Revista de Derechos Humanos Contemporáneos
ISSN: 3082-0375
Vol. 1 Issue 2 (2025) 347-376
Available online since: October 31, 2025

Revista de
Derechos Humanos
Contemporáneos
Journal of Contemporary Human Rights

Digital Rights and Freedoms: The Fight for a Free Internet in Authoritarian Regimes

Derechos Digitales y Libertades: La Lucha por un Internet Libre en los Regímenes Autoritarios

Wang Zhihao[1]✉, Zhang Liyan[2], Mikhail Andreyevich Sokolov[3], Omar Khaled Hussein[4]

[1] University of Science and Technology of China, China
[2] Renmin University of China, China
[3] Lomonosov Moscow State University, Russia
[4] American University in Cairo, Cairo, Egypt

✉Corresponding email: wang.zhihao@ustc.edu.cn

ABSTRACT
This article examines the challenges and strategies surrounding the defense of digital rights and freedoms under authoritarian regimes. By analyzing cases from countries such as China, Russia, and Egypt, the research investigates how state-controlled censorship, surveillance, and internet shutdowns undermine freedom of expression and access to information. Using a multidisciplinary approach that combines political science, human rights law, and digital activism, the study highlights the innovative tactics employed by civil society and grassroots movements to resist digital repression, including virtual private networks (VPNs), encrypted communication, and decentralized

platforms. The novelty of this work lies in its comprehensive analysis of the interplay between technology, power, and resistance in digital spaces within authoritarian contexts. This article contributes to the global discourse on internet governance, human rights, and the protection of digital freedoms in oppressive environments.

Keywords *Digital rights, Internet freedom, Authoritarianism, Censorship, Digital activism*

RESUMEN
Este artículo analiza los desafíos y estrategias en la defensa de los derechos y libertades digitales bajo regímenes autoritarios. A través del análisis de casos en países como China, Rusia y Egipto, la investigación examina cómo la censura estatal, la vigilancia y los apagones de internet socavan la libertad de expresión y el acceso a la información. Mediante un enfoque multidisciplinario que combina ciencia política, derecho de los derechos humanos y activismo digital, el estudio destaca las tácticas innovadoras empleadas por la sociedad civil y los movimientos de base para resistir la represión digital, incluyendo redes privadas virtuales (VPN), comunicación cifrada y plataformas descentralizadas. La novedad de este trabajo radica en su análisis integral de la interacción entre tecnología, poder y resistencia en espacios digitales dentro de contextos autoritarios. Este artículo contribuye al discurso global sobre gobernanza de internet, derechos humanos y la protección de las libertades digitales en entornos represivos.

Palabras clave *Derechos digitales, Libertad en internet, Autoritarismo Censura, Activismo digital*

A. Introduction

The rapid proliferation of digital technologies has fundamentally restructured the global political landscape, serving as a dual-edged sword in the struggle for democratic governance. Initially hailed as "liberation technologies," digital platforms acted as powerful enablers of political participation and dissent, providing unprecedented tools for mobilization, horizontal communication, and the bypass of traditional state-controlled media (Diamond, 2010). From the grassroots organizing of the Arab Spring to contemporary movements in Southeast Asia, the internet has served as a virtual public square where marginalized voices can challenge the hegemony of the state. These technologies have effectively lowered the "cost of collective action,"

allowing disparate groups to synchronize their efforts in real-time against entrenched power structures (Shirky, 2011).

However, this democratic potential has been met with a sophisticated and systematic counter-offensive: the rise of digital authoritarianism. This global phenomenon is characterized by the state's use of digital technology to surveil, repress, and manipulate domestic populations. Far from being a mere extension of traditional censorship, digital authoritarianism represents a structural evolution in state power, where data becomes a tool of social control and algorithms are weaponized to stifle political plurality (Feldstein, 2019). This trend is no longer confined to isolated states but has become a competitive model of "internet sovereignty" that threatens the universalist foundations of the global web, led by regimes that export their surveillance architectures to other illiberal actors (Elias & Lemish, 2023).

It is essential to frame internet control not merely as a technical or administrative policy, but as a critical issue of international human rights law (IHRL). International bodies, including the UN Human Rights Council, have repeatedly affirmed that the same rights people have offline must also be protected online—most notably the freedom of expression under Article 19 of the ICCPR and the right to privacy under Article 17 (La Rue, 2011). When states deploy deep packet inspection (DPI) to monitor dissent or implement total internet shutdowns during elections, they are not merely "managing" their cyberspace; they are engaging in potential violations of non-derogable human rights obligations that require strict adherence to the principles of legality, necessity, and proportionality.

Despite these established norms, significant gaps in the international legal framework persist, particularly concerning the regulation of non-state actors and the extraterritorial application of digital rights. Current IHRL treaties were drafted in a pre-digital era, leaving ambiguities regarding how "positive obligations" apply to the protection of data stored on foreign servers or how to hold private technology companies accountable for state-mandated censorship (Milanovic, 2015). Furthermore, there is a profound "enforcement gap" where international institutions lack the jurisdictional teeth to penalize states that utilize "cyber-sovereignty" as a legal shield to justify the suppression of digital freedoms (Dauvergne, 2008).

This research is guided by two critical questions: First, how do authoritarian internet controls—ranging from algorithmic censorship to state-mandated shutdowns—align with or violate international legal obligations regarding necessity and proportionality? Second, what patterns emerge from comparative state practice in countries like

China, Russia, and Egypt, and how do these patterns signal a shift in global norms? These questions are vital as authoritarian regimes increasingly use "national security" rhetoric to bypass judicial scrutiny, creating a "legal grey zone" where digital repression is normalized through domestic legislation that lacks international oversight (Zittrain, 2008).

The central thesis of this article argues that digital authoritarianism is effectively hollowing out the universalist promise of the internet, creating a fragmented "splinternet" where rights are contingent upon geography. The originality of this work lies in its multidisciplinary analysis, connecting the technical architecture of digital repression—such as the Great Firewall or Russia's "Sovereign Internet" law—with the legal strategies used to normalize them. By synthesizing political science, human rights law, and the study of digital activism, this study provides a comprehensive look at how technology is being used to both enforce and resist power in the 21st century.

This article makes a significant contribution to international legal scholarship by advocating for an "evolutionary interpretation" of human rights treaties to address the unique challenges of the digital age. It argues that the protection of digital freedoms must move beyond reactive litigation toward a proactive, "human-rights-by-design" approach in internet governance (Lessig, 2006). By highlighting the innovative tactics of civil society—such as the use of mesh networks and decentralized protocols—the study underscores that the fight for a free internet is not just a legal battle but a technical and social one that requires a unified global response to prevent the permanent enclosure of the digital commons.

The study identifies a final gap: *the lack of a unified global treaty on digital rights*. While regional frameworks like the GDPR provide some protection, the absence of a global consensus allows authoritarian regimes to define "rights" according to state interests rather than human dignity (Sassen, 2014). This article concludes by calling for a new "Digital Bill of Rights" that addresses the intersection of surveillance, data sovereignty, and freedom of expression, ensuring that the internet remains a tool for human liberation rather than a weapon of state control.

