

Fear Is the Power That Can Do Anything

Digital Authoritarianism in
Egypt, Iraq, and Tunisia

The Phoenix Project
2026



Table of Content

Summary

I. Overview of Legal Architecture of Digital Control in Egypt, Iraq, and Tunisia

A. Egypt

- Legal Architecture Governing Digital Speech and Activities

- Legal Architecture Governing the Day-to-Day Activities of Digital Rights Organizations

- Impact on Digital Rights Organizations

- Online State-Backed Harassment of Digital Rights Groups and Activists

B. Iraq/Kurdistan Region of Iraq (KRI)

- Legal Architecture Governing Digital Speech and Activities

 - Kurdistan Region of Iraq

- Legal Architecture Governing the Day-to-Day Activities of Digital Rights Organizations

 - Repeated Attempts to Enact a Cybercrime Law

- State Restrictions on Public Access to Websites and Applications

- Slow Digital Transformation in Iraq and the KRI

- Citizen Reporting and Public Morality

- Administrative and Financial Penalties for Civil Society Organizations

- Militias in the Iraqi Digital Landscape

C. Tunisia

- Legal Architecture Governing Digital Speech and Activities

- Legal Architecture Impacting Digital Rights Organizations' Day-to-Day Activities

- Targeting of Anti-Racist, Migrant and Refugee Rights Groups

II. Advocacy Strategies Employed by Digital Rights Groups in Egypt, Iraq and Tunisia

A. "Cause Lawyering": Offensive and Defensive Strategic Litigation

- Egypt

- Iraq/Kurdistan Region of Iraq (KRI)

- Tunisia

B. Deepening Government Relationships

C. Maintaining Low Profiles and Adopting Digital Security Measures

- Digital Security Precautions

- Self-Censoring Online

 - Speech about the Regional Escalation

- Physical Safety Precautions

 - Checkpoints

 - Office-Related Precautions



- D. Increasing Awareness of Digital Safety Practices, Media Literacy Campaigns, Fact-Checking
- E. Conducting and Publishing Research in Coalitions
- F. Engaging in Platform Accountability Efforts
 - Iraqi Digital Rights Organizations' Engagement with Platforms
 - Persistent Platform Gaps
 - Telegram
 - Content Moderation Efforts are not Language-Responsive
 - Artificial Intelligence, Disinformation, and Platform Responsibility

III. Constraints on Digital Rights Groups Across Egypt, Iraq and Tunisia

- A. Mental Health Struggles
- B. Weak Institutionalization of Digital Security Practices
- C. Low Public Trust Undermining Efficacy
- D. Struggles with Regional Coordination
- E. Challenges in Fundraising
 - Global Funding Squeeze
 - Organizations Struggle to Fundraise for Themselves and Funder Affiliations Put Them at Risk
 - Funding as a Moral and Political Choice

IV. Recommendations

- To All Rights and Civil Society Organizations
- To Donors Who Fund Digital Civil Society Organizations and Initiatives
- To Social Media Companies
- To the Government of Egypt
- To the Federal Government of Iraq and the Kurdistan Regional Government
- To the Government of Tunisia
- To The Governments of Egypt, Tunisia, and Iraq
- To the Public

Methodology

Acknowledgements



Summary

Digital authoritarianism in Southwest Asia and North Africa (SWANA) no longer operates through isolated acts of internet censorship or surveillance. Governments increasingly combine the use of telecommunications infrastructure, vague criminal and counterterrorism laws, media regulations, financial investigations, online smear campaigns, and pressure on technology companies to regulate public life both online and offline. Repressive practices that once appeared exceptional have become normalized. Governments continue to expand their legal and technical capacity to surveil, intimidate, and punish critics.

This report examines how digital authoritarianism affects digital rights organizations and civil society writ large in Egypt, Iraq, and Tunisia. It draws on interviews and written correspondence with 20 civil society representatives, journalists, researchers, lawyers, and digital rights experts alongside a review of relevant laws, government policies, media reporting, and research by digital rights and human rights organizations. Seven interviewees focused on Iraq and the Kurdistan Region of Iraq (KRI), six on Egypt, four on Tunisia, and three on wider SWANA regional trends.

The three countries present distinct configurations of digital control. Egypt offers one of the region's most centralized and institutionally integrated models. Since the military takeover led by Abdel Fattah al-Sisi in 2013, Egyptian authorities integrated the country's legal, telecommunications, media regulatory, and security institutions into an apparatus capable of monitoring online activity, restricting communications, blocking websites, prosecuting peaceful speech, and targeting critics in and outside the country.

Egyptian authorities also built a legal enclosure around civil society itself. The 2019 NGO law restricts research, surveys, partnerships, registration, and foreign funding while allowing authorities to dissolve organizations, freeze assets, and prosecute staff. Security agencies compound these restrictions through arrests, office raids, travel bans, and long-running legal cases against civil society actors. Egypt once had hundreds of independent organizations and rights groups. Today, only a fraction remains, and many of the country's most experienced advocates now work from exile. Those that remain often keep a low profile and rely primarily on defensive litigation to protect individuals and preserve small openings for rights-based work.

Tunisia represents a later but rapidly accelerating version of this trajectory. Interviewees identified President Kais Saied's 2021 consolidation of power as the key inflection point in the country's downward spiral. The civic and media freedoms that followed the 2011 revolution have steadily eroded as Saied weakened parliament, concentrated executive power, and deployed overlapping



criminal, financial, and administrative tools against peaceful critics. Decree-Law 54 of 2022 has become the most consequential instrument in Tunisia's digital crackdown. Authorities use its vague prohibitions on false information and online harm to prosecute peaceful speech, often alongside counterterrorism, financial-crimes, or money-laundering charges. These procedures drain staff time and push organizations into defensive survival mode. One interviewee described the developments in Tunisia as following the same "blueprint" that Egypt established between 2013 and 2019. This report does not find evidence that Egyptian and Tunisian authorities consciously coordinated their approaches or that one government directly influenced the other. It does, however, find an observable convergence.

Iraq presents a different configuration shaped by decades of war, occupation, political fragmentation, and the influence of armed groups. Digital authoritarianism operates through three overlapping centers of authority: the federal government in Baghdad, the Kurdistan Regional Government, and militias or other armed and party-aligned actors. This fragmentation gives some Iraqi and Kurdish organizations more operational room, but it does not make the digital environment safe. Pressure often falls unevenly on individual civil society workers rather than entire organizations. Authorities and armed groups target individuals through criminal cases, online harassment, or physical violence. Organizations may remain legally registered while their staff censor themselves or avoid work involving corruption, militias, gender, sexuality, or senior political figures. Outdated penal, counterterrorism, and telecommunications laws give authorities wide discretion to punish online expression while providing inadequate remedies for genuine digital harms.

Despite these differences, the three country cases reveal a common logic. Authorities use vague and overbroad concepts such as national security, terrorism, public order, family values, social stability, and foreign interference to create an environment in which almost any online activity can become criminal. These terms allow officials to treat criticism as a threat, recast human rights advocacy as a foreign agenda, and portray women, LGBTQ+ people, migrants, refugees, journalists, and activists as sources of moral or social disorder.

These narratives do not remain confined to official rhetoric. They are often amplified by "digital mobs" – networks of pro-government, partisan, or self-appointed users who harass critics and direct public anger toward vulnerable or marginalized groups. Economic insecurity helps make these tactics effective. Across the three countries, political actors and online campaigns exploit poverty, unemployment, and declining economic mobility to redirect frustration toward women, refugees, migrants, LGBTQ+ people, and other marginalized communities rather than toward state failures. Digital mobs do more than harass individual critics, they can help build public support for broader repression.



The uncertainty created by these laws serves an important political function. Governments do not need to prohibit every form of conduct in advance. They can decide retrospectively which posts, comments, videos, research projects, funding relationships, or organizational activities deserve punishment. Individuals and organizations must therefore anticipate how officials, judges, security agents, political parties, armed groups, or members of the public might interpret their conduct. Fear becomes a form of governance. As “Diyar,” an Iraqi human rights expert said, “Fear is the power that can do anything.”

Digital repression frequently moves into the physical realm. Online smear campaigns often precede arrests, office raids, financial investigations, and prosecutions. Doxxing exposes activists to violent assaults or assassination. Police and security agents search phones at checkpoints and detain people based on content found. Journalists and rights defenders face travel bans, asset freezes, years of pretrial detention, threats against their families, and pressure to leave their countries. Several people interviewed for this report now live in self-exile because remaining at home became too dangerous.

Artificial intelligence (AI) intensifies these risks by enabling an environment flooded with manipulated images, deepfakes, AI-generated sexualized content, and false political material to spread faster than civil society organizations can document or verify them. At the same time, Egypt, Iraq, and Tunisia lack clear, rights-respecting frameworks for addressing these harms without expanding state control over peaceful online expression.

Social media companies play a central role in this environment. They do not simply host the speech, harassment, and disinformation documented in this report. Their policies help determine what users can say, which content remains available, which government requests receive compliance, and whose reports of abuse result in action. Civil society organizations’ ability to influence these companies has narrowed over the past decade. In the SWANA region, content moderation failures are more pronounced in Arabic dialects and the Kurdish language.

Digital rights organizations use several strategies to navigate these conditions. Lawyers pursue criminal defense and, where possible, strategic litigation. Organizations document prosecutions, train lawyers, conduct security audits, operate emergency helpdesks, publish research through coalitions, educate the public, and engage selected government officials and platform representatives. These strategies differ according to the available legal and political space.

Direct engagement with governments generally offers limited results. Outcomes often depend on the personal interest and risk tolerance of an individual official. Both officials and civil society organizations frequently deny these relationships publicly because of the dangers associated with them. In Iraq, government cooperation has produced some progress on discrete issues such as violence



against women, but politically sensitive topics such as geoblocking remain far harder to address.

Organizations undertake this work amidst a severe funding and capacity crisis. The 2025 cuts to United States foreign assistance and democracy and human rights programs abruptly ended projects, social services, and employment across the SWANA region. European donors fill only part of the gap, often through smaller and more restrictive grants that require organizations to reshape their priorities around donor interests. Foreign funding can also expose organizations to legal investigations and smear campaigns.

These conditions impose a profound human cost. Interviewees described burnout, anxiety, depression, second-hand trauma, and a persistent fear of arrest, attack, or retaliation against themselves or family members. Staff supporting survivors of blackmail, trafficking, harassment, and online violence absorb repeated accounts of severe abuse while receiving limited mental health support themselves. The research also identified the paradox that people who understand surveillance and digital threats often maintain inconsistent digital hygiene practices themselves.

The interviews nevertheless reveal continued resilience. Civil society organizations continue to litigate, document abuses, train lawyers, support survivors, engage platforms, develop local-language tools, and build coalitions despite immense pressure. They secure the removal of life-threatening content, challenge abusive laws, protect individuals facing prosecution, and preserve public access to digital safety resources. These successes, however, remain fragile. Litigation requires independent lawyers, usable laws, and courts willing to provide remedies. Emergency response programs require trained staff and sustained funding. Platform accountability requires companies to invest in local expertise and maintain reliable channels for civil society engagement. Regional solidarity requires accessible, SWANA-based spaces that organizations can shape around their own priorities. All of this work also requires specialized mental health support for the people carrying it out.

Digital rights organizations cannot indefinitely compensate for failing state institutions, abusive security actors, weak platform safeguards, and inconsistent donor commitments. Meaningful support must strengthen their ability not only to respond to the next emergency, but also to build durable institutions, retain staff, protect sensitive information, and develop long-term strategies. The persistence of these organizations under extraordinary pressure offers reason for hope. Their survival, however, should not depend on resilience alone.



I. Overview of Legal Architecture of Digital Control in Egypt, Iraq, and Tunisia

A. Egypt

Egypt presents one of the most consolidated cases of digital authoritarianism in the SWANA region. Based on six interviews with digital rights activists, civil society representatives, and a lawyer, SMEX found that over the last two decades (and particularly after Abdel Fattah al-Sisi's 2013 military takeover), Egyptian authorities constructed a system of infrastructural, legal, and security mechanisms that work in lockstep to give the state near-total control over the country's digital environment and the ability to threaten its dissidents living abroad. The threat of repression spares no one, including human rights defenders, lawyers, journalists, social media personalities, and television show hosts.¹

Digital rights organizations operating in this highly repressive environment face well-documented patterns of heightened legal risk, harassment, surveillance, and financial strangulation, while interviewees described severe personal repercussions from government targeting, including self-exile, mental health struggles, and economic hardship discussed further below.

