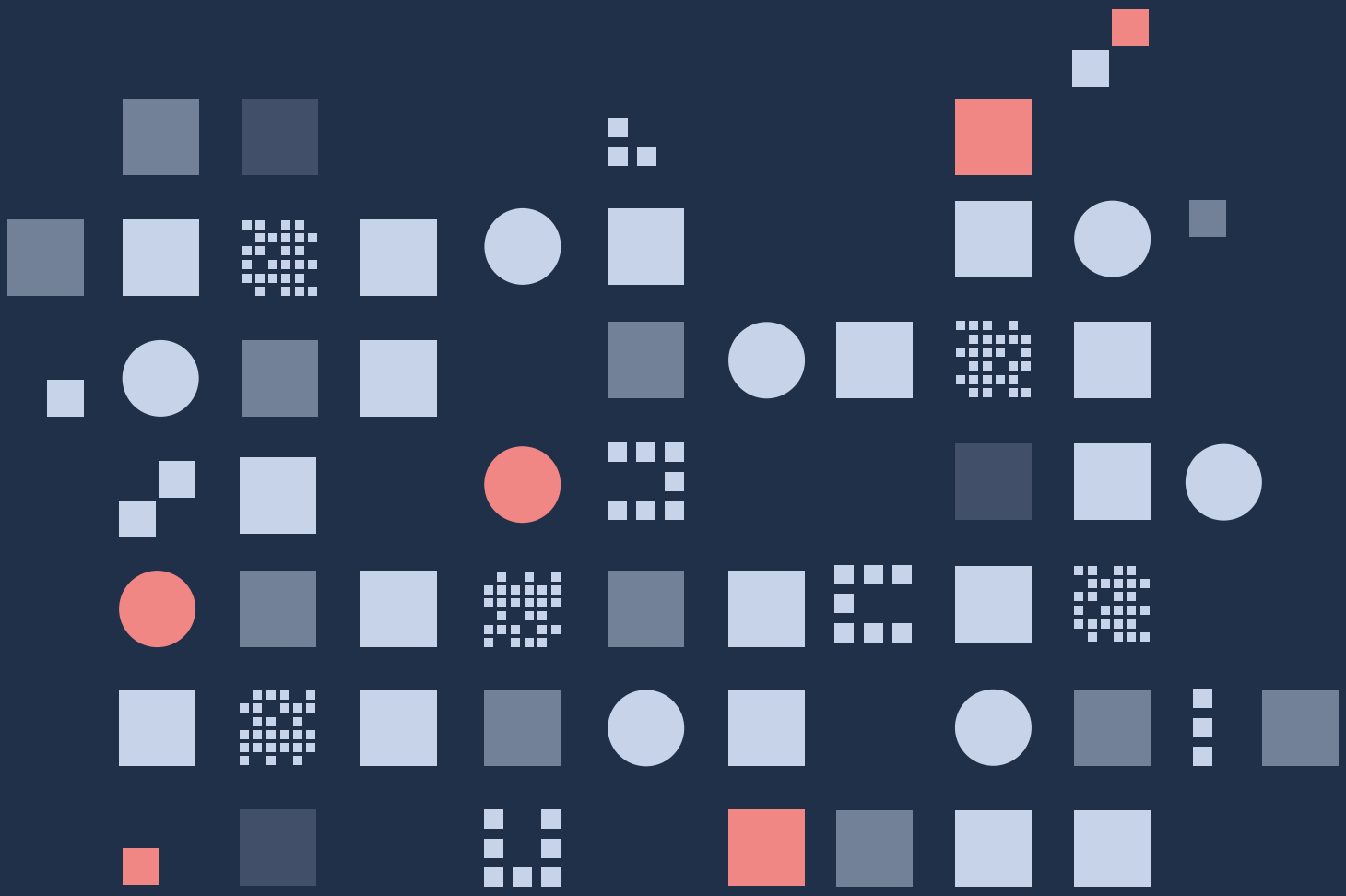
# An ever-tightening net:

## Restrictions on online expression under cybercrime laws and content restrictions in Africa, the Middle East and Türkiye



GLOBAL PARTNERS DIGITAL

July 2024

This report seeks to highlight the dangers of cybercrime legislation and online content regulations in Africa, the Middle East and Türkiye which restrict online expression in ways that violate international human rights law. It also aims to provide strategic guidance for civil society organisations and technology companies to push back against these restrictions and to advocate for more rights-respecting approaches to cybercrime and online content governance.

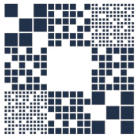
Our findings are grounded in a broad review of 155 legal frameworks which address illegal or harmful online content or activity across 69 countries in Africa, the Middle East and Türkiye. Through research and analysis based on international human rights law, we demonstrate that many of these laws include restrictions on online speech which are incompatible with international standards and guidance on permissible restrictions on freedom of expression. The report also includes seven in-depth case studies, produced with insight from local experts, which illustrate the ways in which these cybercrime laws and content regulations are being used to crush dissent and crack down on human rights defenders, political dissidents, journalists, LGBTQ+ individuals and other marginalised groups seeking to express themselves online. We provide concrete recommendations for technology companies and CSOs seeking to defend human rights and online civic space in these repressive environments, and outline the essential components of cybercrime and content regulations that respect and promote human rights.

## ACKNOWLEDGEMENTS

This report was authored by Jacqueline Rowe on behalf of Global Partners Digital, with input from Maria Paz Canales (Head of Legal, Policy and Research, Global Partners Digital) and, Ian Barber (Legal Lead, Global Partners Digital).

The report was also strengthened by some case studies, feedback and insights from ARTICLE 19 regional offices in West Africa, East Africa, Tunisia and MENA; Dr Ernest Yaw Ako Esq., Barrister and Solicitor of the Supreme Court of Ghana and Lecturer, Faculty of Law, University of Cape Coast, Ghana; John Frinjuah; Mohammad Shamma, the Country Representative for DIGNITY (Danish Institute Against Torture) Jordan Office; and Sawsan, Zaideh, media researcher and independent journalist.

The development of this report was made possible with support from Meta's Africa, the Middle East and Türkiye Public Policy team. Global Partners Digital had full editorial independence on the content of the report.



GLOBAL PARTNERS DIGITAL

# Contents

# 1. EXECUTIVE SUMMARY

The internet and digital technologies bring countless advantages but also pose novel dangers that governments worldwide are racing to address through new legislation. Many legal frameworks which seek to address illegal online content are genuinely aimed at protecting individuals from harm. However, authoritarian governments are using concern about "harmful" online content as a pretext for restricting legitimate expression and targeting marginalised groups. By criminalising a wide range of poorly-defined types of online speech, such as "immoral content", "insults to the state" or advocacy of government-labelled "terrorism" which does not meet international criteria for terrorist activity, these governments are tightening their control over what individuals can and cannot say on the internet – which, in many cases, is the last avenue for protest and advocacy left open to those living under repressive regimes.

While this is a global issue, this report focuses specifically on cybercrime laws and content restrictions implemented by governments in Africa, the Middle East and Türkiye, where cybercrime and online content restrictions have proliferated in recent years. Most of these governments are party to international and regional human rights treaties which enshrine the right to freedom of expression, which cannot be restricted except under narrow circumstances in pursuit of a specific and legitimate aim. More than a quarter of the 69 countries in the region of focus are also signatories or members to the Council of Europe's Cybercrime Treaty ("The Budapest Convention"), which is broadly considered to be the global standard for rights-respecting cybercrime legislation and provides for criminal sanctions only for specific and narrowly defined categories of online content, such as online child pornography, racist and xenophobic propaganda, and denial or justification of genocide.

This report highlights that the approaches to cybercrime and digital governance taken by many governments in Africa, the Middle East and Türkiye are not aligned with these sources of international guidance on appropriate measures to address illegal content online. We reviewed over 150 legal frameworks from governments in these regions which criminalise or otherwise restrict forms of expression online which governments deem to be "harmful", including cybercrime frameworks, e-communications laws, restrictions on online disinformation or defamation, and online platform regulations, as well as relevant provisions in penal codes, anti-terror laws and press and media standards. We also worked with local experts to conduct in-depth case studies on cybercrime laws and content restrictions in Ghana, Jordan, Iraq, Saudi Arabia, Tunisia, Türkiye and Uganda. Through this research, we found that:

- Many of the content restrictions examined purport to be in the interests of public safety, such as restrictions on sharing terrorist or violent content online or on sharing information which would undermine national security. However, these sweeping restrictions are broadly defined, not tied to concrete risks of public harm, and not aligned with international definitions of terrorism or terrorist content. These laws are frequently enforced against peaceful activists, journalists and human rights defenders.

→ ***For example, Jordan's Cybercrime Law (see page no. 21) imposes severe penalties for vague offences in the name of national security, including sharing content online that "exposes public morals", "stirs up strife" or motivates violence. These provisions have been used to detain and prosecute journalists and activists.***

- Over a third of the legal frameworks considered include restrictions on sharing false information which lack sufficient clarity over how information should be defined as "true" or "false" and can be arbitrarily applied to government-critical expression. Many individuals prosecuted under these laws have received harsh criminal penalties, contradicting guidance from human rights experts that criminal penalties for disinformation are almost always disproportionate.

→ ***For example, Tunisia's Cybercrime Decree (page no. 24) – which was passed into law during a state of emergency in 2022 without parliamentary approval – imposes prison terms of up to ten years for sharing false news or statements online. Several journalists, politicians, students, and civil society activists have been prosecuted for this offence, including reputable TV hosts and a Former member of the Electoral Commission.***

- Several governments in the region are restricting forms of expression which should never be restricted under international human rights law and pose no clear risk of public harm, including expressions of sexual diversity, criticism of public figures, and advocacy for the rights of marginalised groups, including women, the LGBTQI+ community and religious minorities. Such restrictions enforce authoritarian value systems online and stifle the diversity of voices and perspectives essential for democratic societies.

→ ***For example, Saudi Arabia's anti-terror law (page no. 27) has been used to enforce extremely long prison sentences on hundreds of individuals in recent years for criticising the kingdom and its leadership online; and Uganda's Anti-Homosexuality Act and Ghana's Family Values Bill (page no. 32) both provide for prison sentences for sharing any material online which might promote or advocate for LGBTQI+ identities or activities, effectively silencing all forms of LGBTQI+ expression and allyship.***

- Many restrictions on online speech in the region are formulated and enforced in ways that risk not only individuals' rights to freedom of expression but also a range of related rights including the rights to freedom of opinion, freedom of assembly and association, political participation, non-discrimination and linguistic and cultural rights.

→ ***For example, women and the LGBTQI+ community have been disproportionately targeted by complaints submitted to Iraq's new cyber-morality reporting platform (see page no. 33), reporting higher rates of arrest and an increase in hate speech against female influencers after the launch of the platform.***

- Several governments in the region are also beginning to apply civil or criminal restrictions to online platforms for hosting content deemed to be illegal or harmful, through stringent monitoring and takedown requirements under threat of heavy fines or even prison sentences for platform employees. Such frameworks further tighten government control over online expression and increase risks of over-censorship by platforms.

  → ***For example, frequent amendments to Türkiye's Internet Law (see page no. 38) have drastically increased the scope of applicable criminal, administrative and financial sanctions technology companies face for non-compliance with government demands to share user data or remove content, even where doing so contradicts the platforms' internal human rights policies.***

In the context of this "ever-tightening net" on what individuals can do and say online, it is extremely challenging for civil society organisations (CSOs) in the region to advocate for legal reform, and direct engagement in policy processes can be difficult or impossible. Technology companies are also increasingly struggling to uphold their human rights obligations in regulatory environments which impose more stringent restrictions on their content moderation practices with harsh sanctions in place for non-compliance. We collate ten recommendations for technology companies and CSOs working to push for more rights respecting cybercrime legislation:

## Recommendations for advocacy strategies

**01** Document the benefits of rights-respecting internet regulations and the harms of authoritarian ones

**02** Build public awareness

**03** Provide legal aid and training

**04** Build coalitions with other CSOs for advocacy

**05** Encourage technology companies to form coalitions

**06** Collaborate with National Human Rights Institutions and alliances

**07** Raise concern with international human rights mechanisms

**08** Capitalise on relevant commitments, international processes and events

**09** Strategically litigate

**10** Make the economic case for a free, open and secure internet

We also highlight the need for proportionate, rights-respecting responses to cybercrime and online content which poses direct risks to the rights or reputations of others or to public safety. This is essential not just at the domestic level but also internationally, as the UN finalises and begins to implement the first global treaty on cybercrime. We outline ten essential principles for governments and policymakers developing cybercrime legislation to consider:

## Principles for rights-respecting cybercrime-legislation

**01** International frameworks for online content governance and cybercrime restrictions must be grounded in international human rights law

**02** Pluralistic free expression online must be protected

**03** Criminal restrictions on online content should be reserved for only the most egregious content types

**04** Content which is restricted by law must be clearly and narrowly defined

**05** Harmful online content which cannot be permissibly restricted under international human rights law should be addressed through alternative measures

**06** Legal content that may pose risks to children requires a nuanced approach

**07** Engaging diverse stakeholders is key to developing effective and future-proof cybercrime and content regulations

**08** Platforms must continually improve their approach to content governance in all jurisdictions in which they operate

**09** Cybercrime laws and content regulations must include robust procedural safeguards that are able to provide accountability and transparency for enforcement

**10** Criminal restrictions on online content should be enforced by an independent judicial authority

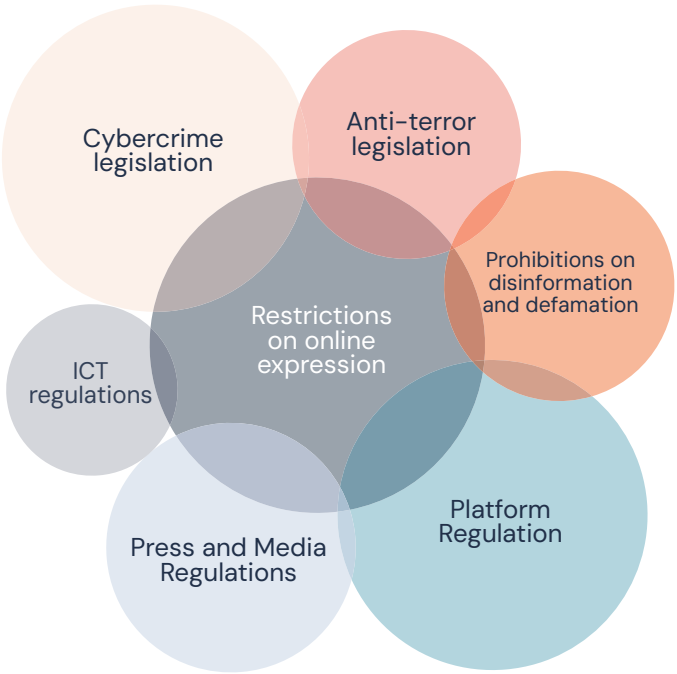
**11** When enforcing platform regulations, online safety regulators must operate with full independence from the executive

## 2. BACKGROUND

The internet and digital technologies are essential for the enjoyment of human rights in the digital age, facilitating greater civic engagement and democratising access to information. Yet they also introduce risks of digital harms and new forms of criminal activity in the digital environment. "Cybercrime" lacks a universal definition but broadly refers to crimes that are committed using computers and information communication technologies (ICTs). Some cybercrimes are unique to these technologies (such as unauthorised access) and are referred to as core cyber crimes or cyber-dependent crimes, while others (such as fraud or content-related offences) may be amplified using technology and are referred to as cyber-enabled.

The focus of this paper is broadly on content-related cyber offences, namely legal restrictions on what individuals can say and share online. In Africa, the Middle East and Türkiye, many of these restrictions are found in cybercrime legislation, but others are found in a range of other types of legal frameworks, as illustrated in Figure 1. In particular, states are increasingly turning their regulatory efforts towards online platforms, in some cases implementing far-reaching requirements for platforms to monitor and proactively remove a range of content types. Both cybercrime treaties and international and regional human rights law provide relevant rules and standards for how governments in Africa, the Middle East and Türkiye should approach harmful online content.

Figure 1 **Types of legislation which may include restrictions on online expression in Africa, the Middle East and Türkiye**



**Illegal vs. harmful content**

The term "illegal content" varies between jurisdictions, and often does not align with the definition of content which may be restricted or criminalised under international human rights law. To complicate matters further, several countries have introduced laws which prohibit or restrict content described in the legislation as "harmful", rendering these forms of "harmful" expression illegal (regardless of whether or not such expression would actually be considered harmful under international human rights standards).