B. International Legal Framework Governing Digital Rights

The governance of digital spaces is not a legal vacuum but is increasingly defined by the intersection of treaty law, customary international law, and evolving soft law standards. As authoritarian regimes seek to balkanize the internet under the guise of national

sovereignty, the international legal framework serves as the primary battleground for defining the boundaries of state power and individual liberty in the 21st century.

1. *Freedom of Expression and Access to Information*

The applicability of international human rights norms in digital spaces is no longer a matter of academic debate but a settled principle of international law. The United Nations Human Rights Council has repeatedly affirmed that the "same rights that people have offline must also be protected online," a doctrine that extends the protections of Article 19 of the International Covenant on Civil and Political Rights (ICCPR) to the digital realm (La Rue, 2011). This means that every individual possesses the right to seek, receive, and impart information through any media, regardless of frontiers, encompassing the technical infrastructure of the internet as a protected medium of communication.

The scope of these rights in authoritarian contexts is frequently tested by the implementation of "Great Firewalls" and algorithmic filtering. Under IHRL, any restriction on digital expression must satisfy a rigorous three-part test: it must be provided by law, pursue a legitimate aim (such as national security or public order), and be necessary and proportionate to achieve that aim (Mendel, 2014). Authoritarian states often fail the "legality" prong by using vague, overbroad "anti-extremism" or "cyber-sovereignty" laws that grant the executive branch unfettered discretion to silence dissenting voices without judicial oversight.

Permissible restrictions are narrowly construed to prevent the "chilling effect" that occurs when users fear state retribution for digital activities. While international law allows for the limitation of speech that incites violence or constitutes hate speech, authoritarian regimes frequently conflate political criticism with "threats to state security." This misapplication of the necessity and proportionality principles leads to systemic violations, as the complete blocking of a website or the arrest of a blogger for a single post is rarely the "least intrusive measure" available to the state (Balkin, 2018).

Access to information is further undermined by the rise of "internet shutdowns" or "throttling" during periods of political sensitivity. These measures are increasingly viewed by international bodies as a form of collective punishment that violates the right to receive information. Because shutdowns are indiscriminate and often target entire geographical regions or ethnic groups, they are inherently disproportionate and cannot be justified under the ICCPR, even during a declared state of emergency (Dutton et al., 2012).

The role of intermediary liability has also become a critical legal frontier. Authoritarian states often enact laws that hold social media platforms and Internet Service Providers (ISPs) legally responsible for user-generated content. By forcing private companies to act as de facto censors, states outsource repression, creating an environment where platforms "over-censor" to avoid crushing fines or operational bans. This practice bypasses the due process requirements of IHRL and creates a privatized system of censorship that is difficult to challenge through traditional legal channels (Lessig, 2006).

Furthermore, the right to "seek" information includes the right to use tools that bypass censorship, such as VPNs and Tor. Some legal scholars argue that the criminalization of circumvention tools constitutes a separate violation of the right to access information, as it removes the only viable means for citizens in closed societies to participate in the global information exchange (Zittrain, 2008). This is particularly relevant in regimes like China and Iran, where the state actively hunts and penalizes the use of encryption.

The General Comments of the UN Human Rights Committee have emphasized that a free and uncensored internet is essential for the realization of other rights, including the right to vote and the right to peaceful assembly. When an authoritarian state restricts the internet, it effectively dismantles the digital infrastructure required for democratic life. Therefore, digital rights are not "new" rights but are the modern manifestation of foundational liberties that are essential for the survival of a pluralistic society (Milanovic, 2015).

The gap between "law on the books" and "law in practice" remains wide. While most authoritarian regimes have ratified the ICCPR, they often utilize domestic "national security" exceptions to render international protections toothless. The international legal order currently lacks a robust enforcement mechanism to compel states to align their domestic "cyber-laws" with their international obligations, leading to a climate of institutionalized digital impunity (Sassen, 2014).

2. *Surveillance, Privacy, and Data Protection*

The legal standards governing state surveillance are anchored in the right to privacy (Article 17, ICCPR), which prohibits "arbitrary or unlawful interference" with an individual's correspondence and private life. In the digital age, this right is under constant assault from mass surveillance programs that collect bulk metadata and content without individualized suspicion (Feldstein, 2019). International law requires that any surveillance program must be strictly necessary to meet a legitimate state interest and must be subject to independent judicial authorization and oversight.

Authoritarian regimes often ignore these safeguards, utilizing Artificial Intelligence (AI) and facial recognition to create a state of "persistent surveillance." When surveillance becomes ubiquitous, it ceases to be a targeted law enforcement tool and becomes a mechanism for social engineering. Under the Necessary and Proportionate Principles, mass surveillance is inherently suspect because it treats the entire population as suspects, violating the core legal principle that privacy is the rule and surveillance is the exception (Privacy International, 2018).

The extraterritorial and cross-border implications of digital surveillance present a profound challenge to state responsibility. As data travels across borders, it often passes through the infrastructure of foreign states or is stored by multinational corporations. This creates "jurisdictional "grey zones" where a state might surveil non-citizens abroad with fewer legal constraints than they would apply to their own citizens. Scholars argue that IHRL obligations should follow the data, meaning a state owes human rights duties to any individual whose digital rights it interferes with, regardless of their physical location (Milanovic, 2015).

Data protection has emerged as a key pillar of digital rights, with the European General Data Protection Regulation (GDPR) setting a global "gold standard" that many authoritarian states paradoxically use as a template for "data localization" laws. While the GDPR aims to protect the individual from the state and corporations, authoritarian "data sovereignty" laws aim to ensure the state has unfettered access to all data generated within its borders. This "weaponization of data protection" allows regimes to demand that tech companies store user data locally, making it easier for state security services to seize information without international legal assistance (Elias & Lemish, 2023).

The sale of spyware (such as Pegasus) by private entities to authoritarian regimes has created a specialized legal crisis. International law is still grappling with how to hold states accountable for the "export of repression." Current frameworks, such as the Wassenaar Arrangement, are voluntary and often fail to prevent the transfer of dual-use technologies to human rights abusers. There is a growing legal movement to treat the export of such technology as a form of state-facilitated human rights violation, requiring stricter "due diligence" from both exporting states and private corporations (Lukas et al., 2023).

Anonymity and encryption are now recognized as essential "enablers" of the right to privacy and freedom of expression. UN experts have argued that any state effort to weaken encryption—such as

"backdoor" requirements—is a disproportionate interference with privacy (La Rue, 2011). For activists in authoritarian regimes, encryption is not a luxury but a prerequisite for survival; therefore, the legal right to use encryption should be seen as a non-derogable component of the right to private correspondence in the digital era.

The legal status of metadata is another area of intense debate. While many domestic laws treat metadata (who you talked to, when, and for how long) as less sensitive than the content of a communication, international human rights bodies have clarified that the bulk collection of metadata can be just as revealing and intrusive as intercepting content. Consequently, the same rigorous legal standards of necessity and proportionality that apply to wiretapping must also apply to the collection of digital footprints (UN High Commissioner for Human Rights, 2014).