Gender and sexuality cut across Egypt's digital repression, shaping both who authorities target online and which advocacy groups face the greatest risks for supporting them.² Women, girls, and LGBTQ+ people face disproportionate targeting by state officials who monitor social media in the name of upholding "public values," while also facing harassment, abuse, and doxxing by private actors online.³ Likewise, digital rights groups and activists serving LGBTQ+ people,

¹ Human Rights Watch, "Egypt: Rights Defender Charged with Terrorism," January 22, 2025, <https://www.hrw.org/news/2025/01/22/egypt-rights-defender-charged-terrorism>; Human Rights Watch, "Of Egyptian Prisons and Exile: a Story of Separation," March 24, 2026, <https://www.hrw.org/news/2026/03/24/of-egyptian-prisons-and-exile-a-story-of-separation>; Human Rights Watch, "Egypt Journalist Detained Over Facebook Posts," October 8, 2025, <https://www.hrw.org/news/2025/10/08/egypt-journalist-detained-over-facebook-posts>; Human Rights Watch, "Egypt Mass Crackdown Targets Online Content Creators," September 10, 2025, <https://www.hrw.org/news/2025/09/10/egypt-mass-crackdown-targets-online-content-creators>; Human Rights Watch, "Egypt's LGBT Crackdown Expands Stifle Journalists," January 25, 2019, <https://www.hrw.org/news/2019/01/25/egypts-lgbt-crackdown-expands-stifle-journalists>.

² BBC News, YouTube, "How Egyptian police hunt LGBT people on dating apps - BBC News," January 31, 2023, https://www.youtube.com/watch?v=CEM_LRpeifs.

³ Berkman Klein Center for Internet & Society, "Digital Crime Scenes," 2022, <https://cyber.harvard.edu/publication/2022/digital-crime-scenes>; ARTICLE 19, "Queer Resistance to Digital Oppression," <https://www.article19.org/queer-resistance-to-digital-oppression/>; Human Rights Watch, "All This Terror Because of A Photo: Digital Targeting and Its Offline Consequences," February 21, 2023, <https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt>; Speak Up, "Reality of Cyberbullying and Blackmail Crimes in Egypt," March 25, 2024, <https://speakuppeg.com/2024/03/25/reality-of-cyberbullying-and-blackmail-crimes-in-egypt/>; Asmaa Fathy, SMEX, "Egypt Online Violence Against Women on the Rise," January 30, 2024, <https://smex.org/egypt-online-violence-against-women-on-the-rise/>; SMEX, "Doxxing of Residential Information Targeting Vulnerable Groups: Online and Offline Harms," February 8, 2022,

migrants and refugees, and other marginalized communities must often work quietly or risk exposing the very people they support - or themselves - to further harm.⁴

Among the three countries examined in this report, Egypt's system of digital control is the most centralized, creating the most restrictive and challenging legal environment for the digital rights organizations interviewed. This does not necessarily reflect a more technically advanced legal system, but rather a more established and integrated one. This finding builds on a substantial body of research by rights groups documenting how Egypt's authorities draw on an overlapping set of laws, each extending state power into a different dimension of online life.⁵ "Fareid," an Egyptian digital rights expert, characterized the government's approach as increasingly "preemptive," as authorities criminalize conduct that might facilitate criticism or popular mobilization before it can gain traction.⁶ "Hassan," another Egyptian digital rights expert, summarized the approach bluntly: "the default is to criminalize everything."⁷

The 2018 Press, Media, and Supreme Council for Media Regulation (SCMR) Law constitutes one of the central pillars of this legal architecture.⁸ The cybercrime, counterterrorism, and telecommunications laws make up the other major levers at the government's disposal to exert control over digital spaces.

The 2018 SCMR law does not distinguish between print and online content and treats personal websites, blogs, and social media accounts with 5,000 or more followers as "media outlets," sweeping ordinary individuals into a framework built

<https://smex.org/report-doxxing-of-residential-information-targeting-vulnerable-groups-online-and-offline-harms/>.

⁴ Human Rights Watch, "Egypt Security Forces Abuse Torture LGBT People," October 1, 2020, <https://www.hrw.org/news/2020/10/01/egypt-security-forces-abuse-torture-lgbt-people>; Human Rights Watch, "Egypt Police Target Sudanese Refugee Activists," March 27, 2022, <https://www.hrw.org/news/2022/03/27/egypt-police-target-sudanese-refugee-activists>.

⁵ SMEX phone interview with "Fareid," May 14, 2026; Egyptian Initiative for Personal Rights report, "Virtual Freedom: Towards Ending the Cybercrime Law's Repression of Online Freedom of Expression in Egypt," September 2, 2025, <https://eipr.org/en/publications/virtual-freedom-towards-ending-cybercrime-laws-repression-online-freedom-expression>; Association for Freedom of Thought and Expression, "The Internet and the Law in Egypt Series (Second Part: Digital media)" August 19, 2021, <https://afteegypt.org/wp-content/uploads/2021/08/The-Internet-and-the-Law-in-Egypt-Series-Second-Part-Digital-media.pdf>.

⁶ SMEX phone interview with "Fareid," May 14, 2026.

⁷ SMEX phone interview with "Hassan," April 17, 2026.

⁸ ARTICLE 19, "Egypt: 2018 Law on the Organisation of Press, Media, and the Supreme Council of Media: Legal analysis," March 18, 2019, <https://www.article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-Final-Nov-2018.pdf>; Rana Mamdouh, Mada Masr, "Egypt's New Media Laws: Rearranging Legislative Building Blocks to Maximize Control," July 17, 2018, <https://www.madamasr.com/en/2018/07/17/feature/politics/egypts-new-media-laws-rearranging-legislative-building-blocks-to-maximize-control>.



for media organizations.⁹ The law also empowers the regulating body – the SCMR – to block or disrupt websites and halt publication of print media without judicial authorization, including over vague “national security concerns.” The SCMR lacks meaningful independence from the executive.¹⁰

The 2018 Cybercrime Law complements the SCMR Law by imposing its own criminal penalties and a parallel website blocking mechanism.¹¹ Article 7 authorizes the blocking of websites that threaten national security or the national economy, while article 25 criminalizes content that violates the “family principles or values of Egyptian society.” Judges and prosecutors retain wide discretion to interpret these terms.¹² Together, the two 2018 laws legitimized the already well-established practice of blocking independent media sites, including those belonging to rights groups.¹³ Over the last decade, authorities blocked hundreds of websites.¹⁴

The Telecommunications Law of 2003 defines national security expansively and gives authorities the ability to “commandeer telecommunication services and networks of any operator or service provider” with due cause.¹⁵ Egyptian judges extended the Telecommunications Law’s concept of national security further in 2013, when the Administrative Court interpreted the term as encompassing the vague notion of “social national security.”¹⁶ The ruling established a precedent for

⁹ ARTICLE 19, “Egypt: 2018 Law on the Organisation of Press, Media, and the Supreme Council of Media: Legal analysis,” March 18, 2019, <https://www.article19.org/wp-content/uploads/2019/03/Egypt-Law-analysis-Final-Nov-2018.pdf>; Tahrir Institute for Middle East Policy, “The Law Regulating the Press, Media, and the Supreme Council for Media Regulation,” May 15, 2019, <https://timep.org/wp-content/uploads/2018/12/SCMR-Law-5-15-2019-1.pdf>; Amnesty International, “Dozens of News Sites Blocked as Egypt Ramps Up Digital Censorship,” June 13, 2017, <https://www.amnesty.nl/actueel/dozens-of-news-sites-blocked-as-egypt-ramps-up-digital-censorship>.

¹⁰ Association for Freedom of Thought and Expression, “The Supreme Council for Media Regulation: A Reading into the competencies and practices,” April 22, 2019, <https://afteegypt.org/en/legislations-en/legislative-analysis-en/2019/04/22/17432-afteegypt.html>.

¹¹ Egypt Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, available <https://www.wipo.int/wipolex/en/legislation/details/19959>.

¹² Global Freedom of Expression Department at Columbia University, “The Case of the Egyptian TikTok Influencers,” n.d., <https://globalfreedomofexpression.columbia.edu/cases/the-tiktok-girls-case>.

¹³ Human Rights Watch, “Egypt Blocks Human Rights Watch Website,” September 7, 2017, <https://www.hrw.org/news/2017/09/07/egypt-blocks-human-rights-watch-website>; Reporters Without Borders, “RSF website blocked in Egypt,” August 17, 2017, <https://rsf.org/en/rsf-website-blocked-egypt>; Mai Amer, Arab Reform Initiative, “On the Egyptian State’s Policy of Blocking Websites,” January 27, 2025, <https://www.arab-reform.net/publication/on-the-egyptian-states-policy-of-blocking-websites/>.

¹⁴ Arab Network for Human Rights Information, “منظمات حقوقية تطالب السلطات المصرية بالتوقف عن ممارسة الرقابة على الإنترنت وحجب مواقع الويب,” November 4, 2020, <https://ifex.org/ar/human-rights-organizations-call-on-egypts-government-to-end-internet-censorship-and-website-blocking/>.

¹⁵ Article 67 of Egypt’s Telecommunications Law No. 10 of 2003, available <https://www.tra.gov.eg/wp-content/uploads/2020/11/Law-No-10-of-2003.pdf>; 2022 amendments to the Telecommunications Law No. 10 of 2003, available <https://www.eastlaws.com/legislation-full-text/ar/egypt/law/26-12-2022/no-172?type=1&id=2072930>; Freedom House, “Freedom on the Net 2024: Egypt,” <https://freedomhouse.org/country/egypt/freedom-net/2024>.

¹⁶ Masaar, “Blocking Websites in Egypt: ‘Techniques and Laws,’” May 2021, <https://masaar.net/wp-content/uploads/2021/05/Blocking-websites-in-Egypt-EN.pdf>.

using the law to restrict online content. The 2015 Counterterrorism Law reinforces this framework by defining terrorism widely and allowing authorities to apply “national security concerns” to a range of expression and conduct.¹⁷

The powers outlined in the Telecommunications Law extend beyond media regulation and into the everyday tools people use to communicate and protect their privacy, such as encryption tools and messaging platforms.¹⁸ The law restricts the use of encryption equipment without written authorization and gives authorities wide latitude to regulate telecommunications technologies, including tools used to circumvent blocking or secure digital communications.¹⁹ The National Telecommunications Regulatory Authority (NTRA) oversees the “implementation of licenses, permits, regulatory frameworks and resolutions.”²⁰ Like the SCMR, the NTRA lacks meaningful independence from the executive.²¹

These four laws are enforced through a broader institutional network that includes the SCMR, the NTRA, the National Security Agency (NSA), Public Prosecution, and courts. The NSA, a notoriously abusive branch of the interior ministry, oversees domestic security and plays a central role in cybercrime and counterterrorism efforts.²² “We’ve been seeing an ongoing consolidation and higher integration between Egypt’s telecom, legal, and security layers,” Hassan told SMEX.²³ “There are fewer points of contact within the government.” His comments capture how these institutions increasingly operate through overlapping channels of regulation, investigation, and prosecution.

This institutional convergence is reinforced by the centralization of telecommunications infrastructure, previously documented by SMEX.²⁴ Telecom

¹⁷ Counterterrorism Law No. 33 of 2019, available https://www.atlanticcouncil.org/wp-content/uploads/2015/09/Egypt_Anti-Terror_Law_Translation.pdf; Human Rights Watch, “Egypt: Counterterrorism Law Erodes Basic Rights,” August 19, 2015, <https://www.hrw.org/news/2015/08/19/egypt-counterterrorism-law-erodes-basic-rights>.

¹⁸ Masaar, “Amendments to the Telecommunications Law: New Restrictions on the Use and Operation of Telecommunications Equipment,” May 1, 2023, <https://masaar.net/en/amendments-to-the-telecommunications-law-new-restrictions-on-the-use-and-operation-of-telecommunications-equipment/>.

¹⁹ SMEX phone interview with “Fareid,” May 14, 2026; SMEX, “What is DPI Technology, and Why is Egypt Abusing It?” August 16, 2023, <https://smex.org/what-is-dpi-technology-and-why-is-egypt-abusing-it-2/>; Association for Freedom of Thought and Expression, “Internet without surveillance .. How can the Egyptian government end the policy of mass surveillance?” June 3, 2021, <https://afteegypt.org/en/research-en/policy-papers-en/2021/06/03/22766-afteegypt.html>; ARTICLE 19, “Egypt: Telecommunication Regulation Law,” April 2015, <https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report---English.pdf>.