***In this paper, "harmful content" refers to content which may not be restricted by law but which may still pose genuine risks to individuals or societies, while illegal content refers to content which is restricted by national law in a given jurisdiction, whether or not these restrictions adhere to international standards on freedom of expression.***

## Cybercrime treaties

The Council of Europe's **Budapest Convention**[1] was adopted in 2001, the first international treaty to address internet and computer network crimes. It has 72 parties and 21 signatories, including 18 countries in Africa, the Middle East and Türkiye. The original treaty included only child pornography as a content-based offence, and a later protocol extended content-based offences to include distributing racist and xenophobic material, threats and insults based on racial, ethnic or religious categories, and denial or justification of genocide or crimes against humanity.[2] The Council of Europe's guidance on the implementation of the treaty stresses that criminalisation of content not defined in the convention should be used only as a last resort and in accordance with the three-part test.[3]

The African Union's **Malabo Convention on Cyber Security and Personal Data Protection**[4] entered into force in 2023 after slow ratification. It has only been ratified by 15 member states[5] and has faced criticism for vague definitions and an absence of procedural safeguards, but its content-related offences align with the Budapest convention, focusing on child pornography and xenophobic or racist hate speech.[6] In contrast, the **Arab Convention on Combating Information Technology Offences,**[7] adopted by the League of Arab States in 2010, includes a much broader range of content-related offences, such as pornography, gambling, advocacy of terrorism, religious fanaticism and dissension. It has not yet been formally activated due to slow ratification.[8]

The United Nations is also developing a **Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes**, following a 2019 General Assembly resolution. Despite extensive negotiations over a three-year period, the final session in January 2024 ended without consensus. Disagreements centre primarily on the scope of criminal offences and the application of

procedural measures, and the inclusion of human rights safeguards to procedural measures and international cooperation. Regardless of the final outcome of the UN process (still pending at the time of writing), the council of Europe Budapest convention – with its narrowly defined content-based offences – is likely to remain a global standard for rights-respecting cybercrime regulations.

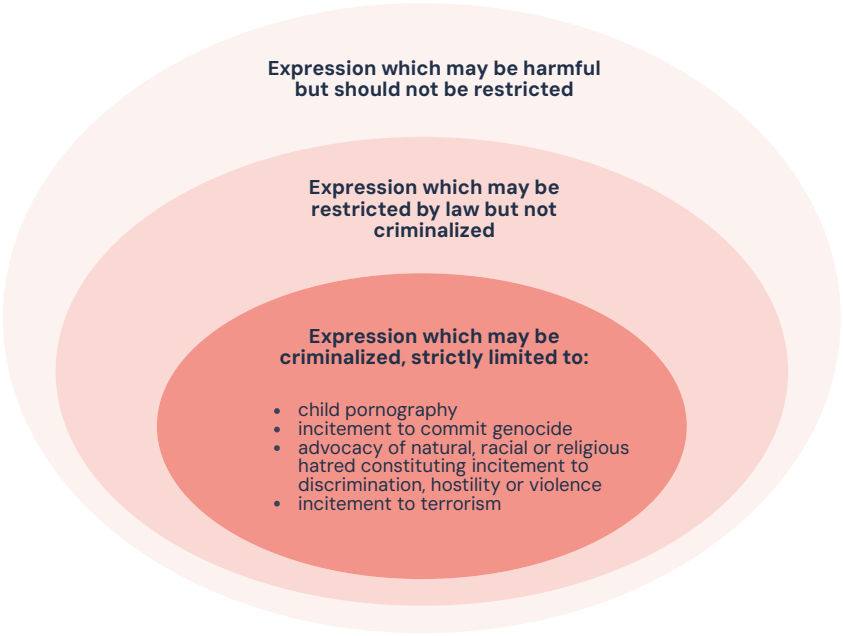
## Human rights law

International human rights law applies at all times and focuses on states' obligations to respect, protect and fulfil human rights. It offers a clear framework for governments to determine what expression should be protected or restricted, including in the online environment and in relation to content-based cybercrimes.[9] The International Covenant on Civil and Political Rights (ICCPR) – which has been ratified by all countries in Africa, the Middle East and Türkiye apart from Saudi Arabia, the UAE, Oman and South Sudan – guarantees everyone's right to hold opinions without interference and to seek, receive and impart information and ideas across borders and through any media.[10] The right to freedom of expression is also enshrined in the African Charter on Human and Peoples' Rights[11] and the Arab Charter on Human Rights,[12] although the latter has faced considerable criticism for divergence from internationally agreed standards and an absence of meaningful mechanisms for monitoring or enforcement.[13]

Under international human rights law, restrictions on freedom of expression must be provided by law, in pursuance of a legitimate aim, and must be necessary and proportionate to achieving that specific legitimate aim; this is known as the "three-part test" for permissible restrictions on freedom of expression. Article 19(3) of the ICCPR defines the "legitimate aim" of a restriction on freedom of expression as (a) respecting the rights or reputations of others or (b) protecting national security, public order, public health or morals. States may enjoy a range of other legitimate interests beyond those laid out in this article, including economic, diplomatic and political interests; but pursuits of those broader aims must not involve measures that restrict the exercise of freedom of opinion and expression.[14]

The three-part test provides that restrictions on freedom of expression must be tied to specific and tangible harm, and implemented as narrowly as possible.[15] For example, broad prohibitions on speech that might "upset social order" or which lacks "social morality"; rules against advocating for "terrorism" without a clear definition of what terrorism is; and the criminalisation of speech that "threatens national security" without a demonstrable link to a tangible national threat, are all impermissible restrictions.[16] The Special Rapporteur on the promotion and protection of freedom of opinion and expression has further clarified that not all online expression which may be harmful to individuals or to the public should be restricted by law or criminalised, with different types of harmful expression requiring different legal and technological responses (see Figure 2).[17] Only four narrowly defined types of harmful expression may be criminalised by states – child pornography, incitement to commit genocide, advocacy of national, racial or religious hatred which constitutes incitement to discrimination, hostility or violence, and incitement to terrorism. These restrictions must still adhere to the three-part test.

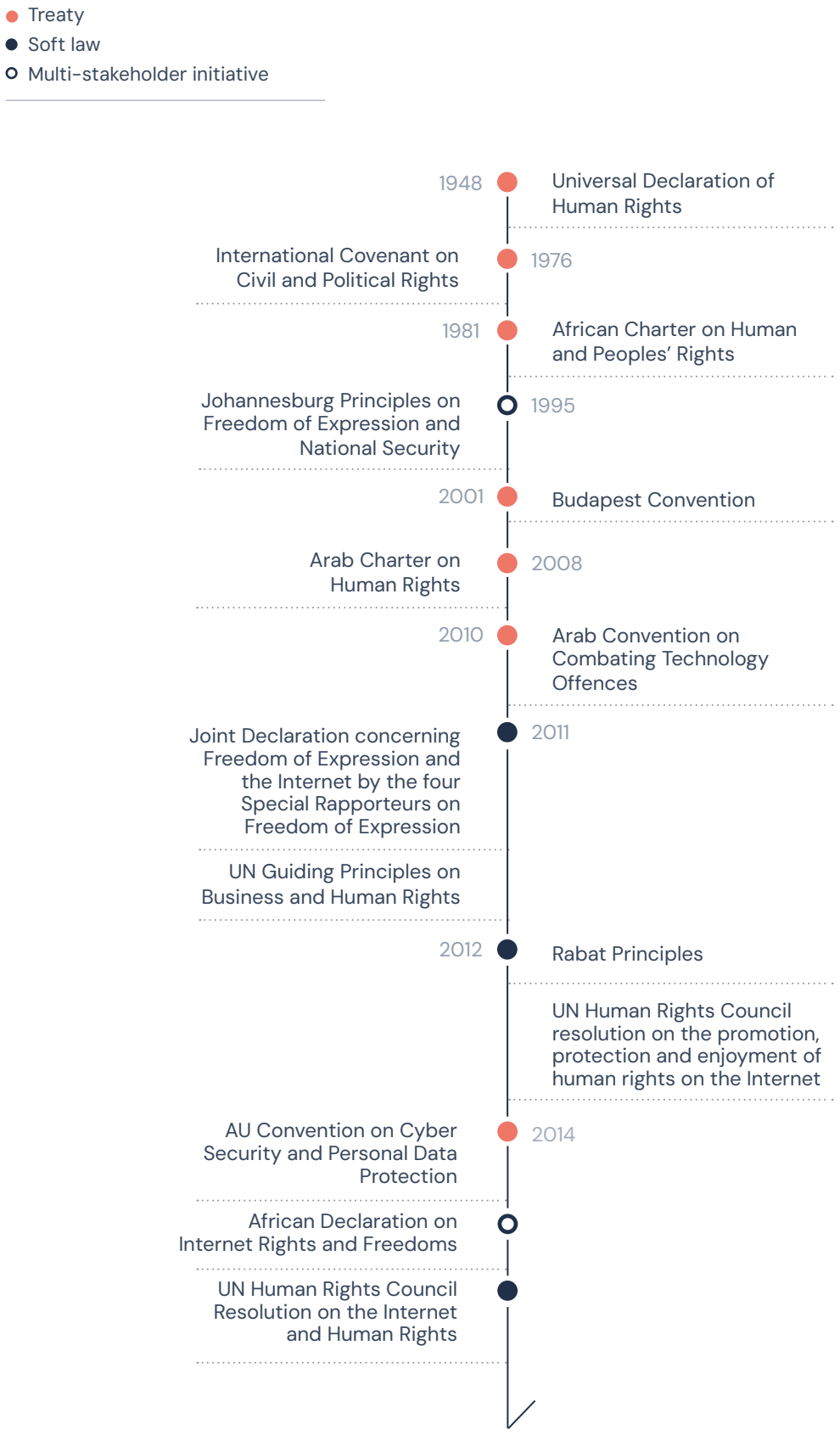
Figure 2 **Three types of harmful content identified by the UN Special Rapporteur on the promotion and protection of freedom of opinion and expression**

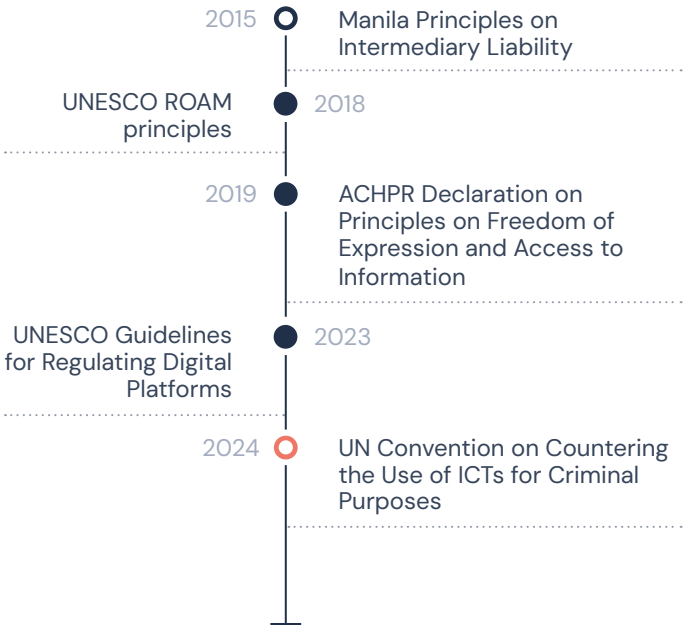



Freedom of expression standards must also be adhered to in government efforts to regulate online platforms. The OHCHR B-Tech team have provided guidance on how governments should regulate technology companies in line with the **UN Guiding Principles on Business and Human Rights**,[18] and UNESCO's **Guidelines for the Governance of Digital Platforms** for states stress that content regulations must comply with the three-part test, be evidence-based and proportionate, include procedural safeguards, and be implemented by an independent body.[19] Several international multi-stakeholder initiatives like the **Manila Principles on Intermediary Liability**, The **Santa Clara Principles on Transparency and Accountability in Content Moderation** and the **Global Network Initiative (GNI) Principles on Freedom of Expression and Privacy** also reinforce core principles of respect for human rights in content moderation decisions and disclosure and transparency with users and regulators.[20]

The sources of regional and international law and guidance discussed above, along with additional principles, guidance and instruments relevant to freedom of expression in the digital environment, are illustrated in Figure 3.

Figure 3 **Timeline of key international, regional and multistakeholder instruments relevant to criminalisation of online expression in Africa, the Middle East and Türkiye**

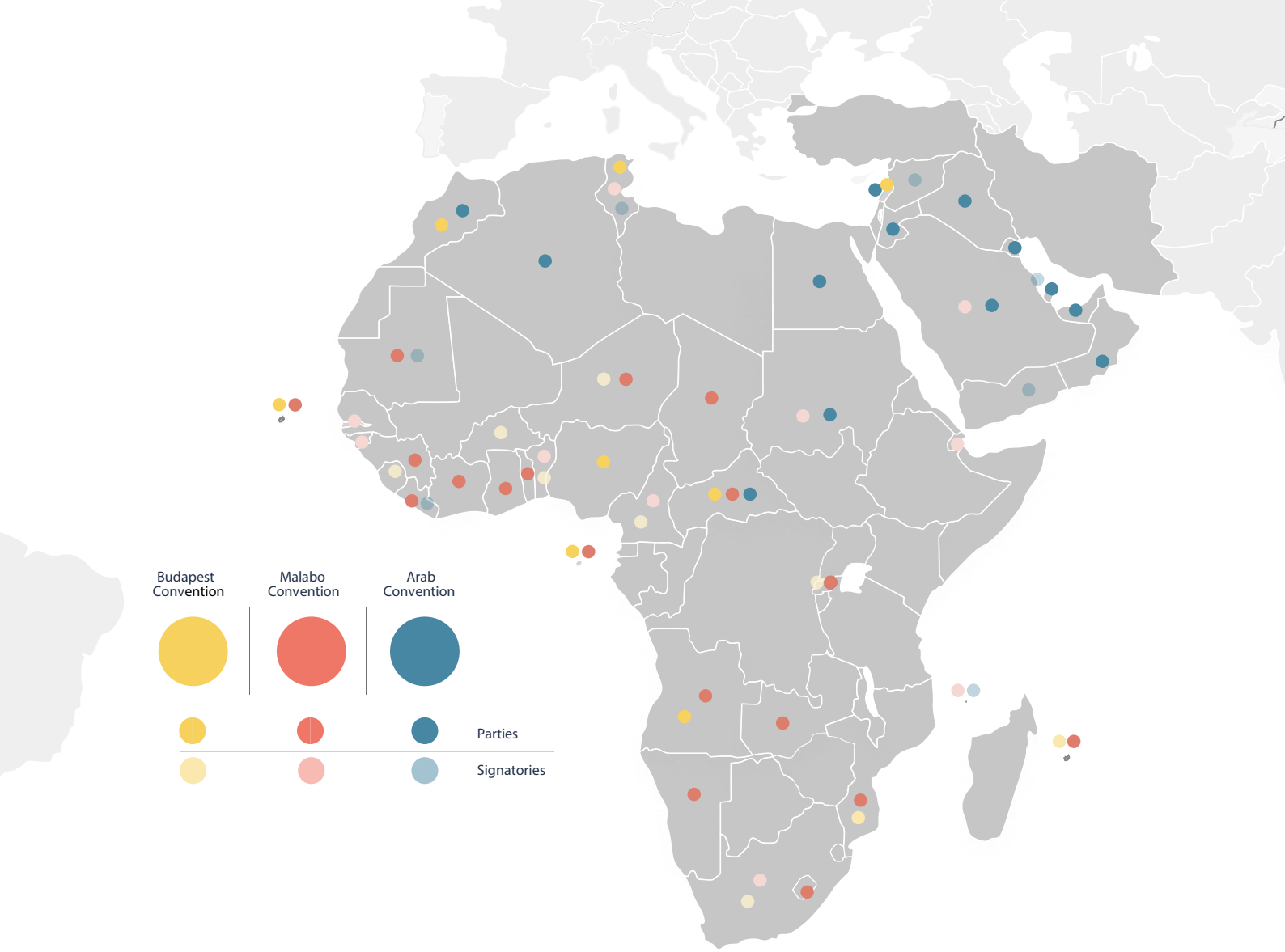





## 3. CYBERCRIME AND ONLINE CONTENT LAWS RESTRICTING FREEDOM OF EXPRESSION IN AFRICA, THE MIDDLE EAST AND TÜRKIYE

In Africa, the Middle East and Türkiye, cybercrime restrictions posing risks to human rights have proliferated in recent years, beginning as laws with a primarily procedural or technical focus, progressing to defining the sharing of a range of content types online as "cybercrimes", and culminating in stringent regulations on the content that online platforms are permitted to host. While some countries in the region have only criminalised narrowly defined content types in line with international human rights standards and the Budapest Convention, many have taken more restrictive approaches and routinely enforce criminal restrictions on a broad range of online expression which do not comply with the three-part test on freedom of expression.

