

Digitally Silenced: Information Control and the Closure of Civic Space in the Middle East and Africa

Chiara Innocenti, Diyara Demir, Elisabedi Koridze,
Martina Malaman, Ypke Wu, Rueida Muhamed

Middle East & Africa Team – 30.04.2026



Photo source: A map with flags marking destinations © Lara Jameson / Pexels, 2024.



Rivervismarkt 5, 2513 AM The Hague, Netherlands



info@ghrd.org



+ 31 62 72 41006



<https://www.ghrd.org>

CONTENTS

INTRODUCTION	5
1. DIGITAL REPRESSION AND CIVIC SPACE	6
1.1 Legal Framework	6
1.2 Typologies of Digital Repression	7
2. OPERATIONAL DIMENSIONS OF DIGITAL REPRESSION	9
2.1 Surveillance & Monitoring	9
2.1.2. <i>What are Biometric Systems, and why do they Affect Human Rights?</i>	9
2.1.2. <i>What is Spyware?</i>	10
2.1.3. <i>Rwanda</i>	12
3.1.4. <i>Morocco</i>	12
2.1.5. <i>The Kingdom of Saudi Arabia</i>	13
2.1.6. <i>United Arab Emirates</i>	14
2.2 Legal and Regulatory Frameworks	15
2.2.1 <i>Egypt's Legal Architecture</i>	15
2.2.2 <i>Saudi Arabia's Legal Architecture</i>	16
2.2.3 <i>Jordan's Legal Architecture</i>	18
2.2.4 <i>Uganda's Legal Architecture</i>	18
2.2.5 <i>Nigeria's Legal Architecture</i>	19
2.2.6 <i>Cross-regional Patterns</i>	21
2.3 Internet Shutdowns and Platform Blocking as Governance Instruments	22
2.4 Disinformation & Narrative Control	26
2.4.1 <i>Iran</i>	26
2.4.2 <i>Saudi Arabia</i>	27
2.4.3 <i>Sudan</i>	29
2.4.4 <i>Ethiopia</i>	30
3. IMPACT ON HUMAN RIGHTS	30
4. INTERNATIONAL LEGAL FRAMEWORK & GAPS	32
4.1 Gaps in the Implementation	32
4.1.2 <i>Technology running faster than Law</i>	32
4.1.2 <i>Lack of Accountability</i>	33
CONCLUSION	34

Abbreviations	Full terms
CESCR	Committee on Economic, Social and Cultural Rights
CRC	Convention on the Rights of the Child
CRS Officers	Compagnies Républicaines de Sécurité (Republican Security Corps)
ECHR	European Convention on Human Rights
EU	European Union
EUAA	European Union Agency for Asylum
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Agency for Law Enforcement Cooperation
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICCPR	International Covenant on Civil and Political Rights
ICRMW	International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
ID	Identification
IOM	International Organization for Migration
IRC	International Rescue Committee
NGO	Non-Governmental Organisation
NGO HRO	NGO Human Rights Observers
NGO MSF	NGO Médecins Sans Frontières (Doctors Without Borders)
OHCHR	Office of the United Nations High Commissioner for Human Rights

PICUM	Platform for International Cooperation on Undocumented Migrants
RIBs	Rigid Inflatable Boats
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
WHO	World Health Organization

INTRODUCTION

Civic space is the environment that allows individuals and civil societies to communicate, express their opinion, and discuss issues of importance (FRA, n.d.). In order to create a meaningful space to foster political, social, cultural and legal life in a society, civic spaces must remain open and free from censorship or violence. A pluralistic civic space not only guarantees the freedom of expression, association, and assembly, it also promotes democratic dialogue to maintain sustainable growth in society.

It is thus possible to consider civil space as a cornerstone for democratic states. When information and participation are publicly accessible, civic freedoms promote engagement and challenge policies to better societal needs. It holds governments accountable and better aligns local and national level governance (OECD, 2022). Consequently, the restriction of civic space feeds into systemic failings and other human rights violations, allowing governments to abuse their power. In recent years, civic space restrictions are increasingly documented globally. The rollback of civic freedoms erodes fundamental rights and democratic values, and often grants traction to authoritarianism and political polarisation (Narsee and Willamo, 2025).

Digital repression is understood as the use of technologies by governments to control and suppress citizens and activists. Through the proliferation of new and emerging technologies, it is also easier for governments to deploy new strategically repressive instruments (Glowacka et al., 2021).

In the case of the Middle East and Africa as well, civic space restrictions are not a new phenomenon but a widespread tool that governments employ for political control (CIVICUS, 2022). The most reported ways of digital repression observed in these regions are harassment, censorship and disinformation campaigns, and surveillance. Additionally, digital repression has a strong correlation to the type of regime, with authoritarian governments most likely to employ these methods (Feldstein, 2023). While the strategies are not a one-size-fits-all form, it often depends on the available resources, political objectives, and the government's capacity.

The rise of digital repression in the region is driven by a combination of political, technological, and legal factors. Governments in the Middle East and Africa have expanded their digital capabilities to suppress online expressions by civilians, activists and other dissent voices. By enacting restrictive cyber laws and controlling online spaces, they are able to shut down civilian access to maintain power. Social media and online platforms have simplified the mobilisation and spread of information, which in turn have been perceived by these governments as a threat to the narrative they seek to control. Moreover, the weak institutional safeguards and lack of judicial oversight, along with the rapid growth of available digital toolkits, has enabled states to adopt repressive measures with little constraint.

This report will provide an evaluation of civic repression throughout the Middle East and Africa. The first chapter outlines the main legal frameworks and different forms of repressive techniques governments often employ to control and limit civic liberties. The analysis then focuses on the specific typologies, using different countries as examples. The final chapter explores the limitations and gaps from a legal standpoint, critically examining the lack of accountability and the slow process of new regulations. The report concludes with recommendations to different stakeholders and highlights the necessary reforms and mechanisms to ensure a free civic space and ensuring the enjoyment of all civic liberties.

1. DIGITAL REPRESSION AND CIVIC SPACE

1.1 Legal Framework

The United Nations Commissioner for Human Rights considers five elements to maintain a safe civic environment: compliance with international legal standards that ensure human rights, an active civil society, access to information, participation in decision-making, and support for civil society (UN Human Rights Council, 2016).

The normative framework for civic space is widely codified under international law. The key aspects of civic space addressed under international human rights law include the freedom of opinion and expression, the freedom of peaceful assembly, and the freedom of association. Significantly, these freedoms are not only recognised as fundamental human rights, but also an important aspect of political participation and civil liberty.

Firstly, freedom of opinion and expression is protected under Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). It implies the right to receive information regardless of the source, embracing diverse expressions and ideas. While certain exceptions are foreseen under ICCPR Article 19(3), including for reasons of national security, these remain governed by law and must be necessary. Similarly, Article 20 of ICCPR restricts the freedom of expression in cases where one was to incite or engage in war propaganda, hate speech, and discriminant or violent acts. Thus, while governments have the responsibility to prohibit inciteful speech, they are not allowed to abuse their power to silence peaceful dissent. The right to freedom of opinion and expression therefore translates into media freedom and the rights to access information (UNDP, 2021).

Secondly, the freedom of peaceful assembly, enshrined in Article 20 of the UDHR and Article 21 of the ICCPR, protects protests, rallies, meetings, and any non-violent gatherings. Assemblies are protected in public, private or even online, as clarified by General Comment No. 37 (UNDP, 2021). The fact that this right is intrinsically linked to the freedom of expression must be highlighted, as a restriction of the right to peaceful assembly often also limits freedom of expression (OHCHR, n.d.).

Thirdly, the freedom of association is protected under Article 20 of the UDHR and Article 22 of the ICCPR. It protects the right of individuals to collectively pursue common interest by forming unions, parties and other organisations. It encompasses the right to be or not to be associated with political, religious, cultural or other fields, without governmental intervention. Individuals have the right to seek resources and engage in advocacy without fear of reprisals. As with Article 21, Article 22(2) imposes restrictions on situations where the interest of national security, public order, and the rights and freedoms of others are imposed upon.

These international human rights treaties are binding upon ratification, creating responsibilities and legal obligations for states. They are not only legally obligated to protect and promote these rights, but must also refrain from acts that would interfere or limit the recognised rights. Furthermore, the Siracusa Principles explain that no limitation of the rights above can be interpreted in such a way that would compromise the essence of the right itself and can only be applied when there is genuine necessity and proportionality (ECOSOC, 1985). Nevertheless, derogations, where states are allowed to temporarily suspend the exercise of certain rights, are allowed in situations of public emergency pursuant to Article 4 of the ICCPR.

In terms of regional legal frameworks, the African Charter on Human and Peoples' Rights (ACHPR) recognises the same freedoms to protect civic spaces. In 2021, the ACHPR also adopted its Resolution 475, upholding the freedom of expression, association and assembly even in crises (ACHPR, 2021). Despite having a clear regional framework in Africa, these mechanisms lack enforcement power, allowing local governments to disregard the protection of these rights. In the Middle East, both the Arab League and the Organisation of Islamic Cooperation recognise the three main freedoms aforementioned. Yet, in practice, most Member States place restrictive national measures that severely limit the freedoms within their civic spaces.

1.2 Typologies of Digital Repression

Digital repression manifests through different tactics employed by governments to surveil, coerce, manipulate, and control individuals that pose a challenge to the state. As digital technologies become an important feature of civic engagement, states increasingly shift strategies to operate online. The main types of digital repression include, surveillance, censorship, social manipulation and disinformation, internet shutdowns, and digital harassment and targeted persecution online (Feldstein, 2021). These strategies are often also simultaneously employed to form a comprehensive system that restricts civic space.

Surveillance practices include a wide variety of technologies. They involve the collection and analysis of digital data by the state through spyware and data extraction technologies (Büchi et al., 2022). These practices create an environment of fear and social control, discouraging dissent and limiting civil participation. Specific techniques include the deployment of spyware for targeted or collective monitoring, cyber patrolling to track behaviour, the use of

location tracking and broader forms of privacy exploitation, large-scale network and data monitoring (Villarreal, 2025). In combination, these tools significantly undermine civil liberties by enabling state authorities to identify, target and stigmatise dissenting individuals (Sombatpoonsiri, 2024).

Censorship represents another central pillar to digital repression, relying on filtering mechanisms and regulatory frameworks to suppress the spread of information that might contradict the government or regime's narratives (UNESCO, 2026). Governments usually employ techniques to shape online discourse, including information coercion, where content is forcefully removed or altered, and content filtering that blocks access to certain websites and keywords. While censorship can be justified in certain contexts to protect public safety and security, it becomes problematic when it deprives society of essential information (Cornelius, 2018).

In addition to censorship, governments may also employ disinformation campaigns to distort public understanding. Disinformation is defined as the deliberate circulation of false information, which allows governments to control the narrative and obscure criticism (Perez-Escobar et al, 2023). With the purpose of deceiving and misleading the public, it actively reshapes the information available and allows governments to exert control over these aspects of society (Guess and Lyons, 2021).

Internet disruption is a more direct form of digital repression that has been observed in certain countries across the Middle East and Africa. This technique involves restriction or the complete shutdown of digital networks. Governments usually implement internet shutdowns during political unrest, protests or other mass mobilisation to limit the spread of information and to control the narrative (Baum and van Rooyen, 2025). Other times, the imposition of partial connectivity restrictions can also effectively slow down civic activity, communications, and other services, making digital blackouts a direct assault on human rights.

Lastly, digital harassment and targeted online persecution represent a more targeted form of repression. By employing intimidation and humiliation in virtual environments, such practices undermine one's ability to participate fully in public and civic life. Most reported cases have been cyberaggression towards women and girls, targeting both their personal and public lives (EIGE, 2025). Digital harassment or cyberbullying can involve behaviour such as sending threats, viruses to sabotage, creating rumours, making defamatory comments or impersonating the victim directly, and in more extreme cases, the use of pornography and offensive graphic content (CCOHS, n.d.). Indeed, civil society and human rights activists have also repeatedly been victims of digital harassment, forcing them to shut down operations (CIVICUS, 2022). In many instances, harassment campaigns are carried out by the state or state-affiliated actors to discourage participation and the sharing of opinions. In turn, this functions as a form of self-censorship where individuals restrict their online engagement themselves.

Significantly, these forms of digital repression are reinforced by cybersecurity and cybercrimes laws that expand government control over the digital sphere (Baum and van

Rooyen, 2025). These legal frameworks enable governments to institutionalise surveillance and censorship practices with little oversight. As a result, individuals are increasingly monitored and penalised for expressing political views or engaging in civic discourse online. The combined use of technological tools and legal mechanisms thus not only violates fundamental rights, but also undermines democratic principles at their core.

2. OPERATIONAL DIMENSIONS OF DIGITAL REPRESSION

Methods of digital surveillance have increasingly become tools for controlling and silencing critical voices (Office of the United Nations High Commissioner for Human Rights, 2024). Governments have been expanding their capacity for digital surveillance globally by procuring new technologies to target journalists and human rights defenders (Office of the United Nations High Commissioner for Human Rights, 2024). In the past decade, this can be seen by the exposure of pervasive abuse of tools such as the Pegasus spyware (Office of the United Nations High Commissioner for Human Rights, 2024).

The countries selected in this section: Rwanda, Morocco, Saudi Arabia and the United Arab Emirates, were chosen as illustrative case studies because they have been repeatedly identified in credible reports by organisations such as Amnesty International, Human Rights Watch and Citizen Lab. The selective criteria focused on the availability of publicly accessible evidence and investigative reporting as well as regional representation across Africa and the Middle East to demonstrate how surveillance practices operate in different political contexts.

2.1 Surveillance & Monitoring

2.1.1 What are Biometric Systems, and Why Do They Affect Human Rights?

Biometric technologies are highly intrusive tools used to gather and analyse personal data in order to enable the unique identification of a person (ARTICLE 19, 2021) by including DNA, fingerprints, voice patterns or cardiac signatures. One of the most common forms of biometric technologies is facial recognition (ARTICLE 19, 2021). The increasing availability of large databases and improved machine learning, as well as the low-cost development and deployment of biometric technologies, has made biometric systems preferable for states and private actors. Justifications given are often the protection of national security, the efforts to counter terrorism measures, crime prevention and public safety. Alternatively, another justification given is the fact that authorities can justify the use of these technologies for delivering services, such as the development of “smart cities” (ARTICLE 19, 2021).

The biometric system is concerning due to many factors. States and private actors typically store the data collected in databases for far longer than needed, creating concerns for individuals' privacy. The collected data are also easy to reuse for purposes different from the original intentions, which is illegal (ARTICLE 19, 2021). Long-term storage of these technologies also enables massive security breaches (ARTICLE 19, 2021).

The processors of biometrics do not often meet the necessity and proportionality tests, which are central to the protection of the rights to freedom of expression and privacy (ARTICLE 19, 2021, p. 16). To meet this requirement, any technology must represent that it is the only way to achieve the legitimate aim and that it is the least invasive way to do it (ARTICLE 19, 2021).