²⁰ National Telecom Regulatory Authority, “Regulations,” n.d., <https://www.tra.gov.eg/en/regulations/>.

²¹ Association for Freedom of Thought and Expression, “The Internet and the Law in Egypt Series (First Part: Centralization of Telecommunications),” June 29, 2021, <https://afteegypt.org/en/legislations-en/legislative-analysis-en/2021/06/29/23250-afteegypt.html>.

²² Human Rights Watch, “Egypt: Apparent Extrajudicial Killings,” May 14, 2025, <https://www.hrw.org/news/2025/05/14/egypt-apparent-extrajudicial-killings>; Human Rights Watch, “Egypt: Spate of Free Speech Prosecutions,” August 29, 2024, <https://www.hrw.org/news/2024/08/29/egypt-spate-free-speech-prosecutions>.

²³ SMEX phone interview with “Hassan,” April 17, 2026.

²⁴ SMEX, “Produced, tested, deployed: The militarization of technology in the SWANA region,” July 15, 2026,

Egypt, a state-owned company, owns most of the country's telecommunications infrastructure.²⁵ Service providers such as Vodafone and Orange must rent access to this infrastructure, and the Telecommunications Law requires operators to provide national security bodies with the technical capabilities needed to access communications and user data.²⁶ The state can act unilaterally if private operators resist.²⁷ The contracts governing most of these arrangements are not public and there is little transparency regarding government data access requests. This dynamic places telecommunications companies in a dual bind: adhering to the government's requests may put them at risk of violating international human rights law, but if they do not, they risk their relationship with the Egyptian government, and by extension, their access to the Egyptian market.²⁸

These legal and institutional arrangements are reinforced by an ever-expanding surveillance apparatus fueled by monitoring systems and malware purchased from European companies – acquisitions that SMEX, Privacy International, and other rights groups have documented while emphasizing the opacity surrounding such transfers.²⁹ “There is a massive black hole [of information] when it comes to import and export of tech between Egypt and [Western countries],” Hassan said.³⁰ “Egyptian rights defenders are facing digital attacks and constant surveillance using Western technology that these countries would not deploy against their own citizens.” His comments reflect a broader concern among rights advocates that surveillance technologies subject to significant legal and regulatory safeguards in their countries of origin are often exported to

<https://smex.org/wp-content/uploads/2026/07/Militarization-of-tech-in-the-SWANA-region-Research.pdf>.

²⁵ Egypt Independent, “Newspaper: Army will control 60% of Egypt's national entity for telecommunications,” May 11, 2015,

https://www.egyptindependent.com/newspaper-army-will-control-60-egypt-s-national-entity-telecommunications/#google_vignette.

²⁶ Country Legal Frameworks Resource, “Egypt: Provision of Real-time Lawful Interception Assistance,” n.d., <https://clfr.globalnetworkinitiative.org/country/egypt/>.

²⁷ SMEX phone interview with “Hassan,” April 17, 2026 The Guardian, “Vodafone says Egyptian authorities forced it to send pro-Mubarak texts,” February 3, 2011,

<https://www.theguardian.com/world/2011/feb/03/vodafone-mubarak-text-messages>; Privacy

International, “State of Privacy in Egypt,” January 26, 2019,

<https://privacyinternational.org/state-privacy/1001/state-privacy-egypt>.

²⁸ Human Rights Watch, “Joint Open Letter to Social Media Companies on Censorship in Türkiye,” May 8, 2025,

<https://www.hrw.org/news/2025/05/08/joint-open-letter-social-media-companies-censorship-turkiye>;

Human Rights Watch, “Shutting Down the Internet to Shut Up Critics,” January 14, 2020,

<https://www.hrw.org/world-report/2020/country-chapters/global-5>.

²⁹ Yilmaz, Ihsan; Mamouri, Ali; Akbarzadeh, Shahram & Omer, Muhammad, “Authoritarian Diffusion in the Cyberspace: How Egypt Learns, Emulates, and Cooperates in Digital Authoritarianism,” European Center for Populism Studies (ECPS), May 9, 2025, <https://doi.org/10.55271/rp0097>; SMEX, “What is DPI Technology, and Why is Egypt Abusing It?” August 16, 2023,

<https://smex.org/what-is-dpi-technology-and-why-is-egypt-abusing-it-2/>, Access Now, “Open NGO Letter to EU Member States and Institutions Regarding the Export of Surveillance Equipment,” July 11, 2017,

<https://www.accessnow.org/press-release/ngo-letter-to-eu-member-states-on-surveillance-exports/>;

Privacy International report, “The President's Men? Inside The Technical Research Department, The Secret Player In Egypt's Intelligence Infrastructure,” February 24, 2016,

<https://privacyinternational.org/report/666/presidents-men-inside-technical-research-department-secret-player-egypts-intelligence>.

³⁰ SMEX phone interview with “Hassan,” April 17, 2026.



governments with far weaker protections against abuse.³¹ Authorities repeatedly deploy these technologies on peaceful critics, including those abroad.³²

Yet the legal framework governing digital life is only one front. In the same period as these legal developments, Egyptian authorities built equally restrictive legal architecture around civil society itself, most consequentially via its law governing nongovernmental organizations.

Legal Architecture Governing the Day-to-Day Activities of Digital Rights Organizations

Egyptian authorities designed the “Law on Regulating the Work of Civil Associations” – Law No. 149 of 2019, but commonly referred to as the “NGO law” – to prohibit a wide range of normal activities carried out by civil society organizations.³³ Parliament passed an amended version of the law in 2019 that removed the prison penalties included in the 2017 version, but maintained the severe restrictions that NGOs contend with today.³⁴ “This is how Egypt closed civil society,” said “Laila,” an independent Egyptian digital expert, referring to the NGO law.³⁵

Under the NGO Law, organizations face fines up to one million Egyptian pounds for violations of rules that make their work nearly impossible if followed fully.³⁶ Organizations cannot conduct field research or surveys without government permission, and authorities retain broad powers to dissolve groups, dismiss their

³¹ Human Rights Watch, “Looking the Other Way: EU Failure to Prevent Surveillance Exports to Rights Violators,” May 12, 2026, <https://www.hrw.org/report/2026/05/12/looking-the-other-way/eu-failure-to-prevent-surveillance-exports-to-rights>; Human Rights Watch, “Bulgaria Licensed Surveillance Exports to Rights Violators,” June 18, 2026, <https://www.hrw.org/news/2026/06/18/bulgaria-licensed-surveillance-exports-to-rights-violators>;

Amnesty International, “New EU Dual Use Regulation agreement ‘a missed opportunity’ to stop exports of surveillance tools to repressive regimes,” March 25, 2021, <https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/>.

³² Access Now, “Espionage for repression: hack-for-hire phishing campaign targets civil society in MENA,” April 8, 2026, <https://www.accessnow.org/wp-content/uploads/2026/04/Espionage-for-repression-forensic-analysis-of-a-cross-border-hack-for-hire-campaign-targeting-civil-society-in-MENA-2026.pdf>.

³³ Youm7, “البرلمان يوافق نهائياً بأغلبية الثلثين على قانون تنظيم العمل الأهلي,” July 15, 2019, https://www.youm7.com/story/2019/7/15/%D8%A7%D9%84%D8%A8%D8%B1%D9%84%D9%85%D8%A7%D9%86-%D9%8A%D9%88%D8%A7%D9%81%D9%82-%D9%86%D9%87%D8%A7%D8%A6%D9%8A%D8%A7-%D8%A8%D8%A3%D8%BA%D9%84%D8%A8%D9%8A%D8%A9-%D8%A7%D9%84%D8%AB%D9%84%D8%AB%D9%8A%D9%86-%D8%B9%D9%84%D9%89-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AA%D9%86%D8%B8%D9%8A%D9%85-%D8%A7%D9%84%D8%B9%D9%85%D9%84-%D8%A7%D9%84%D8%A3%D9%87%D9%84%D9%89/4334528#goog_rewarded.

³⁴ Human Rights Watch, “Egypt: New Law Will Crush Civil Society,” June 2, 2017, <https://www.hrw.org/news/2017/06/02/egypt-new-law-will-crush-civil-society>; Human Rights Watch, “Egypt: New NGO Law Renews Draconian Restrictions,” July 24, 2019, <https://www.hrw.org/news/2019/07/24/egypt-new-ngo-law-renews-draconian-restrictions>.

³⁵ SMEX phone interview with “Laila,” May 22, 2026.

³⁶ Amnesty International, “Egypt: NGO law threatens to annihilate human rights groups,” May 30, 2017, <https://www.amnesty.org/en/latest/press-release/2017/05/egypt-ngo-law-threatens-to-annihilate-human-rights-groups/>.

boards, and prosecute their staff for “harming national unity” or public order.³⁷ Receiving foreign funding without prior approval results in a violation, with penalties as severe as life imprisonment.³⁸

Some groups chose to scale back or terminate operations in Egypt even before parliament ratified the restrictive 2017 NGO Law. Human Rights Watch, for example, voluntarily ended its physical presence in Egypt in 2014 when it closed the Cairo office it had maintained since 2007 and withdrew its staff and NGO registration application.³⁹ The organization cited the “shrinking space for independent organizations in Egypt” for its decision. Other prominent rights organizations closed their local offices or moved their regional programming outside Egypt after authorities raided their offices and arrested staff between 2011 and 2015.⁴⁰ “We used to have hundreds of peers, now tens, and the number is still shrinking,” Hassan said.⁴¹

Together with the digital governance laws described above, the NGO law completes a legal enclosure around civil society. Organizations that survive the restrictions on what they say online still must contend with restrictions on what they research, whom they partner with, and how they fund themselves. For Egypt's digital rights organizations, caught squarely at the intersection of both regimes, the consequences are existential.

Impact on Digital Rights Organizations

Hassan summarized the cumulative impact of this legal and institutional environment on him and his colleagues in the past decade:

“Some of us were kidnapped, arrested, our homes broken into. We’re dealing with political persecution and endless legal cases brought against us. Some of our colleagues are banned from travel and can’t access their bank accounts. We have been targeted and face smear campaigns and surveillance. We can’t really fundraise, our operating

³⁷ Amnesty International, “Egypt: NGO law threatens to annihilate human rights groups,” May 30, 2017, <https://www.amnesty.org/en/latest/press-release/2017/05/egypt-ngo-law-threatens-to-annihilate-human-rights-groups/>.

³⁸ Human Rights Watch, “Egypt: New NGO Law Renews Draconian Restrictions,” July 24, 2019, <https://www.hrw.org/news/2019/07/24/egypt-new-ngo-law-renews-draconian-restrictions>.

³⁹ Human Rights Watch, “Q&A: Egypt Mass Killings report ‘All According to Plan,’” October 1, 2014, <https://www.hrw.org/news/2014/10/01/qa-egypt-mass-killings-report-all-according-plan>.

⁴⁰ Amy Austin Holmes, “Civil Society from Alexandria to Aswan: Survival Strategies,” May 31, 2018, <https://timep.org/2018/05/31/civil-society-from-alexandria-to-aswan-survival-strategies/>; The Egyptian Initiative for Personal Rights, “After a hearing at the European Parliament on the crisis of human rights in Egypt: Government refers CIHRS to investigation,” June 10, 2015, <https://eipr.org/en/press/2015/06/after-hearing-european-parliament-crisis-human-rights-egypt-govt-refers-cihrs>; Human Rights Watch, “Egypt: Renewed Crackdown on Independent Groups,” June 15, 2015, <https://www.hrw.org/news/2015/06/15/egypt-renewed-crackdown-independent-groups>.

⁴¹ SMEX phone interview with “Hassan,” April 17, 2026.



space is very constrained. The mental burnout and mental impact is huge. It is not a peaceful environment...it has been very challenging."⁴²

One of the clearest, public illustrations of what this environment does to a digital rights organization is the case of the Arab Network for Human Rights Information (ANHRI), one of the country's most prominent groups working on digital rights and free expression, which closed in 2022 after 18 years in operation.⁴³ Its founder Gamal Eid, a prominent and well-awarded rights defender, documented abuses by Egyptian authorities and advocated for free expression for decades.⁴⁴ Leading up to the closure, authorities banned Eid from travel and froze his assets.⁴⁵ He also alleges Egyptian security forces or individuals directed by them violently assaulted him twice in 2019.⁴⁶ Authorities arrested several ANHRI staff members, and impeded Eid's ability to bring the organization in compliance with the NGO law requirements due to the asset freeze.⁴⁷

ANHRI said in an announcement about its closure:

"While all independent human rights organizations in Egypt face harassment, persecution and threats, the security forces' targeting of ANHRI's has been particularly severe and hostile, ranging from arresting members of the ANHRI team, thefts, violent physical assaults, and illegal summons, all the way to attempts to recruit some staff members as informants on ANHRI, and is part of a growing list of violations and harassment."⁴⁸

⁴² SMEX phone interview with "Hassan," April 17, 2026.