The variation in domestic approaches to cybercrime and online content governance across Africa, the Middle East and Türkiye is illustrated by governments' divergent commitments to regional frameworks on cybercrime (see Figure 4), as well as their engagement in the UN negotiations on the international cybercrime treaty. For example, Angola, Benin, Cabo Verde and the Central African Republic have vocalised support for strengthening the treaty's human rights safeguards;[21] while Egypt – on behalf of the Arab group – has opposed a proposed article requiring states to respect human rights in their implementation of the convention, claiming such an article would interfere with state sovereignty. Several countries in Africa, the Middle East and Türkiye also supported a proposal to delete safeguards around criminalising child sexual abuse material, which could lead to the criminalisation of consensual image sharing among teenagers and repression of sexual diversity.[22]




- Algeria
- Angola
- Bahrain
- Benin
- Burkina Faso
- Cameroon
- Cape Verde
- Chad
- Comoros
- Cote d'Ivoire
- Djibouti
- Egypt
- Gambia
- Ghana
- Guinea
- Guinea-Bissau
- Iraq
- Israel
- Jordan
- Kuwait
- Lesotho
- Liberia
- Mauritania
- Mauritius
- Morocco
- Mozambique
- Namibia
- Niger
- Nigeria
- Oman
- Palestine
- Qatar
- Rwanda
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Sierra Leone
- South Africa
- Sudan
- Syria
- Togo
- Tunisia
- United Arab Emirates
- Yemen
- Zambia

Figure 4 **Signatories and Parties to the Council of Europe's Budapest Convention, the African Union's Malabo Convention and the Arab League's Arab Convention on Combating Information Technology Offences in Africa, the Middle East and Türkiye.**[23]

To better understand the approaches of individual countries in Africa and the Middle East towards content-related cybercrimes and harmful online content, we mapped laws in the region relating to criminal online activity or illegal or harmful online content, including cybercrime frameworks, e-communications laws, restrictions on online disinformation or defamation, and online platform regulations, as well as relevant provisions in countries' penal codes, anti-terror and anti-blasphemy laws, and press and media standards.* Of the resulting collection of 186 pieces of legislation, 31 were excluded because they were repealed, never passed, or contained only procedural or technical rules about telecommunications companies or software houses and did not relate to the permissibility of content hosted online. The remaining 155 pieces of legislation were explored through desk research, and seven countries were selected for further investigation, based on the number and scope of their restrictions on online expression and the severity of their enforcement. These "case studies" (Ghana, Jordan, Iraq, Saudi Arabia, Tunisia, Türkiye and Uganda) were conducted via interviews and research with local experts.

There are many ways of categorising these laws and proposals, which vary considerably from country to country, but for the purposes of this paper we consider and discuss regulations according to the following taxonomy:

- content restrictions which purport to address legitimate aims under the three-part test, such as preventing terrorism or violence or protecting the rights and reputations of others, but which in practice are misused to censor political criticism (section 3.1);
- restrictions on sharing false information, which may in certain limited circumstances be directed at limiting genuine threats to democratic freedoms and human rights but which in practice are arbitrarily applied to a range of legitimate expression (section 3.2);
- content restrictions which have no basis in international human rights law but are used to enforce narrow and authoritarian value systems and narratives online, including restrictions on blasphemy, criticism of monarchies and political and religious leaders, expressions of sexual diversity and advocacy for human rights or gender equality (section 3.3); and
- content restrictions which are imposed upon platforms rather than upon individuals, requiring platforms to comply with a range of government demands impacting how individuals can use the platform to express themselves (section 3.4).

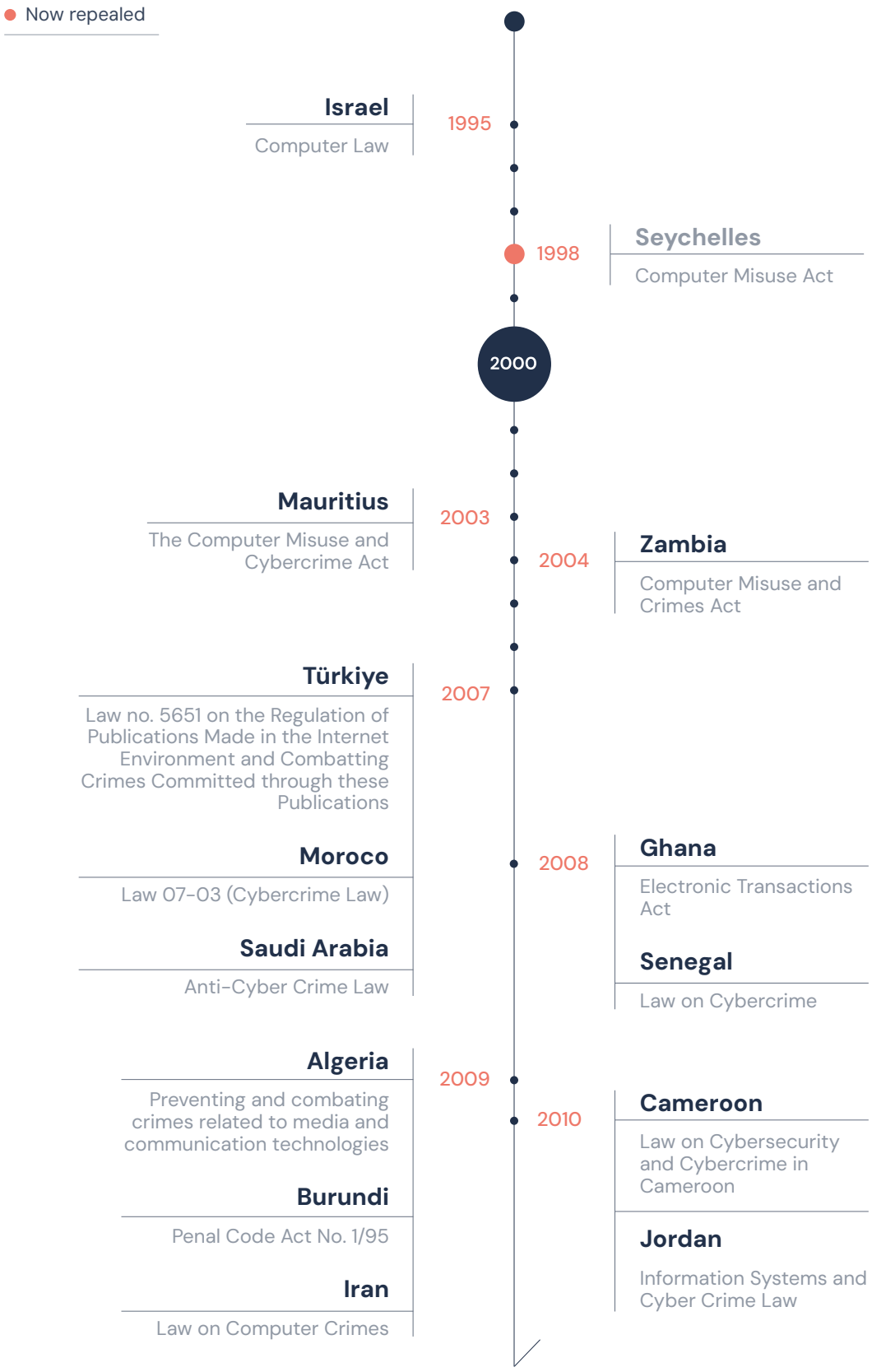
*The mapping excludes restrictions on online advertising, non-consensual sharing of intimate images (NCSII) or child sexual abuse material (CSAM), focusing instead on content restrictions that silence political expression or criticism. Cybercrime provisions that enable government surveillance or restrict online anonymity, while undoubtedly relevant to a restrictive environment for freedom of expression, are beyond the scope of this paper, as are internet shutdowns and extra-legal direct government actions to suppress online expression, such as torture or arbitrary detention. This paper examines only regulatory restrictions or proposals and their enforcement.

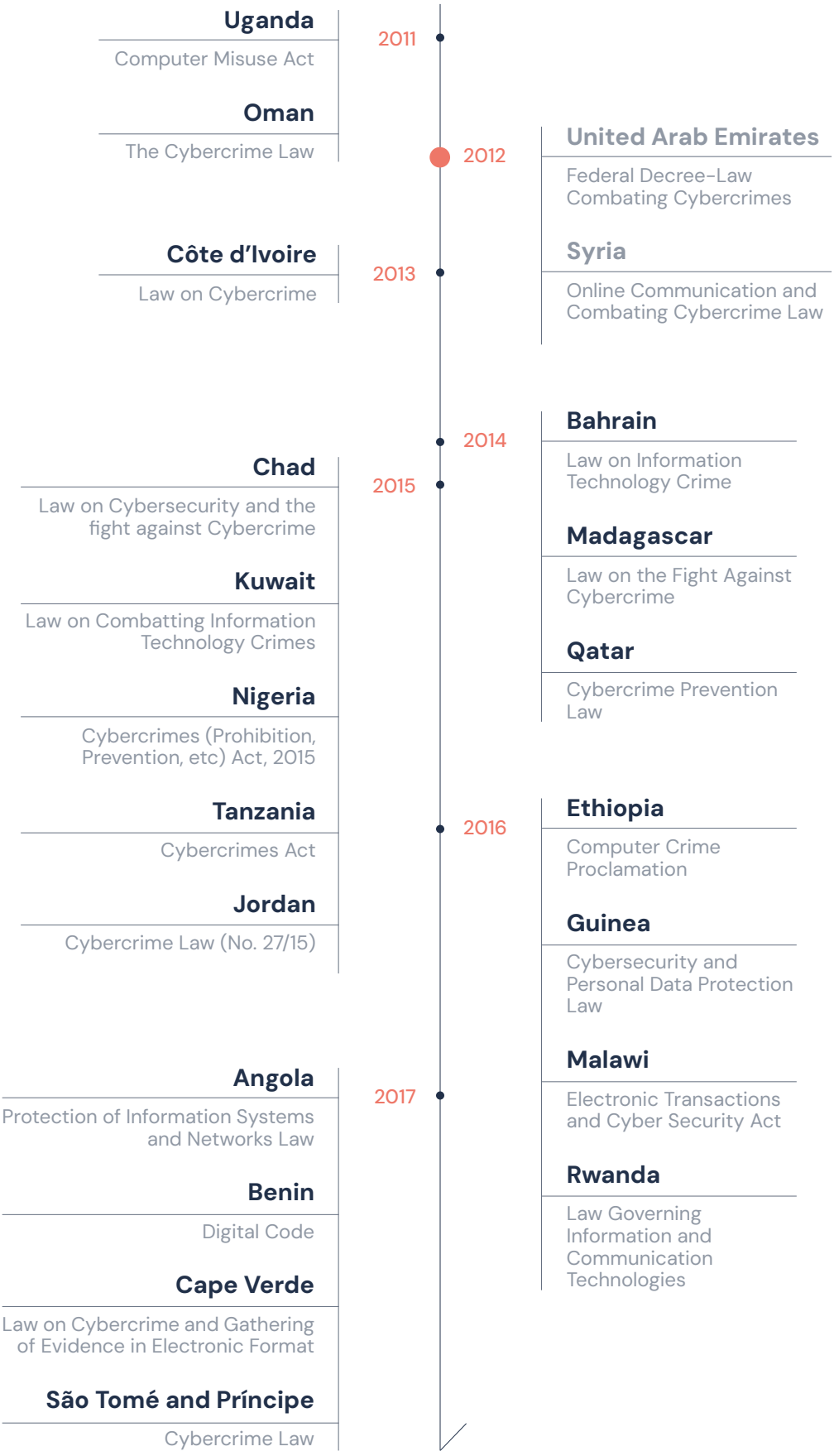
## 3.1 The smokescreen of "public safety" concerns

Almost all countries in Africa, the Middle East and Türkiye have regulations addressing types of online content that pose genuine risks of harm to individuals, including child sexual abuse material, content inciting terrorism or violence, and content infringing on others' rights or reputations, such as defamation and harassment. These restrictions are often found in cybercrime laws (see Figure 5 for a timeline of cybercrime laws in Africa, the Middle East and Türkiye), as well as penal codes and anti-terror laws. While these laws may, in principle, be directed at protecting individuals from malicious cyber activities and harmful content, many use vague definitions of prohibited content types exceeding the scope of permissible restrictions under international freedom of expression guidelines. Most of these restrictions are not tied to a specific or demonstrable public harm, carry disproportionate penalties, and lack procedural safeguards to ensure accountability in enforcement. These characteristics facilitate the use of these legal frameworks to suppress and discourage individuals from exercising their right to freedom of expression online. For example:

- In 2023, **Egypt's** counterterrorism law was used to imprison lawyers and human rights activists for speech critical of the government on social media, charged with "using websites to promote ideas inciting the commission of terror acts".[24]
- **Ethiopia's** Computer Crime Proclamation criminalises dissemination of content that "incites fear, violence, chaos or conflict." Two YouTube journalists were arrested in 2023 under this charge for inciting violence using social media.[25]
- A **Malawian** journalist who reported on corruption allegations against a prominent businessman was arrested on charges including "publication of news likely to cause fear or public alarm" under the Electronic Transactions and Cybersecurity Act. [26]
- In 2019, a **Nigerian** journalist and human rights activist was detained for "threatening public safety, peaceful co-existence, and social harmony", including on charges of cybercrime under the cybercrime law, for organising a protest on socio-economic conditions in Nigeria using the hashtag #RevolutionNow;[27]
- In **Saudi Arabia**, an activist was sentenced to six years in prison (later extended to 34 years) for tweeting about women's and human rights issues. The charges – under the Cybercrime and Counterterrorism Laws – included disrupting public order, undermining social stability, and supporting criminal activity.[28]

Figure 5 **Passage of Cybercrime Laws in Africa, ME and Türkiye**




Uganda
Computer Misuse Act
2011
Oman
The Cybercrime Law
2012
United Arab Emirates
Federal Decree-Law Combating Cybercrimes
Côte d'Ivoire
Law on Cybercrime
2013
Syria
Online Communication and Combating Cybercrime Law
2014
Bahrain
Law on Information Technology Crime
Chad
Law on Cybersecurity and the fight against Cybercrime
2015
Madagascar
Law on the Fight Against Cybercrime
Kuwait
Law on Combatting Information Technology Crimes
Qatar
Cybercrime Prevention Law
Nigeria
Cybercrimes (Prohibition, Prevention, etc) Act, 2015
Tanzania
Cybercrimes Act
2016
Ethiopia
Computer Crime Proclamation
Jordan
Cybercrime Law (No. 27/15)
Guinea
Cybersecurity and Personal Data Protection Law
Angola
Protection of Information Systems and Networks Law
2017
Malawi
Electronic Transactions and Cyber Security Act
Benin
Digital Code
Rwanda
Law Governing Information and Communication Technologies
Cape Verde
Law on Cybercrime and Gathering of Evidence in Electronic Format
São Tomé and Príncipe
Cybercrime Law


2018
Palestine
Presidential Decree on Cybercrime
Botswana
Cybercrime and Computer Related Crimes Act
Egypt
Anti-Cyber and Information Technology Crimes Law
Gabon
Ordinance on Cybersecurity and Cybercrime
2019
Mali
Law on the Suppression of Cybercrime
Niger
Law relating to the suppression of cybercrime
2020
Kenya
Computer Misuse and Cybercrimes Act
Lebanon
Electronic Transactions and Personal Data Law
Republic of the Congo
Law on the fight against Cybercrime
2021
Rwanda
Law on the prevention and punishment of cyber crimes
Sudan
Anti-Cybercrime Law
Togo
Law on Cybersecurity and Fight against Cybercrime
Seychelles
Cybercrimes and Other Related Crimes Act
Sierra Leone
The Cyber Security and Crime Act
South Africa
Cybercrimes Act
United Arab Emirates
Federal Decree Law on Combatting Rumours and Cybercrimes
Zambia
Cybersecurity and Cybercrimes Act
Zimbabwe
Cyber and Data Protection Act

2022

**Burundi**

Law Concerning the Prevention and Repression of Cybercrime

**eSwatini**

Computer Crime and Cybercrime Act

**Libya**

Law combating cybercrime

**Syria**

Counter Cybercrime Law

**Tunisia**

Decree-Law on Cybercrimes

**Uganda**

Computer Misuse (Amendment) Act

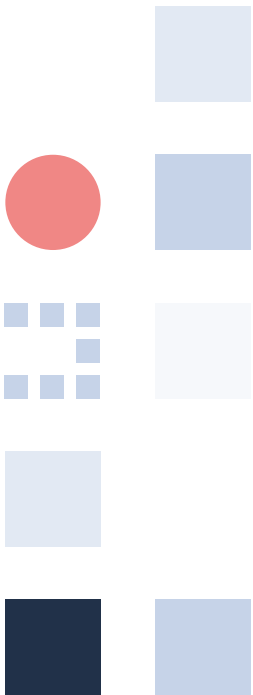
2023

**South Sudan**

Cyber Security and Computer Misuse Act

**Jordan**

Cybercrime Law (No. 17/23)



# CASE STUDY

National security concerns in Jordan's Cybercrime Law

**Freedom House Index:** 33/100 (Not Free)
**Freedom on the Net Index:** 47/100 (Partly Free)
**Governance:** Parliamentary Monarchy
**Ratifications:** ICCPR; Arab Charter on Human Rights; Arab Convention on Combating Information technology Offences

---

The Jordanian government has adopted a security-oriented approach to internet regulation, notably tightening control over online expression and activism after the Arab Spring. Interviewees noted that the **Press Syndicate Law of 2012** enabled authorities to control and censor news websites through a licensing system, and a series of evolving internet regulations – the **Electronic Transactions Act of 2001**, the **Information System Crimes Law of 2010**, the **Cybercrime Law No. (27) of 2015** and its more recent replacement, the **Cybercrime Law No. (17) of 2023** – have expanded restrictions on online expression, empowering authorities to censor and arrest individuals.[29] Participants also noted that the anti-terror law, the penal code, and emergency legislation passed during the COVID-19 pandemic have also allowed the government to restrict online civic space and suppress digital dissent.