Issues with the use of biometrics also arise when their misuse results in profiling and categorising people based on age, gender and skin colour. Moreover, they can be used to control the narrative on what people are doing, with whom, how they feel, and even how they are likely to behave in the future (ARTICLE 19, 2021). For example, cameras can use facial recognition technologies in subways, shopping centres and streets to identify individuals. Such practices have influenced and deterred people from participating in public assemblies or expressing ideas or religious beliefs in public, fearing repercussions as a result of the absence of anonymity (ARTICLE 19, 2021).

These technologies are particularly damaging for journalists, human rights defenders, and those belonging to minority groups, since biometrics can be used to target and monitor specific categories of people, track their behaviour and profile them based on their characteristics or behaviour (ARTICLE 19, 2021).

Biometric and digital identification systems are increasingly being imposed across Africa. Promoted as a tool to modernise service delivery, enhance electoral integrity, and strengthen state capacity, these systems are becoming central to how identity and citizenship are managed (Atlantic Council, 2025). Such systems are used in national identification schemes and voter registration, making them deeply embedded in Africa's political, social and economic landscape. Despite this, many countries in Africa lack adequate legal frameworks and robust digital security to prevent unauthorised access to sensitive data (Atlantic Council, 2025).

Over the past decade, the Gulf Cooperation Council (GCC) countries have been enacting personal data protection laws in order to regulate the collection and processing of their citizens' personal information. Despite the advancement, many instruments contain provisions allowing exceptions based on "public interest or security purposes". These provisions, in the hands of governments known for being highly suppressive against political dissent and criticism, may effectively legitimise and institutionalise mass data collection under the pretext of national security (Americans for Democracy & Human Rights in Bahrain, 2025).

2.1.2 What is Spyware?

Spyware is malicious software that is covertly installed on a user's device to collect information without their knowledge and transmit it to another unauthorised entity (Amnesty International, 2023). In its more advanced forms, spyware allows unlimited access to a device by default, making it almost impossible for the user to detect it (Amnesty International, 2023).

While there are different types, global attention has focused on Pegasus, a spyware developed by the Israeli company NSO, which is sold exclusively to governments with the intention of tracking criminals and terrorists (Allen & La Lime, 2021). Pegasus is one of the world's most sophisticated surveillance technologies (Allen & La Lime, 2021) that can infect the phones of targets through a variety of mechanisms: in some cases, it involves a message such as SMS, iMessage, WhatsApp, or an email that includes a link to a website (Kaldani & Prokopets, 2022). When clicked, the link delivers malicious software to the device (Kaldani & Prokopets, 2022). Otherwise, a “zero-click” attack is employed, which allows infections by simply receiving a message with no user interaction required (Kaldani & Prokopets, 2022).

The implications of this are that spyware of a similar calibre to Pegasus does not require the user to do anything. All that is required for a successful attack is having a particularly vulnerable app or operating system installed (Allen & La Lime, 2021). Once infiltrated, Pegasus can harvest all data from the device, using the camera and microphone in real time. It can also extract contacts, call logs, web searches, web browsing history, photos, videos, and location records, as well as information from commonly used apps, such as Facebook (Allen & La Lime, 2021).

In 2021, Amnesty International conducted the Pegasus Project, a collaborative investigation with over 80 journalists from 17 media organisations, coordinated by Forbidden Stories (Amnesty International Security Lab, 2021). The collaboration revealed how NSO's Pegasus has been used to facilitate human rights violations around the world on a massive scale. This followed the revelation of 50,000 phone numbers that were potentially being surveilled (Amnesty International Security Lab, 2021). During the investigation, technicians at the Amnesty International Security Lab were able to identify traces of NSO's zero-click attack.

The investigation found that at least 180 journalists in 20 countries were selected as potential targets with Pegasus. Saudi journalist Jamal Khashoggi's family members were targeted with Pegasus software before and after his murder in Istanbul in October 2018 by Saudi operatives (Amnesty International Australia, 2021). According to Amnesty International, his wife, Hanan Elatr, was repeatedly targeted with the spyware between September 2017 and April 2018, as was his son (Amnesty International Australia, 2021). The case has become one of the most cited examples of accusations connecting Pegasus-related surveillance leading to the killing of a journalist (Amnesty International Australia, 2021).

Another prominent spyware is Predator, created by Intellexa, a mercenary spyware company, which, like the NSO Group, sells its products to governments (Amnesty International Security Lab, 2025). Predator and Pegasus are comparable forms of commercial spyware, both capable of covertly infiltrating mobile devices and enabling extensive surveillance of targeted individuals.

Intellexa has been surrounded by repeated public exposure, criminal investigations, and financial sanctions (Amnesty International Security Lab, 2025). For example, in 2023, United States (US) officials placed Intellexa on a blacklist after determining that its surveillance tools posed a threat to national security (Fox, 2023). The same year, the Creek Data Protection Authority fined the company for failing to comply with its standards (Amnesty International Security Lab, 2025). Despite this, an investigation by Amnesty International states that Intellexa's Predator is still employed to unlawfully surveil activists, journalists, and human rights defenders around the world (Amnesty International Security Lab, 2025). In 2024, Teixeira Cândido, an Angolan journalist, jurist, and press freedom activist, was targeted with Predator (Amnesty International Security Lab, 2026). In summer 2025, a human lawyer from Balochistan received a malicious link over WhatsApp from an unknown sender that has been attributed to Pegasus (Amnesty International Security Lab, 2025).

2.1.3 Rwanda

For autocratic regimes such as that of Rwanda, the appeal of digital surveillance is evident. Spyware offers an easy-to-use platform able to simultaneously track domestic political dissidents, international activists, and foreign governments (Allen & La Lime, 2021). According to Amnesty International, Rwanda used Pegasus against 3,500 people in 2021 (Allen & La Lime, 2021). This list includes activists, journalists, political opponents, foreign politicians and diplomats (Allen & La Lime, 2021). A report published by the Organised Crime and Corruption Reporting Project (OCCRP) in 2024 revealed that Rwanda wiretapped various phone conversations of Uganda's top officials, including ex-Prime Minister Ruhakana Rugunda and former Foreign Affairs Minister Sam Kutesa (Oduor, 2024).

During the 1994 Rwandan genocide, Paul Rusesabagina, a Rwandan human rights activist and luxury hotel manager, sheltered more than 1,200 people from the violence. After leaving Rwanda, Rusesabagina became a vocal critic of President Paul Kagame and a political opposition figure (Frost, 2021), while he was living in the US and Belgium until his arrest by the Rwandan government in 2022 (Kirchgaessner & Taylor, 2022). Rusesabagina was tricked by Rwandan officials into boarding a private plane in Dubai that was flying to Kigali (Kirchgaessner & Taylor, 2022). In a seven-month-long trial that followed his arrest, Rusesabagina was accused of being the founder, leader and sponsor of violent extremist terrorists operating in various places in the region and abroad (Frost, 2021). Reports stated that his daughters' and nephew's mobile phones were hacked nearly a dozen times in 2020 through Pegasus (Kirchgaessner & Taylor, 2022). According to Amnesty International's Pegasus Project, the software was used to specifically monitor his daughter Carine

Kanimba's private calls and discussions with US, European and British government officials (Kirchgaessner, 2021).

Similarly, Jean Bosco Gasasira, a journalist and Editor-in-Chief of the independent newspaper Umuvugizi, who fled from Rwanda after multiple threats against his life (Pfenniger, 2024). Gasasira was granted asylum in Sweden, but intimidation tactics continued. In 2017, Sweden expelled a Rwandan diplomat for allegedly spying on Rwandan refugees in the country (Meldrum, 2017): the action came after reports of the President of Rwanda at the time sending agents overseas to silence critics emerged (Meldrum, 2017). The efforts to crack down on Gassasiro did not halt: in 2020, staff at the Rwandan embassy reported to the local media how his relatives were offered 5 million kronor (490,000 €) at the time in exchange for the address of Gassasiro (Pfenniger, 2024).

2.1.4 Morocco

Morocco is one of NSO Group's largest clients and has used Pegasus to target about 10,000 phone numbers (Allen & La Lime, 2021). Alongside Rwanda, Morocco seems to be among the few African states publicly linked to the use of Pegasus to spy on foreign government officials (Allen & La Lime, 2021).

Moroccan journalists were among the first worldwide to oppose the use of spyware in early 2015. The Pegasus Project later validated what Moroccan journalists had long suspected (Committee to Protect Journalists MENA Staff, 2022); however, the Project was unable to analyse the phones of all of those named as surveillance targets to confirm the install the spyware, an issue highlighted by the Moroccan government to deny ever using the spyware (Committee to Protect Journalists MENA Staff, 2022).

In November 2021, just months after the Pegasus Project publication, two phones belonging to prominent Sahraoui human rights activist Aminatou Haidar were targeted and infected with Pegasus spyware. The phones of journalists are often targets of spyware because their phones are more than personal devices: they often hold months or years of sensitive reporting work, valuable contacts, photographs, and documents (Musoke, 2025).

The Moroccan government has often been called out by domestic and international organisations for its crackdown on civic space. In 2021, Moroccan journalists and press freedom advocates accused Moroccan authorities of using trumped-up sexual assaults and "moral" charges to retaliate against their work. According to the reports, sex crime charges have become a tool to use against journalists, because such offences often dampen public support for the accused (CPJ Middle East and North Africa Program, 2021). Charging a journalist with sexual assault and rape is also a tool to prevent international and national solidarity with the journalist. For example, in 2025, the Moroccan court sentenced prominent activist Fouad Abdelmoumni *in absentia* to six months in prison and fined him 2,000 dirhams (208 USD) over a Facebook post on French-Moroccan relations (Human Rights Watch, 2026).

2.1.5 The Kingdom of Saudi Arabia

Saudi Arabia's absolute monarchy restricts almost all political and civil liberties. The regime relies on extensive surveillance and criminalisation of dissent (Freedom House, 2022). Censorship and high-tech surveillance systems remain prevalent in the country, with Saudi leadership increasing its reliance on global providers of spyware to monitor the online footprint of Saudi residents (Freedom House, 2022). The Saudi government has been accused of using NSO Pegasus spyware to monitor and silence Saudi human rights defenders for years with impunity, according to Human Rights Watch (Human Rights Watch, 2024).

In 2018, the Citizen Lab concluded that a Canadian-based Saudi activist's phone was infected with spyware, allowing full access to their device. Another investigation by the organisation in 2020 also revealed that two other exiled Saudi dissidents, a New York Times journalist and an Amnesty International staff member, were victims of the spyware attack (Human Rights Watch, 2024).

In 2024, Saudi human rights defender Yashya Assiri brought a case against Saudi Arabia to the United Kingdom High Court on allegations of targeting him with spyware between 2018 and 2020 (Human Rights Watch, 2024).

Citizen Lab reported in 2021 that Saudi authorities had likely started additionally using Predator spyware (Freedom House, 2022). The report was based on NSO groups' 2021 transparency report, mentioning that it had cut off a client, which was later revealed to be Saudi Arabia. After the incident, IP addresses in Saudi Arabia began to match Predator fingerprints, further indicating the potential switch (Freedom House, 2022).

2.1.6 United Arab Emirates

The authorities in the United Arab Emirates (UAE) continue to crack down on human rights and freedoms, including targeting human rights activists, enacting repressive laws, and using the criminal justice system as a tool to eliminate the human rights movement (El Hosseiny, 2023). Ahmed Mansoor, one of the UAE's most prominent human rights defenders, who received the Martin Ennals Award for Human Rights Defenders in 2015 and was a member of the Human Rights Watch Middle East and North Africa Advisory Committee, was arbitrarily imprisoned in 2018 (Human Rights Watch, 2025). The report suggests that the UAE government used Pegasus against him (Thiébaud, 2023). Mansoor was sentenced to 10 years in prison for harming the state's reputation, among other offences (Human Rights Watch, 2025). He was held in solitary confinement and denied access to glasses and most personal hygiene items, as well as any reading materials, television or radio, according to independent rights groups (Human Rights Watch, 2025). These measures violate the prohibition against torture and other cruel, inhuman or degrading treatment or punishment in Article 16 of the UN Convention against Torture (UN General Assembly, 1984).

Surveillance is not only employed to extract information but also to intrude into private life and intimate space (Thiébaud, 2023). Spying on communication with family and loved ones is a form of psychological violence, aiming to silence victims (Human Rights Watch, 2025);

a type of abuse women are particularly vulnerable to. Al Jazeera journalist Ghada Oueiss' phone was hacked, and a private photo of her in a swimsuit was circulated on Twitter (Thiébaud, 2023). This resulted in immense social media harassment from accounts suggesting a connection to Saudi Arabia or the UAE (Committee to Protect Journalists, 2021).

In recent years, the headlines have reported on the video and voice calling app ToTok, which worked in the UAE as a substitute for the banned international apps such as WhatsApp and Skype (Thiébaud, 2023). Millions of users had already downloaded ToTok before the New York Times reported that it is used as a tool by the UAE intelligence service to access users' conversations, movement, and other personal information (Thiébaud, 2023).

2.2 Legal and Regulatory Frameworks

Across the Middle East and Africa, governments have been increasingly using legal frameworks, like anti-cybercrime laws or laws against non-governmental organisations (NGOs), to diminish dissent. Several countries, including Egypt, Saudi Arabia, Jordan, Uganda and Nigeria, have passed or amended laws that criminalise online dissent as terrorism, require NGOs to seek permission for regular civic work, and allow security agencies broad discretion to block websites, freeze assets and arrest journalists.

The following sections focus on two specific tools of lawfare. The first is legislation that criminalises speech, and the second is association laws that criminalise organising. Used together, they shrink civic space from both sides. Human rights groups have documented a consistent pattern of vague drafting, harsh penalties, and selective enforcement that targets activists, journalists and human rights defenders while shielding officials from scrutiny.

2.2.1 Egypt's Legal Architecture

Over the past decade, Egypt has built an extensive legal framework in regard to civic space. For example, Law No. 149 of 2019 on Regulating the Work of Civil Associations replaced the internationally condemned Law No. 70 of 2017 after pressure from the European Union and the United States (Human Rights Watch, 2019). While the 2019 law removed imprisonment as previously included in the 2017 statute for independent NGO workers, it retained almost every other restriction (Human Rights Watch, 2019; TIMEP, 2019). The 2019 law defines “civic work” as “any non-profit work aiming at developing the society”, a definition so broad that a wide range of activity is not considered lawful without prior registration with the Ministry of Social Solidarity (Human Rights Watch, 2021a). Implementing Regulations, issued as Prime Ministerial Decree No. 104 in January 2021, tightened the scope further, requiring associations to update their records monthly with the Ministry and granting inspectors the power to enter offices without prior announcement (Human Rights Watch, 2021b). Article 14 of the law also limits the extent of work by NGOs to “social development” aligned with state plans, and Article 24 makes foreign funding dependent on government approval within 60 days (CIHRS, 2021). Violations result in fines

of up to one million Egyptian pounds, which are roughly 64,000 US dollars, replacing imprisonment (Human Rights Watch, 2019).