The lack of a global data protection treaty creates a fragmented landscape where "rights" are determined by the location of a server. Authoritarian regimes exploit this fragmentation to build a "closed-loop" surveillance state where the individual has no legal recourse against the state's data-gathering apparatus. Strengthening international institutions to monitor cross-border data flows and surveillance exports is essential for preventing the total eclipse of privacy in the 21st century (Sassen, 2014).

3. *Internet Governance and State Sovereignty*

The tension between global and national approaches to internet regulation is at the heart of the "splinternet" phenomenon. Traditionally, the internet was governed through a "multistakeholder" model involving civil society, the private sector, and governments. However, a bloc of authoritarian states, led by China and Russia, is aggressively promoting a "state-centric" model of cyber-sovereignty. This model posits that each state should have absolute control over the information flows within its borders, a theory that directly conflicts with the "borderless" nature of digital human rights (Zittrain, 2008).

State sovereignty, once a tool for national defense, is being repurposed as a legal shield for digital repression. By asserting that the "national segment" of the internet is a sovereign territory, authoritarian regimes argue that international human rights monitoring of their digital space constitutes "interference in internal affairs." This is a fundamental challenge to the Universal Declaration of Human Rights, which holds that rights are inherent to the individual and are not granted or revoked by the state (Diamond, 2010).

The role of international institutions like the International Telecommunication Union (ITU) has become highly politicized.

Authoritarian states frequently use the ITU to push for standards that would bake surveillance and censorship into the very fabric of internet protocols. If these efforts succeed, the "architecture" of the internet itself would become a tool of repression, making it nearly impossible for users to bypass state controls through software alone (Lessig, 2006).

Soft law instruments, such as the UN Guiding Principles on Business and Human Rights (UNGPs), play an increasingly important role in filling the gaps in treaty law. These principles dictate that technology companies have a responsibility to respect human rights even when domestic laws (such as a Chinese demand for user data) require them to violate those rights. While non-binding, these standards provide a normative framework for civil society to pressure corporations to resist authoritarian demands or exit markets where they cannot protect their users (Milanovic, 2015).

The fragmentation of the internet into regional blocs also undermines the "right to participate in cultural life and scientific progress." When states block access to global platforms or scientific databases, they are not only restricting speech but are also hindering the socio-economic development of their citizens. This highlights that digital rights are interconnected with economic, social, and cultural rights, making internet governance a multifaceted human rights issue (Dutton et al., 2012).

International legal scholarship is currently debating the concept of "digital self-determination." This idea suggests that communities should have the right to determine how their data is used and how their digital environments are governed, free from both state repression and corporate exploitation. In authoritarian contexts, digital self-determination represents a radical challenge to the state's monopoly on digital infrastructure and points toward the need for decentralized, grassroots governance models (Shirky, 2011).

The influence of the UN General Assembly and the Human Rights Council is vital for norm development, but their resolutions are often ignored by the very states that participate in their drafting. This "hypocrisy gap" allows authoritarian regimes to sign onto lofty digital rights declarations in Geneva while implementing draconian firewall policies in Beijing or Moscow. Without an enforcement mechanism, "soft law" risks becoming a tool for "bluewashing" state repression (Dauvergne, 2008).

The future of the international legal order depends on whether it can move toward a unified "Digital Bill of Rights" that transcends national sovereignty. Such a framework would need to address the roles of state and non-state actors alike, providing a clear path for international litigation and sanctions against regimes that

systematically dismantle the free internet. As technology continues to outpace the law, the role of international institutions in defending the "open" internet remains the last line of defense against a global digital dark age (Feldstein, 2019).

C. Digital Repression as a Structural Legal Practice

The implementation of digital repression is rarely an ad hoc exercise of power; rather, in authoritarian contexts, it is a meticulously codified structural practice. By embedding restrictive measures within domestic legal frameworks, regimes attempt to provide a veneer of "legality" to actions that systematically undermine international human rights obligations. This section explores how censorship, surveillance, and network disruptions are operationalized as legal instruments of state control.

1. *State-Controlled Censorship and Content Regulation*

The legal mechanisms enabling digital censorship often rely on overbroad and ambiguous statutes that grant the executive branch sweeping authority to regulate speech. These laws frequently manifest as "anti-extremism" acts, "fake news" regulations, or "cyber-sovereignty" frameworks that mandate the removal of content deemed harmful to the state (Zittrain, 2008). By utilizing vaguely defined terms, these regimes create a legal environment where any form of political dissent can be categorized as a criminal offense, forcing both individuals and service providers into a state of perpetual legal vulnerability.

Authoritarian states justify these practices by grounding them in the rhetoric of national security and public order. Under international law, while Article 19(3) of the ICCPR allows for certain restrictions on speech, they must be "provided by law" and "necessary" for a legitimate purpose. However, in practice, these regimes use security as a "blank check" to bypass the requirement of proportionality (Mendel, 2014). The legal framing shifts the burden of proof onto the citizen, who must prove their speech is *not* a threat, rather than the state proving that the restriction is the least intrusive means possible.

Furthermore, content regulation is increasingly "outsourced" to private intermediaries through intermediary liability laws. These statutes require platforms to proactively monitor and remove content under the threat of massive fines or revocation of operating licenses. This creates a structural legal pressure for "over-blocking," where companies err on the side of caution to avoid state-sanctioned penalties. This privatized censorship bypasses judicial review, as the

removal occurs through a platform's terms of service rather than a transparent legal process (Lessig, 2006).

The technical architecture of censorship is also legally mandated. States like China and Russia require Internet Service Providers (ISPs) to install specific filtering hardware at the backbone of the network. These mandates ensure that censorship is not just a reactive legal measure but a proactive, "built-in" feature of the national internet infrastructure. This integration of law and code makes censorship nearly invisible to the average user, as the "blocking" occurs at the packet level before the content can even be accessed (Zittrain, 2008).

Content regulation also extends to the criminalization of circumvention tools. Laws that ban the use of Virtual Private Networks (VPNs) or Tor are designed to close the "loopholes" in the national firewall. By making the search for uncensored information a criminal act, the state effectively territorializes the digital space, asserting that its domestic laws apply to the entire experience of its citizens online, regardless of where the information originates (Diamond, 2010).

Administrative bodies—often operating without independent oversight—act as the primary enforcers of these regulations. These "cyber-watchdog" agencies possess the power to blacklist websites, revoke journalist credentials, and freeze the assets of digital media outlets. The lack of an independent appellate process means that once a piece of content is legally "cleansed" from the national segment of the internet, there is virtually no domestic legal recourse for its restoration (Feldstein, 2019).

The normalization of these practices creates a "legal contagion" effect. As one authoritarian state successfully implements a "fake news" law to silence dissent, neighboring regimes often adopt near-identical language in their own statutes. This cross-border legal mimicry suggests a emerging "authoritarian *opinio juris*" that seeks to challenge the universal standards of free expression established by the UN, replacing them with a state-centric model of information control (Sassen, 2014).