The **2023 Cybercrimes Law** is considered by local activists to be the primary legal tool used by authorities to target civil society activists and journalists. It imposes severe penalties for vague offences which are not properly defined, such as "exposing public morals", "stirring up strife" and "insulting religion", as well as sharing content which attacks or defames someone's character, which is false, or which motivates violence. It also allows judicial authorities to order content removals and demand access to user information and requires large online platforms to establish local offices or face advertising bans and throttling.[30]

Though governments may indeed need to limit hate speech, calls for violence, defamation or harassment online where these restrictions are consistent with the three-part test on permissible restrictions to freedom of expression, the vague categories in Jordan's Cybercrime Law allow for discretionary interpretation of such terms and are easily misused to prosecute journalists and activists. For instance, in spring 2024, at least three journalists were detained and interrogated for their online activities and content. One was acquitted, one is awaiting trial (at the time of writing) and one has been sentenced to one-year imprisonment on offences including "inciting strife" under Article 15 of the cybercrimes law.[31]

It is clear that restrictions on content which pose risks to public safety in Jordan's Cybercrime law are being misused to censor government-critical speech and limit free expression, resulting in a climate of increased self-censorship online by journalists, human rights advocates, news editors and the general public. Some newsrooms reportedly publish certain articles that may be perceived as controversial only in print and not on their website, in order to evade charges under the cybercrime law. Independent and freelance journalists are particularly vulnerable as they do not enjoy the limited protections afforded to media employees and outlets under the national media and press legal framework.

When the law was proposed, a coalition of CSOs called for amendments to align it with international standards, and also launched an online campaign highlighting the threats of the draft law to freedom of expression online and urging the King not to ratify the law.[32] However, the bill was passed rapidly without proper dialogue and consultation, and advocacy efforts succeeded only in reducing some fines.

Interviewees noted that Jordan's security-focused approach to cybercrime and public safety both mimics and influences similar approaches elsewhere in the Arab region, particularly the UAE.[33] This regulatory stance will likely impact Jordan's leadership in developing the Unified Arab Strategy for Dealing with International Media Companies[34], shaping regional trends beyond Jordan's domestic context.

### Current proposals for cybercrime legislation in Africa, the Middle East and Türkiye:

- In **Gambia**, the draft cybercrime bill proposed earlier this year raises many human rights concerns, including a broad range of vaguely defined speech offences and making the leaders of media organisations and civil society groups individually criminally liable for the content they publish online.[35]
- The government of **Iraq** has introduced multiple versions of a cybercrime law since 2011, all of which have been withdrawn due to strong criticism from civil society concerning their potential impacts on freedom of expression. A recent draft, proposed in 2023, would have criminalised the use of an information network or device to attack religious, moral, family, or social principles, with no clear or precise definition provided for these concepts or what sort of content would be seen as attacking them.[36] The draft has been withdrawn from the parliamentary schedule, but there are likely to be further attempts.[37]
- **Lesotho's** Computer Crime and Cyber Security Bill, proposed in 2022, is largely aligned with the Budapest convention but includes provisions which criminalise the sharing of "offensive" or "false" information with intent to threaten, abuse, insult or mislead others.

## 3.2 The problem of disinformation

Disinformation can be a cause for concern for many governments and may pose risks to individuals' rights to health, to political participation and a range of other human rights. However, legal restrictions on disinformation are, by nature, highly ambiguous and unable to fulfil the three-part test for permissible restrictions on freedom of expression. They lack sufficient clarity over how information is defined as "true" or "false", often including vague definitions which empower authorities to interpret the restrictions in an arbitrary fashion. Furthermore, they lack a legitimate aim as it is very difficult to identify a clear and specific link between an individual's sharing of false information online and the nebulous harms that disinformation restrictions purport to prevent, which are overly broad. This is why special rapporteurs for freedom of expression from four intergovernmental organisations released a declaration in 2017 stating that general prohibitions on "false news" or similar categories are incompatible with international standards for restrictions on freedom of expression.[38] The *UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* has also stated that the imposition of criminal penalties for sharing disinformation is almost always disproportionate.[39]

All but six countries in Sub-Saharan Africa[40] and the majority of countries in North Africa and the Middle East have some form of legal restriction in place relating to sharing disinformation or false news.[41] Nearly one-third of the laws investigated as part of this research included a prohibition on disinformation and such prohibitions were especially common in cybercrime laws, disinformation-specific laws, penal codes, press and media laws and platform regulations. Many of these are broadly-worded criminal restrictions which carry disproportionate sanctions and are frequently used to censor political speech online. For example:

- **Algeria's** Penal Code criminalises the intentional dissemination of "false or slanderous information or news likely to undermine public security or order" and the distribution of misinformation or propaganda that is likely to harm the national interest.[42] Multiple journalists have been arrested and sentenced to imprisonment – and even death – under these restrictions.[43]
- In **Egypt,** at least sixteen journalists have been charged with spreading false information since 2020,[44] mostly under the 2018 law Regulating the Press and Media which treats any social media account with over 5,000 followers as a media outlet subject to penalties for publishing fake news.[45]
- A **Syrian** TV presenter was arrested in 2021 for spreading false news under the cybercrime law, following a series of Facebook posts she made which were critical of the Syrian government.[46]
- **Tanzania's** Cybercrimes Act criminalises the sharing of false information with intent to deceive; and the Electronic And Postal Communications (Online Content) Regulations require internet companies to address and restrict "false, untrue, or misleading" content. Both laws have been used to arrest journalists and suspend media outlets.[47]
- **Türkiye's** 2022 "disinformation" law amended a number of regulations to criminalise sharing false information with one to three years' imprisonment. Action taken under this law includes the arrest of three journalists in November 2023 for their coverage of alleged corruption in the Turkish judiciary and prison system.[48]

# CASE STUDY

Disinformation provisions in Tunisia's Cybercrime Decree

**Freedom House Index:** 51/100 (Partly Free)
**Freedom on the Net Index:** 59/100 (Partly Free)
**Governance:** Democratic Republic
**Ratifications:** ICCPR; Arab Convention on Combating Information Technology Offences; Budapest Convention; Malabo Convention

---

Tunisia's current multi-party democratic system was established after the 2011 revolution against dictatorship; it is one of the youngest democracies in the world. Since the revolution, restrictions on journalism and media coverage were relaxed, independent media regulators introduced, and the Tunisian Internet Agency stopped blocking websites.[49] However, defamation, slander and insult to public officials remained criminalised under the **Penal Code**,[50] and an **anti-terror law** passed in 2015 prohibits "praising terrorism" defined in broad terms, posing risks to freedom of expression.[51]

In July 2021, Tunisian President Kais Saied declared a state of emergency and assumed all executive powers, claiming this was necessary for national security and stability in the face of the coronavirus pandemic, economic crisis and political deadlock.[52] Under the state of emergency, the President passed **Decree-Law No. 54, known as the Cybercrime Decree-Law**, in 2022. The decree is similar to earlier versions of a cybercrime law which were never submitted to parliament due to a lack of consensus. Provisions on the collection of electronic evidence, unauthorised access, computer fraud and traffic data interception are aligned with the Budapest Convention, but certain key procedural safeguards are absent and Article 24 includes several content-based offences not envisaged in the Budapest convention. These include the offence of disseminating false news or statements online "with the aim of infringing on the rights of others, harming public security or national defence, or spreading terror among the population," punishable with up to 5 years' imprisonment or a fine, or up to ten years' imprisonment where the content targets a public official.

The vague definition of false news potentially criminalises a wide range of content and activities which should not be restricted and permits arbitrary application of the restriction; even "liking" particular posts may be considered as promoting certain content types under the law.[53] The Decree duplicates existing offences in Tunisia's **Penal Code**, **Decree Law No.115** and the **Telecommunications Code**, and additionally remains an interim regulation which has not been subjected to the usual process of parliamentary scrutiny and approval. Several journalists, politicians, students, and civil society activists have already been prosecuted

under the Cybercrime Decree-Law, mostly on charges of sharing false information.[54] For example, in May 2024, two Tunisian TV hosts were sentenced to a year's imprisonment for "spreading false news" and "defaming others" in relation to government-critical commentary online and in the media;[55] and previously a Former member of the Electoral Commission was prosecuted for his criticism of the Board of the Electoral Commission.[56] Harsh enforcement of the Decree-Law has contributed to an atmosphere of fear and self-censorship regarding expression in the digital sphere, particularly among journalists and activists.

Civil society organisations have launched awareness campaigns to highlight the threats that it poses to freedom of expression online, and also engaged in advocacy efforts to amend it through discussions and deliberations with members of Parliament. Groups of parliamentarians have also submitted proposals to amend the Decree-Law, including article 24, and to have the Decree-Law submitted to the usual processes of parliamentary approval.[57] At the time of writing, written responses to both requests have not been received.

**Current proposals for restrictions on disinformation in Africa, the Middle East and Türkiye:**

- In 2023, **Moroccan** lawmakers proposed a draft criminal law including strict penalties for social media users who post "fake news" online.[58]
- **Niger** published an ordinance in June 2024 which reinstates criminal penalties for defamation, insults, and publication of materials likely to undermine public order.[59]
- A notice issued by **South Africa's** Film and Publications Board in March 2024 imposed criminal sanctions on individuals and ISPs for posting or hosting disinformation. The notice has since been withdrawn, but disinformation remains a priority area for the FPB.[60]

## 3.3 Online expression restrictions which enforce authoritarian values

Similar to the restrictions on content examined above, there are regulations that criminalise blasphemy, expressions of sexual diversity, pornography, criticism of public figures or constituted bodies, or content which is considered to be "immoral" or "indecent" as prohibited expression. These restrictions – many of which are broadly worded and not linked to any specific public harm or intention to cause harm – would never be considered as permissible under international human rights law. They disproportionately criminalise and censor the expression of traditionally marginalised groups and pose grave threats to pluralistic democratic societies and a range of human rights, including freedom of opinion and expression, freedom of assembly and association, non-discrimination and linguistic and cultural rights.

### 3.3.1 Restrictions on criticism of political systems or figures

Many countries in Africa, the Middle East and Türkiye enforce criminal restrictions on insulting or defaming public figures (lèse-majesté), which contradict guidance from the Human Rights Committee which states that speech-related offences "should not provide for more severe penalties solely on the basis of the identity of the person that may have been impugned".[61] These provisions are ripe for abuse to censor political criticism and erode accountability for public figures:

- An **Angolan** TikToker was sentenced to six months in prison in 2023 (later extended to two years) for "outrage against the state, its symbols and bodies" under the Angolan penal code, in relation to a TikTok she posted in which she criticised the president.[62]
- After **Iran's** President died in a helicopter crash earlier this year, authorities arrested at least seven people for their social media posts about the incident on charges of "insulting" officials and "disturbing public opinion" under the penal code.[63]
- **Tunisia's** Cybercrime Law provides for doubly harsh penalties for speech which slanders or attacks public officials, and the penal code also criminalises "insulting the president". In 2023, a journalist received eight months in prison for Facebook posts condemning the arrest of the leader of Tunisia's opposition party.[64]
- In **Türkiye,** over 200,000 people have been accused of defaming the president since 2015 under the Penal Code; this includes many individuals prosecuted in relation to content they shared online.[65]
- In **Zambia,** many activists, citizens, journalists and political opponents posting on social media have been sentenced to imprisonment in recent years for "defaming the president" under the Penal Code.[66] Defamation of the president was abolished as a criminal offence by the President in 2022, but the leader of the opposition party was sentenced to 18 months imprisonment in May 2024 for this exact offence for remarks he made in 2021 which were televised and shared on social media.[67]

# CASE STUDY

Severe punishments for online criticism of religious or public figures in Saudi Arabia

**Freedom House Index:** 8/100 (Not Free)
**Freedom on the Net Index:** 24/100 (Not Free)
**Governance:** Absolute Monarchy
**Ratifications:** Arab Charter on Human Rights

---

Saudi Arabia is an absolute monarchy and restricts almost all civil and political rights and fundamental freedoms. It is one of the few states in the world that has neither signed nor ratified the ICCPR and instead of a Penal Code or Constitution, its Basic Law 1992 is based on the Quran and the life and teachings of the prophet Muhammad.[68] The **Anti-Cybercrime Law,** passed in 2007, criminalises dissemination of any material which impinges on "public order, religious values, public morals, or privacy" through an information network or computer. This offence is punishable with up to five years' imprisonment or a fine and has been routinely enforced against lawyers and human rights activists speaking out against repression on social media.[69]

In 2014, Saudi Arabia introduced the **Law for the Crimes of Terrorism and its Financing**, which defined acts of terrorism incredibly broadly, including attempting to disturb public order or harm the state, its reputation or its national unity.[70] It granted the Ministry of Interior powers to hold terror suspects without charge or trial for up to a year with no opportunity for appeal.[71] In 2017, the *UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* criticised Saudi Arabia for enforcing this law against human rights defenders, writers, bloggers, journalists and other peaceful critics in a manner completely incompatible with international human rights law and standards.[72]

The 2014 anti-terror law was replaced in 2017 by **The Penal Law for Crimes of Terrorism and its Financing**, which broadened the scope of acts considered to be terrorism even further and also transferred authority for enforcement to two bodies that report directly to the king.[73] While the previous prohibition on "insulting the reputation of the State" was removed, the current law instead includes criminal penalties of five to ten years in prison for portraying the king or crown prince, directly or indirectly, "in a manner that brings religion or justice into disrepute." Even harsher punishments are provided for academics and activists under Article 35, which provides for imprisonment of a minimum 15 years for anyone who "misuses" their academic or social status or media influence to "promote terrorism".[74]

The anti-terror law has been used to enforce extremely disproportionate sentences on hundreds of individuals for criticising the kingdom and its leadership online or even in private messages. Recent examples include:

- In October 2022, a 72-year-old Saudi American man with less than 200 Twitter/X followers was sentenced to 16 years in prison while visiting family in Saudi Arabia, in relation to 14 tweets critical of the kingdom which he had posted while in America over the previous seven years. He was charged with harbouring a terrorist ideology, trying to destabilise the kingdom and supporting and funding terrorism.[75]
- In August 2023, a retired Saudi teacher was sentenced to death because of his Twitter/X and YouTube activity. The two Twitter/X accounts linked to his case had ten followers combined and less than 1,000 tweets, mostly retweets of well-known critics of the Saudi government and royal family.[76]
- In 2021, a former Red Crescent aid worker was sentenced to 20 years in prison in relation to a satirical Twitter/X account that mocked conservative religious and government figures.[77]
- In 2023, a Yemeni man visiting Saudi Arabia was arrested after his private WhatsApp messages criticising the Crown Prince were leaked to authorities. He is awaiting trial.[78]

The anti-terror law and the cybercrime law are also used to suppress and punish a range of other speech-related offences, including speech which is supportive of women's rights and minority groups.[79] Authorities also routinely block websites and content deemed "offensive" to the state or its leaders.[80]

### 3.3.2 Restrictions on expressions of sexual diversity online

Hostility and discrimination against LGBTQI+ people offline in Africa, the Middle East and Türkiye is mirrored in legal restrictions on LGBQTI+ content online. Many countries in the region still criminalise same-sex sexual relationships or promotion of LGBTQI+ identities in their penal codes or through anti-LGBTQI+ legislation, and several countries also have cybercrime or platform regulations which explicitly criminalise LGBTQI+ -related online content or which include broad provisions that are selectively and disproportionately used to arrest or intimidate LGBTQI+ individuals or their supporters. For example:

- While **Egypt** does not explicitly criminalise same-sex sexual relations, a number of laws including the Cybercrime Law are frequently used to target LGBTQI+ individuals for sharing pro-LGBTQI+ content online or using dating apps for same-sex relationships.[81] Examples include, the Law on Combating of Prostitution (which criminalises "incitement to debauchery", interpreted by authorities to apply to consensual same-sex conduct), the Cybercrime Law (which restricts online content which undermines "family values"

or "public morals"), and the Penal Code (which criminalises acts of "public indecency," "inciting debauchery," and having or distributing materials deemed to violate "public decency"). There are also numerous reports of entrapment of LGBTQI+ individuals by police forces through social media and dating apps.[82]

- In **Iraq**, where same-sex sexual relationships are criminalised under the penal code, an LGBTQI+ rights advocate was sentenced to death in 2022 on charges of "corruption on earth", including through "promoting homosexuality". This was in relation to her online advocacy for LGBTQI+ rights and her participation in a BBC documentary on the treatment of LGBTQI+ people in Iraq.[83]
- **Kenya's** penal code criminalises same-sex sexual activity, and the Kenya Film Classification Board has restricted the circulation of certain films and content on online streaming services – including Netflix – on the basis that they normalise same-sex relationships.[84] The KFCB also ordered a comedian to remove episodes of his YouTube show *Wife Material* in 2021, calling the videos pornographic.[85]
- Four trans women were sentenced to three years in prison in **Oman** in 2018 following the circulation of images from a private birthday party on the instant messaging application Snapchat. Their sentence was based on charges of immoral conduct and imitating the opposite sex under the Penal Code and producing or distributing material that violates "public ethics," and "assisting" in the production or distribution of such material under the Cyber Crime Law.[86]

# CASE STUDY

Anti-LGBQT+ content laws in Uganda and Ghana

## Uganda

**Freedom House Index:** 34/100 (Not Free)
**Freedom on the Net Index:** 51/100 (Partly Free)
**Governance:** Autocratic/democratic hybrid
**Ratifications:** ICCPR

In Uganda, online expression and cybercrimes are primarily governed by the **Computer Misuse Act, 2011** (updated in 2022) and the **Communications Act, 2013**. The Computer Misuse Act as amended includes hate speech, sending or sharing malicious or unsolicited information, and the "misuse of social media" as content-related cybercrimes, posing concerns for freedom of expression.[87] The Communications Act provides broad powers to the Uganda Communications Commission (UCC), a regulatory body whose members are appointed by the Minister of Information and Communications Technology. The UCC is also required to follow policy guidelines and regulations issued by the Minister without parliamentary approval, leading to criticisms regarding its independence and concerns about the UCC's interference with media freedoms.[88]

Against this backdrop, Uganda passed the **Anti-Homosexuality Act** in 2023, which aims to prohibit any form of sexual relationships between persons of the same sex and to prohibit the promotion or recognition of sexual relations between persons of the same sex and related matters. While the law and its harsh penalties raise a huge range of human rights concerns which have prompted international condemnation,[89] of particular interest for this research report is section 11(2)(b) of the Act, which makes it an offence for a person to knowingly disseminate any material promoting or encouraging homosexuality, including through a computer or the internet.