Foreign organisations face an additional licensing fee of up to 50,000 Egyptian pounds under Article 66, rising to 200,000 Egyptian pounds on renewal, an impossible amount to pay for smaller and grassroots NGOs (ICNL, 2026a). By October 2022, only 32,000 of the 52,500 NGOs operating in Egypt had managed to register, and after the deadline of April 11th, 2023, those that failed to register were forcibly closed and their assets were frozen (Human Rights Watch, 2023a). Several leading groups chose to dissolve their organisation rather than comply, for example, the Arab Network for Human Rights Information ended 18 years of operations on January 10th, 2022, because of the law's restrictions (Human Rights Watch, 2023a).

Tackling cybercrime, Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes came into force on August 15th, 2018: its 45 provisions reach far beyond genuine cybercrime. Article 7 empowers investigators to block any Egyptian or foreign website that appears to be a threat to “national security or the national economy” (Andersen, 2025). Article 25 criminalises online content violating “the familial values and principles of Egyptian society”, punishable by up to two years in prison and fines of up to ten million Egyptian pounds. The law does not clearly define what is meant under these terms, making the application very broad and oftentimes confusing. Article 27 further penalises the use of accounts to commit any offence under the law, while Article 2 requires service providers to keep user data for 180 days (Mujally and Bälz, 2018). Executive monitoring extends to any social media account with more than 5,000 followers, which is automatically classified as a media outlet subject to state oversight (PPLAAF, 2025).

The way the two frameworks meddle can be seen in the prosecution of the Egyptian Initiative for Personal Rights (EIPR),¹ one of the country's most prominent remaining human rights organisations. In November 2020, shortly after hosting a briefing with 13 Western ambassadors and diplomats at EIPR's Cairo office, three of the organisation's directors, Gasser Abdel-Razek, Karim Ennarah, and Mohamed Basheer, were arrested and charged on grounds for joining a terrorist group and spreading false news. The arrests were widely understood as retaliation for the meeting, and though the three were released on bail in December 2020 after international pressure, the charges were never formally dropped and their assets remained frozen for years (UN News, 2020).

On August 27th, 2025, Ennarah was detained for 12 hours at a checkpoint and investigated in Case No. 6952/2025 on charges of “broadcasting false news and using a website to commit a crime” (EIPR, 2025). On January 19th, 2025, Hossam Bahgat, also an EIPR director, was charged in Case No. 6/2025 with financing a terrorist group and spreading false news, following an EIPR report on dire conditions in the 10th of Ramadan Prison (Correction and

¹ An NGO strengthening and protecting basic rights and freedoms in Egypt, through research, advocacy and supporting litigation in the fields of civil liberties, economic and social rights, and criminal justice.

Rehabilitation Center 6)² (Amnesty International, 2025a). Bahgat has been unlawfully detained by the authorities multiple times before. In 2016, they arbitrarily banned him from travelling and froze his assets in Case 173, also known as the foreign funding case, that targeted dozens of NGOs and froze their assets (Amnesty International, 2025; Bahgat, 2015). Case 173 was opened in 2011 and only closed in 2024. Taken together, these prosecutions show that even Egypt's most prominent NGO, the one allowed to operate inside the country, cannot escape a pattern of revolving-door harassment (Hossaini, 2025).

2.2.2 Saudi Arabia's Legal Architecture

Saudi Arabia relies on three legal frameworks that effectively outlaw independent civic life. The Anti-Cyber Crime Law of 2007 (Royal Decree M/17) criminalises, under Article 6, the creation of any content that “impinges on public order, religious values, public morals, or privacy”, with penalties of up to five years in prison and fines of up to three million riyals (Dig Watch, 2007). The Law for Combating Terrorism and its Financing of 2017 (Royal Decree M/21) defines terrorism in exceptionally broad terms: as a result, Articles 30, 34, 43, and 44 have been routinely applied to tweets criticising the Kingdom, with the law criminalising “describing the King or the Crown Prince in a way that undermines religion or justice” (Laws on Countering Terrorism Worldwide, n.d.; Human Rights Watch, 2017). The Law on Associations and Foundations of 2015 (Royal Decree M/8), with its Charity Associations and Foundations Bylaw issued on March 22nd, 2016, gives the Ministry of Labour and Social Development sole discretion to license NGOs and unilaterally dissolve them (ADHRB, 2016; ICNL, 2019).

Registration may be denied for “violations of Islamic Sharia”, “contradictions to public morals” or “breaches of national unity”, all terms left largely undefined (ADHRB, 2016; ICNL, 2019). Some foreign associations cannot register at all, and unless an organisation is officially licensed with the Saudi Ministry of Social Affairs (MoSA), holding gatherings as an association is considered illegal. Registering with the Saudi government as an autonomous right organisation is however almost impossible. The Adala Center for Human Rights, an NGO monitoring abuses including torture in the Kingdom, was denied registration by the MoSA in December 2011 on the grounds that its objectives did not align with regulations. After a prolonged 13-month appeal, Saudi courts upheld the decision, forcing the organisation to shut down (ADHRB, 2016).

The result is a state in which no independent human rights organisation operates legally, and prosecution is channeled through the Specialised Criminal Court (SCC), originally established for terrorism cases (ADHRB, 2016). On January 9th, 2024, the SCC secretly sentenced Manahel al-Otaibi, a 29-year-old fitness instructor, to eleven years in prison under Articles 43 and 44 of the Counter-Terrorism Law, after she was initially charged under the Anti-Cyber Crime Law for tweets supporting the #EndMaleGuardianship hashtag – an online campaign calling for the abolition of Saudi Arabia's male guardianship system, which

² For further information, see <https://www.amnesty.org/en/latest/news/2025/03/egypt-detainees-punished-for-protesting-their-detention-in-cruel-conditions/>.

requires women to obtain a male relative's permission for major decisions such as travel and marriage – and for posting images on Snapchat in which she was not wearing an abaya (Amnesty International, 2024a). While in detention, she had been subject to torture, several other forms of abuse, and enforced disappearance (Amnesty International, 2025b; Washington Center for Human Rights, 2024).

Salma al-Shehab was sentenced to 27 years in prison on January 25th, 2023, also under terrorism provisions, for tweets supporting women's rights; her sentence was eventually reduced and she was released in February 2025 (Amnesty International, 2025c). Similarly, Mohammed bin Nasser al-Ghamdi, a retired teacher, was sentenced to death in July 2023 for tweets “in which he critici[s]ed the Saudi King and Crown Prince and Saudi's foreign policy, called for the release of detained religious clerics and protested increased prices” and for uploading YouTube videos with fewer than ten followers where he is vocally critical; the sentence was reduced to 30 years imprisonment in September 2024 (Amnesty International, 2024b).

By January 2024, Amnesty International had documented 69 individuals prosecuted solely for peaceful expression, of which 32 of them were carried out over social media posts (Amnesty International, 2024c). Between December 2024 and February 2025, Saudi Arabia released at least 44 prisoners, though many remained under travel bans and surveillance (Human Rights Watch, n.d.a). Although Vision 2030, the Kingdom's flagship economic and social reform plan launched in 2016 to diversify the economy beyond oil and open the country to tourism and entertainment, projects an image of modernisation, these reforms coexist with the criminalisation of online hashtag movements and the freedom of expression.

2.2.3 Jordan's Legal Architecture

On August 12th, 2023, Jordan adopted Cybercrime Law No. 17 of 2023, which entered into force in September 2023 and has since raised significant concerns regarding restrictions on digital rights and freedom of expression (Dentons, 2023). The law, replacing the 2015 statute, was rushed through parliament in less than a month with no meaningful consultation (Abu Yahia and Heldt, 2023). Article 15 criminalises “sending or resending fake news targeting the national security and community peace” without requiring a personal complaint from any affected party, meaning the state can prosecute on its own initiative. Article 17 criminalises online expression that “provokes strife or sedition, threatens societal peace, incites hatred, calls for or justifies violence, or insults religions”, carrying sentences of one to three years and fines of 5,000 to 20,000 Jordanian dinars, roughly 7,000 to 28,000 US Dollars (Burns, 2024; RSF, 2024a). Article 33 allows prosecutors to order the removal, blocking or interception of any online content.

Between August 2023 and August 2024, Amnesty International documented hundreds of charges, and Jordan's National Centre for Human Rights reported 3,170 prosecutions in 2024 alone under the new law, overwhelmingly under Articles 15 and 17 (Human Rights Watch, n.d.b; Amnesty International, 2024d). Following the start of the war in Gaza in October

2023, numerous cases targeted pro-Palestine speech. Among others, journalist, playwright and satirist Ahmad Hassan al-Zoubi was arrested on July 2nd, 2024 to serve a one-year sentence from 2023 for a Facebook post criticising the authorities' response to strikes on Gaza (Amnesty International, 2024d; RSF 2024b).

Lawyer Moutaz Awwad was fined 5,000 Jordanian dinars on July 22nd, 2024 under Article 17 for tweets criticising Arab governments' policies toward Israel and expressing pro-Palestine sentiment (Amnesty International, 2024d). Activist Samer al-Qassem was sentenced to three months and fined 5,000 dinars in June 2024 over a TikTok video about Palestinian refugees (Amnesty International, 2024d). Jordan's Law on Societies (Law No. 51 of 2008) also requires Interior Ministry approval for foreign funding and public meetings (ICNL, 2025). The authorities also banned TikTok in December 2022 and blocked the satirical outlet Al-Hudood, further narrowing the space for online expression (Abu Yahia and Heldt, 2023; Freedom House, 2024).

Together, these measures have produced a marked chilling effect. Journalists, lawyers and ordinary social media users now face the real prospect of prosecution for criticising the government, commenting on the war in Gaza or sharing content online, with self-censorship becoming widespread.

2.2.4 Uganda's Legal Architecture

Uganda's Computer Misuse Act of 2011 was amended on October 14th, 2022 when President Yoweri Museveni signed an amendment, adding new offences for "hate speech", "malicious information" and "misuse of social media" with penalties of up to seven years in prison and fines of 15 million Ugandan shillings (Malik, 2022; LOC, 2023). In January 2023, the Constitutional Court declared Section 25 of the original Act concerning "offensive communication" as unconstitutionally vague. However Section 24 on cyber harassment remains in force, while the 2022 amendments add broader offences characterised with similarly vague language (Kigongo and Wesaka, 2023; Article 19, 2023; Nanfuka, 2023).

The law has been used against critics ranging from poet Stella Nyanzi, jailed in 2019 under Section 25 of the original Act for a Facebook poem insulting President Museveni and his late mother, to novelist Kakwenza Rukirabashaija, who was arrested in December 2021 over tweets mocking Museveni and his son, army commander Muhoozi Kainerugaba, tortured in detention and forced to flee to Germany (Nanfuka, 2023; Human Rights Watch, 2022; Monitor, 2022). His charges remain pending before Buganda Road Court (Kakuru Advocates, 2023). Furthermore, in December 2024, several TikTok users were arrested for content about the First Family (ICNL, 2026b).

The Non-Governmental Organisations Act of 2016, substantially amended by the Non-Governmental Organisations (Amendment) Act, 2024, abolished the semi-autonomous NGO Bureau and reintegrated it into the Ministry of Internal Affairs, centralising direct state control over registration, permits, and deregistration (Amnesty International, 2024e). The

law, combined with the Public Order Management Act of 2013 and the Anti-Terrorism Act of 2002, gives the state broad powers to freeze NGO bank accounts and suspend operations (ICNL, 2026b).

The Anti-Homosexuality Act, 2023, largely upheld by the Constitutional Court, further prevents civic space by criminalising the “promotion” of homosexuality, a provision explicitly used to ban Sexual Minorities Uganda (SMUG) and other organisations working on Lesbian, Gay, Bisexual and Transgender (LGBTQIA+) rights. The Court has rejected SMUG’s registration request in March 2024 on public interest grounds (Human Rights Watch, 2024). In the run-up to the January 2026 elections, authorities cut internet access nationally, and in February 2026 the Uganda Communications Commission banned independent reporting that “disputed” the official results (ICNL, 2026b).

The shutdown was imposed on January 13th, 2026, two days before polling, and lasted roughly five days, while social media platforms remained blocked for nearly two weeks. Crucially, banking services and the Electoral Commission’s own portal stayed online, which meant that the state retained control of the official narrative while opposition agents, independent journalists and citizens lost the means to document what was happening at polling stations in real time. African Union observers, led by former Nigerian President, Goodluck Jonathan, publicly stated that the blackout disrupted effective observation of the vote and increased suspicion of the results, in which President Yoweri Museveni was declared the winner with 71.65 percent of the vote.

The February decision then prohibited broadcasters from reporting vote counts from any source other than the Electoral Commission, meaning that independent reporting of the election was first cut off, and then retroactively criminalised. In April 2025, 11 environmental defenders, known as the #KCB11, were arrested after attempting to deliver a letter to the Kampala branch of Kenya Commercial Bank (KCB) protesting the bank’s decision to help finance the East African Crude Oil Pipeline. They were detained for 85 days before being released on bail in July 2025 (ICNL, 2026b). The #KCB11 is part of the broader StopEACOP coalition, which opposes the TotalEnergies-led pipeline on environmental and human rights grounds.

What emerges is a layered system of control. The Computer Misuse Act reaches online speech, the 2024 NGO amendment reaches organisations, and the Anti-Homosexuality Act reaches an entire community, while internet shutdowns close the gaps around elections. Each measure has a facade of legality, yet the combined effect is a civic space in which dissent carries a real risk of prosecution.

2.2.5 Nigeria’s Legal Architecture

While Nigeria has maintained a vibrant tradition of investigative journalism and civic activism ranging from the #EndSARS protests of 2020 to ongoing mobilisation against insecurity and corruption, the country’s civic space has increasingly narrowed, primarily

through the use of cybercrime legislation against journalists, bloggers and peaceful critics. Nigeria's Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 was enacted to address online fraud, a legitimate aim in a country with a serious cybercrime problem. However its Section 24, which criminalised messages deemed "grossly offensive", "indecent" or causing "annoyance", quickly became the government's weapon of choice against critical voices. The Economic Community of West African States (ECOWAS) Court of Justice ruled in 2020 and again in 2022 that Section 24 was vague, arbitrary and in violation of the African Charter on Human and Peoples' Rights, ordering Nigeria to amend or repeal the provision (Freedom House, 2024). The Socio-Economic Rights and Accountability Project (SERAP) underlined the section "escalating restrictions including arbitrary arrests, digital surveillance and website blocking" (Agbo, 2025a).

The statute was then amended under the Cybercrimes (Amendment) Act 2024 on February 28th, 2024, implementing ECOWAS rulings. The amendment narrowed Section 24, applying only to pornographic messages or knowingly false messages the sender delivers with the intent of causing a law and order breakdown or posing a threat to life (Freedom House, 2024). The maximum three-year prison sentence and 25 million naira fine for cyberbullying was, however, kept. Additionally, key terms such as "false information", "cyberstalking", "insult", "hatred", and "harassment", are still only vaguely defined, leaving room for misuse of the law against dissent and critics, ultimately silencing and censoring civil society groups (U.S. Mission Nigeria, 2025). Civil society groups had warned from the beginning that the reform was insufficient, as the retained phrase "breakdown of law and order" equally remains open to abuse, allowing the authorities to treat critical reporting as a threat to public order (Paradigm Initiative, 2024). The amendment also expanded surveillance powers, allowing security agencies to stop communications without a court order in cases considered urgent (Gyang, 2025). In April 2025, Nigeria's own National Human Rights Commission warned that the Act maintained strong potential for abuse against activists, journalists and ordinary social media users (U.S. Mission Nigeria, 2025).