⁴³ Arab Network for Human Rights Information, "In the absence of the bare minimum of the rule of law and respect for human rights The Arabic Network for Human Rights Information decides to suspend its activities," January 10, 2022, <https://web.archive.org/web/20220110111041/https://www.anhri.info/?p=28614&lang=en>.

⁴⁴ GCHR, "Gamal Eid selected as Defender of Human Rights & Freedom of Expression for April 2017," April 10, 2017, <https://www.gc4hr.org/gamal-eid-selected-as-defender-of-human-rights-freedom-of-expression-for-april-2017/>; Frontline Defenders, "Gamal Eid," n.d., <https://www.frontlinedefenders.org/en/profile/gamal-eid>;

⁴⁵ Amnesty International, "Egypt: Asset freeze is a shameless ploy to silence human rights activism," September 17, 2016, <https://www.amnesty.org/en/latest/press-release/2016/09/egypt-asset-freeze-is-a-shameless-ploy-to-silence-human-rights-activism/>.

⁴⁶ Human Rights Watch, "Egypt: Prominent Rights Defender Attacked," November 2, 2019, <https://www.hrw.org/news/2019/11/02/egypt-prominent-rights-defender-attacked>; Human Rights Watch, "Egypt: Rights Activist Assaulted," December 30, 2019, <https://www.hrw.org/news/2019/12/30/egypt-rights-activist-assaulted>.

⁴⁷ Human Rights Watch, "Egypt: Prominent Rights Defender Attacked," November 2, 2019, <https://www.hrw.org/news/2019/11/02/egypt-prominent-rights-defender-attacked>; Human Rights Watch, "Egypt: Rights Activist Assaulted," December 30, 2019, <https://www.hrw.org/news/2019/12/30/egypt-rights-activist-assaulted>.

⁴⁸ Arab Network for Human Rights Information, "The most important instances of persecution and blatant violations that ANHRI and its team were subjected to which drove them to announce the suspension of their activities starting today, January 10, 2022," January 10, 2022, <https://web.archive.org/web/20220110110211/https://www.anhri.info/?p=28606&lang=en>; Arab Network for Human Rights Information, "In the absence of the bare minimum of the rule of law and respect for human rights The Arabic Network for Human Rights Information decides to suspend its activities," January 10, 2022, <https://web.archive.org/web/20220110111041/https://www.anhri.info/?p=28614&lang=en>.



Countless other Egyptian rights actors faced administrative barriers that similarly restricted or terminated their ability to carry out their work.⁴⁹

Online State-Backed Harassment of Digital Rights Groups and Activists

Rights groups have documented smear campaigns and hate speech by state-controlled media and online actors as a systemic form of repression against human rights defenders in Egypt. These campaigns commonly portray rights defenders as traitors, foreign agents, terrorists, or threats to national security and often accompany judicial harassment, physical attacks, and other reprisals.⁵⁰ Laila highlighted an additional dimension of this documented pattern: such campaigns often precede legal and physical crackdowns, helping to delegitimize targets, reduce public sympathy, and generate support for subsequent prosecutions.⁵¹ As she put it, “We have to connect the online activity with offline crackdown.”⁵²

Documented cases illustrate this relationship. Human rights defender Hossam Bahgat of the Egyptian Initiative for Personal Rights (EIPR), for example, was repeatedly targeted by pro-government media smear campaigns portraying EIPR and Bahgat’s work as a threat to national security.⁵³ Similar online campaigns targeted veteran rights defender Bahey el-Din Hassan as well as other prominent Egyptian activists.⁵⁴ Rights organizations have extensively documented how state-backed “electronic brigades” viciously target Egyptian civil society through

⁴⁹ UN Communication, AL EGY 10/2025, December 31, 2025,

<https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=30650>.

⁵⁰ Reporters Without Borders, “President Sisi’s Puppets: TV presenters used to wage war on journalism,” June 30, 2022,

<https://rsf.org/en/egyptian-tv-presenters-who-smear-journalists-government-s-behest>; EuroMed Rights, “Death threats against CIHRS Director, Bahey el-Din Hassan,” April 18, 2018,

<https://euromedrights.org/publication/death-threats-against-cihrs-director-bahey-el-din-hassan/>;

Frontline Defenders, “Smear campaign incites violence against human rights defenders in Egypt,” n.d.,

<https://www.frontlinedefenders.org/en/case/smear-campaign-incites-violence-against-human-rights-defenders-egypt#case-update-id-5796>; Amnesty International, “Egypt: Human Rights Group and its Director Threatened and Smeared,” February 26, 2024,

<https://www.amnesty.org/en/latest/news/2024/02/egypt-human-rights-group-and-its-director-threatened-and-smeared/>.

⁵¹ SMEX phone interview with “Laila,” May 22, 2026.

⁵² SMEX phone interview with “Laila,” May 22, 2026.

⁵³ Amnesty International, “Egypt: End shocking reprisal campaign against leading Egyptian rights group,” November 20, 2020,

<https://www.amnesty.org/en/latest/press-release/2020/11/egypt-end-shocking-reprisal-campaign-against-leading-egyptian-rights-group/>.

⁵⁴ EuroMed Rights, “Death threats against CIHRS Director, Bahey el-Din Hassan,” April 18, 2018,

<https://euromedrights.org/publication/death-threats-against-cihrs-director-bahey-el-din-hassan/>;

Frontline Defenders, “Smear campaign incites violence against human rights defenders in Egypt,” n.d.,

<https://www.frontlinedefenders.org/en/case/smear-campaign-incites-violence-against-human-rights-defenders-egypt#case-update-id-5796>; Amnesty International, “Egypt: Human Rights Group and its Director Threatened and Smeared,” February 26, 2024,

<https://www.amnesty.org/en/latest/news/2024/02/egypt-human-rights-group-and-its-director-threatened-and-smeared/>.

social media platforms.⁵⁵ In 2020, X removed thousands of accounts linked to the Egyptian government and pro-government media.⁵⁶

“Gamal,” an Egyptian lawyer and free expression advocate, situated these practices within a broader political strategy, arguing that the state uses digital mobs not only to punish or smear critics, but also to build a social basis for repression.⁵⁷ As authorities under al-Sisi improved their ability to monitor and punish online speech, he said, they also learned how to direct public anger away from state failures and toward women, refugees, activists, and other people who could be portrayed as “immoral” or disloyal. Pro-government users and self-appointed “honorable citizens” attack these people, report their posts, and file complaints – creating a controlled form of public participation in which users criticize each other rather than the government’s behaviors.

Available evidence supports this broader pattern of leveraging digital mobs to redirect critique of a country’s human rights record, although it does not establish a government mandate behind every smear campaign.⁵⁸ Comparable tactics appear in Iraq and Tunisia, and elsewhere in the SWANA region, such as Morocco.⁵⁹ Rights groups have long connected the Egyptian government’s efforts

⁵⁵ Reporters Without Borders, “President Sisi’s Puppets: TV presenters used to wage war on journalism,” June 30, 2022,

<https://rsf.org/en/egyptian-tv-presenters-who-smear-journalists-government-s-behest>.

⁵⁶ Julian Borger, “Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments,” *The Guardian*, April 2, 2020,

<https://www.theguardian.com/technology/2020/apr/02/twitter-accounts-deleted-linked-saudi-arabia-serbia-egypt-governments>.

⁵⁷ SMEX phone interview with “Gamal,” June 18, 2026.

⁵⁸ Arabi Facts Hub, “مصر: هكذا قاد مقربون من الرئاسة حملة رقمية ضد إطلاق سراح علاء عبد الفتاح,” November 15, 2022,

<https://arabifactshub.com/ar/articles/details/4387>; EuroMed Rights, “Dangerous liaisons: social media as a (flawed) tool of resistance in Egypt,” September 15, 2020,

https://euromedrights.org/wp-content/uploads/2020/09/Study_on_social_media_in_Egypt.pdf;

Akbarzadeh et. al, “Social media, conspiracy theories, and authoritarianism: between bread and geopolitics in Egypt,” March 4, 2025,

<https://www.tandfonline.com/doi/full/10.1080/19331681.2025.2474000#abstract>; Dania Akkad,

“Revealed: Seven years later, how Facebook shuts down free speech in Egypt,” January 30, 2018, Middle East Eye,

<https://www.middleeasteye.net/news/revealed-seven-years-later-how-facebook-shuts-down-free-speech-egypt>;

Digital Forensics Lab, “Pro-government Twitter accounts targeted head of Egyptian Engineers Syndicate,” October 19, 2023,

<https://dfrlab.org/2023/10/19/twitter-hashtags-egypt/>.

⁵⁹ Freedom House, “Freedom on the Net 2024: Tunisia, Key Developments, June 1, 2023 – May 31, 2024,” <https://freedomhouse.org/country/tunisia/freedom-net/2024>; Layli Faroudi, “They went out to protest. Then the police attacked them on Facebook,” WIRED, April 15, 2021,

<https://www.wired.com/story/tunisia-police-facebook/>; Al-Rawi, Ahmed, Chris Tenove, and Peter Klein, “The Networked Trolling of Critical Journalists and News Organizations in Iraq” *Journalism and Media* 4, no. 4: 1130-1140, <https://doi.org/10.3390/journalmedia4040072>.

Dina Sadek and Ali Chenrose, “Dubious Moroccan Facebook and Twitter accounts boost content critical of journalist Omar Radi and European Parliament,” May 11, 2023,

<https://dfrlab.org/2023/05/11/dubious-moroccan-facebook-and-twitter-accounts-boost-content-critic-al-of-journalist-omar-radi-and-european-parliament/>.

to control internet discourse to the political threats posed by online organizing.⁶⁰ Commentary published before the 2011 revolution documented the Egyptian government's anxiety about a potential "Facebook revolution."⁶¹ Nearly every Egyptian interviewee echoed this analysis.⁶² "The government wants to control what image of itself is exported, but more importantly they are afraid of the ability for people to collectively organize and exchange ideas freely," Fareid said.⁶³ Interviewees also pointed to the April 6 Youth Movement and the 2011 revolution, arguing that these moments reinforced the perception among Egyptian authorities that online spaces represent a potential challenge to state control.⁶⁴

Efforts to control criticism extend beyond Egypt's borders, reflecting a broader regional turn toward transnational digital repression aimed at limiting the influence of exiled activists and critics.⁶⁵ In May 2026, Egyptian authorities sought to geoblock the accounts of 12 Egyptian dissidents already living in exile.⁶⁶

B. Iraq/Kurdistan Region of Iraq (KRI)

Iraq presents a distinct case within the regional landscape of digital authoritarianism, shaped in large part by its post-conflict status. Decades of war, US-led occupation, and ongoing militia activity produced a state apparatus that is under-resourced, and in many ways functionally subordinate to armed non-state

⁶⁰ Association for Free Thought and Expression, "Isolation.. The cutting of communication during the January 2011 revolution," April 17, 2018, <https://afteegypt.org/en/research-en/monitoring-reports-en/2018/04/17/15041-afteegypt.html>;

Association for Free Thought and Expression, "New laws.. The thick stick of the state to control the Internet," September 4, 2018, <https://afteegypt.org/en/legislations-en/legislative-analysis-en/2018/09/04/15717-afteegypt.html>;

Access Now, "Two years from Tahrir, no progress on telcos and rights," January 25, 2013, <https://www.accessnow.org/two-years-from-tahrir-telecoms-still-lack-rights-respecting-principles/>;

Osama Diab, "Egyptian government fears a Facebook revolution," The Guardian, October 21, 2010, <https://www.theguardian.com/commentisfree/2010/oct/21/egypt-facebook-revolution>;

Adrian Shahbaz, "Four Years On, Egypt Has Pulled the Plug on a Digital Revolution," Freedom House, February 9, 2015, <https://freedomhouse.org/article/four-years-egypt-has-pulled-plug-digital-revolution>.

⁶¹ Osama Diab, "Egyptian government fears a Facebook revolution," The Guardian, October 21, 2010, <https://www.theguardian.com/commentisfree/2010/oct/21/egypt-facebook-revolution>.

⁶² SMEX phone interview with "Laila," May 22, 2026; SMEX phone interview with "Fareid," May 14, 2026.