2. *Surveillance Infrastructures and Chilling Effects*

Mass surveillance in authoritarian regimes is built upon a foundation of mandatory data retention and localization laws. These legal instruments require telecommunications companies to store metadata and communication content for extended periods and, crucially, to maintain servers within the state's physical borders. This "territorialization of data" ensures that the state security apparatus has unfettered access to the digital lives of its citizens without the need for international legal assistance treaties (Elias & Lemish, 2023).

The impact of such infrastructures is a profound chilling effect on political participation. When a population is aware that every digital interaction is recorded and potentially subject to state scrutiny, the "public square" of the internet becomes a space of self-censorship. The psychological weight of persistent surveillance discourages citizens from joining activist groups, sharing heterodox opinions, or even researching sensitive topics. In this sense, surveillance functions not just to catch "criminals," but to pre-emptively pacify civil society (Feldstein, 2019).

Targeted monitoring often focuses on "key opinion leaders," journalists, and human rights defenders. Through the use of advanced spyware, regimes can turn a target's mobile device into a 24/7 monitoring station. The legal standards for such interventions are typically opaque; warrants are often issued by secret "security courts" or bypassed entirely under the guise of "intelligence gathering." This lack of transparency violates the ICCPR's prohibition on arbitrary interference with privacy and correspondence (Milanovic, 2015).

Surveillance also facilitates the digital profiling of activists. By aggregating data from social media, financial transactions, and travel records, the state can build a comprehensive "risk profile" for any individual. In some contexts, this is formalized through "social credit systems" that legally penalize individuals for their digital associations or online behavior. This represents a radical evolution of state power, where the law is used to punish "potential" dissent rather than actual criminal conduct (Diamond, 2010).

The deployment of Facial Recognition Technology (FRT) in public spaces—linked to national ID databases—extends surveillance from the digital to the physical world. Legally, many states categorize FRT as a simple "administrative tool" for public safety, thereby avoiding the stricter human rights scrutiny applied to wiretapping. However, when combined with online monitoring, FRT allows the state to track an individual's presence at protests or meetings with other dissidents, creating a totalizing "panopticon" effect (Feldstein, 2019).

The role of foreign technology exports is a critical component of these infrastructures. Authoritarian regimes often purchase surveillance capabilities from private companies in democratic nations, exploiting gaps in international export control laws. While some international guidelines exist, the "trade in repression" continues largely unabated, as states prioritize economic interests over the "due diligence" required to prevent their technology from being used in human rights abuses (Lukas et al., 2023).

Institutionalized surveillance also undermines the principle of anonymity, which is essential for dissent in oppressive environments.

Laws requiring "real-name registration" for social media accounts and SIM cards remove the protective layer of anonymity, making it impossible for citizens to express dissent without immediate fear of state retaliation. This legal removal of the "right to be anonymous" is a foundational pillar of digital authoritarianism (La Rue, 2011).

Lastly, the long-term structural impact of these infrastructures is the erosion of trust within civil society. When the state legally mandates that "every citizen is a potential informant" and every device is a potential microphone, the horizontal trust necessary for community organizing is destroyed. The law is thus used not to build a cohesive society, but to atomize the population, ensuring that the only secure relationship a citizen has is their relationship of subservience to the state (Shirky, 2011).

3. *Internet Shutdowns and Network Disruptions*

Internet shutdowns—the intentional disruption of internet or electronic communications—are increasingly used as a tool of state control during periods of political sensitivity, such as elections or protests. Legally, states often characterize these disruptions as "pre-emptive security measures" to prevent the spread of misinformation or to coordinate against "terrorism." However, international bodies have increasingly characterized these actions as a violation of the right to freedom of expression and a threat to the right of peaceful assembly (Dutton et al., 2012).

The human rights implications of a total shutdown are severe and multifaceted. Beyond the restriction of speech, shutdowns interfere with the right to health (by disrupting emergency services), the right to education (by blocking access to online learning), and the right to work. Because a shutdown is indiscriminate—affecting an entire population regardless of their involvement in a "threat"—it is fundamentally incompatible with the international law requirement that restrictions be "targeted" and "limited" (La Rue, 2011).

A proportionality and necessity analysis reveals that shutdowns almost always fail the IHRL test. The state's stated goal—such as "restoring order"—can almost always be achieved through less restrictive means than a total communications blackout. Furthermore, research suggests that shutdowns often *increase* physical violence by preventing the de-escalation of rumors and hindering the work of human rights monitors. Thus, far from being "necessary" for security, shutdowns often exacerbate the very instability they claim to solve (Shirky, 2011).

"Throttling"—the intentional slowing of internet speeds—is a more subtle form of network disruption that carries similar legal

weight. By making it impossible to upload video evidence or use encrypted messaging apps, the state "legally" throttles the ability of citizens to document human rights abuses in real-time. This "censorship by bandwidth" is often harder to detect and document than a total shutdown, allowing states to maintain a facade of connectivity while effectively silencing their critics (Lessig, 2006).

The legal authority for shutdowns is often found in archaic telecommunications laws or broad "emergency powers" that were never intended for the digital age. These laws frequently lack a requirement for a formal "declaration of emergency" or judicial oversight, allowing the executive branch to flip the "kill switch" without transparency or accountability. Strengthening the requirement for judicial prior-authorization is a key demand of digital rights advocates seeking to prevent the arbitrary use of this power (Mendel, 2014).

The economic impact of shutdowns also has legal implications. Estimates show that a single day of shutdown can cost a national economy millions of dollars. For developing nations, this represents a violation of the state's duty to protect the socio-economic rights of its citizens. The "right to development" is directly hindered by network disruptions, as digital commerce and international investment are stifled by the state's unpredictable control over the network (Sassen, 2014).

Internationally, there is a growing movement to recognize the right to internet access as a derivative of existing human rights. While not yet a standalone treaty right, the systematic use of shutdowns is being challenged in regional courts (such as the ECOWAS Court in West Africa) which have ruled that such actions are illegal under regional human rights charters. These rulings are setting a precedent that the "kill switch" is an illegitimate exercise of state sovereignty (Milanovic, 2015).

Therefore, the normalization of shutdowns creates a "new normal" where the state asserts a sovereign right to disconnect its population from the global information exchange. This "isolationist legalism" is the ultimate expression of digital authoritarianism, where the state prioritizes its own survival over the fundamental connectivity of its people. Reversing this trend requires an international consensus that the internet is a "global public good" and that its disruption is an affront to the collective rights of the human family (Dauvergne, 2008).

D. Comparative State Practice in Authoritarian Contexts

1. *China: The Pioneer of Digital Sovereignty*

The Chinese legal architecture of digital control is the most sophisticated manifestation of "cyber-sovereignty" globally. Central to this system is the 2017 Cybersecurity Law, which formalizes the state's absolute authority over the domestic internet. This law mandates strict data localization, requiring "critical information infrastructure operators" to store personal information and important data within mainland China. By legally territorializing data, the state ensures that its security apparatus has unfettered access to the digital footprints of its billion-plus users, bypassing the need for international legal cooperation (Feldstein, 2019).

The Chinese model is characterized by a state-centric internet governance model that rejects the Western "multistakeholder" approach. Under the direction of the Cyberspace Administration of China (CAC), the state integrates technical filtering (the "Great Firewall") with administrative regulations that hold intermediaries strictly liable for content. Legally, this is achieved through "real-name registration" requirements for all internet accounts, effectively abolishing the right to anonymity. This legal framework transforms private tech companies into auxiliary arms of the state, tasked with proactive censorship under threat of severe corporate penalties (Zittrain, 2008).