To date, we are not aware of any instances where section 11(2)(b) has been used to arrest, investigate or prosecute any individuals in relation to sharing pro-LGBTQI+ content online. However, offences relating to the "promotion of homosexuality" carry penalties of up to twenty years' imprisonment for individuals and heavy fines or cancellation of a licence for legal entities. The threat of such harsh sanctions undoubtedly has a chilling effect on individuals' online expression, particularly for those within the LGBTQI+ community for whom even sharing their experiences or seeking support online could result in arrest and prosecution.

## Ghana

**Freedom House Index:** 80/100 (Free)
**Freedom on the Net Index:** 65/100 (Partly Free)
**Governance**: Multiparty democracy
**Ratifications:** ICCPR

In Ghana, a recent legislative proposal also poses a threat to the free expression of LGBTQI+ individuals online. **The Promotion of Proper Human Sexual Rights and Family Values Bill** was originally proposed in 2021, and received Parliamentary approval in February 2024. At the time of writing, the President has not yet signed it into law, pending the results of two court cases being brought against the bill on the grounds that it is unconstitutional. Although the bill has not yet been signed by the President, police have previously unlawfully used it to arrest 21 LGBTQI+ activists who were holding a human rights education meeting, on grounds that they were promoting homosexuality.[90]

Same-sex sexual conduct between men is already a criminal offence in Ghana, punishable by up to three years in prison. If passed, the Bill would introduce prison sentences of between three and five years in prison for a much broader range of LGBTQI+ activities, including not identification as an LGBTQI+ person, undergoing gender reassignment surgery, showing affection in public or portraying oneself as a gender other than one's sex assigned at birth. Clause 12 criminalises (amongst other things) the sharing of any material which might promote any of the "offences" detailed in the Bill through any form of media or electronic device, including via social media platforms, punishable with a minimum of five and a maximum ten years' imprisonment. These provisions pose grave risks to the basic rights of LGBTQI+ individuals to openly express their identities and to the free expression of those sharing support for or information about LGBTQI+ people online. The broad scope of activities and expression that may fall in scope of this provision will also further discourage individuals from participating in online communities, sharing information or engaging in digital activism for fear of reprisal.

Also extremely concerning is Subsection 4 of Clause 12, which makes owners of accounts or platforms where such material is circulated criminally liable for the content, unless they can demonstrate appropriate due diligence in attempting to prevent it. This provision places significant legal and operational responsibilities on platforms, requiring them to implement stringent monitoring and compliance systems to detect and remove pro-LGBTQI+ content, contradictory to international human rights standards and the UN Guiding Principles on Business and Human Rights. Threat of sanctions may also result in platform owners adopting overly cautious content moderation policies, leading to the removal of a broad range of other legitimate content and stifling of free discourse.

In both Ghana and Uganda, public reception to these restrictions are complex, with many claiming that LGBTQI+ values and lifestyles are an imposition of Western culture and antithetical to "African values". Uganda's Anti-LGBTQI+ law has sadly received a majority backing from the Ugandan population, reflecting the deeply ingrained social and cultural opposition to homosexuality in the country. However, interviewees pointed out that criminal restrictions on homosexuality in both Ghana and Uganda were originally imposed under British colonial rule,[91] and that intolerance of sexual diversity on the basis of religion can itself be seen as a legacy of colonialism and the promotion of conservative Christian values by European missionaries, given that many indigenous communities in Africa were previously accepting of diverse genders and sexualities.[92]

## Censorship of expression by marginalised groups and their advocates

In addition to laws targeting pro-LGBTQI+ online content, many other laws seek to restrict and suppress those fighting for equal rights of other marginalised groups, including women and ethnic or linguistic minorities. For example:

- More than a dozen female influencers have been arrested since 2020 in **Egypt** on charges of inciting "debauchery" and "violating family values" under the cybercrime law, often in relation to social media posts in which the women are accused of inappropriate dress or dancing.[93]
- Dozens of Palestinian citizens of **Israel** – who make up 20 percent of the country's population – have been arrested in connection with social media posts about the war in Gaza under Israel's anti-terrorism law, which was amended in 2023 to criminalise systematically viewing publications from a terrorist organisation.[94]
- In **Kuwait**, those expressing online support for the Bidun people – a stateless group whose claims to Kuwaiti nationality are rejected by the Kuwaiti government – are frequently harassed by authorities. For example, a human rights defender advocating for the Bidun people was interrogated by the Department to Combat Electronic and Cyber Crime in relation to two tweets she made in 2020; another Bidun activist served two and a half years in prison for "insulting the emir".[95]
- **Libyan** authorities arrested seven activists in 2022 on charges of spreading atheism and criticising Islam, in relation to content they shared on Facebook and Clubhouse promoting the Tanweer movement (a CSO known for its support of civic education, religious freedoms and minority rights).[96]
- Several **Turkish** activists, journalists and academics have received prison sentences for sharing pro-Kurdish content or commentary online, including on charges of terrorism, disseminating propaganda, and disrupting the unity of the state under the internet law and the anti-terrorism law.[97]

# CASE STUDY

Iraq's cyber morality laws disproportionately target women

**Freedom House Index:** 30/100 (Not Free)
**Freedom on the Net Index:** 43/100 (Partly Free)
**Governance:** Multiparty democracy
**Ratifications:** ICCPR

---

Iraq's **Penal Code** includes restrictions on defamation and insulting political and religious symbols, as well as sharing content which is against "public integrity or decency". With vague definitions for these content types, the Penal Code has frequently been used to prosecute individuals for sharing speech which is critical of public officials and religious leaders,[98] and is also the rationale for the blocking of several websites in Iraq deemed to be contrary to "public decency", including porn websites[99] and news websites with government-critical content.[100]

The penal code also forms the basis for a new reporting platform launched by the Ministry of the Interior in January 2023. The "*Balegh*" ("report", in Arabic) platform encourages citizens to report any content which "violates public morals, contains negative or indecent messages, or undermines social stability".[101] The platform reportedly received 96,000 reports within its first month,[102] and TikTok and Instagram content creators are the most frequently targeted with complaints. The frequency of arrests in relation to Balegh platform reports, including in relation to content would not be considered offensive even by the standards of the general public,[103] has significantly increased online self-censorship and created an environment of fear and uncertainty about what content could be considered to violate public morals. Many influencers – particularly those which create dance or music related content – issued apologies for all previous content they posted due to fear of prosecution.

Interviewees note that women and the LGBQTI+ community are disproportionately targeted through the *Balegh* platform; more women being arrested on the basis of complaints than men, and hate speech against female influencers reportedly increased after its launch. Many female and LGBQTI+ social media users in Iraq use fake names and refrain from posting photos out of fear of both persecution by members of the public and prosecution by the authorities. In one case, a female TikTok dancer was sentenced to six months in prison for indecent content, but was shot dead in a violent attack before beginning her sentence.
While the *Balegh* platform was initially received as a positive policy initiative by the public and various activists and civil society organisations, interviewees noted that public opinion has shifted in recent months. Dissatisfaction with the Balegh platform may therefore provide an opportunity to engage the general public – who are not normally particularly aware of digital policy processes – in discussions about content and platform governance.

**Current proposals for authoritarian online content restrictions in Africa, the Middle East and Türkiye:**

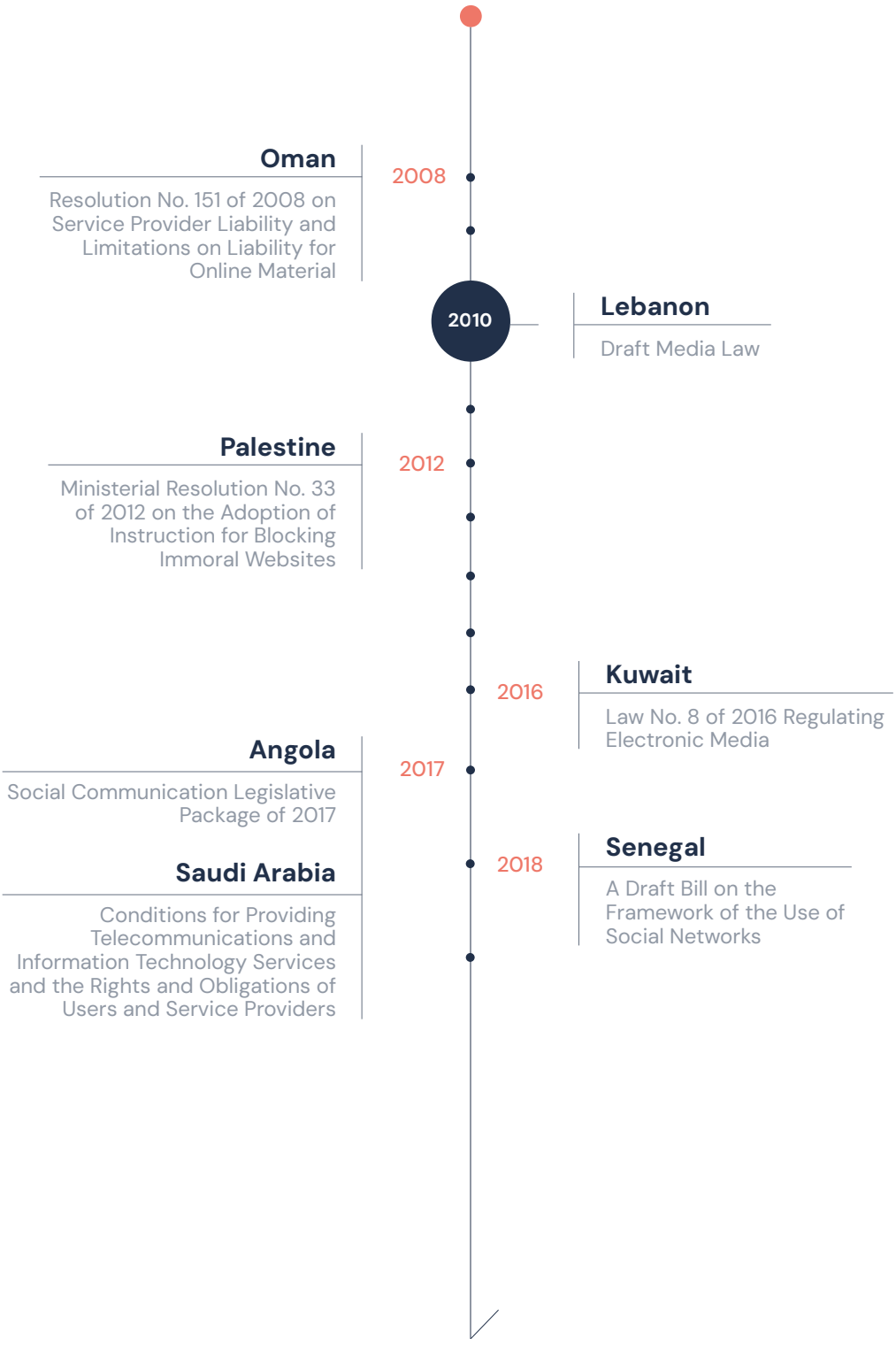
- In **Iran**, the Hijab and Chastity Bill is nearing its final steps to become law. It includes harsh criminal penalties for posting photos of unveiled women on social media, as well as protesting against hijab rules.[104]
- **Kenyan** lawmakers are considering the Family Protection Bill, which – like Uganda's Anti-Homosexuality Act – would make the dissemination of any content which promotes or encourages homosexuality a criminal offence subject to up to ten years' imprisonment;[105]
- **Saudi Arabia's** draft Penal Code includes a range of restrictions applicable to online expression, including "questioning the integrity of the judiciary", "indecent acts" and "words affecting honour". The draft also maintains the death penalty for charges of blasphemy and apostasy, including for children.[106]

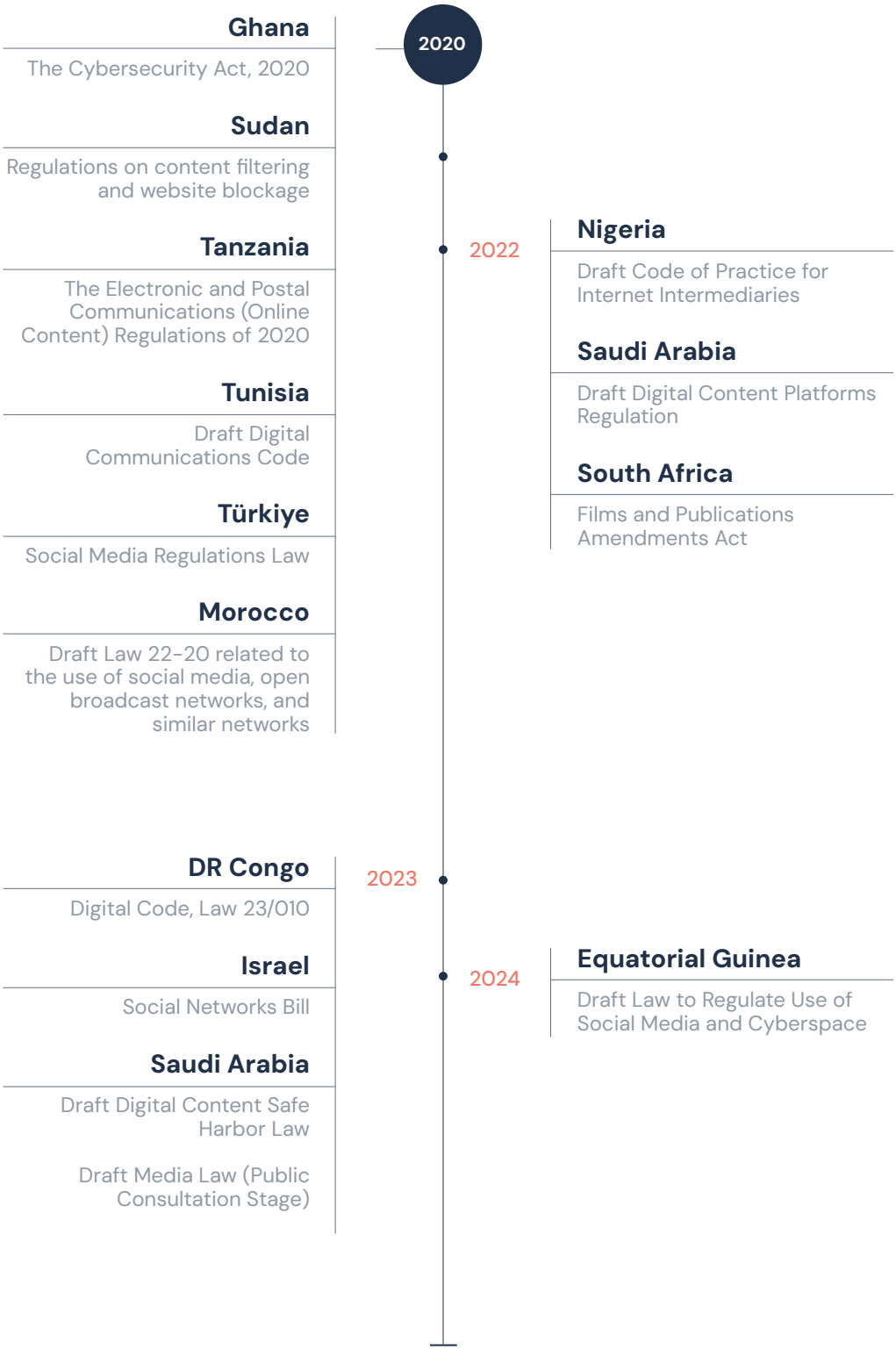
## 3.4 Tightening the net around online platforms

Several countries in Africa, the Middle East and Türkiye are beginning to introduce not just restrictions on what individuals can say or do online but also restrictions on what content platforms can host. These requirements on platforms are primarily laid out in platform regulation laws (see Figure 6), but are also sometimes included in amendments to existing press and media laws or cybercrime legislation. In traditional notice-and-takedown systems, platforms are only liable for illegal content if they fail to remove it after having been notified by the relevant authority. While some policy initiatives in Africa, the Middle East and Türkiye mimic the proportionate and rights-focused approach taken in the EU's Digital Services Act, many pose a range of concerns from a human rights perspective, including:

- Overly broad definitions of illegal or harmful content that platforms must restrict, sometimes contradicting other local laws on permissible content;
- Requiring platforms to proactively monitor for prohibited content (which has been shown to result in over-censorship[107]);
- Requiring platforms to comply with orders from a regulatory body which is not sufficiently independent from executive bodies or influence;
- Demands that platforms remove access to prohibited content not just within the domestic jurisdiction but also extraterritorially, impacting speech of the diaspora;
- Threatening platforms with harsh penalties, such as bandwidth throttling or even criminal liability of platform employees, for non-compliance.