⁶³ SMEX phone interview with "Fareid," May 14, 2026.

⁶⁴ Adrian Shahbaz, "Four Years On, Egypt Has Pulled the Plug on a Digital Revolution," Freedom House, February 9, 2015, <https://freedomhouse.org/article/four-years-egypt-has-pulled-plug-digital-revolution>;

PBS video, "Egypt's Facebook Faceoff," February 22, 2011, <https://www.pbs.org/video/frontline-egypts-facebook-faceoff/>;

Shabab 6 April, "عاطف إسماعيل : دولة", November 17, 2012, <https://shabab6april.wordpress.com/>.

⁶⁵ Egyptian Human Rights Forum, "Platformed Repression: Egypt's Digital Targeting of Exiles and Dissidents," May 22, 2026, <https://egyptianforum.org/en/platformedrepression/>; ALQST, "Meta blocks human rights accounts from reaching audiences in Saudi Arabia and the UAE," May 20, 2026, <https://www.alqst.org/ar/posts/1190>.

⁶⁶ Egyptian Human Rights Forum, "Platformed Repression: Egypt's Digital Targeting of Exiles and Dissidents," May 22, 2026, <https://egyptianforum.org/en/platformedrepression/>.

actors with their own agendas and enforcement capabilities.⁶⁷ Between 2003-2004, the US-led Coalition Provisional Authority dismantled and re-established many of Iraq's state institutions, including the Communications and Media Commission that remains today.⁶⁸ These dynamics shape digital repression in ways that diverge sharply from the more administratively coherent crackdowns in Egypt or Tunisia.

Based on seven interviews with Iraqi civil society representatives and digital rights actors, SMEX found that digital authoritarianism operates in Iraq through three overlapping and competing centers of power: a weakened central government in Baghdad, non-state militias and armed actors, and the Kurdistan Regional Government (KRG). This fragmentation produces an environment less administratively coherent than its regional counterparts, but no less dangerous. Even so, interviewees described greater operational leeway than their Egyptian or Tunisian counterparts, especially in the KRI. Rather than targeting digital rights organizations through a consistent combination of registration pressure, prosecution, funding scrutiny, surveillance, and smear campaigns, pressure in Iraq often falls unevenly on individual advocates, journalists, and organizers, while their organizations may remain formally intact.

This relative operational space does not mean that digital rights groups can speak freely. Organizations may continue operating while individual advocates face arrest, harassment, and other reprisals when their work attracts attention online. Interviewees identified gender and sexuality, government corruption, politicians, and militias as especially sensitive topics for them to work on or speak about online.⁶⁹

Iraq's outdated and highly discretionary legal system poses a central obstacle to digital rights work. The absence of a coherent, modern cybercrime and digital rights framework means organizations do not always face the same technically sophisticated legal architecture seen in Egypt. Instead, they navigate a less predictable collection of pre-internet laws and uneven enforcement practices. The KRI is generally considered more permissive than federal Iraq when it comes to people's ability to speak online; however, this appears due to weaker enforcement mechanisms, lower technical capacity, and a less developed digital monitoring apparatus than due to stronger legal protections.

⁶⁷ Rend al-Rahim, "Unfinished Business: Nation-Building in Iraq Since 2003," Arab Center Washington DC, March 21, 2023, <https://arabcenterdc.org/resource/unfinished-business-nation-building-in-iraq-since-2003/>; Paul Salem et. al, "Special Briefing: The legacy, lessons, and future course of Iraq 20 years since the U.S. invasion," <https://mei.edu/commentary/special-briefing-legacy-lessons-and-future-course-iraq-20-years-us-invasion/>.

⁶⁸ 2004 Coalition Provisional Authority Number 65, Iraqi Communications and Media Commission, available https://govinfo.library.unt.edu/cpa-iraq/regulations/20040320_CPAORD65.pdf; Council on Foreign Relations, "Iraq: The Bremer Edicts," January 27, 2005, <https://www.cfr.org/backgrounders/iraq-bremer-edicts>.

⁶⁹ David Gritten, "Iraqi activist jailed over tweet 'insulting' Iran-backed militia force," December 7, 2022, <https://www.bbc.com/news/world-middle-east-63890358>.

Iraq's constitution formally protects freedom of opinion and expression, including expression "using all means," as well as freedom of the press, publication, assembly, and demonstration.⁷⁰ Article 38 nevertheless conditions those rights on "public order and morals," leaving room for authorities to restrict speech through vague morality, security, and public order justifications. Iraq lacks a dedicated law on freedom of opinion and expression, allowing authorities to restrict this right through other statutes despite the constitutional guarantee.⁷¹

Rights groups including SMEX have documented a strong morality-based logic influencing government restrictions on online expression in both federal Iraq and the KRI.⁷² "Diyar," a Kurdish human rights expert, said authorities justify restrictions in the name of morals, customs, or religious principles and then turn those concepts against people who criticize or oppose them.⁷³ He described an enforcement environment dictated by "trends." Officials allegedly monitor social media for viral and popular content and mobilize quickly if that content displeases them. This makes online expression especially precarious for people working on gender, sexuality, or online gender-based violence.

This morals-driven approach creates a point of comparison with Egypt, though the two systems operate differently. Egypt has embedded morality policing within a more consolidated legal and institutional architecture; in Iraq, authorities and pro-government allies invoke morals, customs, religious principles, and family values through a more fragmented system to portray criticism as a social threat. In both contexts, "morality" violations act as a bridge between online vilification and formal punishment

Legal Architecture Governing Digital Speech and Activities

Iraq's legal framework comprises a patchwork of largely pre-internet era statutes and media regulations, including the 1969 Penal Code and 2005 Counterterrorism law. The result gives authorities broad discretion to punish peaceful online speech while failing to provide clear rules for prosecuting modern digital harms, including

⁷⁰ Iraqi Constitution of 2005, available at https://www.constituteproject.org/constitution/Iraq_2005.

⁷¹ Rasha Khalid Hilool, "Policy Paper: Freedom of Opinion and Expression for Women in Iraq from a Civil Legal Perspective," Baghdad Women's Association, May 4, 2024, <https://bwa-iraq.org/freedom-of-opinion-and-expression-for-women-in-iraq-from-a-civil-legal-perspective/>.

⁷² Zeinab Ismail, "More Control: Iraq's Alarming Cybercrime Law," August 3, 2023, <https://smex.org/more-control-iraqs-alarming-cybercrime-law/>; SMEX, "Joint Statement: Iraqi authorities must cease their chilling crackdown on free speech," March 3, 2023, <https://smex.org/joint-statement-iraqi-authorities-must-cease-their-chilling-crackdown-on-free-speech/>; Safaa Ayyad, "Iraq's Controversial 'Ballegh' Platform for 'Combating Indecent Content,'" February 15, 2023, <https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content>.

⁷³ SMEX phone interview with "Diyar," May 9, 2026.



blackmail, doxxing, hacking, and online gender-based violence.⁷⁴ “Omar,” an Iraqi digital rights activist, said their broad and vague nature means that Iraqi authorities “can turn the law against anyone.”⁷⁵

The 1969 Penal Code remains one of the primary tools used to regulate online expression, even though it predates the internet by decades.⁷⁶ Rights groups including SMEX have documented how the Iraqi penal code contains vague defamation and insult provisions that criminalize acts such as insulting broad concepts such as the state, public integrity, and public decency.⁷⁷ SMEX has also extensively documented both federal Iraq and KRI authorities’ use of penal code articles 210, 226, 403, 433, and 434 against peaceful critics for their social media posts, claiming threats to national security.⁷⁸ The legal gaps are especially pronounced for women and girls.⁷⁹ The Iraqi Penal Code does not explicitly use the term “harassment,” forcing survivors and advocates to rely on provisions written around assault, indecent advances, or public modesty.⁸⁰

Iraq’s 2005 Law on Counterterrorism adds a further layer of risk to digital rights organizations and online users because of its broad definition of terrorism and severe penalties.⁸¹ The law contains only six articles but defines terrorism and crimes against state security in sweeping terms, including acts that “threaten national unity” or public “stability.”

This outdated legal environment constrains digital rights organizations in two directions. It exposes advocates, journalists, and civil society actors to selective prosecution for online speech while also limiting their ability to meaningfully support survivors of cybercrimes because the legal framework does not clearly define modern digital offenses, digital evidence standards, or procedural safeguards. “Yasmine,” an Iraqi women’s rights and digital safety expert, said digital crimes on Telegram, for example, are especially difficult to address because Iraq still relies on its penal code rather than a cybercrime law tailored to the structure of online abuse. Telegram bots, channels, and data leak networks have

⁷⁴ Human Rights Watch, “‘We Might Call You in at Any Time’: Free Speech Under Threat in Iraq,” June 15, 2020,

<https://www.hrw.org/report/2020/06/15/we-might-call-you-any-time/free-speech-under-threat-iraq>.

⁷⁵ SMEX phone interview with “Omar,” April 16, 2026.

⁷⁶ Iraq Penal Code of 1969, available <https://www.refworld.org/legal/legislation/natlegbod/1969/103522>.

⁷⁷ Zeinab Ismail, “More Control: Iraq’s Alarming Cybercrime Law,” August 3, 2023, <https://smex.org/more-control-iraqs-alarming-cybercrime-law/>; Human Rights Watch, “‘We Might Call You in at Any Time’: Free Speech Under Threat in Iraq,” June 15, 2020,

<https://www.hrw.org/report/2020/06/15/we-might-call-you-any-time/free-speech-under-threat-iraq>.

⁷⁸ SMEX, “Joint Statement: Iraqi authorities must cease their chilling crackdown on free speech,” March 3, 2023,

<https://smex.org/joint-statement-iraqi-authorities-must-cess-their-chilling-crackdown-on-free-speech/>.

⁷⁹ INSM, “دراسة أنسمية جديدة: الإطار القانوني والمؤسسي للعنف ضد النساء والفتيات الميسر بالتكنولوجيا في العراق,” January 2026, <https://insm-iq.org/?p=2094>

⁸⁰ Balsam Mustafa, “Your Mobile Phone is Your Weapon Against Harassment,” November 9, 2022, <https://iohriq.org/100.html#>.

⁸¹ Iraq Counterterrorism Act No. 13 of 2005, available https://www.unodc.org/uploads/icsant/documents/Legislation/Iraq/Iraq/English/Act_No_13_2005_EN_G.pdf.

proliferated, she said, because “there is no one controlling them and no clear penalties for their behavior.”⁸²

Kurdistan Region of Iraq

The Kurdistan Region of Iraq (KRI) has its own legal architecture, but interviewees described it as similarly outdated and inconsistently applied. Press Law No. 35 of 2007 formally protects journalist activity, including the right to obtain information of public interest and publish that information without fear of arrest.⁸³ It also ascribes financial penalties for violations for defamation-related reporting offenses, rather than arrest or detention.⁸⁴ It requires the Kurdistan Regional Government (KRG) to inform the Kurdistan Journalists Syndicate of legal actions against journalists when the case relates to their professional work.

In practice, KRG authorities often bypass these protections by prosecuting journalists under the 1969 Penal Code, the KRI's Law No. 21 of 2003 Law on Counterterrorism, or the 2008 Law No. 6 to Prevent the Misuse of Telecommunications Equipment instead.⁸⁵ The 2008 telecommunications law allows prison sentences and fines for vague acts such as threatening, insulting, spreading false information, or disclosing private communications online, offering a loophole for authorities to carry out arrests and detention for speech otherwise destined for a lesser punishment under the 2007 Press Law.⁸⁶ The 2003 counterterrorism law, frequently leveraged against journalists, allows for punishments up to life in prison for harming the stability of the KRI.⁸⁷

⁸² SMEX phone interview with “Yasmine,” June 5, 2026.

⁸³ Kurdistan Region of Iraq, Press Law No. 35 of 2007, available at <https://presidency.gov.krd/krp/docs/PressLaw-KRI.pdf>.

⁸⁴ Shamal Aqrabi, “Parli in Iraq's Kurdistan passes softer media law,” Reuters, September 23, 2008, <https://www.reuters.com/article/middleeastCrisis/idUSANW319038/>.