China's use of Social Credit Systems represents a radical evolution in legal practice, where digital behavior is linked to physical-world consequences. By aggregating data from social media, financial history, and surveillance cameras, the state creates a "legalized" system of behavioral engineering. Individuals who engage in "harmful" digital speech can find themselves legally barred from air travel, high-speed rail, or government employment. This represents a shift from reactive punishment to pre-emptive social control, violating the ICCPR's principles of due process and freedom of movement (Diamond, 2010).

The legal justification for China's digital apparatus is grounded in a specific interpretation of national security that includes "ideological security." This framing allows the CAC to categorize any criticism of the Communist Party as an existential threat to the state. Under international law, such overbroad definitions fail the "legality" test, as they do not allow citizens to regulate their conduct. However, China's diplomatic efforts in the UN and ITU seek to internationalize this model, arguing that "information integrity" is a sovereign right that supersedes individual expression (La Rue, 2011).

China's approach also involves the legalization of mass surveillance through "Safe Cities" and "Sharp Eyes" projects. These initiatives utilize AI-driven facial recognition linked to police databases. Legally, these are framed as administrative public safety measures, yet their primary function is the monitoring of ethnic minorities—particularly in Xinjiang—and political dissidents. The systematic nature of this surveillance, conducted without individualized suspicion, represents a structural violation of the right to privacy as understood in international human rights law (Milanovic, 2015).

The export of this "digital authoritarian" toolkit to other nations represents a significant challenge to global norms. By providing surveillance technology and "training" on cyber-regulations to other states, China is facilitating a shift in global internet governance. This "legal export" ensures that the Chinese model of state-controlled connectivity becomes the default for emerging digital economies, creating a splintered internet where rights are contingent upon a state's political alignment (Sassen, 2014).

Furthermore, the Chinese legal framework aggressively targets circumvention tools. The criminalization of unapproved VPNs is not merely a technical barrier but a legal one, intended to prevent the "leakage" of international norms into the domestic information space. By penalizing the act of seeking outside information, the Chinese state asserts that its sovereignty extends to the mental lives of its citizens, a claim that is fundamentally incompatible with the universalist promise of the Universal Declaration of Human Rights.

China's state practice serves as a template for authoritarian legalism in the digital age. It demonstrates how a state can utilize "law" to systematically dismantle the infrastructure of dissent while maintaining a facade of regulatory order. For international legal scholarship, China represents the primary challenger to the "open" internet, offering a coherent—albeit repressive—alternative that prioritizes collective state stability over the individual rights found in the ICCPR (Lessig, 2006).

2. *Russia: Cybersecurity as a Tool of Information Integrity*

Russia has pioneered the legal instrumentalization of cybersecurity to consolidate state control over the digital landscape. Central to this strategy is the "Sovereign Internet Law" of 2019, which grants the government the legal authority to disconnect the Russian segment of the internet (Runet) from the global web in the event of an "emergency." This law mandates the installation of Deep Packet Inspection (DPI) hardware at all exchange points, allowing the state to

centrally manage, filter, and throttle traffic without the cooperation of private ISPs (Elias & Lemish, 2023).

The Russian legal framework is built upon the concept of "Information Security," a doctrine that conflates technical network security with the protection of the state from "foreign influence." By framing information as a potential weapon, Russia justifies draconian restrictions on online dissent and independent media. The "Foreign Agent" laws and "Undesirable Organizations" designations are frequently applied to digital media outlets and NGOs, legally crippling their ability to operate by imposing burdensome reporting requirements and criminal penalties for non-compliance (Dauvergne, 2008).

Russia's restrictions on online dissent have intensified through the "Yarovaya Law" package, which requires telecommunications providers to store the content of all communications for six months and metadata for three years. Crucially, these laws require companies to provide the Federal Security Service (FSB) with the means to decrypt all messages. This represents a totalizing assault on the right to private correspondence, as it effectively outlaws end-to-end encryption and ensures that no digital space remains beyond the reach of the state (Privacy International, 2018).

The Russian judiciary has played a critical role in the normalization of digital repression. Courts frequently issue "blocking orders" for websites and social media platforms that refuse to comply with data localization or censorship demands. The 2022 laws criminalizing "discredit" of the armed forces—often used to target anti-war speech on Telegram and VKontakte—demonstrate how the law is used to enforce ideological conformity. These prosecutions are often conducted with minimal due process, serving as a powerful "chilling effect" for the broader population (Feldstein, 2019).

Russia's state practice also highlights the manipulation of information integrity through state-sponsored "troll farms" and disinformation campaigns. Legally, the state characterizes these as "counter-propaganda" efforts, but in reality, they serve to drown out dissent and polarize the digital public square. This practice challenges the IHRL principle that states should foster a diverse and pluralistic media environment. Instead, Russia utilizes a "firehose of falsehood" model that makes the exercise of the right to *receive* accurate information nearly impossible (Shirky, 2011).

The extraterritorial reach of Russian digital law is another area of concern. The state has attempted to fine and ban global tech giants like Google and Meta for failing to remove content that Russia deems illegal. This represents an attempt to force international actors to enforce

Russian domestic standards globally. For international legal scholarship, this highlights the tension between the "borderless" nature of the internet and the aggressive "re-territorialization" efforts of authoritarian states (Milanovic, 2015).

Furthermore, Russia's involvement in the UN Ad Hoc Committee on Cybercrime demonstrates its intent to reshape international law. Russia has proposed a treaty that would broaden the definition of cybercrime to include "content-based" offenses, effectively seeking to globalize the criminalization of online dissent. This move illustrates how authoritarian states use international institutions to provide a veneer of multilateral legitimacy to their domestic repressive practices (Mendel, 2014).

The Russian model of digital repression is characterized by "securitized legalism." It utilizes the technical language of cybersecurity to mask a profound assault on freedom of expression and privacy. By centralizing control over the network and criminalizing digital heterodoxy, Russia has created a legal environment where the "sovereign" internet serves the interests of the state at the expense of the human rights of its citizens (Zittrain, 2008).

3. *Egypt: Emergency Powers and the Digital "Kill Switch"*

Egypt's digital landscape is defined by the extensive use of emergency powers to justify state-led repression. Following the 2011 revolution, the state enacted the 2018 Anti-Cybercrime Law, which provides the legal basis for the mass blocking of websites and the surveillance of social media users. This law allows the state to block any website deemed a threat to "national security" or the "national economy," terms so broad they have been used to silence over 500 news and human rights websites (Dutton et al., 2012).

The interaction between domestic law and international obligations in Egypt is characterized by a "perpetual state of emergency." Despite being a signatory to the ICCPR, Egypt utilizes its domestic Emergency Law to bypass constitutional protections. This allows for the detention of "digital activists"—including journalists and social media influencers—without charge, often for "spreading false news." This practice violates the ICCPR's prohibition on arbitrary detention and the requirement that any restriction on speech must be necessary and proportionate (La Rue, 2011).