Figure 6 **Passage of Platform Regulation Laws in Africa, the Middle East and Türkiye**




2020
Ghana
The Cybersecurity Act, 2020
Sudan
Regulations on content filtering and website blockage
Tanzania
The Electronic and Postal Communications (Online Content) Regulations of 2020
Tunisia
Draft Digital Communications Code
Türkiye
Social Media Regulations Law
Morocco
Draft Law 22-20 related to the use of social media, open broadcast networks, and similar networks
2022
Nigeria
Draft Code of Practice for Internet Intermediaries
Saudi Arabia
Draft Digital Content Platforms Regulation
South Africa
Films and Publications Amendments Act
2023
DR Congo
Digital Code, Law 23/010
Israel
Social Networks Bill
Saudi Arabia
Draft Digital Content Safe Harbor Law
Draft Media Law (Public Consultation Stage)
2024
Equatorial Guinea
Draft Law to Regulate Use of Social Media and Cyberspace

Reflecting the trend in increasing platform regulation, particularly amongst countries in the Middle East, the League of Arab States has initialised a process to draft a **Unified Arab Strategy for Dealing with International Media Companies**,[108] which is likely to include requirements for online platforms to provide reporting channels, establish legal representation in Arab countries, and remove illegal content within 24 hours of complaint. The definition of "illegal content" will include disinformation, electoral interference, incitement of hate or social unrest, promotion of criminal or extremist entities, and acts threatening national security, and sanctions for platforms for non-compliance include heavy fines or temporary suspensions.[109]

At the domestic level, recent actions taken by governments in Africa, the Middle East and Türkiye to increase control over online platforms and their moderation strategies include:

- **Iran's** Supreme Council of Cyberspace (SCC) attempted to pass a bill in 2022 which would have required international technology companies to have a legal representative in Iran and cooperate with government requests for user data or content removals or face throttling or blocking by the government.[110] While the bill has not yet passed Parliamentary approval, reports indicate that the SCC has already partially implemented the bill, with users observing disrupted access to WhatsApp, Twitter, Telegram, Instagram and Clubhouse.[111]
- In March 2024, the **Iraqi** Ministry of Communications formally requested that the government ban TikTok, arguing that the app has contributed to "the erosion of the country's social unity".[112] The Communications and Media Commission of Iraq also proposed a Draft regulation for Digital Content in 2023, seeking the power to order platforms to remove content which is "low" or "indecent" or which violates "public and private taste" or promotes "immorality".[113]
- The **Nigerian** government banned Twitter for seven months in 2021 in response to Twitter's deletion of a post by the president that violated the platform's content guidelines.[114] After lifting the Twitter ban in 2022, Nigeria's communications regulator approved a Code of Practice for Internet Intermediaries, which requires online platforms to remove a range of vaguely defined content types within 48 hours.[115] CSOs have expressed a range of concerns about the Code and its impact on online expression.[116]
- In January 2024, **Rwanda's** Ministry of Information, Communication, Technology, and Innovation issued an Instruction on Online Child Protection, requiring platforms to take various steps to address any content which "has the ability to influence negatively the development of the child". Suggested measures include implementing content filtering and age verification tools and providing user reporting mechanisms.[117]

# CASE STUDY

Türkiye's growing demands on online platforms

**Freedom House Index:** 33/100 (Not Free)
**Freedom on the Net Index:** 30/100 (Not Free)
**Governance:** Multiparty democracy
**Ratifications:** ICCPR

Despite early democratic and economic gains under Türkiye's ruling Justice and Development Party (AKP), the past decade has seen a considerable decline in democratic freedoms and increasingly severe repression and authoritarian governance.[118] Turkish authorities have aggressively used the **Penal Code, criminal defamation laws, the anti-terrorism law**[119] and the **Internet Law** to prosecute journalists, activists, media outlets and opposition politicians for online dissent,[120] with many convicted simply for liking or sharing content.[121] By the end of 2022, over 700,000 websites had been blocked in Türkiye, most by Türkiye's Information and Communications Technologies Authority (BTK), which is nominally independent but with little judicial oversight and with its members appointed by the Turkish president.[122]

Amidst this backdrop, the government amended the **Internet Law** in 2020 to require social media companies to respond to authorities' requests to block or remove content within 48 hours, or face a fine of up to 5 million euros. Platforms with over one million Turkish daily users were also required to establish representatives in Türkiye, or risk fines, advertising bans and throttling of internet bandwidth by up to 90 per cent.[123] Many CSOs advised technology companies not to set up representative offices at the time, as it would inevitably lead to their implication in human rights abuses.[124] Reports indicate that the Turkish government "played" technology companies against each other, telling multiple companies that all others had already complied with the order and that they alone would lose business if they did not comply in time. Most technology companies appointed legal companies as their representatives but without physical employees.

In 2022, the government moved again to tighten control over online platforms, passing a "censorship law" amending the Internet Law, the Press Law and the Turkish Penal Code among other laws. Technology companies with over 10 million daily users were required to set up legal companies in Türkiye rather than simply representative offices or persons, which drastically increases the scope of applicable criminal, administrative and financial sanctions companies face for non-compliance with internet regulations. The new law also introduced heavier sanctions on companies not complying with content removal requests, including up

to six-month bans on advertising and 50 per cent bandwidth reduction – which can be increased to 90 per cent after 30 days.[125]

Under the new regulations, social media companies can also be compelled to identify users accused of cybercrimes including sharing "false information", and are obliged to proactively report users sharing content that "endangers security of life or property", a content category which is not properly defined in the law.[126] Private messaging services must also establish companies in Türkiye, obtain a licence from the BTK, and comply with secondary regulations to be issued by the BTK.

With these regulations, the Turkish government has significant power to require social media companies and messaging platforms to censor online content in line with demands from the AKP, even where doing so contradicts the platforms' internal policies or human rights procedures. Platforms must negotiate the risks of compliance with risks of services being completely blocked, which poses additional human rights risks during sensitive periods. For example, the day before Türkiye's 2023 Presidential elections, Turkish authorities ordered Meta to remove 110 content items containing corruption allegations against the Turkish government within four hours. While the content in question did not violate its community standards, Meta chose to remove the content and notify the users in question rather than risk a complete service shutdown during the voting period, a time when access to information and communication is particularly crucial.[127]

### Current proposals for platform regulations in Africa, the Middle East and Türkiye:

- **Equatorial Guinea** has released a draft Law to Regulate Use of Social Media and Cyberspace, which will reportedly require social media providers to implement blocking mechanisms to protect users from illegal, offensive or inappropriate content.[128]
- In August 2023, the **Nigerian** National Information Technology Development Agency set up a multi-stakeholder steering committee to draft legislation on Online Harm Protection.[129]
- **Saudi Arabia** has released drafts of a new Digital Content Safe Harbor Law and a new Media Law, both of which will require digital platforms to remove protected speech or restrict its visibility.[130]

## 4. PUSHING BACK AGAINST RESTRICTIVE CONTENT LEGISLATION

CSOs across Africa, the Middle East and Türkiye tirelessly advocate for more rights-respecting laws governing what people can say and do online and what content platforms can legally host. In many countries in the region, direct engagement with parliamentarians or policymakers may not be possible due to the local political or regulatory climate, or because there are no formal mechanisms for multi-stakeholder input into policy processes. Below are some alternative measures that CSOs and companies can take to positively influence the development of rights-respecting internet regulations.

1. **Document the benefits of rights-respecting internet regulations and the harms of authoritarian ones**. Monitoring and reporting on the implementation and impact of internet regulations can build an evidence base for the efficacy of rights-respecting responses. For example, the Council of Europe has reported on the positive impact of the Budapest convention on cybercrime capacities and harmonisation around the world;[131] and the Closing Spaces Database documents incidents of press abuses, digital closure and censorship in West Africa.[132] It will be vital to carry out similar monitoring and reporting for the impacts of the EU's DSA, to provide a compelling rationale for countries to adopt comparable models of platform regulation grounded in transparency, strong protections for freedom of expression and human rights due diligence.

2. **Build public awareness.** CSOs are, in some cases, able to mobilise the public by raising awareness of the dangers or impacts of repressive internet laws, resulting in persuasive campaigns and petitions that policymakers may not be able to ignore. For example, Moroccan CSOs successfully opposed a 2020 draft law criminalising online in March 2020, resulting in its suspension.[134] Similarly, Iraqi CSOs have halted the development of the draft cybercrime law multiple times in recent years as well as the 2023 Draft regulation for Digital Content. When technology companies share takedown or data access orders from governments, this can also help educate the public on how legislation is being enforced in practice to censor online expression.

3. **Provide legal aid and training.** Journalists and human rights defenders at risk of prosecution under cybercrime and online content laws benefit greatly from training on how to respond to judicial harassment. For example, in Jordan, CSOs have been working to raise legal awareness among journalists on how to respond when brought in for investigation under the cybercrime law. There is also a need for funders to support legal aid projects for individuals charged under repressive internet legislation, including through rapid relief funds to facilitate fast responses.

4. **Build coalitions with other CSOs for advocacy.** Working in coalitions can facilitate monitoring, knowledge- and resource-sharing and expand the reach of advocacy activities, allowing for swift action when new developments arise. For example, the Iraqi Observatory

for Human Rights recently launched the Coalition to Defend Freedom of Expression in Iraq,[134] and international CSOs have been collaborating to push for greater multi-stakeholder input and stronger human rights safeguards in the UN Cybercrime Treaty.[135]

5. **Encourage technology companies to form coalitions**, including through industry associations and by leveraging multi-stakeholder networks such as the GNI. Coalitions of technology companies responding in the same way to repressive internet legislation will carry more weight than isolated actions. Governments may find it difficult to sanction entire coalitions of major technology companies without facing severe backlash. A united front by technology companies could potentially have successfully resisted the problematic registration requirements under Türkiye's internet regulations.

6. **Collaborate with National Human Rights Institutions (NHRIs) and alliances**. NHRIs are respected partners of the international human rights system, with considerable influence at the UN Human Rights Council. The Global Alliance of National Human Rights Institutions includes thirty-four African and six Middle Eastern NHRIs,[136] and recently announced a new focus on threats to online civic space.[137] CSOs working in countries with accredited NHRIs can collaborate on research and international advocacy.

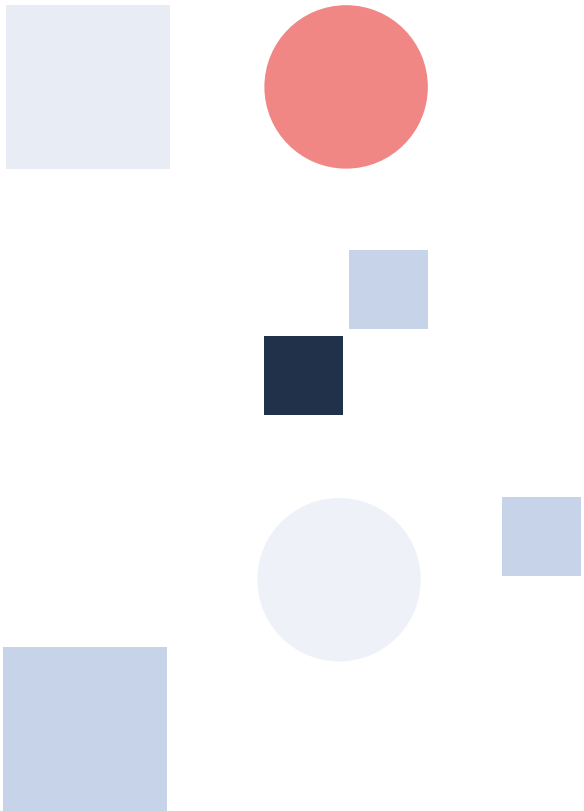
7. **Raise concern with international human rights mechanisms**, such as the country's Universal Periodic Review or by contacting special rapporteurs of relevant subjects. For example, the AU Special Rapporteur on Freedom of Expression and Access to Information can issue letters of urgent appeal to Governments alleged to have violated the right to freedom of expression and access to information;[138] and in recent months the UN *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* has issued communications to countries including Israel, Iran and the United Arab Emirates calling attention to the criminalisation and harassment of peaceful activists and journalists in relation to their online expression.[139]

8. **Capitalise on relevant commitments, international processes and events**. International conferences, negotiations or initiatives relating to cyber and internet governance can provide opportunities to draw attention to online repression in different contexts. For example, many CSOs are using the hosting of the 2024 Internet Governance Forum in Saudi Arabia to call attention to the country's terrible human rights record both online and off, and tailoring their engagement in the conference accordingly.[140] CSOs can also hold governments and platforms to account for not upholding their existing commitments under international law or other pledges, such as the GNI Principles or the Freedom Online Coalition Values; for example through joint statements calling attention to breaches of these responsibilities.

9. **Strategically litigate**. Where a country or region has a strong and independent judicial system, strategic litigation may help prevent, amend or repeal repressive internet laws. For example, the anti-LGBTQI+ bill in Ghana is currently on hold due to Supreme Court challenges;[141] the European Court of Human Rights found that the blocking of YouTube in

Türkiye violated the right to freedom of expression;[142] and Nigeria's Twitter ban was found to be unlawful by the ECOWAS court as it was not based on any law or court order and was not clear what law was breached by the company.[143] Such cases deter governments from attempting to pass repressive legislation and can be a useful tool particularly where there is no participatory regulatory process to engage with the government.

10. **Make the economic case for a free, open and secure internet**. Repression of online expression can result in lost economic opportunity, which in turn negatively impacts individuals' enjoyment of their economic, social and cultural rights. For example, the World Bank halted new loans to Uganda after it passed the anti-LGBTQI+ law, which "fundamentally contradicts the World Bank's values."[144]



# 5. TOWARDS RIGHTS-RESPECTING CYBERCRIME AND CONTENT REGULATIONS

While authoritarian governments often misuse cybercrime laws to target peaceful activists and legitimate expression, the fact remains that cybercrime and illegal content pose real dangers that must be addressed. Governments worldwide are responding to the rapid spread of online material which poses harm to human rights and democratic integrity. However, international consensus on best practice remains elusive, as seen in the recent delays to the UN Cybercrime treaty and the mixed reception of UNESCO's Guidelines on the Regulation of Digital Platforms.[145] Proportionate, rights-respecting responses are needed, tailored to local and regional realities and challenges and incorporating citizens' perspectives through multi-stakeholder policy development. This section outlines some key principles of rights-respecting approaches to cybercrime and harmful online content, based on global best practices.

1. **International frameworks for online content governance and cybercrime restrictions must be grounded in international human rights law**. The forthcoming UN Cybercrime treaty will be crucial in shaping international discourse and best practices, and it must safeguard against repressive content restrictions disguised as "cybercrime" laws which do not align with international human rights standards.

2. **Pluralistic free expression online must be protected**. Internet regulations should aim to promote and protect human rights online and ensure information integrity, focusing on transparency, accountability, and due process rather than content-based restrictions.

3. **Criminal restrictions on online content should be reserved for only the most egregious content types**, such as CSAM and hate speech that incites discrimination or violence. These restrictions must comply with the three-part test: they must be provided for by law, pursue a legitimate aim, and be necessary and proportionate to achieving that stated aim. For instance, Sierra Leone's cybercrime law only includes content-based offences for the distribution of CSAM or racist or xenophobic materials, in line with the Budapest Convention and its Additional Protocol.

4. **Content which is restricted by law must be clearly and narrowly defined**, with sufficient precision for an individual to reasonably know what expression is and is not permitted. Legal restrictions must be tied to a specific public harm, with clear thresholds of actual harm or damage caused before sanctions apply, and any sanctions should be proportionate to the degree of harm caused by the expression in question. For example, Nigeria's Cybercrimes Act includes detailed definitions of what online expression would constitute "racist and xenophobic material" or justification of crimes against humanity or genocide, and provides for graded penalties of up to five years' imprison or a fine upon conviction of this offence.

5. **Harmful online content which cannot be permissibly restricted under international human rights law should be addressed through alternative measures**. These might include digital literacy education, media integrity initiatives, socio-technical interventions by social media platforms, and policy initiatives tackling the root causes of the content in question. For example, the EU's Code of Practice on Disinformation is a set of voluntary standards for technology companies to address disinformation, which also serves as a mitigation measure and Code of Conduct recognised under the DSA.