⁸⁵ Balen Izzat Mika, “Why press law is not implemented? Legal gaps push judges to penal code,” Kirkuk Now, August 15, 2021, <https://kirkuknow.com/en/freePress/66285>; Kurdistan Region of Iraq Law 21 of 2003 on Counterterrorism, available <https://legislation.krd/law-detail/?id=2374>; Iraq Law No. 6 of 2008 to Prevent the Misuse of Telecommunications Equipment, available <https://www.parliament.krd/media/2364/%DB%8C%D8%A7%D8%B3%D8%A7%DB%8C-%DA%98%D9%85%D8%A7%D8%B1%D9%87-6-%DB%8C-%D8%B3%D8%A7%DA%B5%DB%8C-2008-%DB%8C%D8%A7%D8%B3%D8%A7%DB%8C-%D9%82%D9%87-%D8%AF%D9%87-%D8%BA%D9%87-%D9%83%D8%B1%D8%AF%D9%86%DB%8C-%D8%AE%D8%B1%D8%A7%D9%BE-%D8%A8%D9%87-%D9%83%D8%A7%D8%B1%D9%87%DB%8E%D9%86%D8%A7%D9%86%DB%8C-%D8%A6%D8%A7%D9%85%DB%8E%D8%B1%D9%87-%D9%83%D8%A7%D9%86%DB%8C-%D9%BE%D9%87-%DB%8C%D9%88%D9%87-%D9%86%D8%AF%DB%8C-%D9%83%D8%B1%D8%AF%D9%86-%D9%84%D9%87-%D9%87%D9%87-%D8%B1%DB%8E%D9%85%DB%8C-%D9%83%D9%88%D8%B1%D8%AF%D8%B3%D8%AA%D8%A7%D9%86-%D9%80-%D8%B9%DB%8C%D8%B1%D8%A7%D9%82.pdf>.

⁸⁶ Winthrop Rodgers, “A kind of hell for journalists’ : A law in Iraq’s Kurdistan Region was supposed to stop sexist online abuse. Instead, it’s being used to jail journalists,” Columbia Journalism Review, April 6, 2022, https://www.cjr.org/special_report/iraq-kurdistan-law-6.php.

⁸⁷ MENA Rights Group, “Iraq: the escalating crackdown on civic space,” July 2024, https://menarights.org/sites/default/files/2024-09/MRG_IRO_UPRIV_StakeholderSubmission_July2024_Final_0.pdf; Community Peacemakers Teams, “Freedom of Expression Under Threat,” March 6, 2021, <https://cptik.org/reports/2021/3/3/freedom-of-expression-under-threat>.

The irony is that Law No. 6 was not originally framed as a press-repression tool. Kurdish women's groups reportedly supported the legislation as a response to the online harassment and abuse that women and girls were already facing at the time.⁸⁸ Its vague language has nevertheless allowed powerful figures and state actors to turn it against journalists and critics, even as women and girls continue to face online abuse.

Bashdar Hassan, a lawyer representing journalists prosecuted in 2021 under the 2003 counterterrorism law, told local media that "Authorities file lawsuits against journalists per Law No. 21 [the counterterrorism law] to imprison them because if they are tried per journalism law, they face financial penalties only."⁸⁹ Interviewees with expertise in the KRI described the same loophole practice to SMEX.⁹⁰ Aiman said this legal maneuver reflects a broader political narrative in Iraq, in which press freedom and free expression are increasingly portrayed as promoting "foreign or Western agendas."⁹¹ This framing allows authorities to treat peaceful criticism as a threat to sovereignty or public order, justifying harsher punishment than the 2007 Press Law permits.

Authorities in both the KRI and federal Iraq have struggled to keep pace with rapid technological advancements. "Nabil," an independent Kurdish journalist, attributed the problem in the KRI to years of political gridlock. As social media, artificial intelligence, and other digital tools expanded in recent years, the KRI continued to rely on its "very basic" 2008 communications law that "cannot cover the developments of our current times."⁹²

Taken together, this basket of laws in the KRI gives authorities tools to punish journalists, activists, and ordinary users for peaceful online expression, and does not provide the technical specificity needed to address digital harms.

Legal Architecture Governing the Day-to-Day Activities of Digital Rights Organizations

Iraq does not have an NGO law that closes civil society as comprehensively as Egypt's 2019 NGO law or imposes as sweeping restrictions on civil society as Tunisia's Decree-Law 54. Formally, the federal Law on Non-Governmental Organizations, Law No. 12 of 2010, and the KRI's Law No. 1 of 2011 provide the main

⁸⁸ Winthrop Rodgers, "A kind of hell for journalists' : A law in Iraq's Kurdistan Region was supposed to stop sexist online abuse. Instead, it's being used to jail journalists," *Columbia Journalism Review*, April 6, 2022, https://www.cjr.org/special_report/iraq-kurdistan-law-6.php.

⁸⁹ Firman Sadiq, *Kirkuk Now*, "Law Number 21: Nightmare for freedom of press," July 30, 2021, <https://kirkuknow.com/en/freePress/66155>

⁹⁰ SMEX written exchange with "Nabil," May 14, 2026; SMEX phone interview with "Aiman," May 22, 2026.

⁹¹ SMEX phone interview with "Aiman," May 22, 2026.

⁹² SMEX written exchange with "Nabil," May 14, 2026.



legal frameworks for civil society organizations. These laws allow NGOs to establish and operate but also permit significant government oversight.

Rather than a central law informing the government's approach to civil society control, Iraqi digital rights organizations operate inside a looser, fragmented architecture. The Communications and Media Commission (CMC) regulates the state's media and communications infrastructure,⁹³ while the Ministry of Interior and security agencies police online morality and digital content.⁹⁴ Courts and administrative bodies can impose financial penalties⁹⁵ while armed or party-aligned actors can intervene and attack outside clear legal channels.⁹⁶

The CMC is central to this day-to-day architecture.⁹⁷ Established in 2004 by the US-led Coalition Provisional Authority to regulate media and telecommunications, it features a board of commissioners, a director-general, hearing panel and appeals board, and advisory bodies.⁹⁸ Although the order describes the CMC as financially and administratively independent, rights groups and analysts repeatedly raise concerns that its leadership and board composition are subject to political influence and engage in serious rights abuses.⁹⁹

Interviewees identified the CMC as one of the most important bodies in Iraq's digital landscape because of its ability to direct regulatory, financial, and personnel resources toward media control.¹⁰⁰ The CMC's far-reaching abilities matter for digital rights organizations even though they are not themselves "broadcasters" in the literal sense. The CMC can suspend political programs, fine

⁹³ Iraqi Coalition Provisional Authority Order Number 65, Iraqi Communications and Media Commission, available https://govinfo.library.unt.edu/cpa-iraq/regulations/20040320_CPAORD65.pdf.

⁹⁴ Safaa Ayyad, "Iraq's Controversial 'Ballegh' Platform for 'Combating Indecent Content,'" February 15, 2023, <https://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecent-content>.

⁹⁵ Zdravko Ljubas, "Iraqi Media Regulator Suspends Reuters Licence," OCCRP, April 15, 2020, <https://www.occrp.org/en/news/iraqi-media-regulator-suspends-reuters-licence>.

⁹⁶ Haidar Al-Mosawi, "The State of Digital Rights in Iraq: Collaborative Repression Between the Authorities and Technology Companies!" MADR Network, July 8, 2026, <https://madr.network/the-state-of-digital-rights-in-iraq-collaborative-repression-between-the-authorities-and-technology-companies/>.

⁹⁷ SMEX, "Open letter to the Iraqi Communications and Media Commission: Drop the draft regulation of digital content and protect freedom of expression online," March 20, 2023, <https://smex.org/open-letter-to-the-iraqi-communications-and-media-commission-drop-the-draft-regulation-of-digital-content-and-protect-freedom-of-expression-online/>.

⁹⁸ 2004 Coalition Provisional Authority Number 65, Iraqi Communications and Media Commission, available https://govinfo.library.unt.edu/cpa-iraq/regulations/20040320_CPAORD65.pdf.

⁹⁹ Press Freedom Advocacy Association of Iraq, "A Decade of Dire Constitutional Violations: Media observatory report on the violations of the National Communications and Media Commission of Iraq, 2010 - 2020," July 30, 2020, <https://pfaa-iq.com/wp-content/uploads/CMC.pdf>; Shafaq News, "Press freedom group criticizes Iraq's CMC over 28 media sanctions," May 31, 2026, <https://shafaq.com/en/society/Press-freedom-group-criticizes-Iraq-s-CMC-over-28-media-sanctions>; Freedom House, "Iraq: Key Developments, June 1, 2023 – May 31, 2024," <https://freedomhouse.org/country/iraq/freedom-net/2024>; Human Rights Watch, "Letter to the Communication and Media Commission of Iraq," April 12, 2010 <https://www.hrw.org/news/2010/04/12/letter-communication-and-media-commission-iraq>.

¹⁰⁰ SMEX phone interview with "Aiman," May 22, 2026; SMEX phone interview with "Omar," April 16, 2026.

media outlets, restrict media figures, and revoke or threaten licenses.¹⁰¹ These measures narrow the public space available for digital rights organizations without formally banning them.

The CMC has also tried to extend its authority more directly over online expression. Its leaked 2023 draft regulation obligated the CMC to monitor all digital content published, promoted, or advertised by any means.¹⁰² The draft also gave the CMC authority to notify the judiciary or security agencies about content it deems dangerous or sensitive, address official authorities to block pages, and delete content in cases involving national security, public health, or other broad categories. For digital rights organizations, this draft framework is especially consequential. It would not only regulate speech after publication, but it would require the registration, monitoring, and possible removal of the online spaces where organizations publish research, document abuses, and mobilize public pressure.

Aiman said his organization was consulted at an early stage of the drafting process and came away from the experience feeling disillusioned. He said involved lawmakers knew little about cybersecurity and had endeavored to draft as broad a piece of legislation as possible.¹⁰³ SMEX and other rights organizations also criticized the CMC's draft digital content regulation, arguing that the CMC did not have authority to criminalize digital content or impose penalties on internet users so widely.¹⁰⁴ At time of writing, the draft regulation remains pending.

Repeated Attempts to Enact a Cybercrime Law

Iraq has debated cybercrime legislation for more than a decade without enacting it. Parliament first considered the Information Technology Crimes Law in 2011 and withdrew it following sustained civil society opposition in 2013, although it did not formally complete the withdrawal process.¹⁰⁵ Revised versions returned for readings in 2019 and 2020 and resurfaced again in 2022 and 2023, but were

¹⁰¹ Iraqi Observatory for Human Rights, "CMC Bans Political Commentators and Warns Media Outlets," April 6, 2026, <https://iohriq.org/191-.html>; Zdravko Ljubas, "Iraqi Media Regulator Suspends Reuters Licence," OCCPR, April 15, 2020, <https://www.occrp.org/en/news/iraqi-media-regulator-suspends-reuters-licence>; Shafaq News, "Iraq bans political analyst, penalizes two TV channels," June 24, 2026, <https://shafaq.com/en/society/Iraq-bans-political-analyst-penalizes-two-TV-channels>; Shafaq News, "Media regulator fines three Iraqi sports presenters \$11K+," July 2, 2026, <https://shafaq.com/en/society/Media-regulator-fines-three-Iraqi-sports-presenters-11K>.

¹⁰² SMEX, "Open letter to the Iraqi Communications and Media Commission: Drop the draft regulation of digital content and protect freedom of expression online," March 20, 2023, <https://smex.org/open-letter-to-the-iraqi-communications-and-media-commission-drop-the-draft-regulation-of-digital-content-and-protect-freedom-of-expression-online/>.

¹⁰³ SMEX phone interview with "Aiman," May 22, 2026.

¹⁰⁴ SMEX, "Open letter to the Iraqi Communications and Media Commission: Drop the draft regulation of digital content and protect freedom of expression online," March 20, 2023, <https://smex.org/open-letter-to-the-iraqi-communications-and-media-commission-drop-the-draft-regulation-of-digital-content-and-protect-freedom-of-expression-online/>.

¹⁰⁵ Civil society joint statement, "Re: Call to withdraw the draft Cybercrime Law which would severely undermine fundamental right to freedom of expression," March 1, 2019, <https://www.amnesty.org/en/wp-content/uploads/2021/05/MDE1499442019ENGLISH.pdf>.

repeatedly suspended after rights groups warned that the drafts contained vague offenses and severe penalties.¹⁰⁶

The issue resurfaced while SMEX conducted the research for this report. On July 6, 2026, parliament completed the first reading of a new draft Law on Combatting Information Technology Crimes.¹⁰⁷ Early analyses of the 2026 proposal identify some provisions directed at legitimate harms, including blackmail, fraud, and violations of personal privacy. They nevertheless warn that the proposal retains vague language and penalties reaching life imprisonment, while potentially creating overlapping powers among the proposed National Center for Digital Evidence, the Communications and Media Commission, and security agencies.¹⁰⁸ At time of writing, parliament had not announced a second reading.