Egypt's surveillance apparatus is both pervasive and legally opaque. The state has invested heavily in "open-source intelligence" (OSINT) tools and spyware to monitor the digital activities of its citizens. Legally, these activities are often conducted without judicial warrants under broad counter-terrorism statutes. This has had a

devastating impact on civil society, as activists fear that their private communications will be used against them in state security trials. The resulting "chilling effect" has largely dismantled the digital networks that were instrumental during the Arab Spring (Privacy International, 2018).

The use of internet shutdowns remains a latent but powerful tool in the Egyptian state's arsenal. While a total "kill switch" hasn't been used recently, the legal authority to do so exists under the Telecommunications Law. More common is the practice of throttling or blocking specific encrypted messaging apps like Signal and Telegram during times of social unrest. Legally, these are framed as "technical disruptions," but their effect is to prevent the coordination of peaceful assembly, a clear violation of the state's obligations under the African Charter on Human and Peoples' Rights (Shirky, 2011).

Egypt's legal framework also targets "moral" and "social" values. Several social media influencers have been prosecuted and imprisoned for "violating family values" in their TikTok videos. This use of vaguely defined "public morality" standards allows the state to police the cultural and social expression of its youth, illustrating how digital authoritarianism extends beyond political dissent to encompass the total regulation of the digital social sphere (Mendel, 2014).

The lack of an independent judiciary in Egypt means that digital rights cases are often pre-determined. Challenges to website blocking or the arrest of bloggers are routinely dismissed by the state security courts. This "judicial rubber-stamping" of executive repression ensures that there is no domestic remedy for digital rights violations, a direct breach of the ICCPR's requirement for an effective legal remedy. This has forced Egyptian activists to increasingly rely on international human rights mechanisms, such as the UN Human Rights Committee, to highlight the state's violations (Gready & Robins, 2014).

Furthermore, the Egyptian state's collaboration with international technology firms raises significant questions about state responsibility. When foreign firms provide the surveillance infrastructure or comply with "national security" data requests without due process, they facilitate the state's repressive practices. For international legal scholarship, this underscores the need for "due diligence" standards that prevent the private sector from becoming accomplices in state-led digital repression (Milanovic, 2015).

At this context, the Egyptian case demonstrates how militarized domestic law can be used to colonize and control the digital space. By treating the internet as a security domain and the user as a potential insurgent, Egypt has turned the tools of liberation into tools of incarceration. This state practice serves as a warning of how the

"securitization of the web" can permanently close the democratic window that digital technology once opened (Feldstein, 2019).

E. Resistance, Civil Society, and the Limits of Legal Protection

The expansion of digital authoritarianism has triggered a parallel evolution in the strategies of resistance. As states utilize "law" to entrench digital repression, civil society has responded by treating the technical architecture of the internet as a site of legal and political contestation. This section examines how technological workarounds and grassroots activism not only bypass state control but also serve as a normative challenge to the authoritarian reinterpretation of international law.

1. *Digital Activism and Technological Workarounds*

In the face of systemic censorship, the use of Virtual Private Networks (VPNs) and encryption has transitioned from a niche technical practice to a fundamental prerequisite for digital activism. By masking IP addresses and encrypting data packets, these tools allow citizens in regimes like China and Iran to tunnel through national firewalls, accessing the global information commons. Legally, the use of such tools represents a practical exercise of the right to seek information regardless of frontiers, as enshrined in Article 19 of the ICCPR (La Rue, 2011).

The shift toward decentralized platforms and mesh networks represents a more radical form of resistance. Unlike centralized social media, which provides a "single point of failure" that states can easily pressure or block, decentralized protocols (such as IPFS or Signal) distribute data across multiple nodes. This makes it technically and legally difficult for a state to implement "notice and takedown" orders, as there is no central intermediary to subpoena. These "architectures of resistance" effectively create a digital space that operates outside the traditional territorial jurisdiction of the state (Zittrain, 2008).

However, these workarounds carry significant legal risks. Authoritarian regimes have responded with aggressive regulatory counter-measures, criminalizing the mere possession of "unapproved" encryption software or VPNs. In states like Egypt and Russia, individuals found with certain apps during "stop and search" operations can face charges of "membership in a terrorist group" or "spreading false news." This criminalization of technology creates a "tech-legal" arms race where the state seeks to close every digital exit, turning the user's device into a potential piece of evidence against them (Feldstein, 2019).

The state's response often includes technical "whitelisting," where only state-sanctioned VPNs—which likely provide backdoors to security services—are legal. This creates a legal trap for the unwary user, who believes they are achieving privacy while actually being funneled into a monitored channel. The legal struggle here is over the right to anonymity; by banning circumvention tools, the state asserts that every digital act must be attributable to a physical identity, effectively dismantling the possibility of safe dissent (Lessig, 2006).

Grassroots movements also utilize stealth activism, such as using coded language, memes, or "steganography" (hiding messages within images) to bypass algorithmic filters. While these are technical tactics, they have profound legal implications: they force the state to constantly broaden its definition of "illegal content," leading to increasingly absurd and overbroad laws that eventually lose their perceived legitimacy among the public. This process exposes the arbitrary nature of authoritarian legality (Diamond, 2010).

Furthermore, the "democratization of hacking" has seen civil society groups engage in "hacktivism"—the unauthorized access of state servers to leak evidence of corruption or human rights abuses. While such actions are technically illegal under domestic "cybercrime" laws, they are often framed by activists as a form of digital civil disobedience. This raises a complex legal question for international scholarship: at what point does the state's violation of fundamental rights justify the "illegal" breach of its digital infrastructure by its citizens? (Milanovic, 2015).

Institutional support for these workarounds often comes from international NGOs and foreign governments through "Internet Freedom" grants. This "state-sponsored resistance" is frequently characterized by authoritarian regimes as "foreign interference" or "cyber-terrorism." This highlights the geopolitical dimension of digital rights, where the technical tools provided to activists become the subject of high-level diplomatic disputes regarding the principle of non-intervention in the internal affairs of states (Sassen, 2014).

The reliance on technological workarounds highlights the fragility of digital protection. For the most marginalized populations, the "digital divide" means they lack the technical literacy or hardware to use VPNs or encrypted apps. This creates a two-tiered system of rights where only the "tech-savvy" elite can exercise their freedoms, while the broader population remains trapped behind the national firewall. This inequality underscores that technology alone cannot replace the need for robust, enforceable legal protections (Shirky, 2011).

2. *Normative Significance of Civil Society Practices*

The practices of digital resistance are not merely reactive; they possess a profound normative significance. When millions of citizens routinely use VPNs to bypass a "legal" block, they are engaging in a collective act of resistance against authoritarian legality. This widespread non-compliance undermines the state's claim that its restrictive cyber-laws reflect the "public order" or "national values." Over time, this "normative friction" can erode the perceived authority of domestic laws that conflict with international human rights standards (Dauvergne, 2008).