Similarly, in practice, the amendment changed little. On March 15th, 2024, Segun Olatunji, editor of the news outlet FirstNews, was arrested at home by soldiers, blindfolded, flown to Abuja and held in detention for 14 days under the Cybercrimes Act for publishing articles relating to accountability, without clear charges against him (MfWA, 2024; Okakwu, 2024). On May 1st, 2024, Daniel Ojukwu of the Foundation for Investigative Journalism was abducted by police in Lagos, and held incommunicado for ten days over a story alleging procurement fraud by a former presidential aide (Akua, 2025). Reporters Without Borders documented at least eight cases of journalists prosecuted under the amended law in its first months (Reporters Without Borders, 2024c). In January 2025, publisher and activist Omoyele Sowore was charged with 16 counts under the Act for social media posts describing the Inspector General of Police as illegally occupying his office, and SERAP filed a case at the ECOWAS Court against President Tinubu and Nigeria's 36 state governors, challenging what it called the repressive use of the amended Act (Naija Cyber Lawyer, 2026; SERAP, n.d.).

Since 2016, Nigeria has also repeatedly attempted to pass a Non-Governmental Organisations Regulatory Commission Bill, which would require NGOs to re-register every two years and submit assets to a government-appointed commission, which has been repeatedly blocked by civil society coalitions (Agbo, 2025b). In parallel, the Financial Reporting Council of Nigeria's Not-for-Profit Governance Code of 2023 has imposed detailed governance requirements on non-profit organisations, including mandatory board structures, fixed term limits for directors, separate audit and risk committees, and regular public reporting. Civil society groups warn that these rules were designed for large, well-resourced organisations and are effectively impossible for small, community-based or grassroots groups to meet. Because enforcement is discretionary, the Code creates a compliance trap that regulators can apply selectively against organisations doing politically sensitive work, such as human rights or anti-corruption advocacy, while leaving others untouched (Emmason, 2024).

The state has also shown willingness to cut off entire platforms, suspending Twitter for seven months from June 2021 after the company removed a tweet by then President Muhammadu Buhari threatening south-eastern secessionist groups in terms widely understood as invoking the Biafran civil war. Access was restored only after the company agreed to register locally, appoint a country representative, and cooperate with Nigerian authorities on content moderation (Idris and Guest, 2022).

The result is a democracy in which the formal right to speak freely exists on paper but the practical cost of exercising it keeps rising. Cybercrime prosecutions, NGO regulation attempts, governance codes and platform bans each add a new layer of risk, narrowing the space in which journalists, activists and ordinary citizens can operate without fear of arrest or closure.

2.2.6 Cross-regional Patterns

Across these five countries, similar patterns recur. The laws examined share, a reliance on deliberately vague and broad language. Terms such as “false news”, “community peace”, “family values”, “national security”, “breakdown of law and order”, and “promotion of homosexuality” are left undefined, giving prosecutors near-unlimited discretion to decide on what constitutes a crime. A critical tweet, a satirical Facebook post, a leaked prison report, or even a photograph of someone in the wrong clothing can all be pulled into the same net.

Secondly, the counter-terrorism frame is expanding. In Egypt, Saudi Arabia and Jordan, ordinary online expression is increasingly prosecuted as a terrorism offence, which moves cases into specialised courts with weaker fair-trial protections, harsher sentences and limited avenues of appeal. What would elsewhere be treated as defamation or a misdemeanour becomes, in these systems, a matter of national security.

Thirdly, foreign funding has become the main weakness for civil society. Egypt's 60-day government approval regime for foreign grants, Uganda's 2024 recentralisation of NGO

oversight under the Ministry of Internal Affairs, Jordan's Interior Ministry vetting of associations and donations, and Saudi Arabia's outright ban on foreign NGO branches all aim at the same target, cutting off the donor funding on which independent human rights work depends to survive.

Fourth, reform is often more cosmetic than genuine. Egypt's 2019 NGO law, Nigeria's amendment to the 2024 Cybercrimes Law, and Saudi Arabia's prisoner releases in 2024 and 2025 were presented internationally as liberalising steps, yet each was followed within months by new prosecutions under the same or closely related provisions. The headline changes, while the underlying legal architecture does not.

The cumulative effect is a civic space that is not necessarily closed but more so criminalised by default. Organising without a permit, reporting on a prison, posting a hashtag or wearing the wrong clothes online can now trigger prosecution. When the law itself becomes the instrument of repression, appeals to the rule of law begin to lose their meaning.

2.3 Internet Shutdowns and Platform Blocking as Governance Instruments

In the contemporary landscape of global governance, the definition and geographical boundaries of civic space have expanded from physical public spheres into the digital realm. Nowadays, the internet constitutes the primary infrastructure for political participation, human rights monitoring, and most importantly, freedom of expression. By recognising this, governments across the world are increasingly weaponising internet access. More specifically, internet shutdowns, mobile data suspensions, and targeted platform blockings have been normalised, and in doing so, the states aim to control political narratives, silence dissent, and avoid international scrutiny.

According to the comprehensive data compiled by digital rights organisations, the frequency, duration, and severity of the internet disruptions are now breaking the historical records. Some research revealed that 2024 was a record-breaking year, with 296 documented shutdowns across 54 countries (Access Now, 2024). Reportedly, 47 active shutdowns continued into 2025, 35 of which had already been ongoing for more than a year (Access Now, 2024). According to this research, conflict was the leading trigger for internet shutdowns, with perpetrators expanding their arsenal of tools to cut connectivity in situations of war, conflict, and violence, from jamming devices and cutting cables to destroying infrastructure and sabotaging internet service providers (Access Now, 2024).

The Middle East and North Africa (MENA) region stands out as a critical theater where digital repression is both highly sophisticated and socio-economically devastating. Across the MENA region, authorities and other state actors imposed at least 52 internet shutdowns across 15 countries only in 2025, further highlighting the continued rise of digital repression across the region (Access Now, 2026). Similarly, the African continent has witnessed a quiet but aggressive rise in internet repression, more specifically, in 2024, Africa experienced 21

internet shutdowns in 15 countries, very often coinciding with electoral transitions, civilian protests, and armed conflicts (ISS Africa, 2025).

Internet blackouts come in many forms, each of them carefully designed by the governments to achieve specific political or security goals. The United Nations (UN) has explicitly stated that cutting users off from internet access, regardless of the justification provided, is a disproportionate and direct violation of Article 19(3) of the ICCPR, calling on states to maintain access at all times (OHCHR, 2017). Despite this, governments continue to formalise their power to control networks through domestic legislation, embedding what were once exceptional emergency measures into routine administrative law (EFF, 2026). Today, governments use their power to control networks, enacting telecommunications laws that grant central authorities the unilateral power to suspend services in the interest of “public safety”, “sovereignty”, or “national security” (EFF, 2026). In the Middle East, internet shutdowns are deployed both as blunt instruments of state violence during political uprisings and as routine administrative tools for bureaucratic management.

When it comes to digital authoritarianism, Iran’s government has written the modern playbook. Iran’s use of network shutdowns is very closely linked to the violent suppression of political dissent. For example, during the historic November 2019 protests, the Supreme National Security Council (SNSC) imposed a near-total, seven-day nationwide internet cut affecting mobile and broadband connections across the vast majority of the country (Freedom House, 2023). This unprecedented decision to disconnect the country from the global internet was executed without prior notice or parliamentary approval, and left Iran’s citizens in the dark as security forces used violence against demonstrators (Freedom House, 2023).

This brutal pattern was repeated, expanded, and refined during the widespread “Woman, Life, Freedom” protests that erupted in 2022 following the death of Mahsa Amini while in police custody (Freedom House, 2023). In 2022, the state imposed daily mobile-connectivity curfews, often lasting for eight hours, and specifically targeted all remaining accessible western social media platforms (Freedom House, 2023). The regime also utilises digital isolation as a strategic military shield during geopolitical conflicts. For example, in June 2025, following the military clashes involving Israel and the US, Tehran initiated a sweeping 13-day blackout affecting more than 90 million Iranians (American Foreign Policy Council, 2025). These localised cuts and mobile restrictions have become a daily reality for millions in Iran.

The scale and duration of Iranian blackouts have only intensified in recent years. In December 2025, Iran nationals, outraged at decades of repression, were demanding fundamental change and a political system that respects human rights and dignity (Amnesty International, 2026). The protest started with shopkeepers in Tehran’s Grand Bazaar going on strike and closing their shops, but soon after, people joined, and the protest turned into a mass nationwide street demonstration calling for the end of the Islamic Republic system (Amnesty International, 2026). The security forces of Iran not only responded with lethal force and mass arrests, but on January 8th, 2026, the Iranian authorities initiated a near-total

disconnection of the country's telecommunication infrastructure from the global internet (Human Rights Watch, 2026).

Once the blackout was in place, the security forces carried out massacres against protesters, with the shutdown making it almost impossible for victims, journalists, and human rights organisations to document the violations and preserve evidence. This measure, occurring amidst widespread domestic unrest and instability, represents a significant escalation in the state's use of digital restrictions to manage political dissent. The systematic isolation functions not only as a tool for domestic information control, but also as a mechanism to facilitate state actions without the risk of real-time international documentation or domestic coordination. Moreover, according to real-time metrics provided by the internet monitor NetBlocks, by early April 2026, Iran was engaged in a staggering, continuous internet blackout lasting over 48 days or 1,128 hours (NetBlocks, 2026).

If Iran represents the highly securitised and ideological weaponisation of the internet, the Republic of Iraq represents its bureaucratic normalisation and administrative abuse. Since at least 2014, the Iraqi federal government, alongside the Kurdistan Regional Government, has routinely shut down internet access during middle and high school examination periods (Greater Internet Freedom, 2024). According to the Freedom House, authorities implemented 66 internet outages in 2023 alone, the vast majority occurring during academic exams (Freedom House, 2024). Moreover, between late May and mid-September 2025, Iraq experienced 51 exam-related internet shutdowns across both federal Iraq and the Iraqi Kurdistan region, which equates to nearly one nationwide blackout every other day for four months (Access Now, 2025).

Beyond the blunt instrumental use of shutdowns, the Iraqi state continually asserts technical and legal control over the digital civic space to silence civil society. In March 2023, the Ministry of Communications directed all ISPs operating in federal Iraq to link their Domain Name System (DNS) servers directly with the Ministry's centralised DNS, immediately granting the government the ability to block websites across the country (Freedom House, 2024). This capability was swiftly utilised to target civic space. Furthermore, critical and independent media outlets like the news website *Ultra Iraq* and *Al-Hudood* were blocked indefinitely without official justification, widely believed to be retaliation for their coverage of government corruption and political satire (Freedom House, 2024).

In Africa, internet shutdowns frequently intersect with armed conflict, severe ethnic marginalisation, and the rapid erosion of democratic institutions. The Federal Democratic Republic of Ethiopia possesses one of the most extensive, systematic, and brutal histories of internet shutdowns globally, maintaining its status as a leading perpetrator of digital blackouts on the African continent (ISSA Africa, 2025). Since 2016, Ethiopia has shut down the internet at least 26 times (Access Now, 2023). The Ethiopian government's deployment of internet shutdowns represents an instrument of absolute information warfare, utilised to control conflict narratives, hide human rights abuses, and economically and socially isolate

marginalised ethnic regions. The Tigray region lost internet access for nearly two years (November 2020-February 2023) during the conflict.

During this time, the government severed mobile networks, landlines, and the internet, preventing journalists, humanitarian workers, and international observers from reporting on the war or verifying sources' experiences (LSE, 2026). When armed clashes erupted between the Fano militia and federal forces in Amhara in 2023, the internet went down again, this time for about 11 months. In Oromia, where there have been frequent conflicts between the Oromo Liberation Front and the federal government, shutdowns have been more frequent and scattered. The scale of these shutdowns is enormous. Tigray has experienced extended blackouts, Amhara's more intermittent disruptions have totalled roughly 345 days, while Oromia has seen scattered outages totalling 90 to 120 days across three years (LSE, 2026). Reportedly, nationwide shutdowns also affected the capital, Addis Ababa, disrupting everything from banking to business to basic communication between families separated by conflict.

Historically viewed as an anchor of democratic stability and civic freedom in West Africa, the Republic of Senegal has recently experienced severe democratic backsliding, characterised by unprecedented and repeated use of internet shutdowns to manage political crises and suppress civilian protest. During the highly turbulent 2023-2024 period, marked by massive public protests surrounding the judicial conviction and electoral exclusion of popular opposition leader Ousamane Sonko, the outgoing President Macky Sall attempted to unconstitutionally delay the presidential election, repeatedly resorting to digital blackouts (Carnegie Endowment for International Peace, 2024).

On June 1st, 2023, the authorities restricted access to major social media platforms and instant messaging applications in response to deadly street clashes between police and Sonko's supporters that left at least 16 dead (AP News, 2023). When protests persisted, and civil society organisations utilised Virtual Private Networks (VPNs) to bypass the shutdowns, the government drastically escalated its tactics and ordered a temporary suspension of all mobile data internet access across the country for multiple days in June, July, and August 2023 (CIVICUS, 2024). This tactic was deployed again in February 2024, following the postponement of the presidential election, marking the country's third major disruption in less than 12 months (ARTICLE 19, 2024). To justify these blackouts, the government relied on a series of legal loopholes, twisting existing laws to treat public dissent as a national security threat.

The Ministry of Communication defended cutting off mobile data access, claiming it was necessary to stop the spread of "hateful and subversive" messages relayed on social networks amid public disorder (AP News, 2023). To build a legal framework for this action, the state heavily leveraged Article 255 of the Penal Code, which criminalises the dissemination of "false news" or fabricated documents that harm the "morale of the population", or bring "discredit on public institutions" (Digital Rights and Inclusion in Africa Report, 2023). However, Senegalese civil society organisations, alongside international human rights bodies, pointed out that these actions directly violated Article 10 of the Senegalese

Constitution, which guarantees freedom of expression (ARTICLE 19, 2023).

The weaponisation of internet access has fundamentally evolved from a sporadic emergency measure into a normalised, structural pillar of modern state control. As shown, governments around the world increasingly view the digital realm not as a public utility but as a primary battleground for suppressing dissent, concealing human rights abuses, and establishing fake narratives. Whether deployed as an extreme ideological tool of mass isolation in Iran, a routine administrative mechanism in Iraq, a weapon of wartime marginalisation in Ethiopia, or a shield against democratic accountability in Senegal, these digital blackouts systematically dismantle modern civic space.

2.4 Disinformation & Narrative Control

Over the last decade, social media platforms across the Middle East and Africa have gone from being praised as tools of liberation to being condemned as agents of repression. In this regard, the assumption that the internet would have acted as a liberation technology has been challenged by overwhelming evidence to the contrary. Authoritarian regimes in Africa and the Middle East have found ingenious ways to capitalise on digital technologies for repression and control (Lynch, 2021).

