntary network, the GNI has not proven effective in outlining the human rights responsibilities of social media and internet companies.

Another complication mentioned by Douek is the broad language of international law, including freedom of expression. She cites senior lecturer Sejal Parmar, who writes that "global human rights norms — from binding treaty provisions to soft law recommendations of international human rights bodies — are diverse, nuanced, evolving, sometimes inconsistent, and contested, especially in the area of freedom of expression" (quoted in Douek 2021, 53). Likewise, she cites Susan Benesch, who states that "human rights law on speech is confusing and not always applicable to private companies" (quoted in Douek 2021, 53). The vagueness of the language of international human rights law makes it susceptible to varying interpretations, and abuse by governments and companies. Thus, while the UN Guiding Principles and other principles may demand that companies place international law above national laws, international tech companies can easily evade their responsibilities. Douek (2021, 40) argues that the current lack of enforceable global or regional norms allows tech companies to "wrap themselves" in human rights law language in order to give themselves legitimacy.

How to Counter Digital Authoritarianism

Democratic governments should continue to work together to counter a creeping authoritarian encroachment on the internet. Democracies can and should develop common approaches, engage in diplomacy, coordinate best practices and set new standards to protect internet freedom. This includes through initiatives such as the Freedom Online Coalition recently chaired by the Government of Canada, the Technology for Democracy Cohort, and the International Telecommunication Union.

With the rise of national tech and cyber laws and regulations, companies can and should become more transparent about their national operations, particularly with regard to content takedown and demands for access to user data by government authorities. Adopting human rights language is a way for companies to acquire more public legitimacy. France's Duty of Vigilance Act, for example, requires large companies to, among other things, introduce "appropriate measures to identify, prevent and mitigate risks to human rights and the environment."[12]

The European Union is currently working on the adoption of the Corporate Sustainability Due Diligence Directive, which would require companies to undergo an impact assessment and establish due diligence procedures to address adverse impacts of their products and actions on human rights and the environment (European Commission 2022).

12 See www.assent.com/resources/knowledge-article/what-is-the-french-corporate-duty-of-vigilance-law/.

Works Cited

Access Now. 2022. "As Myanmar junta extends control over telcos, surveillance and privacy risks increase." Press release, January 24. www.accessnow.org/press-release/myanmar-junta-surveillance-telcos/.

Al Jazeera. 2021. "Turkey's Erdogan says social media a 'threat to democracy.'" Al Jazeera, December 11. www.aljazeera.com/news/2021/12/11/turkeys-erdogan-says-social-media-a-threat-to-democracy.

Atanesian, Grigor and Nihan Kalle. 2023. "Turkish journalists detained over earthquake reports." BBC, February 24. www.bbc.com/news/world-europe-64759377.

Balkin, Jack M. 2018. "Free Speech is a Triangle." *Columbia Law Review* 118 (7). https://columbialawreview.org/content/free-speech-is-a-triangle/.

BBC. 2023. "BBC News' interview with Elon Musk." BBC, April 12. www.bbc.com/news/av/world-us-canada-65249139.

Buni, Catherine and Soraya Chemaly. 2016. "The Secret Rules of the Internet." *The Verge*, April 13. www.theverge.com/2016/4/13/11387934/internet-moderator-history-youtube-facebook-reddit-censorship-free-speech.

Butler, Daren and Orhan Coskun. 2023. "Anger Over Turkey's Temporary Twitter Block During Quake Rescue." U.S. News, February 9. www.usnews.com/news/technology/articles/2023-02-09/anger-over-turkeys-temporary-twitter-block-during-quake-rescue.

Buyuk, Hamdi Firat. 2023. "Turkey Arrests 24 for 'Provocative' Social Media Posts on Quakes." Balkan Insights, February 20. https://balkaninsight.com/2023/02/20/turkey-arrests-24-for-provocative-social-media-posts-on-quakes/.

Douek, Evelyn. 2021. "The Limits of International Law in Content Moderation." *UC Irvine Journal of International, Transnational, and Comparative Law* 6: 37–76. https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1042&context=ucijil.

European Commission. 2022. *Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937*. COM/2022/71. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071.

Free Expression Myanmar. 2022. "Military's cyber security bill worse than their previous draft." January 27. https://freeexpressionmyanmar.org/militarys-cyber-security-bill-worse-than-their-previous-draft/.