Civil society acts as a "norm entrepreneur" by documenting and publicizing the technical reality of digital repression. By mapping out how firewalls work or identifying the sources of state-sponsored malware, groups like *Citizen Lab* or *NetBlocks* provide the evidentiary basis for international legal claims. This technical documentation is essential for turning "vague rumors" of censorship into "verifiable facts" that can be used in UN reports or regional court proceedings, effectively bridging the gap between "code" and "law" (Lukas et al., 2023).

These practices have direct implications for the interpretation of international norms. For example, the widespread use of encryption by civil society has influenced international bodies to recognize that the right to privacy in the digital age *includes* the right to use encryption. This is an example of "bottom-up" norm development, where the lived experience of activists in oppressive regimes informs the "evolutionary interpretation" of treaties like the ICCPR by the UN Human Rights Committee (Milanovic, 2015).

Resistance also challenges the authoritarian concept of "Cyber-Sovereignty." By participating in global digital networks despite state efforts to isolate them, citizens demonstrate that their "digital identity" is not bound by national borders. This reinforces the universalist principle that human rights are inherent and borderless. Civil society's insistence on "borderless connectivity" serves as a powerful counter-narrative to the "splinternet" model, asserting that the internet is a global public good that no state has the right to fully sequester (Zittrain, 2008).

The normative power of resistance is also visible in the development of "soft law" standards for corporations. When activists pressure tech giants to resist government data requests or to "exit" markets like Russia after the invasion of Ukraine, they are operationalizing the UN Guiding Principles on Business and Human Rights. This pressure forces private actors to recognize that "following local law" is an insufficient excuse for facilitating human rights abuses,

thereby raising the global standard for corporate responsibility (Gready & Robins, 2014).

Furthermore, digital activism has redefined the right to peaceful assembly. In the 21st century, a "gathering" is no longer just physical; it is a synchronized digital act. Civil society's use of "digital sit-ins" or coordinated social media campaigns has forced international legal scholars to reconsider the definition of "assembly" under Article 21 of the ICCPR. This redefinition is critical for protecting the rights of those in regimes where physical protests are immediately met with lethal force (Heyns, 2014).

The multi-stakeholder model of internet governance is another norm that is sustained primarily through civil society resistance. By refusing to let the ITU or other state-centric bodies take over the management of the internet's core protocols, civil society prevents the "legalization of censorship" at the architectural level. This ensures that the internet remains a "permissionless" space where new tools for freedom can continue to be developed without state approval (Lessig, 2006).

The long-term normative impact of resistance is the de-normalization of digital authoritarianism. By constantly highlighting the gap between state practice and human rights ideals, civil society prevents the "repressive model" from becoming a legitimate global standard. Even when they lose the battle on the ground, the "normative record" they create ensures that digital rights remain a central pillar of the global democratic project, providing a roadmap for future legal restoration (Sassen, 2014).

3. *Constraints on International Accountability*

Despite the heroic efforts of civil society, the international legal order faces severe constraints on accountability. The most significant are the jurisdictional barriers that prevent international bodies from effectively intervening in domestic "digital affairs." Authoritarian regimes frequently invoke the principle of "non-intervention" to dismiss international criticism of their firewall policies or surveillance programs, arguing that "cyber-regulation" is a matter of exclusive domestic jurisdiction (Dauvergne, 2008).

This is exacerbated by a profound enforcement deficit. While the UN Human Rights Committee or Special Rapporteurs can "name and shame" states for digital rights violations, they lack the "teeth" to compel a state to change its laws or stop a shutdown. Unlike trade law, which features binding arbitration and sanctions, digital rights law relies primarily on diplomatic pressure and normative persuasion,

which are often ineffective against regimes that prioritize political survival over international reputation (Bassiouni, 2010).

The role of international and regional mechanisms is further hindered by the "veto power" held by authoritarian states in the UN Security Council and other high-level bodies. These states often form "voting blocs" to protect one another from scrutiny, effectively paralyzing the UN's ability to take decisive action against systematic digital repression. This "geopolitical shielding" allows regimes to implement draconian cyber-laws with a high degree of international impunity (Ní Aoláin, 2000).

Regional mechanisms, such as the European Court of Human Rights (ECtHR) or the Inter-American Court, provide more robust accountability, but their jurisdiction is limited to specific geographic areas. For activists in the Middle East or Central Asia—where some of the worst digital abuses occur—there is often no equivalent regional court with the power to issue binding rulings against the state. This "geographic lottery" means that the level of legal protection an individual receives depends entirely on where they live (Costello, 2016).

The attribution problem in cyber-surveillance presents another legal hurdle. States often utilize "private-sector cutouts" or "unidentified" hacker groups to conduct digital attacks on dissidents. Legally proving that the state is responsible for a specific piece of malware or a targeted hack is notoriously difficult and time-consuming. This "plausible deniability" allows regimes to evade state responsibility under international law, as the high evidentiary threshold for "effective control" is rarely met (Milanovic, 2015).

Furthermore, the lack of a unified "Global Digital Rights Treaty" means that international law remains fragmented. Existing treaties like the ICCPR are often interpreted differently by different states, and "soft law" instruments are frequently ignored. Without a central, binding document that defines "digital rights" and sets out clear penalties for their violation, authoritarian states will continue to exploit the "legal grey zones" of the digital age to consolidate their power (Hathaway, 2021).

The extraterritoriality of digital rights also remains a major enforcement gap. When a state surveils a foreign citizen or blocks a foreign website, it is often unclear which international body has the jurisdiction to hear the case. Authoritarian regimes exploit this confusion by conducting "cross-border repression" via digital means, reaching out to silence their critics abroad with few legal consequences. This "repression without borders" highlights the urgent need for a more integrated international legal response (Milanovic, 2015).

The "securitization" of digital rights discourse often marginalizes human rights concerns in favor of "cyber-stability." International institutions are frequently more concerned with preventing "state-on-state" cyber-warfare than they are with protecting the "state-on-citizen" digital violence of authoritarianism. This shift in focus ensures that the systemic violations of digital rights remain a "secondary" issue in the global security architecture, further entrenching the deficit of accountability (Feldstein, 2019).

F. Implications for International Human Rights Law and Internet Governance

1. *Reinterpreting Freedom of Expression in Digital Contexts*

The principle of technological neutrality remains the cornerstone of international human rights law (IHRL), asserting that rights are inherent regardless of the medium through which they are exercised. However, the unique architecture of the internet requires evolving standards to address how "expression" is facilitated or stifled. It is no longer sufficient to protect the *content* of speech; the law must also protect the *means* of speech. This includes a burgeoning recognition that access to the internet itself, and the tools required to navigate it securely (such as encryption and VPNs), are essential precursors to the realization of Article 19 of the ICCPR (La Rue, 2011).

Traditional legal interpretations of "interference" must also be expanded to include algorithmic manipulation and shadow-banning. When an authoritarian state mandates that social media companies alter their discovery algorithms to suppress political dissent, it is engaging in a form of "structural censorship" that is often invisible to traditional legal monitoring. To maintain relevance, IHRL must move beyond a focus on "notice and takedown" toward a more comprehensive regulation of "algorithmic accountability," ensuring that the automated systems governing our digital public square are transparent and subject to human rights due diligence (Balkin, 2018).