This leaves digital rights organizations in a difficult position. Iraq urgently needs laws capable of addressing genuine cybercrimes, but without narrow definitions,

¹⁰⁶ The 2020 version of the draft bill would have allowed authorities to harshly punish expressions deemed a threat to governmental, social, or religious interests, carrying penalties of up to life in prison and large fines. See: MENA Rights Group, "Iraq's new draft Law on Combating Cybercrimes still contains problematic provisions restricting fundamental freedoms," December 1, 2020, <https://menarights.org/en/articles/iraqs-new-draft-law-combating-cybercrimes-still-contains-problematic-provisions>; Human Rights Watch, "Iraq: Scrap Bill to Restrict Free Speech," November 25, 2020, <https://www.hrw.org/news/2020/11/25/iraq-scrap-bill-restrict-free-speech>; Kristen Sibbald, Human Rights Watch, "Iraq Parliament Suspends Draconian Cybercrimes Bill," May 7, 2021, <https://www.hrw.org/news/2021/05/07/iraq-parliament-suspends-draconian-cybercrimes-bill>. Safa Ayyad, SMEX, "Iraqi Cybercrime Draft Law: In Suspension," July 6, 2022, <https://smex.org/iraqi-cybercrime-draft-law-in-suspension/>; Amnesty International, "Iraq: Draft laws threaten rights to freedom of expression and peaceful assembly," July 18, 2023, <https://www.amnesty.org/en/latest/news/2023/07/iraq-draft-laws-threaten-rights-to-freedom-of-expression-and-peaceful-assembly/>.

¹⁰⁷ Following the first reading of the 2026 version of the law, the speaker directed the Security and Defense Committee to consult the National Security Service, the Iraqi Media Network, and the intelligence services before presenting a revised text for a second reading. On July 26, the committee was still reviewing the proposal article by article and announced plans for broader consultations with security agencies and the Ministry of Communications and Information Technology. See: The Iraqi Council of Representatives, "مجلس النواب ينهي قراءة اربعة مقترحات قوانين," July 6, 2026, <https://iq.parliament.iq/blog/%D9%85%D8%AC%D9%84%D8%B3-%D8%A7%D9%84%D9%86%D9%88%D8%A7%D8%A8-%D9%8A%D9%86%D9%87%D9%8A-%D9%82%D8%B1%D8%A7%D8%A1%D8%A9-%D8%A7%D8%B1%D8%A8%D8%B9%D8%A9-%D9%85%D9%82%D8%AA%D8%B1%D8%AD%D8%A7%D8%AA-%D9%82/>; Iraqi Council of Representatives, 2026/ 6 تموز / الإثنين (1) الجلسة (1) "قرارات وتوصيات الجلسة," July 6, 2026, <https://iq.parliament.iq/blog/%D9%82%D8%B1%D8%A7%D8%B1%D8%A7%D8%AA-%D9%88-%D8%AA%D9%88%D8%B5%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%AC%D9%84%D8%B3%D8%A9-1-%D8%A7%D9%84%D8%A5%D8%AB%D9%86%D9%8A%D9%86-%D8%AB%D9%86%D9%8A%D9%86-6-%D8%AA/>; Altaghier News, "لجنة الأمن والدفاع النيابية تناقش مقترح قانون مكافحة جرائم تقنية المعلومات," July 26, 2026, <https://altaghier.tv/2026/07/26/%D9%84%D8%AC%D9%86%D8%A9-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D9%88%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9-%D8%A7%D9%84%D9%86%D9%8A%D8%A7%D8%A8%D9%8A%D8%A9-%D8%AA%D9%86%D8%A7%D9%82%D8%B4-%D9%85%D9%82%D8%AA/>.

¹⁰⁸ INSM, "Position Paper and Legal Opinion on the Draft Iraqi Law on Combating Information Technology Crimes of 2026," July 12, 2026, <https://insm-iq.org/en/?p=1837>; Hisham Kadhim, "Iraq's Cybercrime Law: Increasing suspicion instead of improving regulation," Jummar Media, July 6, 2026, <https://jummar.media/en/2026/07/06/iraqs-cybercrime-law/>; Alsa News, "تحذيرات من نصوص 'فضفاضة' في"، "مشروع قانون جرائم تقنية المعلومات," July 4, 2026, <https://alssaa.com/post/show/55583-%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1%D8%A7%D8%AA-%D9%85%D9%86-%D9%86%D8%B5%D9%88%D8%B5-%D9%81%D8%B6%D9%81%D8%A7%D8%B6%D8%A9-%D9%81%D9%8A-%D9%85%D8%B4%D8%B1%D9%88%D8%B9-%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA/>; Al-Mada News, "مرصد: غرامات تصل إلى 35 مليون دينار في قانون جرائم تقنية المعلومات," July 5, 2026, <https://almadapaper.net/442030/>.

judicial safeguards, and meaningful civil society input, the new cybercrime legislation could simply formalize the same vague, punitive logic that already governs online expression.

State Restrictions on Public Access to Websites and Applications

Iraqi authorities have at times restricted public digital access using broad and blunt measures such as internet shutdowns, app bans, and Domain Name System (DNS) restrictions. These measures do not target digital rights organizations directly, but they disrupt the same communications infrastructure that they rely on to document abuses, access information, and communicate.

The most recurring example is the use of internet shutdowns during national exam periods, allegedly to prevent exam leaks and cheating.¹⁰⁹ However, the government has disrupted internet access for other reasons, including during the 2019 protest movement, when authorities blocked most social media platforms and then cut off internet access more broadly to obstruct demonstrators, under the pretext of national security.¹¹⁰

Iraqi authorities apply a similar logic to platform access. In August 2023, the Ministry of Communications blocked Telegram, citing national security concerns and the need to protect users' personal data after data leaks involving state institutions and citizens. The government lifted the ban days later after Telegram responded to security requirements. In May 2026, the CMC announced that a separate Telegram suspension would be lifted after Telegram pledged to comply with Iraqi regulatory requirements related to content moderation, user protection, and Iraq's legal framework, while a member of parliament said his committee was still awaiting an explanation for why the platform had been suspended in the first place.¹¹¹

KRG authorities did not ban Telegram in 2023 nor in 2026.¹¹²

Iraqi authorities also threatened to block TikTok multiple times. In 2024, Communications Minister Hiyam Al Yasiri requested that the Council of Ministers ban the platform, accusing the app of "dismantling the fabric of Iraqi society" and

¹⁰⁹ Safaa Ayyad, "Will Iraq shut down the internet during the 2024 exams period?" SMEX, June 3, 2024, <https://smex.org/will-iraq-shut-down-the-internet-during-the-2023-exams-period/>; SMEX joint statement, "#NoExamShutdown: Open letter to authorities in Iraq to #KeepItOn during exams," May 8, 2024, <https://smex.org/noexamshutdown-open-letter-to-authorities-in-iraq-to-keepiton-during-exams/>.

¹¹⁰ Mahdi Ahmed, "Digital Rights Violations of Iraqis During the October (Tishreen) Protests: Internet Shutdowns, Platform Blocking, and Phone Searches," INSM, October 2, 2025, <https://insm-iq.org/en/?p=1711>.

¹¹¹ Rudaw English, "Iraq to lift ban on Telegram after platform agrees to regulatory conditions," May 9, 2026, <https://www.rudaw.net/english/categories/iraq/957078>.

¹¹² Netblocks, "Telegram restricted in Iraq over personal data leaks," August 6, 2023, <https://netblocks.org/reports/telegram-restricted-in-iraq-over-personal-data-leaks-9AkJ4o8D>; Shafaq News, "Telegram outage hits Iraqi cities as Kurdistan remains unaffected," April 3, 2026, <https://shafaq.com/en/society/Telegram-outage-hits-Iraqi-cities-as-Kurdistan-remains-unaffected>.

offering no educational or scientific benefit.¹¹³ Hayder Hamzoz, Executive Director of INSM, previously told SMEX that the proposed ban appeared to be an effort by the government to pressure the platform into complying with government content moderation and removal demands, especially where it viewed TikTok content as inconsistent with Iraqi customs and traditions.¹¹⁴

The Iraqi government announced plans in early 2025 to block Google's Domain Name System (DNS) servers in the country. In response to criticism, the Ministry of Communications claimed it only blocks websites based on official orders, not "personal whims."¹¹⁵ 4chan and Internet Archive, major public hubs for information-sharing and discussion, are already banned, among other international websites.¹¹⁶

Internet infrastructure in the KRI is largely autonomous from federal Iraq.¹¹⁷ Consequently, some websites remain blocked in federal Iraq but available in the KRI.¹¹⁸

Slow Digital Transformation in Iraq and the KRI

While the legal frameworks governing online speech and digital rights organizations remain outdated and slow to reform, interviewees described Iraqi authorities and the KRG as gradually pursuing digital transformation across state infrastructure in ways that raise new digital rights questions.¹¹⁹ The shift is most visible in the KRI, where the government has framed a transition to e-government as part of a broader modernization agenda.¹²⁰

Nabil described the KRI's e-government initiatives as early but meaningful steps toward digital governance. Compared to the past three to five years, he said, when

¹¹³ Shafaq News, "العراق يتحرك لحجب تطبيق تيك توك," March 25, 2024, <https://shafaq.com/ar/%D9%85%D8%AC%D8%AA%D9%80%D9%85%D8%B9/%D8%A7%D9%84%D9%8A%D8%A7%D8%B3%D8%B1%D9%8A-%D9%84%D8%B4%D9%81%D9%82-%D9%86%D9%8A%D9%88%D8%B2-%D9%82%D8%AF%D9%85%D9%86%D8%A7-%D8%B7%D9%84%D8%A8%D8%A7-%D9%84%D9%89-%D9%85%D8%AC%D9%84%D8%B3-%D8%A7%D9%84%D9%88%D8%B2%D8%B1%D8%A7-%D9%84%D8%AD%D8%AC%D8%A8-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%AA%D9%8A%D9%83-%D8%AA%D9%88%D9%83>.

¹¹⁴ Safaa Ayyad, "Iraq Threatens to Ban TikTok," SMEX, May 15, 2024, <https://smex.org/iraq-authorities-threaten-to-ban-tiktok/>.

¹¹⁵ Zeinab Ismail and Ragheb Ghandour, "Google's DNS Ban in Iraq Restricts Internet Freedom," SMEX, February 26, 2025, <https://smex.org/googles-dns-ban-in-iraq-restricts-internet-freedom/>.

¹¹⁶ Intellinews, "Iraq blocks 4chan in latest internet crackdown," November 29, 2024, <https://www.intellinews.com/iraq-blocks-4chan-in-latest-internet-crackdown-355802/>.

¹¹⁷ Ameer al Dujaili, "Internet Censorship in Iraq and Its Impact on Useful Content," July 9, 2026, <https://pulse.internetsociety.org/en/blog/2026/07/internet-censorship-in-iraq-and-its-impact-on-useful-content/>.

¹¹⁸ Dana Taib Menmy, "Iraq blocks at least 400 pornographic websites," November 8, 2022, <https://www.newarab.com/news/iraq-blocks-pornographic-websites>.

¹¹⁹ SMEX written exchange with "Nabil," May 14, 2026.

¹²⁰ Several initiatives, such as the KRG Services Portal, the Shafafiat platform, KurdPass, and the digitization of national identity and passport services, illustrate the KRI's gradual shift toward e-government. See: Kurdistan Region of Iraq, Strategy for Digital Governance, n.d., <https://gov.krd/dxs/>; INSM, "About our data, whose control? E-Government and Privacy in the Kurdistan Region," June 15, 2026, <https://insm-iq.org/en/?p=1765>.

most government work still depended on paper files and physical processes, citizens now have access to digital platforms for some state services.¹²¹ But he also stressed that traditional systems remain in place, and that both government employees and citizens need more education and training before digital governance can be implemented comprehensively.

INSM's analysis of e-government and privacy in the KRI captures the central risk.¹²² As public services increasingly rely on digital identity, biometrics, population records, payroll integration, complaints systems, and online applications, the state's ability to collect and combine personal information expands quickly. But, if data collection capacity expands faster than oversight mechanisms are developed, citizens may gain more convenient services while losing meaningful control over their own data.