6. **Legal content that may pose risks to children requires a nuanced approach**, tailored to the specific platform, age group, local context and type of content in question. Rather than requiring all users to verify their age or introducing sweeping restrictions on all content which may pose harm to children, policy responses should focus on ensuring that platforms amend design features which pose disproportionate harm to children and consistently enforce existing content policies designed to prevent unsolicited contact and pathways to graphic and violent content.[146]

7. **Engaging diverse stakeholders is key to developing effective and future-proof cybercrime and content regulations**. This involves engaging government bodies, civil society organisations, technology companies, and the public. For example, the Nigerian government has set up a multi-stakeholder steering group, including CSOs, to guide the development of a new digital platform regulation. It is also important to regularly review and amend policies and laws over time, again through a consultative and multi-stakeholder process.

8. **Platforms must continually improve their approach to content governance in all jurisdictions in which they operate**. Poor or inconsistent moderation of illegal content by online platforms gives credibility to governments' attempts to more harshly restrict what people can say and do online. Platforms must instead invest more resources in local content moderation mechanisms, including through automated and human review to ensure that moderation is both rapid and reliable. Platforms should disclose content policies and any exceptions, providing examples.

9. **Cybercrime laws and content regulations must include robust procedural safeguards that are able to provide accountability and transparency for enforcement**. These frameworks must also ensure that individuals have an effective right of defence and remedy when enforcement is overbroad, inconsistent or discriminatory with respect to certain groups.

10. **Criminal restrictions on online content should be enforced by an independent judicial authority**, within a fully independent and impartial judicial system and respect for the rule of law, as well as a range of procedural safeguards to protect against abuse and provide mechanisms for address.[147] There should also be sufficient training for judges and law enforcement agencies on cybercrime legislation and human rights; for example,

the Commonwealth Secretariat's Cyber Unit recently provided training for judges in Ghana, Malawi and Zambia.[148]

11. **When enforcing platform regulations, online safety regulators must operate with full independence from the executive**, including independence of funding sources and independent appointments. Statutory interventions by the regulator should also be subject to judicial review.[149] Global cooperation through networks such as the Global Online Safety Regulators Network or the Digital Trust and safety Partnership can facilitate knowledge sharing and regulatory harmonisation.

## Notes

1 *Convention on Cybercrime*, opened for signature November 23, 2001, ETS No. 185 (entered into force 1 July 2004) ("Budapest Convention"), https://rm.coe.int/1680081561.

2 Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, opened for signature January 28, 2003, ETS No. 189 (entered into force March 1, 2003), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189, Articles 3-6.

3 Council of Europe, *Freedom of Expression within the Context of Action on Cybercrime – Practical Considerations*, (Council of Europe, 2023), https://www.coe.int/en/web/cybercrime/-/cybercrime-and-freedom-of-expression-discussion-paper.

4 *African Union Convention on Cyber Security and Personal Data Protection*, opened for signature June 27, 2014 (entered into force June 8, 2023) ("Malabo Convention"), https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

5 Nnenna Ifeanyi-Ajufo, "The AU Took Important Action on Cybersecurity at its 2024 Summit", Chatham House, February 23, 2024, https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed.

6 Global Action on Cybercrime Extended, *Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime* (Council of Europe, 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000016806bf0f8.

7 League of Arab States (LAS), *Arab Convention on Combating Information Technology Offences*, opened for signature on December 21, 2010, https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

8 Joyce Hakmeh, *Cybercrime and the Digital Economy in the GCC* (Chatham House, 2017), https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf.

9 UNHRC, "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/20/8, 2012, https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/20/8; UNHRC, "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/26/13, 2014, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/13; UNHRC, "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/32/13, 2016, https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/32/13; UNGA, "Promotion and protection of the right to freedom of opinion and expression", A/66/290, 2011, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A.66.290.pdf, para 15.

10 ICCPR, Article 19.

11 *African Charter on Human and Peoples' Rights*, CAB/LEG/67/3, adopted on June 27, 1981, CAB/LEG/67/3 (entered into force October 21, 1986) ("Banjul Charter"), 27 June 1981, https://www.refworld.org/legal/agreements/oau/1981/en/17306.

12 OHCHR, "Arab Charter on Human Rights: Unofficial translation", May 22, 2004, https://www.ohchr.org/sites/default/files/Documents/Issues/IJudiciary/Arab-Charter-on-Human-Rights-2005.pdf.

13 "Arab rights charter deviates from international standards, says UN official", UN News, January 30, 2008, https://news.un.org/en/story/2008/01/247292#:~:text=The%20Arab%20Charter%20on%20Human,human%20rights%20chief%20said%20today..

14 UN General Assembly (UNGA), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/71/373, 2016, https://www.refworld.org/reference/themreport/unga/2016/en/112959, para. 28.

15 UN Human Rights Committee (UNHRC), "General Comment No. 34. General comment No.34 on Article 19: Freedoms of opinion and expression", CCPR/C/GC/34, 2011, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no34-article-19-freedoms-opinion-and, paras. 21-36.

16 UNHRC, "Racism, Racial Discrimination, Xenophobia And Related Forms Of Intolerance, Follow-Up And Implementation Of The Durban Declaration And Programme Of Action", A/HRC/7/36, 2008, https://documents.un.org/doc/undoc/gen/g08/115/79/pdf/g0811579.pdf?token=4UN-7wAsFeAZWuVgD4Q&fe=true; UNGA Report A/71/373, paras. 18-19; UNHRC, General Comment No. 34, paras. 34 & 50-52; UNHRC, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/29/32, 2015, https://ap.ohchr.

org/documents/dpage_e.aspx?si=A/HRC/29/32, para. 35.

17 United Nations General Assembly, "Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", A/66/290, 2011, http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290, para. 18.

18 OHCHR (Office of the United Nations High Commissioner for Human Rights), Guiding Principles on Business and Human Rights: *Implementing the United Nations "Protect, Respect and Remedy" Framework* (2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed June 13, 2024).

19 UNESCO, *Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach* (UNESCO, 2023), https://www.unesco.org/en/internet-trust/guidelines.

20 See *Manila Principles on Intermediary Liability* (2015), https://manilaprinciples.org/index.html; *The Santa Clara Principles on Transparency and Accountability in Content Moderation* (2018), https://santaclaraprinciples.org/; *Global Network Initiative Principles on Freedom of Expression and Privacy* (Global Network Initiative, 2018), https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf.

21 United Nations Office on Drugs and Crime, Proposal by Canada on behalf of a group of 66 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to further define the scope of the draft Convention, February 5, 2024, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Canada_3.3_05.02.2024.pdf.

22 See Global Initiative Against Transnational Organised Crime, Cyber Convention Check-in, January 26, 2024, https://globalinitiative.net/announcements/cyber-convention-check-in/ (accessed June 13, 2024).

23 Council of Europe, The Budapest Convention (ETS No. 185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention, accessed Jun 13, 2024; AU, "List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention On Cyber Security And Personal Data Protection", September 19, 2023, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf; LAS, "List of Arab Countries that have signed and ratified the Arab Convention on Combatting Information Technology Crimes", http://www.lasportal.org/ar/legalnetwork/Documents

24 Dina Sadek, Layla Mashkoor, Iain Robertson & Andy Carvin, Intentionally Vague: How Saudi Arabia and Egypt Abuse LeWgal Systems to Suppress Online Speech (Atlantic Council, June 2024), https://www.atlanticcouncil.org/wp-content/uploads/2024/06/Intentionally-vague-How-Saudi-Arabia-and-Egypt-abuse-legal-systems-to-suppress-online-speech.pdf.

25 Ethiopian authorities detain journalists Getenet Ashagre and Aragaw Sisay," Committee to Protect Journalists, April 2023, https://cpj.org/2023/04/ethiopian-authorities-detain-journalists-getenet-ashagre-and-aragaw-sisay/amp/.

26 "Malawi Journalist Charged with Cybercrime," International Press Institute (IPI), April 10, 2024, https://ipi.media/malawi-journalist-charged-cybercrime/.

27 Friday Olokor, "Amnesty International: Nigeria Police Should Drop Cybercrime Charges Against Sowore," Arise News, February 15, 2024, https://www.arise.tv/amnesty-international-nigeria-police-should-drop-cybercrime-charges-against-sowore/. The Federal High Court in Abuja later declared his arrest to be unlawful and ordered the State Security Services to pay him compensation. "Court declares Sowore's arrest over #RevolutionNow protest illegal", Premium Times, March 22, 2022, https://www.premiumtimesng.com/news/headlines/518822-court-declares-sowores-arrest-over-revolutionnow-protest-illegal.html?tztc=1.

28 Dina Sadek et. al, Intentionally Vague.

29 Raed Faqir, "The Jordanian Cybercrime Law: A Critical Appraisal," International Journal of Cyber Criminology 7, No. 1 (2013): 24-41, https://www.cybercrimejournal.com/pdf/Faqir2013janijcc.pdf; Dima Samaro and Emna Sayedi, "Cybercrime Law in Jordan: Pushing Back on New Amendments that Could Harm Free Expression and Violate Privacy," Access Now, February 19, 2019, https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/.

30 "Jordan's new proposed cybercrimes law will strongly undermine digital rights," Access Now, July 24, 2023, https://www.accessnow.org/press-release/jordans-cybercrimes-law/.

31 "The Amman Public Prosecutor orders the imprisonment of journalist Heba Abu Taha for a week in connection with an investigation," Skeyes Media, May 15, 2024, https://www.skeyesmedia.org/ar/News/News/15-05-2024/11622; "Electronic Crimes Unit Summons Journalist Rida Yassin Over Post, Investigates and Detains Him for Two Days,"

Skeyes Media, May 6, 2024, https://www.skeyesmedia.org/ar/News/News/06-05-2024/11618; "North Amman Court Rules Journalist Khair Al-Jabri Not Guilty in Incitement Case," Jo24.net, May 8, 2024, https://jo24.net/amp/article/503888; "Sentence of One Year Imprisonment for Colleague Heba Abu Taha," Jordan24, May 6, 2024, https://www.jordan24.com/news/Jordan-News/06-05-2024/11618.

32 "Open Letter to the King of Jordan: Repeal the 2023 Cybercrime Law," Access Now, August 2, 2023, https://www.accessnow.org/press-release/open-letter-to-the-king-of-jordan-repeal-the-2023-cybercrime-law/.

33 "Jordan Cybercrime Law an 'Exact Copy' of UAE's, Report Claims," Arabian Business, August 16, 2023, https://www.arabianbusiness.com/politics-economics/jordan-cybercrime-law-exact-copy-of-uae-report-claims.

34 "Council of Arab Media Ministers approves unified strategy for negotiating with international media companies", Jordan Times, June 21, 2023, https://jordantimes.com/news/local/council-arab-media-ministers-approves-unified-strategy-negotiating-international-media.

35 "The Gambia: Draft cybercrime bill threatens online dissent", ARTICLE 19, March 28, 2024, https://www.article19.org/resources/the-gambia-draft-cybercrime-bill-threatens-online-dissent/#:~:text=The%20majority%20of%20proposed%20offences,%2Desteem'%20of%20political%20figures.

36 "More Control: Iraq's Alarming Cybercrime Law," SMEX, August 3, 2023, https://smex.org/more-control-iraqs-alarming-cybercrime-law/.

37 "Iraqi Cybercrime Draft Law in Suspension," SMEX, July 6, 2022, https://smex.org/iraqi-cybercrime-draft-law-in-suspension/.

38 OHCHR, "Freedom of Expression Monitors Issue Joint Declaration on 'Fake News', Disinformation and Propaganda", March 3, 2017, https://ohchr.org/en/press-releases/2017/03/freedom-expression-monitors-issue-joint-declaration-fake-news-disinformation.

39 UNHRC, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," A/HRC/47/25, April 13, 2021, https://undocs.org/A/HRC/47/25.

40 LEXOTA, www.lexota.org (accessed June 13, 2024).

41 Georgetown University Law Center Global Law Scholars, "Digital Authoritarianism and Disinformation Laws in the Middle East and North Africa", Law and Disinformation in the Digital Age (2023): 20-39, https://www.law.georgetown.edu/wp-content/uploads/2022/04/Law-and-Disinformation-in-the-Digital-Age.pdf.

42 Committee to Protect Journalists and The Tahrir Institute for Middle East Policy, "Joint Stakeholder Submission to the UN Human Rights Council Universal Periodic Review: The People's Democratic Republic of Algeria", October 2022, https://cpj.org/wp-content/uploads/2022/10/UPR-Algeria-2022-CPJ-TIMEP-FINAL.pdf.

43 "Algeria: Conviction of journalist is latest escalation in crackdown on media," Amnesty International, 2023, Amnesty International, April 3, 2023, https://www.amnesty.org/en/latest/news/2023/04/algeria-conviction-of-journalist-is-latest-escalation-in-crackdown-on-media/.

44 Dina Sadek et. al, *Intentionally Vague*; Committee to Protect Journalists, "Database of Attacks on the Press: Journalists Attacked in Egypt (2018-2024)," https://cpj.org/data/location/?cc_fips=EG&start_year=2018&end_year=2024&report-builder-type=year (accessed June 13, 2024)

45 ARTICLE 19, Egypt: 2018 *Law on the Organisation of Press, Media and the Supreme Council of Media* (ARTICLE 19, 2019), https://www.article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-Final-Nov-2018.pdf.

46 "Damascus: TV presenter arrested under cyber-crime law," Reporters Without Borders, February 3, 2021, https://rsf.org/en/damascus-tv-presenter-arrested-under-cyber-crime-law.

47 LEXOTA Tanzania Profile, https://lexota.org/country/tanzania/ (accessed June 17, 2024).

48 "In Türkiye, 3 journalists detained for disinformation, one jailed, 3 others under investigation," Committee to Protect Journalists, November 2, 2023, https://cpj.org/2023/11/in-Türkiye-3-journalists-detained-for-disinformation-one-jailed-3-others-under-investigation/.

49 Olivier Alais, Erik Da Silva, Gabriel Fonlladosa & Gwenn Meurrens, *Digital Freedoms in French-speaking African Countries* (Agence Française de Développement, May 2023), https://www.afd.fr/en/ressources/digital-freedoms-french-speaking-african-countries.

50 Internet Legislation Atlas: Tunisia, https://internetlegislationatlas.org/#/countries/Tunisia/frameworks/content-regulation (accessed June 13, 2024).

51 "Tunisia: Counterterror Law Endangers Rights", Human Rights Watch, July 31, 2015, https://www.hrw.org/news/2015/07/31/tunisia-counterterror-law-endangers-rights.

52 Sarah Yerkes and Maha Alhomoud, "One Year Later, Tunisia's President Has Reversed Nearly a Decade of Democratic Gains", Carnegie Endowment for National Peace, July 22, 2022, https://carnegieendowment.org/posts/2022/07/one-year-later-tunisias-president-has-reversed-nearly-a-decade-of-democratic-gains?lang=en.

53 ARTICLE 19, Tunisia: Decree-law No 54 of 2022 (ARTICLE 19, January 2023), https://www.article19.org/wp-content/uploads/2023/03/Analysis-of-decree-law-54-English.pdf.

54 Aymen Zaghdoudi, "A new blow to freedom of expression in Tunisia", Access Now, March 28, 2023, https://www.accessnow.org/a-new-blow-to-freedom-of-expression-in-tunisia/; "Tunisia: Cybercrime Decree Used Against Critics", Human Rights Watch, December 19, 2023, https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics.

55 "Tunisia court sentences TV pundits to prison for critical political commentary", France 24, May 22, 2024, https://www.france24.com/en/africa/20240522-tunisia-court-sentences-tv-pundits-to-prison-for-critical-commentary.

56 Aymen Zaghdoudi, "A new blow to freedom of expression in Tunisia".

57 "Tunisia: 57 lawmakers demand amending law used to detain journalists", Middle East Monitor, May 30, 2024, https://www.middleeastmonitor.com/20240530-tunisia-57-lawmakers-demand-amending-law-used-to-detain-journalists/

58 "Morocco: Draft criminal law to penalize social media users", IFEX, July 5, 2023, https://ifex.org/morocco-draft-criminal-law-to-penalize-social-media-users/.

59 "Communiqué de presse du Ministère de la Justice et des Droits de l'Homme : Révision de la loi portant répression de la cybercriminalité au Niger", Le Sahel, June 13, 2024, https://www.lesahel.org/communique-de-presse-du-ministere-de-la-justice-et-des-droits-de-lhomme-revision-de-la-loi-portant-repression-de-la-cybercriminalite-au-niger/.

60 "Prison time and fines for 'fake news' social media posts in South Africa withdrawn", Business Tech, April 26, 2024, https://businesstech.co.za/news/lifestyle/769751/prison-time-and-fines-for-fake-news-social-media-posts-in-south-africa-withdrawn/.

61 UNHRC, General Comment No. 34, para. 38.

62 U.S. Department of State, "2023 Country Reports on Human Rights Practices: Angola", https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/angola/ (accessed June 14, 2024).

63 "Iran Arrests Dissidents for Reaction to President Raisi's Death", Iran International, May 26, 2024, https://www.iran-intl.com/en/202405266108.