For example, social media, and the internet in general, was key for backing mass mobilisation during the “Green Revolution” in Iran and the Arab Spring (Marc Owen Jones, 2022). However, the growing discontent online was bound to face opposition from the government. Following the Arab Spring, regimes that survived, most notably Saudi Arabia, made significant investments to sway social media conversation in their favour (Ibid, 2022). Within the MENA region, the ‘change of course’ has capitalised on the growing sense of disillusionment with the Arab Spring and the concomitant rise in counter-revolutionary mobilisation.

In this setting, official state media have emerged as a critical tool for leveraging the internet to the benefit of regimes: in a wide-ranging surveilled environment, coordinated internet actors and linked channels keep an eye on public discourse, promote official narratives, and, above all, identify dissident voices to later target (Ron Deibert, 2015). Thus, state media surveillance becomes crucial in social monitoring. As more than just gathering data, it involves observing who is speaking, what is being said, and how such discourse can be reframed and presented as dangerous, immoral, foreign, or connected to state terrorism (Ibid, 2015). Delegitimising activists is therefore one of the key strategies through which civic space is eroded. By portraying protesters, journalists, and human rights defenders as threats to national security or social stability, states reduce public sympathy for dissent and make repression appear legitimate (Lynch, 2021). This process is often reinforced through legal restrictions, physical intimidation, and online smear campaigns, especially during elections or periods of political tension (Ibid., 2021.). In this way, disinformation and narrative control become integral to the broader architecture of digital repression.

This chapter therefore examines the main strategies through which state media and affiliated actors contribute to digital repression, with particular attention to the delegitimisation of activists and the resulting erosion of civic space.

2.4.1 Iran

Iran's disinformation strategy has been in place since the birth of the regime itself (Hassaniyan, 2022). Here, state media is a strong tool for delegitimising activists, using disinformation to dominate narratives and preserve the system. The government uses channels like the Islamic Republic of Iran Broadcasting (IRIB) to portray dissidents as traitors, puppets in the hands of foreign powers, or moral deviants, undermining public trust and justifying crackdowns. This strategy, which has been honed over decades, is heightened during crises to split opposition and maintain theocratic power (ISD, 2026).

State media in the Islamic Republic employs a variety of tactics to undermine and discredit activists. For example, smear campaigns are one of the primary instruments used to manipulate public perception. Protesters here are frequently accused of being immoral people connected to foreign agents in the Central Intelligence Agency (CIA) or the Mossad. They are also defined as “riotists” or simply affiliated to any opposition to the regime (Hassaniyan, 2022). Employment of fake confessions is another interesting and important strategy. Videos of arrested activists “confessing” their crimes, under coercion, are often produced by the regime (Amnesty International, 2016).

Persian identity narratives are another potent tactic used by the Islamic Republic to repress resistance and shape public opinion. The regime fosters division by orchestrating tensions between Persians and minority groups like Kurds, Baluchis, or Bahá'ís (Hassaniyan, 2022). These are combined with bigger psychological operations, synchronising TV broadcasts, mosque sermons, and Telegram channels managed through the National Information Network (Ibid, 2022). A few recent episodes demonstrate the use of these strategies. In December 2025, multiple protests occurred, during which Iranian media reported that the unrest was the result of foreign-backed riots, plainly referring to the US and Israel, minimising civilian losses caused by the regime's response to them (ISD, 2026).

This narrative of foreign intervention is frequently reinforced by referencing Iran's informal regional connections with the Houthis in Yemen, Hezbollah in Lebanon, and Hamas in Palestine. This so-called axis of resistance is portrayed as anti-Western, and Iran utilises it to back up charges of Western intervention in its domestic affairs headed by the US and Israel, shaping and controlling the internal narrative (Ibid, 2026). The recent start of the war between the US, Israel, and Iran has bolstered this information control apparatus. During blackouts and missile exchanges, IRIB has broadcast AI-generated information, including supposed Iranian wins and false news. As a result, state media continue to amplify disinformation while restricting internet access to direct the public to approved and regulated sources (ISD, 2026). It is needless to mention the use of AI contributes to the saturation of information by fusing altered content with actual footage to affect how people around the world perceive events.

2.4.2 Saudi Arabia

When it comes to digital authoritarianism in the Middle East and North Africa, Saudi Arabia is undoubtedly one of the major players (Lynch, 2022). Saudi media outlets serve as a sophisticated weapon for delegitimising activists, spreading lies and using deception to enforce narrative control and defend the monarchy's authority. The strategy of portraying dissidents as security concerns, particularly by characterising them as puppets in the hands of Qatar and Iran (Ibid, 2022), appears similar to that of Iran, although with a different focus on Western operations, as analysed previously.

One intriguing feature of delegitimisation in this context is that dissidents are also presented as economic saboteurs, in addition to the other labels stated above (Democratic Erosion Consortium, 2021). This emphasises the importance of social story building, which in this case positions Saudi Arabia as one of the Gulf's greatest rentier states. The importance of social narrative here also takes place within the context of the state's Vision 2030 image-rebranding initiative, which is headed by Crown Prince Mohammed bin Salman, better known as "MBS" (Saudi Vision 2030, 2024).

This coordinated strategy, indeed, far from being merely propaganda, floods platforms like X (formerly Twitter) and other similar social media, with fake accounts, bots, and paid influencers, creating trends that mimic broad public support for MBS and his Vision 2030 (Democratic Erosion Consortium, 2021). By manipulating visibility and algorithms, this system does not merely disseminate pro-regime content; it alters what users perceive as public opinion, suffocating critical voices (Ibid, 2021).

In this way, traditional media are outrun in terms of reach and speed, ensuring that the regime's narratives dominate both the domestic and global digital spheres. Bot-driven campaigns are at the centre of this scam, in addition to the establishment of armies of fake accounts and influencers paid to share pro-government hashtags, which artificially boost social media trends and simulate widespread public support (Mancini, 2025). Despite Twitter suspending a significant number of these accounts in 2019, labelling the cases as "coordinated manipulation", these networks continued to operate. Many, in fact, continue to use data obtained by activists through malware like Pegasus for targeted smear operations (Ibid, 2025).

The tactic itself is based on a strategy aimed at creating confusion rather than on denial. By introducing a constant stream of information, algorithms are exploited to distort what users perceive as public opinion without the need for consensus on a single truth. This creates a grey area regarding potential breaches of legal frameworks (Democratic Erosion Consortium, 2021). A key example is the response to the murder of journalist Jamal Khashoggi. In the wake of international outrage, networks of pro-government accounts promoted hashtags designed to show support or divert attention, spread conflicting information and dilute the global debate. The aim was not necessarily to convince everyone of a single alternative truth,

but to create confusion, reduce the visibility of criticism and fragment public discourse (Ibid, 2021).

The operation also extends globally through international co-optation, with state funding channelled to Western media outlets for coverage designed to rebrand MBS as a visionary reformer, thereby helping to sideline investigations into human rights violations (Mancini, 2025). It is indeed important to understand that, at the heart of it all lies a surveillance system based on artificial intelligence, fuelled by advanced technologies imported from China as part of the Belt and Road Initiative (Ibid, 2025). Following the Arab Spring, investment in social media surveillance by the Saudi regime has increased significantly, as have online arrests and content filtering systems. These are used as a tool for internal repression and as a geopolitical lever for the regime itself (Lynch, 2021).

2.4.3 Sudan

In Sudan, state media has long been a cornerstone of government control, evolving from suppression during the Bashir era, to the current sophisticated disinformation machinery of the conflict between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) (Internews, 2025). Similar to previously analysed regimes, Sudan TV and Radio, as well as related social media, systematically delegitimise activists by labelling them as outsiders and traitors. A crucial difference is the idea of foreign intervention: here, dissidents are labelled as RSF puppets (Amnesty International, 2016).

In the Sudanese context, the ecosystem is strongly shaped by the prolonged and persistent conflict. Control over the domestic narrative is established inside a media apparatus weakened by this war (Internews, 2025). Infrastructure has been undoubtedly devastated, and power cuts enabled state voices to dominate public discourse, enriching it with unproven claims, and effectively blocking the establishment of any form of independent media (Ibid, 2025). Moreover, according to an Amnesty International report, civil society has been relentlessly suppressed by arrests and threats (Amnesty International, 2016).

In a society afflicted by constant internal conflict, it is interesting to notice how the strategies of the two parties involved are oftentimes identical. Indeed, the RSF accuses those who criticise the SAF of being genocidal, whereas the SAF claims the RSF's crimes as their own (Ibrahim, 2023). This strategy is obviously employed to feed internal support currents, but in practice, these misleading narratives put human lives in danger, resulting in a serious humanitarian situation that discourages any form of foreign aid intervention.

Beside the disinformation ecosystem, Sudanese state propaganda uses planned smear efforts to undermine the credibility of activists as well. A TIMEP's investigation of the "virtual propaganda warzone" indicates the presence of bots and troll farms, frequently linked to the UAE or Russia, which spread allegations that human rights advocates collaborate with enemies, fuelling offline violence such as targeted killings (Hamid Khalafallah, 2025). For instance, peace advocates in Khartoum are demonised online by being called "separatists", demonstrating once again the power of narrative control. In this approach, media control

traps Sudan in an information war where survival-driven propaganda takes precedence over the truth, delegitimising dissent and contributing to the profitability of conflict.

2.4.4 Ethiopia

Under Prime Minister Abiy Ahmed's Prosperity Party, Ethiopia's media apparatus is used as a sophisticated tool to shape and distort public opinion in an environment marked by internal disputes, ethnic tensions, and an uncertain democratic process (Business and Human Rights Centre, 2025). According to this argument, the media system contributes to the degradation of public space by acting as a digital repression tool, a situation similar to Senegal. Official state agencies such as the Ethiopian News Agency, the Media Army, and EBC Television effectively serve as extensions of the state, spreading misinformation while being financially supported directly by the government (Ibid, 2025).

The strategy of Ethiopia, in the delegitimation of activists, consists mostly of four manipulation tactics: harassment, information blackouts, narrative dilution, and individual defamation (Molla, 2022). This once again results in the labelling of activists occupying public spaces as separatists, terrorists, or foreign agents.

State propaganda also creates false realities rather than just censoring. Notably, ENA broadcasts propagated and exaggerated claimed successes that were never confirmed during the Tigray War in Amhara (Molla, 2022). On the other hand, the Media Army connected opponents like US diplomats to the Tigray People's Liberation Front utilising bots and troll farms (Ibid, 2022). This episode strongly discouraged worldwide examination of the crimes committed during that period (Usmani, 2025). Furthermore, after Abiy took power in 2018, during the height of the COVID-19 pandemic, the enactment of the Hate Speech Proclamation Law criminalised independent fact-checking, allowing the Ethiopian Media Authority to punish or shut down outlets that were not under state control (Business and Human Rights Centre, 2025). Therefore, it is not at all unexpected that civic space in Ethiopia is practically destroyed and manipulated rather than merely limited.

The human toll of this crushing machine is evident: over 200 journalists have been detained since 2019 (HRW, 2024). Online dehumanisation efforts have preceded ethnic conflict, and human rights advocates have been driven into exile (Ibid, 2024). In front of the upcoming elections, for which many global nations have reported unfair conditions (HRW, 2026), this digital authoritarianism undermines promises of liberalisation and transforms platforms into instruments of authority.

3. IMPACT ON HUMAN RIGHTS

The weaponisation of digital infrastructure extends far beyond economic and humanitarian concerns and represents a targeted, structured assault on the core principles of fundamental

human rights. Across the Middle East and Africa, governments are actively trying to create a hostile environment for human rights defenders and systematically exclude civil society from any meaningful role in digital governance.

The integration of blunt network shutdowns with heavily punitive digital laws increases psychological fear and establishes a profound chilling effect across digital platforms. For example, in Iraq, the state has actively fostered a climate of self-censorship through vague cybercrime legislation and moral policing. In January 2023, the Ministry of Interior launched the “Balgh” platform to encourage citizens to report “indecent” or “immoral” social media content (Amnesty International, 2023). Within just a month, the platform received over 96,000 complaints, leading to swift prison sentences for content creators under Article 403 of the Penal Code (Article 19, 2025). Combined with sweeping cybercrime legislation proposals, this mechanism has created an atmosphere of terror and forced independent journalists, civil society activists, and ordinary internet users to self-censor online to avoid prosecution. The Islamic Republic of Iran also employs structural isolation to enforce silence. The February 2024 ban on unlicensed VPN by the Supreme Council for Cyberspace was designed to coerce users onto monitored, state-operated domestic platforms, and severely restrict any remaining safe avenues for free expression (Freedom House, 2024).

Targeted repression of human rights defenders is another issue in the Middle East and Africa. In Ethiopia, the government escalated its crackdown on civil society organisations in recent years. Reportedly, arbitrary arrests and detention are widely used to suppress and target defenders in Ethiopia (The Observatory for the Protection of Human Rights Defenders, 2025). It is very common to arrest and detain defenders without legal grounds or arrest warrants, and such arrests are very often carried out by masked individuals, who also fail to inform the detainees of the reasons for their arrest (The Observatory for the Protection of Human Rights Defenders, 2025).

Journalists are typically the primary targets due to the visibility of their work. According to the Ethiopian Press Freedom Defenders (EPFD), between 2019 and 2024, there were 244 arrests involving 201 journalists and media workers (African Arguments, 2024). Human rights defenders in Ethiopia also face violence and harassment due to their work, furthermore, torture, ill-treatment, and enforced disappearance are serious forms of human rights abuse that rights defenders have continued to face in Ethiopia (The Observatory for the Protection of Human Rights Defenders, 2025).

Targeting the human rights defenders is also very common in Senegal. Recently, in March 2026, the Senegalese National Assembly adopted a new law to increase the prison sentences provided in the Criminal Code for “unnatural acts” from five to ten years (FIDH, 2026). Reportedly, this law also poses a huge threat to the freedom of expression and association, as well as to human rights defenders, civil society organisations, journalists, and lawyers working to protect fundamental human rights (FIDH, 2026).

Authoritarian regimes not only target and harass civil society organisations and human rights defenders, but they also deliberately exclude civil society from the mechanisms of digital policy-making to permanently consolidate state control over the civic space. In March 2026,

Senegal's National Assembly adopted another law establishing the National Media Regulatory Council (CNRM), which is a response to the rapid expansion of digital platforms, social media, and emerging challenges, such as disinformation and AI (ICNL, 2026). However, Senegalese media organisations were excluded from the process of drafting the law (ICNL, 2026).

The above-discussed examples show that regardless of whether a state operates as a theocratic autocracy, a recovering transitional democracy, or a nation embroiled in deep civil conflict, the underlying impulse to sever digital connectivity comes from a shared, desperate desire to exert absolute control over the information ecosystem, suppress civilian dissent, and evade domestic or international accountability. The effects of this digital repression are universally destructive and compounding, especially when it comes to human rights.

4. INTERNATIONAL LEGAL FRAMEWORK & GAPS

While the international legal framework gives significant protections against digital repression (European Parliament, 2021), current legislation was mostly designed before spyware, algorithmic monitoring, coordinated influence operations, and global digital harassment were widespread state control techniques (Anstis & Barnett, 2022). The most important principles include the rights to privacy, expression, association, and effective recourse under instruments like the ICCPR, as well as regional human rights laws. In principle, these regulations should safeguard journalists, activists, and civil society organisations against arbitrary surveillance and online coercion. However, in reality, there are frequent gaps between international jurisdiction, domestic regulation, and enforcement capabilities when it comes to digital repression (Anstis & Barnett, 2022).