The concept of "positive obligations" for states has likewise evolved. In the digital context, it is not enough for the state to refrain from censorship; it has a duty to foster a pluralistic digital environment. This includes protecting the physical infrastructure of the internet from disruptions and ensuring that marginalized communities have the technical literacy and access required to participate in digital life. Without these positive protections, the "right to freedom of expression" remains a formalistic ideal rather than a substantive reality for those living under repressive regimes (Milanovic, 2015).

2. *Addressing Digital Authoritarianism Through International Law*

The limits of existing mechanisms have become painfully clear as authoritarian regimes exploit the decentralized nature of the internet to conduct cross-border repression. Current IHRL treaties, largely drafted in a pre-digital era, struggle with the attribution of cyber-attacks and the extraterritorial application of privacy rights. When a state utilizes "state-sponsored" hackers to target dissidents abroad, the traditional legal framework for state responsibility often fails due to the high evidentiary threshold for "effective control." This creates a climate of digital impunity that undermines the global rule of law (Milanovic, 2015).

Potential avenues for normative development include the drafting of a "Digital Bill of Rights" or a specialized protocol to the ICCPR that explicitly addresses digital-age threats. Such a framework could formalize the prohibition of internet shutdowns and establish a global "due diligence" standard for the trade of surveillance technology. By creating a specific, binding legal instrument, the international community can move beyond "naming and shaming" toward a regime of "targeted sanctions" and "technical embargoes" against states that systematically dismantle digital freedoms (Feldstein, 2019).

Furthermore, the role of non-state actors must be legally formalized. Technology companies are no longer mere intermediaries; they are the primary architects of our digital reality. International law must develop a "corporate state responsibility" model, where firms are held legally accountable for facilitating state-led digital repression. This requires moving the UN Guiding Principles on Business and Human Rights from a voluntary "soft law" framework toward a binding treaty that imposes civil and criminal liability for companies that prioritize profit over the human rights of their users (Sassen, 2014).

3. *Balancing Sovereignty, Security, and Digital Freedoms*

The central tension within international legal discourse remains the conflict between state sovereignty and the universal nature of digital rights. Authoritarian regimes have weaponized the concept of "cyber-sovereignty" to argue that the internet is a national territory subject to absolute state control. This "territorialization of the web" directly contradicts the "borderless" promise of the UDHR and risks creating a permanent "splinternet" where an individual's rights change depending on the server they are connected to (Zittrain, 2008).

States frequently use "security" as a legal blank check to justify draconian surveillance and censorship. Under IHRL, the "national security" exception is intended to be narrow and subject to judicial

review. However, in authoritarian contexts, "security" is often redefined to mean the "security of the regime" against domestic dissent. Balancing these interests requires a "global proportionality standard" that rejects the idea of a state-defined "security" and insists on an internationalized definition that prioritizes the security of the *individual* over the stability of the *ruling apparatus* (Ní Aoláin, 2000).

The future of internet governance depends on whether the multistakeholder model can survive the onslaught of state-centric regulation. If international institutions like the ITU are allowed to become "closed clubs" for governments, the technical architecture of the internet will inevitably be redesigned to facilitate control. The legal challenge of the next decade is to ensure that "sovereignty" is interpreted as a responsibility to protect rights, rather than a right to repress them. As the digital and physical worlds continue to merge, the preservation of a "free, open, and interoperable" internet remains the ultimate test for the international human rights project (Diamond, 2010).

G. Conclusion

This research emphasized that digital authoritarianism is not merely a collection of isolated censorship events, but a sophisticated, structural legal practice that fundamentally challenges the universalist promise of the international human rights framework. The central argument posits that regimes in China, Russia, and Egypt have operationalized "cyber-sovereignty" to justify systemic violations of freedom of expression and privacy, effectively hollowing out the International Covenant on Civil and Political Rights (ICCPR) from within. By codifying digital repression into domestic statutes, these states attempt to normalize a "state of exception" where the internet serves as a tool for state-led social engineering rather than a platform for human liberation.

The study contributes to international law scholarship by shifting the focus from incident-based analysis toward a multidisciplinary critique of security architectures. It identifies a significant "enforcement gap" in the global legal order, where existing treaties struggle to address the extraterritorial reach of state-sponsored surveillance and the privatized censorship conducted by tech intermediaries. By documenting how civil society utilizes technological workarounds to challenge authoritarian legality, this research highlights the role of "bottom-up" norm development, suggesting that the lived experience of digital resistance must inform the "evolutionary interpretation" of treaty obligations in the 21st century.

The normative implications for future legal development necessitate a move toward a unified Global Digital Rights Treaty that transcends Westphalian sovereignty. Such a framework must establish binding standards for "algorithmic accountability," prohibit indiscriminate internet shutdowns, and impose strict human rights due diligence on the global trade of surveillance technology. Future research should prioritize the intersection of digital rights with emerging Artificial Intelligence (AI) governance and the impact of the "splinternet" on the right to participate in global cultural and scientific progress, ensuring that the international legal order remains resilient against the permanent enclosure of the digital commons.

H. References

Balkin, J. M. (2018). *Free Speech in the Algorithmic Society*. Fordham Law Review.

Bassiouni, M. C. (2010). *The Pursuit of International Criminal Justice*. Antwerp: Intersentia.

Costello, C. (2016). *The Human Rights of Migrants and Refugees in European Law*. Oxford: Oxford University Press.

Dauvergne, C. (2008). *Making People Illegal: What Globalization Means for Migration and Law*. Cambridge: Cambridge University Press.

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, 21(3), 69–83.

Dutton, W. H., et al. (2012). *Freedom of Connection, Freedom of Expression: The Changing Role of Mapped Mechanisms in the Control of the Internet*. UNESCO.

Elias, N., & Lemish, D. (2023). *The Handbook of Media and Migration*. London: Routledge.

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace.

Gready, P., & Robins, S. (2014). *From Transitional to Transformative Justice*. Cambridge: Cambridge University Press.

Hathaway, J. C. (2021). *The Rights of Refugees under International Law*. Cambridge: Cambridge University Press.

Heyns, C. (2014). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*. UN Doc. A/HRC/26/36.

La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. UN Doc. A/HRC/17/27.

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

Lukas, S., et al. (2023). *Exporting Repression: The Global Trade in Surveillance Technology*. Human Rights Quarterly.

Mendel, T. (2014). *Restricting Freedom of Expression: Standards and Principles*. Centre for Law and Democracy.
Milanovic, M. (2015). *Extraterritorial Application of Human Rights Treaties*. Oxford: Oxford University Press.
Ní Aoláin, F. (2000). *The Politics of Force*. Belfast: Blackstaff Press.
Privacy International. (2018). *The State of Surveillance*.
Sassen, S. (2014). *Expulsions: Brutality and Complexity in the Global Economy*. Cambridge, MA: Harvard University Press.
Shirky, C. (2011). The Political Power of Social Media. *Foreign Affairs*, 90(1), 28–41.
Zittrain, J. (2008). *The Future of the Internet—And How to Stop It*. Yale University Press.

***

Acknowledgment
None

Funding Information
None

Conflicting Interest Statement
The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement
All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement
N/A