64 "Tunisia: Cybercrime Decree Used Against Critics", Human Rights Watch, December 19, 2023, https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics.

65 "Freedom on the Net: Türkiye", Freedom House, 2023, https://freedomhouse.org/country/Türkiye/freedom-net/2023#C.

66 "Freedom on the Net: Zambia", Freedom House, 2023, https://freedomhouse.org/country/zambia/freedom-net/2023#C.

67 "Zambia: Opposition Figure Sentenced for 'Defaming President", Human Rights Watch, May 23, 2024, https://www.hrw.org/news/2024/05/23/zambia-opposition-figure-sentenced-defaming-president.

68 "Freedom on the Net: Saudi Arabia", Freedom House, 2023, https://freedomhouse.org/country/saudi-arabia/freedom-net/2023#C

69 "Saudi Arabia: Assault on Online Expression",Human Rights Watch, 22 November, 2014, https://www.hrw.org/news/2014/11/22/saudi-arabia-assault-online-expression

70 "Saudi Arabia: New terrorism law is latest tool to crush peaceful expression", Amnesty International, February 3, 2014, https://www.amnesty.org/en/latest/news/2014/02/saudi-arabia-new-terrorism-law-one-more-tool-crush-peaceful-protest/

71 Ibid.

72 "Saudi Arabia must reform 'unacceptably broad' counter-terrorism law – UN rights expert", UN News, May 5, 2017, https://news.un.org/en/story/2017/05/556742#:~:text=%E2%80%9CI%20am%20concerned%20about%20the,Rapporteur%20on%20human%20rights%20and

73 "Saudi Arabia: New Counterterrorism Law Enables Abuse", Human Rights Watch, November 23, 2017, https://www.hrw.org/news/2017/11/23/saudi-arabia-new-counterterrorism-law-enables-abuse

74 Ibid.

75 "Saudi Arabia: US citizen jailed for 16 years over tweets was tortured, says son", Middle East Eye, October 18, 2022, https://www.middleeasteye.net/news/saudi-arabia-us-citizen-jailed-tweets-tortured-son

76 Saudi Arabia: Man Sentenced to Death for Tweets, Human Rights Watch, August 29, 2023, https://www.hrw.org/news/2023/08/29/saudi-arabia-man-sentenced-death-tweets

77 Stephanie Kirchgaessner, "Saudi Arabia jails alleged satirist 'identified in Twitter infiltration'", The Guardian, April 8, 2021 https://www.theguardian.com/world/2021/apr/09/saudi-arabia-jails-alleged-satirist-identified-in-twitter-infiltration

78 ALQST For Human Rights (@ALQST_En), "On 20 November 2023, #Saudi authorities arrested Yemeni man Fahad Ramadan while visiting the country, after private @WhatsApp messages of him criticising the Crown Prince were leaked," Tweet, January 30, 2024, https://x.com/ALQST_En/status/1752365273745629662

79 "Saudi Arabia: Alarming crackdown on online expression", Amnesty International, February 14, 2023, https://www.amnesty.org/en/latest/news/2023/02/saudi-arabia-alarming-crackdown-on-online-expression/; "Saudi Arabia: Woman jailed for 11 years for online expression supporting women's rights", Amnesty International, April 30, 2024, https://www.amnesty.org/en/latest/news/2024/04/saudi-arabia-woman-jailed-for-11-years-for-online-expression-supporting-womens-rights/

80 "Freedom on the Net: Saudi Arabia", Freedom House, 2023

81 Rasha Younes, All this Terror Because of a Photo (Human Rights Watch, 2023), https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt; Afsaneh Rigot, "Egypt's Dangerous New Strategy for Criminalizing Queerness", Slate, December 30, 2020, https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html

82 Ahmed Shihab-Eldin, "How Egyptian police hunt LGBT people on dating apps", BBC, January 30, 2023, https://www.bbc.co.uk/news/world-middle-east-64390817

83 "Iran: Death sentences for LGBTQI activists must be immediately overturned", ARTICLE 19, September 8, 2022, https://www.article19.org/resources/iran-overturn-death-sentences-for-lgbtqi-persons/

84 "Freedom on the Net: Kenya", Freedom House, 2023, https://freedomhouse.org/country/kenya/freedom-net/2023#B

85 Ibid.

86 "Letter Re: Arrests and Convictions Under Oman's 2018 Penal Code", Human Rights Watch, July 13, 2020, https://www.hrw.org/news/2020/07/13/letter-re-arrests-and-convictions-under-omans-2018-penal-code

87 Edrine Wanyama, "Uganda Passes Regressive Law on "Misuse of Social Media" and Hate Speech", CIPESA, September 12, 2022, https://cipesa.org/2022/09/uganda-passes-regressive-law-on-misuse-of-social-media-and-hate-speech/

88 ARTICLE 19, Uganda: Communications Regulatory Authority Bill, 2012 (ARTICLE 19, 2018), https://www.article19.org/data/files/medialibrary/3048/12-04-18-LA-uganda.pdf

89 "Uganda: UN experts condemn egregious anti-LGBT legislation", UN News, March 29, 2023, https://www.ohchr.org/en/press-releases/2023/03/uganda-un-experts-condemn-egregious-anti-lgbt-legislation.

90 "Ghana: President Should Veto Anti-LGBT Bill", Human Rights Watch, March 5, 2024, https://www.hrw.org/news/2024/03/05/ghana-president-should-veto-anti-lgbt-bill

91 In Ghana, under the Offences Against the Person Act of 1861; in Uganda, under the Penal Code in 1950.

92 Mohammed Elnaiem, "The 'Deviant' African Genders That Colonialism Condemned", JSTOR Daily, April 29, 2021, https://daily.jstor.org/the-deviant-african-genders-that-colonialism-condemned/; Jeanette M. Sebaeng, Seepaneng S. Moloko-Phiri, Ramadimetja S. Mogale, and Azwihangwisi H. Mavhandu-Mudzusi, "Same-sex intimate relationships and marriages among African indigenous people", *Working with indigenous knowledge: Strategies for health professionals* (2022, Fhumulani Mavis Mulaudzi and Rachel Lebese): Chapter 11, https://www.ncbi.nlm.nih.gov/books/NBK601357/.

93 Bahar Makooi, "Egypt's female social media influencers face arrest, jail on 'morality' charges", France 24, April 11, 2023, https://www.france24.com/en/middle-east/20230411-egypt-s-female-social-media-influencers-face-arrest-jail-on-morality-charges

94 Sara Monetta, "Israeli Arabs arrested over Gaza social media posts", BBC, October 21, 2023, https://www.bbc.co.uk/news/world-middle-east-67181582

95 "World Report 2022: Kuwait", Human Rights Watch, 2022, https://www.hrw.org/world-report/2022/country-chapters/kuwait

96 "Libya: Concern for members of the Tanweer Movement", Humanists International, March 16, 2022, https://humanists.international/2022/03/libya-concern-for-members-of-the-tanweer-movement/

97 "Freedom on the Net: Türkiye", Freedom House, 2023.

98 "Freedom Of Expression Online In Iraq", Tech4Peace, 16 June 2023, https://t4p.co/blog/2023-06-16-freedom-of-expression-online-in-iraq?lang=en

99 Dana Taib Menmy, "Iraq blocks at least 400 pornographic websites", The New Arab, November 8, 2022, https://www.newarab.com/news/iraq-blocks-pornographic-websites

100 "AlHudood Blocked in Iraq for "Unknown" Reasons", SMEX, February 28, 2024, https://smex.org/alhudood-blocked-in-iraq-for-unknown-reasons/

101 Safaa Ayyad, "Iraq's Controversial "Ballegh" Platform for 'Combating Indecent Content'", SMEX, February 15, 2023, https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content/

102 Ibid.

103 Dina Temple-Raston, "Crowdsourcing morality: How an app allows the Iraqi government to arrest 'indecent' influencers", The World, May 5, 2023, https://theworld.org/stories/2023/05/05/crowdsourcing-morality-how-app-al-

lows-iraqi-government-arrest-indecent

104 Shadi Sadr, "Iran's Hijab and Chastity Bill Underscores the Need to Codify Gender Apartheid", Just Security, April 11, 2024, https://www.justsecurity.org/94504/iran-hijab-bill-gender-apartheid/.

105 "Kenya's anti-gay bill proposes 50-year jail term", AfricaNews, September 20, 2023, https://www.africanews.com/2023/09/20/kenyas-anti-gay-bill-proposes-50-year-jail-term/.

106 "Saudi Arabia: Manifesto for Repression: Saudi Arabia's Forthcoming Penal Code Must Uphold Human Rights in Line with International Law and Standards", Amnesty International, March 19, 2024, https://www.amnesty.org/en/documents/mde23/7783/2024/en/#:~:text=The%20draft%20code%20criminalizes%20acts,forms%20of%20gender%2Dbased%20violence.

107 Daphne Keller, "Empirical Evidence of 'Over-Removal' by Internet Companies under Intermediary Liability Laws", The Center for Internet and Society, October 12, 2015, https://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws (accessed June 17, 2024).

108 Mays Ibrahim Mustafa, "Jordan devising Arab social media strategy", Jordan Times, March 19, 2023, https://jordantimes.com/news/local/jordan-devising-arab-social-media-strategy-%E2%80%94-shboul.

109 "Information Minister chairs 54th session of Council of Arab Ministers of Information," Bahrain News Agency, https://www.bna.bh/en/InformationMinisterchairs54thsessionofCouncilofArabMinistersofInformation.aspx?cms=q8FmFJgiscL2fwIzON1%2BDmnPNofPmCzCmCLXqnUFQFM%3D.

110 "Iran: Parliament's "Protection Bill" will hand over complete control of the Internet to authorities", ARTICLE 19, August 5, 2021, https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/

111 Ibid.

112 Dina Taib Menmy, "Iraq's Ministry of Communications calls for ban on TikTok, citing concerns over social unity", The New Arab, March 28, 2024, https://www.newarab.com/news/iraqi-communications-ministry-urges-government-ban-tiktok.

113 "Iraq: Drop draft digital content legislation and protect free speech online", ARTICLE 19, March 16, 2023, https://www.article19.org/resources/iraq-drop-draft-digital-content-legislation-protect-free-speech-online/

114 "Twitter agrees to Nigeria's demands to end seven-month ban", BBC, January 13, 2022, https://www.bbc.co.uk/news/world-africa-59958417.

115 National Information Technology Development Agency of Nigeria, Approved Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, September 2022, https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf.

116 "An Open Call to NITDA to Review the Updated Code of Practice", Paradigm Initiative, October 21, 2022, https://paradigmhq.org/an-open-call-to-nitda-to-review-the-updated-code-of-practice/.

117 Rwanda, *Ministerial Instructions N° 001/Minict/2024 of 22/03/2012 On Child Online Protection*, 2024, https://www.minijust.gov.rw/index.php?eID=dumpFile&t=f&f=91546&token=d5eb7096a06042554606ab1c4fac9b87b9de3c2e

118 Kemal Kirişci and Amanda Sloat, The rise and fall of liberal democracy in Turkey: Implications for the West (Brookings, 2019), https://www.brookings.edu/articles/the-rise-and-fall-of-liberal-democracy-in-Türkiye-implications-for-the-west/

119 Full name: Law Regulating publications on the internet and suppression of crimes committed by means of such publication.

120 European Commission, Commission Staff Working Document: Türkiye 2022 Report, 2022, https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf

121 "Turkey: ARTICLE 19 tells European Court that terrorist conviction for merely 'liking' content on Facebook is disproportionate", ARTICLE 19, July 1, 2020, https://www.article19.org/resources/Türkiye-ozdemir-ecthr-third-party-submission/

122 "Turkish government banned access to 137,000 websites in 2022", Duvar English, July 24, 2023, https://www.duvarenglish.com/turkish-government-banned-access-to-712000-websites-in-2022-news-62782; "Turkey: Dangerous, dystopian new legal amendments", ARTICLE 19, October 14, 2022, https://www.article19.org/resources/Türkiye-dangerous-dystopian-new-legal-amendments/

123 "Turkey: New Internet law threatens freedom of expression online", ARTICLE 19, July 28, 2020, https://www.article19.org/resources/Türkiye-new-internet-law-threatens-freedom-of-expression-online/

124 "Turkey: YouTube Precedent Threatens Free Expression" ARTICLE 19, December 18, 2020, https://www.article19.org/resources/Türkiye-youtube-precedent-threat-

ens-free-expression/

125 "Turkey: Dangerous, dystopian new legal amendments", ARTICLE 19,

126 "Turkey: Threats to the online environment during elections", ARTICLE 19, May 10, 2023, https://www.article19.org/resources/Türkiye-q-a-on-threats-to-the-online-environment-during-elections/#_Toc134065370

127 "Content Alleged to Violate Turkish Law", Meta Transparency Centre, in "Content Restrictions based on Local Law: Case Studies," Jan-Jul 2023, available at https://transparency.meta.com/reports/content-restrictions/case-studies/ (accessed 17 June 2024).

128 "Guinée Équatoriale: Analyse du Projet Loi Régulant l'Utilisation des Réseaux Sociaux et du Cyberespace" ("Equatorial Guinea: Analysis of the Draft Law Regulating the Use of Social Networks and Cyberspace"), Japap, March 24, 2024.

129 Insight from local experts.

130 Aymen Zaghdoudi, "In Saudi Arabia, no safe harbor for free speech", Access Now, February 29, 2024, https://www.accessnow.org/profile/aymen/.

131 Council of Europe Cybercrime Convention Committee, *The Budapest Convention on Cybercrime: benefits and impact in practice* (Council of Europe, 2020), https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

132 Civic Space Incidents Database, https://closingspaces.org/, accessed Jun 27 2024.

133 Georgetown University Law Center Global Law Scholars, "Digital Authoritarianism and Disinformation Laws in the Middle East and North Africa", p.37

134 A coalition formed in Baghdad to defend freedom of expression", Shafaq, 12 February 2024, https://shafaq.com/en/Iraq/A-coalition-formed-in-Baghdad-to-defend-freedom-of-expression

135 "Letter to the United Nations on Effective Civil Society Participation", Electronic Frontier Foundation, July 20, 2022, https://www.eff.org/deeplinks/2022/07/letter-united-nations-inclusive-civil-society-participation.

136 "Our members", Global Alliance of National Human Rights Institutions, https://ganhri.org/membership/ (accessed June 14, 2024)

137 Global Alliance of National Human Rights Institutions, *GANHRI Statement on Business and Human Rights: the role and experiences of NHRIs* (adopted 8 May 2024), https://ganhri.org/nhris-to-redouble-efforts-on-business-and-human-rights/

138 AU Special Rapporteur on Freedom of Expression and Access to Information in Africa, Inter-session activity report (presented during the 79th Ordinary Session, African Commission on Human and Peoples' Rights, Banjul, The Gambia), May 10, 2024, https://achpr.au.int/en/intersession-activity-reports/freedom-expression-access-information

139 Communications by the Special Rapporteur on freedom of opinion and expression, OHCHR, https://spcommreports.ohchr.org/TmSearch/Mandates?m=24, accessed Jun 27, 2024.

140 "UN: Saudi Arabia must not host 2024 Internet Governance Forum", ARTICLE 19, October 12, 2023, https://www.article19.org/resources/un-saudi-arabia-must-not-host-2024-internet-governance-forum/; "Statement from Paradigm Initiative: Participating in the Internet Governance Forum in Saudi Arabia", Paradigm Initiative, May 7, 2024, https://paradigmhq.org/statement-from-paradigm-initiative-participating-in-the-internet-governance-forum-in-saudi-arabia/

141 Thomas Naadi and Gianluca Avagnina, "Ghana's finance ministry urges president not to sign anti-LGBTQ+ bill", BBC, March 4, 2024, https://www.bbc.co.uk/news/world-africa-68469613.

142 Cengiz and Others v Turkey, App nos. 48226/10 and 14027/11 (European Court of Human Rights, 4 May 2016).

143 "ECOWAS Court victory: Twitter ban in Nigeria declared unlawful", Access Now, July 14, 2022, https://www.accessnow.org/press-release/ecowas-court-nigeria-unlawful-twitter-ban.

144 Thomas Mackintosh & Mercy Juma, "World Bank halts new Uganda loans over anti-LGBTQ+ law", BBC, August 9, 2023, https://www.bbc.co.uk/news/world-africa-66453098

145 Maria Paz Canales, "The final text of UNESCO's Guidelines: a more balanced approach to platform governance", Global Partners Digital, December 5, 2023, https://www.gp-digital.org/the-final-text-of-unescos-guidelines-a-more-balanced-approach-to-platform-governance/

146 5Rights Foundation, Pathways: How digital design puts children at risk (5Rights Foundation, 2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

147 Global Partners Digital, Assessing Cybercrime Laws and NCSS from a Human Rights Perspective (Global Partners Digital, 2022), https://www.gp-digital.org/publication/assessing-cybercrime-laws-from-a-human-rights-perspective/

148 "Commonwealth workshops train 150 African judges in handling cybercrime cases", The Commonwealth, November 15, 2023, https://thecommonwealth.org/news/commonwealth-workshops-train-150-african-judges-handling-cybercrime-cases

149 UNESCO, *Guidelines for the governance of digital platforms*, pp. 30-31.