4.1 Gaps in the Implementation

4.1.2 Technology running faster than Law

The first disparity is that technology is advancing more quickly than legislation. Spyware, platform manipulation, AI-assisted profiling, metadata gathering, and cross-border hacking are examples of today's digital repression, yet international legal frameworks still mostly rely on outdated concepts of territorial injury and visible coercion (Antstis, 2025). This leads to a mismatch: the state may use phone exploits or internet intimidation to target someone overseas, but the law may find it difficult to categorise the behaviour, assign blame, or initiate a reaction (European Parliament, 2021). As a result, legal protection is frequently reactive rather than proactive, arriving only after the harm has already restricted speech or disrupted organisation.

A related issue is the absence of defined regulations governing extraterritorial digital surveillance. States employ hacking, surveillance, intimidation, and harassment against

activists from the diaspora as examined throughout the report, and exiles who reside abroad as part of transnational repression (Antstis, 2025).

The question of whether such behaviour qualifies as a treaty violation has not been fully settled by international human rights law, particularly when the victim is not in the territory of the state committing the violation (Anstis & Barnett, 2022). This uncertainty aids abusive regimes since it allows them to claim that cross-border digital repression falls outside of normal jurisdictional boundaries.

4.1.2 Lack of Accountability

Accountability represents the second significant gap when referring to a framework that protects rights in this context. It is indeed frequently challenging to determine who authorised or carried out abuses, even when they are documented. This is particularly true when spyware, anonymous online networks, or multi-layered state-private collaborations are involved (Deibert, 2015). Due to the high burden of proof placed on victims, the denial of accountability by states, and the slow or missing availability of remedies, there is a significant enforcement deficit (Ibid, 2015). According to a CyberPeace Institute report, there is still little accountability for illicit spyware surveillance due to the lack of efficient investigations, clear procurement regulations, and enforceable remedies (Jordan, 2021). In short, while the law theoretically prohibits abuses, the system frequently lacks the institutions required to make those prohibitions relevant and valuable.

This disparity is exacerbated when authoritarian repressive states employ the law as a tool of control. Unclear cybercrime laws in fact, are increasingly being used to criminalise dissent, and that poorly crafted international cybercrime frameworks might unintentionally legitimise limitations on free expression and privacy (Recanati & Kerley, 2024). Repressive countries can use international acceptance of wide legal terminology as justification for their internal crackdowns. This is why the issue is not simply a lack when applying the law, but also the poor legislation at the international level.

Another structural problem to take into consideration is that international law frequently presumes that harms are observable, attributable, and individually identifiable. In reality, digital repression differs in many ways. It can be distributed across state agencies or within other external actors, making it hard to identify the exact responsible.

Furthermore, digital repression frequently has a chilling impact before any formal arrest or prosecution occurs, indicating that the harm is genuine even when it is impossible to prove. This is especially important for activists, because the threat of surveillance can silence speech and prevent mobilisation. The crucial part in this, is to understand that victims of this phenomenon, most of the time, lack proper access to solutions for their case.

Indeed, as of April 2026, in a press release of April 27th, the OHCHR has stressed that accountability mechanisms must be both effective and readily accessible, and that fundamental freedoms should be protected from systematic digital interference, mainly because rights remain largely declaratory rather than enforceable without such measures in

place (OHCHR, 2026). Consequently, the accountability gap is not merely a procedural concern, but a significant driver of the continuous erosion of civic space.

CONCLUSION

Across the Middle East and Africa, digital repression has become a defining feature of the shrinking civic space. Governments increasingly rely on digital technologies to limit and control the free flow of information. As such, the digital realm is no longer a public utility, but rather the primary battleground for suppressing dissent, concealing human rights abuses, and establishing fake narratives. This report has analysed four main strategies that governments across the region utilise to suppress dissent and exclude contradicting information to the regime.

First, the increasing reliance on digital surveillance technologies to monitor and target journalists and human rights defenders is deeply embedded within the political and social landscape of the region. The use of Pegasus spyware in countries such as Rwanda, Morocco, Saudi Arabia and the UAE demonstrates how intrusive technologies are being deployed. Similarly, biometric technologies, including facial recognition and digital identifying systems, enable the profiling and monitoring of particular people in order to reinforce state control.

Second, governments have developed legal and regulatory frameworks that legitimise repression while maintaining the formal appearance of legality. Anti-cybercrime laws and NGO regulations have systematically allowed states like Egypt, Saudi Arabia, Jordan, Uganda, and Nigeria, to diminish dissent. Characterised by vague and broad language, it manipulates online expressions to be reclassified as terrorism offences or threats to national security. Consequently, the law turns into a tool of control rather than a mechanism of protection.

Third, the weaponisation of internet access has been used as outright state violence, but also an administrative tool. Internet shutdowns and connective restrictions have been used widely in Iran, Iraq, Ethiopia, and Senegal. This section also makes clear that civic repression is not only a feature within autocratic or authoritarian regimes, but can also happen in traditionally strong democratic states such as Senegal. Lastly, disinformation campaigns have been used to delegitimise activists in Iran, Saudi Arabia, Sudan, and Ethiopia. The establishment of false narratives by the government not only conceals abuses, but also portrays human rights defenders as threats.

The direct targeting of civil society organisations and human rights defenders is a pattern that cuts across different political systems. The underlying desire of absolute control has made the restriction of the information ecosystem attractable. In combination with the weak

implementation and lack of defined terms and regulations, governments in these regions are successfully evading accountability. Thus, addressing civic repression in the Middle East and Africa requires coordinated efforts between the state, international community, and technology companies.

To states, governments should ensure that all digital governance measures comply with international human rights standards. Surveillance should be limited to legitimate causes, subject to necessity and proportionality calculations. Other digital suppression techniques should also be amended to end arbitrary restrictions. Governments should ensure independent judicial oversight to guarantee free participation of civil society. Governments should also modify their legislative frameworks and prosecution strategies.

To the international community, stronger accountability mechanisms must be established. International organisations should document cases of digital repression and support local civil society actors. By applying diplomatic pressure when necessary, the protection against the misuse of technology can be strengthened. Also, the international community should condemn the targeting of exiled activists and its diaspora communities. The international community must increase pressure on governments in the Middle East and Africa to comply with international standards.

To technology companies, transparency and due diligence standards must be included when developing new technologies. Companies should assess the human rights risk before providing technologies in repressive environments. Social media platforms should also strengthen their protection for journalists and human rights activists to limit government online harassment.

Ultimately, the expansion of digital repression in the Middle East and Africa reflect the broader struggle over power and accountability. Without stronger legal safeguards and cooperation from all stakeholders, the continued erosion of civic space will have long term impacts for democratic participation and threaten individual rights and freedoms.

- Abu Yahia A and Heldt V, 'Jordan's New Cybercrime Law Passes Despite Freedom Concerns' (The Tahrir Institute For Middle East Policy, 19 October 2023) <https://timep.org/2023/10/19/jordans-new-cybercrime-law-passes-despite-freedom-concerns/> accessed 19 April 2026
- Access Now, 'Authorities in Ethiopia Must Restore Internet Access in Amhara' (12 September 2023) <https://www.accessnow.org/press-release/amhara-internet-shutdown/> accessed 20 April 2026
- Access Now, 'Lives on Hold: Internet Shut-Downs in 2024' (23 February 2025) <https://www.accessnow.org/internet-shutdowns-2024/> accessed 20 April 2026
- Access Now, 'Blocking Millions in MENA: Internet Shutdowns in 2025' (31 March 2026) <https://www.accessnow.org/press-release/blocking-millions-in-mena-internet-shutdowns-in-2025/> accessed 20 April 2026
- Access Now, '#NoExamShutdowns: Lessons from the New Academic Year' (18 September 2025) <https://www.accessnow.org/no-exam-shutdown-new-academic-year/> accessed 20 April 2026
- African Arguments, 'In Abyi's Ethiopia, 200 Journalists Have Been Arrested Since 2019' (3 June 2024) <https://africanarguments.org/2024/06/in-abiyis-ethiopia-200-journalists-have-been-arrested-since-2019/> accessed 22 April 2026
- Agbo E, 'Nigeria: Serap, Editors Decry Widespread Use of Cybercrime Act to Harass Journalists, Activist' (AllAfrica, 11 December 2025) <https://allafrica.com/stories/202512110289.html> accessed 19 April 2026
- Agbo A, 'Twice Upon An Obnoxious NGO Bill' (The Whistler, 2025) <https://thewhistler.ng/twice-upon-obnoxious-ngo-bill/> accessed 23 April 2026
- Akua N, 'How Anti-Cybercrime Laws Are Being Weaponized to Repress Journalism' (Columbia Journalism Review, 2025) <https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php> accessed 20 April 2026
- American Foreign Policy Council (AFPC), 'Iran's Digital Fortress: The Rise of the National Information Network' (August 2025)
- Americans for Democracy & Human Rights in Bahrain (ADHRB), 'ACPRA and Restrictions on Human Rights Organizations in Saudi Arabia' (2016) <https://www.adhrb.org/2016/07/10337/> accessed 19 April 2026

- Americans for Democracy & Human Rights in Bahrain (ADHRB), 'Biometric Surveillance and Personal Data Protection in the Gulf: A Growing Human Rights Concern' (10 November 2025) <https://www.adhrb.org/2025/11/biometric-surveillance-and-personal-data-protection-in-the-gulf-a-growing-human-rights-concern/> accessed 23 April 2026
- Amnesty International, 'Iran: Macabre Propaganda Videos Feature Forced "Confessions" of Executed Sunni Men' (17 November 2016) <https://www.amnesty.org/en/latest/press-release/2016/11/iran-macabre-propaganda-videos-feature-forced-confessions-of-executed-sunni-men/> accessed 28 April 2026
- Amnesty International, 'Sudan: Government Stifling Media and Civil Society' (2 December 2016) <https://www.amnesty.nl/actueel/sudan-government-stifling-media-and-civil-society> accessed 28 April 2026
- Amnesty International, 'Iraqi Authorities Must Cease Chilling Crackdown on Free Speech' (3 March 2023) <https://www.amnesty.org/en/documents/mde14/6511/2023/en/> accessed 22 April 2026
- Amnesty International, 'What Happened at the Protests in Iran?' (20 January 2026) <https://www.amnesty.org/en/latest/campaigns/2026/01/what-happened-at-the-protests-in-iran/> accessed 20 April 2026
- Amnesty International, 'Egypt: Prominent Human Rights Defender Hossam Bahgat Summoned for Interrogations' (2025) <https://www.amnesty.org/en/latest/news/2025/01/egypt-prominent-human-rights-defender-hossam-bahgat-summoned-for-interrogations/> accessed 18 April 2026
- Amnesty International, 'Saudi Arabia: Upcoming Hearing for Imprisoned Women's Rights Activist' (2025) <https://amnesty.ca/urgent-actions/saudi-arabia-upcoming-hearing-for-imprisoned-womens-rights-activist/> accessed 18 April 2026
- Amnesty International, 'Saudi Woman Imprisoned for Tweeting in Support of Women's Rights Released After Four-Year Ordeal' (2025) <https://www.amnesty.org.au/saudi-woman-imprisoned-for-tweeting-in-support-of-women-s-rights-released-after-four-year-ordeal/> accessed 19 April 2026
- Amnesty International, 'Further Information: Manahel al-Otaibi Subjected to Torture in Saudi Prison' (2024) <https://www.amnesty.org/en/documents/mde23/8490/2024/en/> accessed 19 April 2026

- Amnesty International, 'Further Information: Death Sentence for Social Media Posts Commuted: Mohammad bin Nasser al-Ghamdi' (2024)
<https://www.amnesty.org/en/documents/mde23/8746/2024/en/> accessed 19 April 2026
- Amnesty International, 'Manahel Al-Otaibi Subjected to Torture in Prison' (2024)
<https://amnesty.ca/urgent-actions/saudi-arabia-manahel-al-otaibi-subjected-to-torture-in-prison/> accessed 19 April 2026
- Amnesty International, 'Jordan: New Cybercrimes Law Stifling Freedom of Expression One Year On' (2024)
<https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/> accessed 19 April 2026
- Amnesty International, 'Uganda 2024' (2024)
<https://www.amnesty.org/en/location/africa/east-africa-the-horn-and-great-lakes/uganda/report-uganda/> accessed 22 April 2026
- Amnesty International Australia, 'Emergency Update for All Apple Users: Everything You Need to Know About Pegasus Spyware' (23 September 2021)
<https://www.amnesty.org.au/everything-you-need-to-know-about-pegasus-spyware/> accessed 15 April 2026
- Amnesty International Security Lab, 'Case Study: The Pegasus Project' (2021)
<https://securitylab.amnesty.org/case-study-the-pegasus-project/> accessed 15 April 2026
- Amnesty International Security Lab, 'Intellexa Leaks: Predator Spyware Operations Exposed' (4 December 2025)
<https://securitylab.amnesty.org/latest/2025/12/intellexa-leaks-predator-spyware-operations-exposed/> accessed 21 April 2026
- Amnesty International, 'What Is Spyware and What You Can Do to Stay Protected' (12 December 2023)
<https://www.amnesty.org/en/latest/campaigns/2023/12/what-is-spyware-and-what-you-can-do-to-stay-protected/> accessed 14 April 2026
- Andersen, 'Translation of Law No. 175 of 2018' (2025)
<https://eg.andersen.com/translation-law-175-2018/> accessed 18 April 2026
- Anstis S and Barnett S, 'Digital Transnational Repression and Host States' Obligation to Protect against Human Rights Abuses' (2022) 14 *Journal of Human Rights Practice*
- Anstis S, 'Digital Transnational Repression and the Limits of International Human Rights Law in a "Post-Territorial" World' (Binding Hook, 16 September 2025)

<https://bindinghook.com/digital-transnational-repression-and-the-limits-of-international-human-rights-law-in-a-post-territorial-world/> accessed 27 April 2026

Andrew Meldrum, 'Rwanda News: Sweden Expels Rwanda Diplomat for Spying' (PRI/The World, 13 May 2017)
<https://theworld.org/stories/2017/05/13/rwanda-news-sweden-expels-rwanda-diplomat-spying> accessed 20 April 2026

Bahgat H, 'A Coup Busted?' (Mada Masr, 14 October 2015)
<<https://www.madamasr.com/en/2015/10/14/feature/politics/a-coup-busted/>> accessed 18 April 2026

Baum J and van Rooyen M, 'Offline and Silences: Africa's Quiet Rise of Internet Repression' (ISS, 2025)
<https://issafrica.org/iss-today/offline-and-silenced-africa-s-quiet-rise-of-internet-repression#:~:text=In%202024%2C%20shutdowns%20cost%20sub,speech%20or%20assembly%2C%20must%20expand..> (issafrica.org in Bing) accessed 14 April 2026