Glasius, Marlies and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere." *International Journal of Communication* (12): 3795–813.

GNI. 2017a. "GNI Principles on Freedom of Expression and Privacy." May. https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf.

———. 2017b. "Implementation Guidelines for the Principles on Freedom of Expression and Privacy." February. https://globalnetworkinitiative.org/wp-content/uploads/2018/08/Implementation-Guidelines-for-the-GNI-Principles.pdf.

Helft, Miguel. 2010. "Facebook Wrestles with Free Speech and Civility." *The New York Times*, December 12. www.nytimes.com/2010/12/13/technology/13facebook.html?_r=0.

Human Rights Watch. 2018. "Germany: Flawed Social Media Law: NetzDG is Wrong Response to Online Abuse." Human Rights Watch, February 14. www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

Kagubare, Ines and Rebecca Klar. 2023. "Twitter's restriction of Turkish election content sparks fear of precedent." *The Hill*, May 25. https://thehill.com/policy/technology/4019109-twitters-turkey-election-sparks-criticism/amp/.

Mchangama, Jacob and Joelle Fiss. 2019. "The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship." Justitia, November 16. https://globalfreedomofexpression.columbia.edu/publications/the-digital-berlin-wall-how-germany-accidentally-created-a-prototype-for-global-online-censorship/.

Ministry of Electronics and Information Technology. 2021. *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*. February 24. www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

———. 2023. "Government Notifies Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics code) rules, 2021 for an Open, Safe & Trusted and Accountable Internet." Press release, April 6. www.pib.gov.in/PressReleasePage.aspx?PRID=1914358.

Mozur, Paul. 2018. "A Genocide Incited on Facebook, With Posts From Myanmar's Military." *The New York Times*, October 15. www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

Ray, Siladitya. 2023. "Twitter Back Online in Turkey After Government Block." *Forbes*, February 9. www.forbes.com/sites/siladityaray/2023/02/09/twitter-back-online-in-turkey-after-agreeing-to-strong-cooperation-on-tackling-earthquake-related-disinformation/?sh=130d8c502279.

Shahbaz, Adrian and Allie Funk. 2019. *Freedom on the Net 2019: The Crisis of Social Media*. Freedom House. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf.

———. 2021. *Freedom on the Net 2021: The Global Drive to Control Big Tech*. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf.

Shahbaz, Adrian, Allie Funk and Kian Vesteinsson. 2022. *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet*. Freedom House. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf.

Sharwood, Simon. 2023. "India uses emergency powers to order takedown of BBC documentary." *The Register*, January 24. www.theregister.com/2023/01/24/india_bbc_documentary_emergency_takedown/.

Sivaprakasam, Dhevy, Wai Phyo Myant and Méabh Maguire. 2023. "Myanmar's 'counter-terrorism' by-laws must be denounced for what they are — illegal." Access Now, April 19. www.accessnow.org/myanmar-counter-terrorism-law/.

Stockholm Center for Freedom. 2021 "More than 349,000 websites banned in Turkey in last 5 years." August 16. https://stockholmcf.org/more-than-349000-websites-banned-in-turkey-in-last-5-years/.

Twitter. 2021. "Transparency Report: Removal Requests — Jul–Dec 2021." https://transparency.twitter.com/en/reports/removal-requests.html#2021-jul-dec.

UN General Assembly. 2018. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/38/35. April 6. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement.

UN Human Rights Committee. 2011. "International Covenant on Civil and Political Rights." General Comment No. 34. CCPR/C/GC/34. September 12. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

UN Office of the High Commissioner for Human Rights. 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. Geneva, Switzerland: United Nations.

———. 2022. "Myanmar: UN experts condemn military's 'digital dictatorship.'" High Commissioner for Human Rights. Press release, June 7. www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship.

Wade, Peter. 2021. "Facebook Bowed to Vietnam Government's Censorship Demands: Report." *Rolling Stone*, October 25. www.rollingstone.com/politics/politics-news/facebook-vietnam-censorship-1247323/amp/.

Yayboke, Erol and Samuel Brannen. 2020. "Promote and Build: A Strategic Approach to Digital Authoritarianism." Center for Strategic and International Studies Brief. October 15. www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager Jenny Thiel
Senior Publications Editor Jennifer Goyder
Graphic Designer Abhilasha Dewan

For publications enquiries, please contact publications@cigionline.org.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org