Büchi M, et al, 'The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda' (2022) DOI:10.1177/20539517211065368 accessed 13 April 2026

Burns E, 'Jordan Cybercrimes Law Breaches International Human Rights: Amnesty International' (JURISTnews, 2024)
<<https://www.jurist.org/news/2024/08/jordan-cybercrimes-law-breaches-international-human-rights-amnesty-international/>> accessed 19 April 2026

Cairo Institute for Human Rights Studies (CIHRS), 'Egypt: Legal Commentary on Regulations of NGO Law n. 149 for 2019 on Civic Associations' (2021)
<<https://cihrs.org/egypt-legal-commentary-on-regulations-of-ngo-law-n-149-for-2019-on-civic-associations/?lang=en>> accessed 18 April 2026

Carnegie Endowment for International Peace, 'Senegal: From Constitutional Crisis to Democratic Restoration' (1 April 2024)
<<https://carnegieendowment.org/research/2024/04/senegal-from-constitutional-crisis-to-democratic-restoration>> accessed 20 April 2026

CCOHS, 'Internet Harassment or Cyberbullying' (n.d.)
<<https://www.ccohs.ca/oshanswers/psychosocial/cyberbullying.html>> accessed 15 April 2026

CIVICUS, 'Rwanda: UN Rights Review Should Shed Light on Civic Space Restrictions' (20 January 2021)
<<https://www.civicus.org/index.php/media-resources/news/united-nations/geneva/4833-r>>

- wanda-un-rights-review-should-shed-light-on-civic-space-restrictions> accessed 20 April 2026
- CIVICUS, ‘The Civic Space Crisis: A Story Foretold’ (2022)
<<https://monitor.civicus.org/globalfindings/TacticsOfRepression/>> accessed 15 April 2026
- CIVICUS, ‘Overcoming Digital Repression in Senegal’ (2024)
- Committee to Protect Journalists, ‘Al-Jazeera Journalist Ghada Oueiss Hacked, Harassed in Apparent Effort to Smear Jamal Khashoggi’ (17 February 2021)
<<https://cpj.org/2021/02/ghada-oueiss-hacking-harassment-jamal-khashoggi/>> accessed 16 April 2026
- CPJ MENA Staff, ‘In Morocco, Journalists – and Their Families – Still Struggle to Cope with Spyware Fears’ (Committee to Protect Journalists, 13 October 2022)
<<https://cpj.org/2022/10/morocco-journalists-families-spyware-fears/>> accessed 21 April 2026
- CPJ Middle East and North Africa Program, ‘Morocco’s New Tactic to Punish Journalists: Charge Them with Sex Crimes’ (Committee to Protect Journalists, 18 March 2021)
<<https://cpj.org/2021/03/moroccos-new-tactic-punish-journalists-charge-sex-crimes/>> accessed 23 April 2026
- Cornelius I, ‘Censorship, Freedom of Speech and Freedom of Expression’ in *Information Policies and Strategies* (Cambridge University Press, 2018)
<<https://www.cambridge.org/core/books/abs/information-policies-and-strategies/censorship-freedom-of-speech-and-freedom-of-expression/A2295BA837EBEDFDAE7B8277E68E58E6>> accessed 14 April 2026
- Deibert R, ‘Cyberspace under Siege’ (2015) 26 *Journal of Democracy* 64
- Deibert R, ‘Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile’ (Knight First Amendment Institute, 2015)
<<https://knightcolumbia.org/content/silenced-by-surveillance-the-impacts-of-digital-transnational-repression>>
- Democratic Erosion Consortium, ‘Saudi Government Social Media Manipulation’ (20 May 2021)
<<https://democratic-erosion.org/2021/05/20/saudi-government-social-media-manipulation/>>

- Dentons, 'Cybercrime Law in Jordan' (2023)
<https://www.dentons.com/en/insights/alerts/2023/october/16/cybercrime-law-in-jordan>
 accessed 19 April 2026
- Dig Watch, 'Anti-Cyber Crime Law | Saudi Arabia' (2007)
<https://dig.watch/resource/anti-cyber-crime-law-saudi-arabia> accessed 18 April 2026
- EIGE, 'Online Violence is Real Violence: A Call for Safe Spaces' (2025)
<https://issafrica.org/iss-today/offline-and-silenced-africa-s-quiet-rise-of-internet-repression#:~:text=In%202024%2C%20shutdowns%20cost%20sub,speech%20or%20assembly%2C%20must%20expand..> (issafrica.org in Bing) accessed 15 April 2026
- Egyptian Initiative for Personal Rights (EIPR), 'Five Years of Arbitrary Travel Bans and Asset Freezes against Three EIPR Directors' (2025)
<https://eipr.org/en/press/2025/11/five-years-arbitrary-travel-bans-and-asset-freezes-against-three-eipr-directors> accessed 18 April 2026
- Electronic Frontier Foundation (EFF), 'Digital Hopes, Real Power: The Rise of Network Shutdowns' (15 April 2026)
<https://www.eff.org/deeplinks/2026/04/digital-hopes-real-power-rise-network-shutdowns> accessed 20 April 2026
- Emmason J, 'Nigeria's Closing Civic Space and the Non-Profit Governance Code 2023' (Leadership, 2024)
<https://leadership.ng/nigerias-closing-civic-space-and-the-non-profit-governance-code-2023/> accessed 23 April 2026
- European Parliament, 'Digital Technologies as a Means of Repression and Social Control' (2021) PE653636, Subcommittee on Human Rights
- Eva Thiébaud, 'UAE's High-Tech Toolkit for Mass Surveillance and Repression' (*Le Monde diplomatique*, January 2023) <https://mondediplo.com/2023/01/05uae> accessed 26 April 2026
- Ewang A, 'Nigerian Journalist's Detention Threatens Press Freedom' (Human Rights Watch, 2024)
<https://www.hrw.org/news/2024/05/09/nigerian-journalists-detention-threatens-press-freedom> accessed 21 April 2026
- Feldstein S, 'Global Patterns of Digital Repression' in *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (2021)
<https://doi.org/10.1093/oso/9780190057497.003.0003> accessed 13 April 2026

- Feldstein S, 'Understanding the Incentives Driving Digital Repression' (*Global Policy*, 2023)
<<https://www.globalpolicyjournal.com/blog/06/03/2023/understanding-incentives-driving-digital-repression>> accessed 10 April 2026
- FIDH, 'The Discriminatory Law against LGBTIQ+ People Must Not Be Enacted' (17 March 2026)
<<https://www.fidh.org/en/region/Africa/senegal/senegal-the-discriminatory-law-against-lgbtq-people-must-not-be>> accessed 22 April 2026
- FRA, 'Civic Space' (n.d.) <<https://fra.europa.eu/en/cooperation/civil-society/civil-society-space>> accessed 10 April 2026
- Freedom House, 'Freedom on the Net 2022: Saudi Arabia' (2022)
<https://freedomhouse.org/country/saudi-arabia/freedom-net/2022#footnote3_J6mprGkM0Io4RM-dq1AUjpfUe-S7G1FLLrxsTzULVY_r6Exx5A1eAhv> accessed 24 April 2026
- Freedom House, 'Freedom on the Net 2023: Iran' (2023)
<<https://freedomhouse.org/country/iran/freedom-net/2023>> accessed 20 April 2026
- Freedom House, 'Freedom on the Net 2024: Iraq' (2024)
<<https://freedomhouse.org/country/iraq/freedom-net/2024>> accessed 20 April 2026
- Glowacka D et al, 'Digital Technologies as a Means of Repression and Social Control' (European Parliament's Subcommittee on Human Rights, 2021)
<[https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU\(2021\)653636](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653636)> accessed 10 April 2026
- Guess A and Lyons B, 'Misinformation, Disinformation, and Online Propaganda' in *Social Media and Democracy* (2021) DOI:10.1017/9781108890960 accessed 14 April 2026
- Gyang H, 'Nigeria's Cybercrime Reform' (2025)
<<https://naltf.gov.ng/nigerias-cybercrime-reform/>> accessed 21 April 2026
- Hamid Khalafallah, 'Beyond the Battlefield: Sudan's Virtual Propaganda Warzone' (The Tahrir Institute for Middle East Policy, 14 January 2025)
<<https://timep.org/2025/01/14/beyond-the-battlefield-sudans-virtual-propaganda-warzone/>>
- Hassaniyan A, 'How Longstanding Iranian Disinformation Tactics Target Protests' (The Washington Institute, 1 November 2022)
<<https://www.washingtoninstitute.org/policy-analysis/how-longstanding-iranian-disinformation-tactics-target-protests>>
- Hossaini R, 'HRW Condemns Charges against Prominent Egyptian Rights Defender' (*JURISTnews*, 2025)

<<https://www.jurist.org/news/2025/01/hrw-condemns-charges-against-prominent-egyptian-rights-defender/>> accessed 18 April 2026

Human Rights Watch, 'Saudi Arabia: New Counterterrorism Law Enables Abuse' (23 November 2017)

<<https://www.hrw.org/news/2017/11/23/saudi-arabia-new-counterterrorism-law-enables-abuse>> accessed 18 April 2026

Human Rights Watch, 'Egypt: New NGO Law Renews Draconian Restrictions' (24 July 2019)

<<https://www.hrw.org/news/2019/07/24/egypt-new-ngo-law-renews-draconian-restrictions>> accessed 18 April 2026

Human Rights Watch, 'Egypt: Restrictions on Civic Work Underscored Implementing Regulations Stifle Independent Work' (16 April 2021)

<<https://www.hrw.org/news/2021/04/16/egypt-restrictions-civic-work-underscored>> accessed 18 April 2026

Human Rights Watch, 'Egypt Should Withdraw NGO Registration Deadline' (15 July 2021)

<<https://www.hrw.org/news/2021/07/15/qa-legal-framework-and-environment-nongovernmental-groups-ngos-egypt>> accessed 18 April 2026

Human Rights Watch, 'Q&A: Legal Framework and Environment for Nongovernmental Groups (NGOs) in Egypt' (24 March 2023)

<<https://www.hrw.org/news/2023/03/24/egypt-should-withdraw-ngo-registration-deadline>> accessed 18 April 2026

Human Rights Watch, 'Uganda: Ensure Justice for Detained, Tortured Author' (11 February 2022)

<<https://www.hrw.org/news/2022/02/11/uganda-ensure-justice-detained-tortured-author>> accessed 20 April 2026

Human Rights Watch, 'Uganda: Court Upholds Anti-Homosexuality Act' (4 April 2024)

<<https://www.hrw.org/news/2024/04/04/uganda-court-upholds-anti-homosexuality-act>> accessed 20 April 2026

Human Rights Watch, 'Iran's Internet Blackout Concealing Atrocities' (12 January 2026)

<<https://www.hrw.org/news/2026/01/12/irans-internet-blackout-concealing-atrocities>> accessed 20 April 2026

Human Rights Watch, 'Saudi Arabia Events of 2025' (n.d.)

<<https://www.hrw.org/world-report/2026/country-chapters/saudi-arabia>> accessed 18 April 2026

- Human Rights Watch, 'Jordan Events of 2025' (n.d.)
<<https://www.hrw.org/world-report/2026/country-chapters/jordan>> accessed 18 April 2026
- Human Rights Watch, 'Saudi Arabia: UK Court Accepts Case About Saudi Spyware Use' (22 October 2024)
<https://www.hrw.org/news/2024/10/22/saudi-arabia-uk-court-accepts-case-about-saudi-spyware-use#:~:text=%E2%80%9CThe%20Saudi%20government%20has%20been,times%20between%202018%20and%202020.> (hrw.org in Bing) accessed 23 April 2026
- Human Rights Watch, 'UAE: Ahmed Mansoor's 15-Year Sentence Upheld' (7 March 2025)
<<https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoors-15-year-sentence-upheld>> accessed 26 April 2026
- Human Rights Watch, 'World Report 2026: Morocco and Western Sahara (Events of 2025)' (2026)
<<https://www.hrw.org/world-report/2026/country-chapters/morocco-and-western-sahara>> accessed 23 April 2026
- HRW, 'Ethiopia: Halt Crackdown against Human Rights Groups' (18 June 2024)
<<https://www.hrw.org/news/2024/06/18/ethiopia-halt-crackdown-against-human-rights-groups>>
- HRW, 'EU's Relations with Ethiopia Ignore Grim Human Rights Reality' (22 April 2026)
<<https://www.hrw.org/news/2026/04/22/eus-relations-with-ethiopia-ignore-grim-human-rights-reality>> accessed 28 April 2026
- Ibrahim I, 'How Disinformation Campaigns Endanger Lives in Sudan' (*SMEX*, 19 May 2023)
<<https://smex.org/how-disinformation-campaigns-endanger-lives-in-sudan/>>
- Idris A and Guest P, 'How Twitter Rolled Over to Get Unblocked in Nigeria' (*Rest of World*, 2022)
<<https://restofworld.org/2022/how-twitter-rolled-over-to-get-unblocked-in-nigeria/>> accessed 24 April 2026
- Institute for Security Studies (ISS Africa), 'Offline and Silenced: Africa's Quiet Rise of Internet Repression' (19 December 2025)
<<https://issafrica.org/iss-today/offline-and-silenced-africa-s-quiet-rise-of-internet-repression>> accessed 20 April 2026
- Internet Society, 'Policy Brief: Internet Shutdowns' (28 October 2025)
<<https://www.internetsociety.org/resources/policybriefs/2025/internet-shutdowns/>> accessed 20 April 2026

- International Center for Not-for-Profit Law (ICNL), 'Civic Freedom Monitor: Saudi Arabia' (2019) <<https://www.icnl.org/resources/civic-freedom-monitor/saudi-arabia>> accessed 18 April 2026
- International Center for Not-for-Profit Law (ICNL), 'Civic Freedom Monitor: Jordan' (2025) <<https://www.icnl.org/resources/civic-freedom-monitor/jordan>> accessed 19 April 2026
- International Center for Not-for-Profit Law (ICNL), 'Egypt Civic Freedom Monitor' (2026a) <<https://www.icnl.org/resources/civic-freedom-monitor/egypt>> accessed 18 April 2026
- International Center for Not-for-Profit Law (ICNL), 'Uganda Civic Freedom Monitor' (2026b) <<https://www.icnl.org/resources/civic-freedom-monitor/uganda>> accessed 20 April 2026
- International Center for Not-for-Profit Law (ICNL), 'Civic Freedom Monitor: Rwanda' <<https://www.icnl.org/resources/civic-freedom-monitor/rwanda>> accessed 20 April 2026
- International Center for Not-for-Profit Law (ICNL), 'Civic Freedom Monitor: Senegal' (4 April 2026) <<https://www.icnl.org/resources/civic-freedom-monitor/senegal>> accessed 22 April 2026
- Jordan K, 'Accountability for Illegal Surveillance by Spyware | Cyberpeace Institute' (*CyberPeace Institute* 25 August 2021) <<https://cyberpeaceinstitute.org/news/accountability-for-illegal-surveillance-by-spyware/>> accessed 27 April 2026
- Karine Pfenniger, 'Espionage, Threats, Suspicious Deaths: Rwanda Tries to Silence Its Opponents Abroad' (Forbidden Stories, 28 May 2024; modified 3 June 2024) <<https://forbiddenstories.org/espionage-threats-suspicious-deaths-rwanda-tries-to-silence-its-opponents-abroad/#:~:text=TIME%20%20min.-,Espionage%2C%20threats%2C%20suspicious%20deaths:%20Rwanda%20tries%20to%20silence%20its,troubling%20disappearances%20of%20exiled%20Rwandans.&text=Our%20research%20suggests%20that%20Rwanda,to%20the%20NGO%20Freedom%20House>> accessed 20 April 2026
- Kigongo, J. and Wesaka, A. (2023). Offensive speech law fails court test. Monitor. Retrieved April 20, 2026
<https://www.monitor.co.ug/uganda/news/national/offensive-speech-law-fails-court-test-4082840>.
- Laws on Countering Terrorism Worldwide, 'Saudi Arabia' (n.d.) <<https://counterterrorlaw.info/country/saudi-arabia>> accessed 18 April 2026
- Library of Congress (LOC), 'Uganda: Computer Misuse (Amendment) Act Enacted' (2023) <<https://www.loc.gov/item/global-legal-monitor/2023-01-05/uganda-computer-misuse-amendment-act-enacted/?locId=ealln>> accessed 20 April 2026

- London School of Economics (LSE), 'Ethiopia's Digital Blackouts Are an Attempt to Turn Off Accountability' (19 January 2026)
<<https://blogs.lse.ac.uk/africaatlse/2026/01/19/ethiopias-digital-blackouts-are-an-attempt-to-turn-off-accountability/>> accessed 20 April 2026
- Lynch J, 'Iron Net: Digital Repression in the Middle East and North Africa' (*European Council on Foreign Relations*, 29 June 2022)
<<https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/>>
- Lynch M, 'Digital Activism and Authoritarian Adaptation in the Middle East' (*Project on Middle East Political Science*, 4 August 2021)
<<https://pomeps.org/digital-activism-and-authoritarian-adaptation-in-the-middle-east>>
- Mancini G, *Surveillance Technologies in Egypt and Saudi Arabia: From Domestic Control to Geopolitical Leverage* (Thesis, 2025)
- Marc Owen Jones, *Digital Authoritarianism in the Middle East* (Oxford University Press, 2022)
- Malik O, 'An Overview of Uganda's Computer Misuse Amendment Act 2022' (*Securiti*, 2022)
<<https://securiti.ai/blog/uganda-computer-misuse-amendment-bill-2022/>> accessed 20 April 2026
- Matt Fox, 'Irish-Linked Spyware Used in Brazen Attacks – Report' (*BBC News NI*, 21 October 2023) <<https://www.bbc.com/news/articles/c0wxr9rnnxeo>> accessed 21 April 2026
- Michael Oduor with OCCRP, 'Report: Rwanda Used Israeli Spy Tech to Tap Phones of Top Ugandan Officials' (*Africanews*, 13 August 2024)
<<https://www.africanews.com/2021/07/22/report-rwanda-used-israeli-spy-tech-to-tap-phones-of-top-ugandan-official/>> accessed 16 April 2026
- Mednick S, 'Senegal's Government Suspends Mobile Internet Access amid Days of Deadly Clashes' (*AP News* 4 June 2023)
<<https://apnews.com/article/senegal-clashes-opposition-phone-network-cut-b7091604fbe0944f9cffa2df71363639>> accessed 14 May 2026
- MfWA, 'Nigeria: Gagging of Dissenting Voices on Social Media Continue Unabated' (2024)
<<https://mfwa.org/country-highlights/nigeria-gagging-of-dissenting-voices-on-social-media-continue-unabated/>> accessed 20 April 2026
- Molla MG Saba Mah'derom and Kisanet Haile, 'Four Ways the Ethiopian Government Manipulates the Media' (*African Arguments*, 1 February 2022)
<<https://africanarguments.org/2022/02/four-ways-the-ethiopian-government-manipulates-the-media/>>

- Monitor, 'HRW Urges Uganda to Investigate Kakwenza's Torture Claims' (2022)
<https://www.monitor.co.ug/uganda/news/national/hrw-urges-uganda-to-investigate-kakwenza-s-torture-claims--3713528> accessed 20 April 2026
- Mujally H and Bälz K, 'The New Egyptian Anti-Cybercrime Law Regulates Legal Responsibility for Web Pages and Their Content' (*Mondaq*, 2018)
<https://www.mondaq.com/security/820028/the-new-egyptian-anti-cybercrime-law-regulates-legal-responsibility-for-web-pages-and-their-content> accessed 18 April 2026
- Naija Cyber Lawyer, 'When "Clout" Becomes a Crime: What Blessing CEO and Trevor Jacob Have in Common' (2026) <https://naijacyberlawyer.blogspot.com/?m=0-> accessed 23 April 2026
- Nanfuka J, 'A Section of Uganda's Computer Misuse Act Outlawed! But, the Greater Part of the Law Remains Thorny' (*CIPESA*, 2023)
<https://cipesa.org/2023/01/a-section-of-ugandas-computer-misuse-act-outlawed-but-the-greater-part-of-the-law-remains-thorny/> accessed 20 April 2026
- Narsee A and Willamo K, 'Civic Space Report 2025' (*European Civic Forum*, 2025)
<https://civic-forum.eu/civicspace25#:~:text=Civic%20Space%20Report%202025%20%E2%80%93%20Out,Read%20the%20full%20report!> accessed 10 April 2026
- Nathaniel Allen and Matthew La Lime, 'How Digital Espionage Tools Exacerbate Authoritarianism Across Africa' (*Brookings Institution*, 19 November 2021)
<https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/#:~:text=That%20African%20leaders%20are%20both,for%20purposes%20of%20international%20espionage.> (brookings.edu in Bing) accessed 14 April 2026
- OECD, *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance* (2022)
https://www.oecd.org/content/dam/oecd/en/publications/support-materials/2022/12/the-protection-and-promotion-of-civic-space_c8a8caac/Civic%20Space%20Highlights-4a_ENG_final.pdf accessed 10 April 2026
- Office of the United Nations High Commissioner for Human Rights (OHCHR), *Trends in Digital Rights Across the Middle East and North Africa: Expansion of Digital Surveillance and Impacts on Journalists and Human Rights Defenders* (OHCHR, 2024)
- OHCHR, 'UN Experts: Safeguard Human Freedoms from Systematic Digital Interference, Surveillance and Chilling Effects on Civic Space' (2026)
<https://www.ohchr.org/en/press-releases/2026/04/un-experts-safeguard-human-freedoms-systematic-digital-interference> accessed 27 April 2026
- Okakwu E, 'Chained and Blindfolded: Nigerian Journalist Segun Olatunji Recounts His Detention' (*Committee to Protect Journalists*, 2024)

<<https://cpj.org/2024/07/chained-and-blindfolded-nigerian-journalist-segun-olatumji-recounts-his-detention/>> accessed 23 April 2026

Paradigm Initiative, ‘Senegal Country Report’ (April 2024)

Paradigm Initiative, ‘Press Release: Coalition Lauds Cybercrimes Act Amendment and Urges FG to Further Safeguard Freedom of Expression’ (2024)

<<https://paradigmhq.org/press-release-coalition-lauds-cybercrimes-act-amendment-and-urges-fg-to-further-safeguard-freedom-of-expression/>> accessed 21 April 2026

Perez-Escolar M et al, ‘A Systematic Literature Review of the Phenomenon of Disinformation and Misinformation’ (2023) 11(2) *Media and Communication*

<<https://doi.org/10.17645/mac.v11i2.6453>> accessed 14 April 2026

Public Platform for Litigation Against Authoritarianism in Africa (PPLAAF), ‘Egypt’ (2025)

<<https://www.pplaaf.org/country/egypt.html>> accessed 18 April 2026

Recanati M and Kerley B, ‘Big Question: How Are Cybercrime Laws Weaponized to Legalize Repression?’ (*National Endowment for Democracy*, 16 December 2024)

<<https://www.ned.org/big-question-how-are-cybercrime-laws-weaponized-to-legalize-repression-2/>>

Reporters Without Borders (RSF), ‘Jordanian Reporter Gets One Year in Prison under Draconian New Cybercrime Law’ (2024a)

<<https://rsf.org/en/jordanian-reporter-gets-one-year-prison-under-draconian-new-cybercrime-law-0>> accessed 18 April 2026

Reporters Without Borders (RSF), ‘Jordan’s Cybercrime Law Is a Tool for Repressing Journalists’ (2024b)

<<https://rsf.org/en/jordan-s-cybercrime-law-tool-repressing-journalists>> accessed 18 April 2026

Reporters Without Borders (RSF), ‘Nigeria: At Least Eight Journalists Prosecuted under Cybercrime Law Despite New Amendment’ (2024c)

<<https://rsf.org/en/nigeria-least-eight-journalists-prosecuted-under-cybercrime-law-despite-new-amendment>> accessed 23 April 2026

Ronald Musoke, ‘Uganda: New Report Details Surveillance and Spyware Network That Is Endangering Journalists and Human Rights Activists’ (*Business & Human Rights Resource Centre*, 11 August 2025)

<<https://www.business-humanrights.org/en/latest-news/uganda-new-report-details-surveillance-and-spyware-network-that-is-endangering-journalists-and-human-rights-activists/>> accessed 20 April 2026

Salma El Hosseiny, ‘UAE Must Open Up Civic Space and Release Human Rights Defenders Ahead of COP28’ (*International Service for Human Rights*, 1 May 2023)

<<https://ishr.ch/latest-updates/joint-statement-uae-human-rights-record-ahead-of-cop28/>>
accessed 26 April 2026

Saudi Vision 2030, ‘Saudi Vision 2030’ (Vision2030.gov.sa, 2024)
<<https://www.vision2030.gov.sa/en>>

Sesan G, ‘Shrinking Civic Space, Digital Funding, and Legitimacy in a Post-Truth Era’
(*Carnegie Endowment for International Peace*, 2025)
<<https://carnegieendowment.org/research/2025/07/shrinking-civic-space-digital-funding-and-legitimacy-in-a-post-truth-era>>

SERAP, ‘SERAP Takes Tinubu Govt, Governors to ECOWAS Court over “Misuse of Cybercrimes Act”’ (n.d.)
<<https://serap-nigeria.org/2025/01/12/serap-takes-tinubu-govt-governors-to-ecowas-court-over-misuse-of-cybercrimes-act/>> accessed 23 April 2026

Sombatpoonsiri J, ‘Intersectional Powers of Digital Repression: How Activists Are Digitally Watched, Charged, and Stigmatised in Thailand’ (2024)
<<https://ijoc.org/index.php/ijoc/article/view/21411>> accessed 14 April 2026

Stephanie Kirchgaessner, ‘Hotel Rwanda Activist’s Daughter Placed Under Pegasus Surveillance’ (*The Guardian*, 19 July 2021)
<<https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>> accessed 16 April 2026

Stephanie Kirchgaessner and Diane Taylor, ‘Nephew of Jailed “Hotel Rwanda” Dissident Hacked by NSO Spyware’ (*The Guardian*, 18 July 2022)
<<https://www.theguardian.com/world/2022/jul/18/nephew-of-jailed-hotel-rwanda-dissident-hacked-by-nso-spyware>> accessed 16 April 2026

‘Sudanese Media Ecosystem’ (*Internews*, 2025)

Tamar Kaldani and Zeev Prokopets, ‘Pegasus Spyware and Its Impacts on Human Rights’ (*Council of Europe*, June 2022)
<<https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8>> accessed 15 April 2026

Tech 4 Peace (T4P), ‘Internet Shutdown in Iraq: A Violation of Human Rights and Significant Economic Losses’ (13 May 2024)
<<https://t4p.co/blog/2024-05-13-the-cost-effectiveness-of-internet-shutdowns-in-iraq?lang=en>> accessed 20 April 2026

The Observatory for the Protection of Human Rights Defenders, *The Illusion of Progress: Ethiopia’s Human Rights Defenders Under Attack* (December 2025)

- The Tahrir Institute for Middle East Policy (TIMEP), ‘Law No. 149 of 2019 NGO Law’ (Update, 21 August 2019) <<https://timep.org/wp-content/uploads/2019/08/NGOLaw20198.21.pdf>> accessed 18 April 2026
- UN General Assembly, *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (10 December 1984)
- UN Human Rights Commission, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* (E/CN.4/1985/4, 1984) accessed 11 April 2026
- UN Human Rights Council, *Report of the UN High Commissioner for Human Rights on the Practical Recommendations for the Creation and Maintenance of a Safe and Enabling Environment for Civil Society, Based on Good Practices and Lessons Learned* (A/HRC/32/20, 2016) <<https://digitallibrary.un.org/record/841791?v=pdf>> accessed 11 April 2026
- UN Human Rights Office (OHCHR), *Report on the Role of Digital Access Providers* (30 March 2017) <<https://www.ohchr.org/en/calls-for-input/report-role-digital-access-providers>> accessed 20 April 2026
- UNDP, *Legal Frameworks for Civic Space* (2021) <<https://www.undp.org/sites/g/files/zskgke326/files/2021-12/UNDP-ICNL-Legal-Frame-work-for-Civic-Space-A-Primer-EN.pdf>> accessed 11 April 2026
- UNESCO, *Silenced Voices: Why Freedom of Expression Is Receding Worldwide* (2025) <<https://www.unesco.org/en/articles/silenced-voices-why-freedom-expression-receding-worldwide>> accessed 14 April 2026
- United Nations (UN) News, ‘UN Rights Experts Condemn Retaliatory Arrests of Activists in Egypt’ (2020) <<https://news.un.org/en/story/2020/11/1078652>> accessed 18 April 2026
- United States Mission Nigeria, ‘Preventing Misuse of the Cybercrimes Act: Protecting Free Speech and Unlocking Economic Growth’ (*U.S. Embassy and Consulate in Nigeria*, 2025) <<https://ng.usembassy.gov/preventing-misuse-of-the-cybercrimes-act-protecting-free-speech-and-unlocking-economic-growth/>> accessed 21 April 2026
- Usmani S, ‘It’s No Longer Shrinking, It’s Being Crushed: Why the Closure of Civic Space in Ethiopia Should Matter to the U.S.’ (*Amnesty International USA*, 9 May 2025) <<https://www.amnestyusa.org/blog/its-no-longer-shrinking-its-being-crushed-why-the-closure-of-civic-space-in-ethiopia-should-matter-to-the-u-s/>>
- Vicky Frost, “‘Hotel Rwanda’ Hero to Terrorist Show Trial: Paul Rusesabagina’s Daughters on the Fight for His Freedom’ (*The Guardian*, 21 December 2021) <<https://www.theguardian.com/global-development/2021/dec/21/hotel-rwanda-hero-to-ter>

rorist-show-trial-paul-rusesabaginas-daughters-on-the-fight-for-his-freedom> accessed 16 April 2026

Washington Center for Human Rights, 'Saudi Female Activist Sentenced to 11 Years for Social Media Posts and Dress Code Violation' (2024)
<<https://washingtoncentre.org/saudi-female-activist-sentenced-to-11-years-for-social-media-posts-and-dress-code-violation/>> accessed 19 April 2026