Citizen Reporting and Public Morality

The Ministry of Interior's "Ballegh" application demonstrates how the existing gap between Iraq's old laws and the emergence of new forms of digital media has created a vacuum that is being filled by policing rather than protection.¹²³ Launched in January 2023, Ballegh allows users to report social media content that allegedly violates public morals, contains "negative and indecent" messages, or undermines social stability.¹²⁴ Interviewees described Ballegh as part of a growing citizen reporting infrastructure that lacks transparent standards, public accountability, and clear safeguards against misuse.¹²⁵

The Ministry of Interior, when launching the app, said "offensive" content is as "dangerous as organised crime...one of the causes of destruction of the Iraqi family and society."¹²⁶ The same "family values" framing appeared in the ministry's own explanation of how Ballegh works. Ayad Radhi, the Interior Ministry IT administrator in charge of the app, told The Record that the government was

¹²¹ Sarah Sanbar, "Broken Promises of Compensation for Sinjaris," Rudaw, July 13, 2024, <https://www.rudaw.net/english/categories/opinion/810384>.

¹²² INSM, "About our data, whose control? E-Government and Privacy in the Kurdistan Region," June 15, 2026, <https://insm-iq.org/en/?p=1765>.

¹²³ Article 19, "Iraq : Balgh platform marks two years as a tool of repression," January 16, 2025, <https://www.article19.org/resources/iraq-balgh-platform-marks-two-years-as-tool-of-repression/>.

¹²⁴ Iraqi News Agency, "وزارة الداخلية: تشكيل لجنة لمتابعة المحتويات بمواقع التواصل ومحاسبة صانعيها," January 16, 2023, <https://ina.iq/175883--.html>; Safa Ayyad, "Iraq's Controversial 'Ballegh' Platform for 'Combating Indecent Content,'" February 15, 2023, <http://smex.org/irags-controversial-ballegh-platform-for-combating-indecent-content/>.

¹²⁵ SMEX phone interview with "Omar," April 16, 2026.

¹²⁶ SMEX, "منصة 'بلغ' العراقية 'لمحاربة المحتوى الهابط' تثير الجدل," February 13, 2023, <https://smex.org/ar/%D9%85%D9%86%D8%B5%D8%A9-%D8%A8%D9%84%D9%91%D8%BA-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82%D9%8A%D8%A9/>; "TikTokers jailed as Iraq targets 'decadent content,'" France 24, February 16, 2023, <https://www.france24.com/en/live-news/20230216-tiktokers-jailed-as-iraq-targets-decadent-content>.

protecting “family values” and said the most reported content usually involved videos that violated “the core principles of the Iraqi family.”¹²⁷

Tens of thousands of social media posts have been reported since its launch, with 14 people charged during Ballegh’s inaugural year for publishing “indecent content.”¹²⁸ The cases were prosecuted under the penal code framework.¹²⁹ An Iraqi judge told local media that cases opened up against content creators could even be tried transnationally as long as the content targeted Iraqis or Iraqi society.¹³⁰

Yasmine told SMEX that her organization’s monitoring suggests that Ballegh reports most often affect content creators, social media personalities, and journalists.¹³¹ She said her organization has tried to understand how reports are reviewed, what safeguards exist to prevent abuse, and whether decisions reflect real-time reports or the “mood” of the government or Interior Ministry, but officials have not meaningfully engaged with those questions.

Iraqi rights activists, politicians and lawyers have stated the campaign against social media influencers is an attempt to “direct public opinion” and that it signals a prelude to a wider crackdown on free expression online.¹³² Hayder Hamzoz repeated a similar sentiment when he previously told SMEX that the campaign was an “early warning” about the trajectory of digital freedom because it appeared “biased, retaliatory and deterrent.”¹³³

The Iraqi Observatory for Human Rights (IOHR) connects this online campaign to real-life violence faced by women content creators:

A systematic campaign, orchestrated by political actors and armed groups, aims to ‘liquidate’ active female presence from the public domain... The IOHR further asserts that current events are not merely

¹²⁷ Dina Temple-Raston and Sean Powers, “Crowdsourcing morality: How an app allows the Iraqi government to arrest ‘indecent’ influencers,” The Record, May 2, 2023,

<https://therecord.media/iraq-ballegh-app-interview-interior-ministry-click-here>.

¹²⁸ Iraqi News Agency, “القضاء يكشف تفاصيل مكافحة المحتوى الهابط وأعداد المتهمين ويفصح عن لائحة مرتقبة للنشر بمواقع التواصل,” February 13, 2023, <https://ina.ig/178165--.html>.

¹²⁹ Saman Dawod, “Cases against social media influencers raise concerns over freedoms in Iraq,” May 10, 2023, <https://amwaj.media/en/article/iraq-influencers-social-media>.

¹³⁰ Iraqi News Agency, “القضاء يكشف تفاصيل مكافحة المحتوى الهابط وأعداد المتهمين ويفصح عن لائحة مرتقبة للنشر بمواقع التواصل,” February 13, 2023, <https://ina.ig/178165--.html>.

¹³¹ SMEX phone interview with “Yasmine,” June 5, 2026.

¹³² Saman Dawod, “Cases against social media influencers raise concerns over freedoms in Iraq,” May 10, 2023, <https://amwaj.media/en/article/iraq-influencers-social-media>; France 24, “TikTokers jailed as Iraq targets ‘decadent content,’” February 16, 2023,

<https://www.france24.com/en/live-news/20230216-tiktokers-jailed-as-iraq-targets-decadent-content>;

Dina Temple-Raston and Sean Powers, “Crowdsourcing morality: How an app allows the Iraqi government to arrest ‘indecent’ influencers,” May 2, 2023,

<https://therecord.media/iraq-ballegh-app-interview-interior-ministry-click-here>; Iraqi Observatory for Human Rights, “Arbitrary arrests over ‘low-quality content’ may pave way for restricting freedoms,” February 13, 2023, <https://iohriq.org/114-.html>.

¹³³ Safa Ayyad, “Iraq’s Controversial ‘Ballegh’ Platform for ‘Combating Indecent Content,’” February 15, 2023, <http://smex.org/iraqs-controversial-ballegh-platform-for-combating-indecnt-content/>.

isolated violations, but rather a full-fledged 'Strategy of Displacement' that utilizes digital incitement as a precursor to physical assassination or forced social exclusion.¹³⁴

In April 2024, an unidentified gunman shot Iraqi influencer Ghufraan Mahdi Sawadi, known as Um Fahad, dead outside her home in Baghdad.¹³⁵ She previously received a six-month prison sentence for social media videos authorities deemed to violate public decency and morals.¹³⁶ Her killing followed the September 2023 fatal shooting of another prominent social media figure, Noor Alsaffar, in Baghdad, and several other influencers.¹³⁷

Administrative and Financial Penalties for Civil Society Organizations

Iraqi civil society organizations also face financial and administrative barriers that limit their ability to withstand legal or political pressure.¹³⁸ A 2022 study found that registering an organization can take months or years.¹³⁹ It also found that many organizations rely on internal donations, membership fees, founders' personal resources, or international aid, while politicized organizations can use their connections to capture grants and civil society opportunities. This does not amount to the same systematic financial suffocation seen in Egypt or Tunisia, but it leaves Iraqi organizations with limited buffers when they face lawsuits, administrative pressure, or reputational attacks.

Militias in the Iraqi Digital Landscape

A key distinguishing factor of Iraq's digital environment is the role of militias, specifically factions of the Popular Mobilization Forces (PMF). Rights organizations have documented coordinated harassment campaigns, doxxing, and physical

¹³⁴ Iraqi Observatory for Human Rights, "The Systematic Erasure: Excluding Women from Iraq's Public Sphere," March 8, 2026, <https://iohriq.org/188-.html>.

¹³⁵ Kathryn Armstrong, "Iraqi TikTok star Om Fahad shot dead in Baghdad," April 26, 2024, <https://www.bbc.com/news/world-middle-east-68910812>.

¹³⁶ EuroMed Human Rights Monitor, "Iraq: Decision to convict imprisoned content creators is unjustified, must be reversed," February 15, 2023, <https://euromedmonitor.org/en/article/5540/Iraq:-Decision-to-convict-imprisoned-content-creators-is-unjustified,-must-be-reversed>.

¹³⁷ Abbas al-Khashali, "مقتل 'أم فهد' .. اغتيالات تطل 'مشاهير' الانترنت," May 2, 2024, DW Arabic, <https://www.dw.com/ar/%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82-%D8%A7%D9%84%D9%8A%D9%88%D9%85-%D9%85%D9%82%D8%AA%D9%84-%D8%A3%D9%85-%D9%81%D9%87%D8%AF-%D8%A7%D8%BA%D8%AA%D9%8A%D8%A7%D9%84%D8%A7%D8%AA-%D8%AA%D8%B7%D8%A7%D9%84-%D9%85%D8%B4%D8%A7%D9%87%D9%8A%D8%B1-%D8%A7%D9%84%D8%A7%D9%86%D8%AA%D8%B1%D9%86%D9%8A%D8%AA/audio-68979423>; Nadeen Ebrahim, Nechirvan Mando, "Prominent Iraqi TikToker fatally shot in Baghdad amid crackdown on LGBTQ community," BBC News, September 28, 2023, <https://www.cnn.com/2023/09/27/middleeast/iraq-lgbtq-shot-intl>.

¹³⁸ SMEX phone interview with "Aiman," May 22, 2026

¹³⁹ Marsin Alshamary and Sura Maqsood, "The Landscape of Civil Society in Iraq," June 2022, Konrad Adenauer Stiftung, <https://cnxus.org/the-iraqi-knowledge-sharing-platform/wp-content/uploads/2022/07/The-Landscape-of-Civil-Society-in-Iraq.pdf>.

intimidation perpetrated by PMF affiliates.¹⁴⁰ This makes Iraq distinct from Egypt or Tunisia, where repression more often flows through centralized state institutions. In Iraq, non-state and quasi-state armed actors can help set the terms of online speech even when they do not formally control the legal process.

Rights groups and media reporting support this pattern. “Electronic armies” linked to powerful pro-Iran factions accuse critics of collaborating with Israel or the United States, a charge that can expose them to serious danger.¹⁴¹ Several Iraq experts mentioned Steven Nabil, an Iraqi journalist who covered Iranian-backed militias and subsequently faced intimidation, death threats, and harassment. Researchers have identified him as one of the most frequently trolled Iraqi journalists.¹⁴²

The same tactics carry a gendered dimension. Yasmine said some Telegram channels that publish hate speech and incite violence against women activists are linked to militias.¹⁴³ She pointed to the case of Reham Yacoub, whose image was circulated on a militia-run Telegram channel alongside accusations that she worked with the US embassy. She was later killed by unidentified gunmen after repeated threats.¹⁴⁴

C. Tunisia

Tunisia presents one of the most visible cases of accelerating digital authoritarianism in the SWANA region. SMEX found that since President Kais Saied’s 2021 consolidation of power, Tunisian authorities have developed and deployed a system of laws and administrative procedures that increasingly resemble the consolidated digital control apparatus exhibited by Egypt. Conditions actively deteriorated while SMEX conducted the research for this report with dozens of Tunisian NGOs at imminent risk of closure.¹⁴⁵ The rapidly

¹⁴⁰ Mahdi Ahmed, “Digital Rights Violations of Iraqis During the October (Tishreen) Protests: Internet Shutdowns, Platform Blocking, and Phone Searches,” INSM, October 2, 2025, <https://insm-iq.org/en/?p=1711>; Freedom House, “Freedom on the Net 2023,” <https://freedomhouse.org/country/iraq/freedom-net/2023>; Kathryn Armstrong, “Iraqi TikTok star Om Fahad shot dead in Baghdad,” April 26, 2024, <https://www.bbc.com/news/world-middle-east-68910812>.

¹⁴¹ Asharq al-Awsat, “‘Electronic Armies’ Threaten Activists, Media in Iraq,” September 6, 2019, <https://english.aawsat.com/home/article/1889676/electronic-armies-threaten-activists-media-iraq>; Zainab Almashat, “‘My questions are turned into a weapon to kill me’: the deadly war against Iraq’s journalists,” March 22, 2023, <https://www.theguardian.com/global-development/2023/mar/22/deadly-war-against-iraq-journalists-killed>.

¹⁴² Al-Rawi, Ahmed, Chris Tenove, and Peter Klein, “The Networked Trolling of Critical Journalists and News Organizations in Iraq” *Journalism and Media* 4, no. 4: 1130-1140, <https://doi.org/10.3390/journalmedia4040072>.

¹⁴³ SMEX phone interview with “Yasmine,” June 5, 2026.

¹⁴⁴ Taif Alkhudary and Hayder Al-Shakeri, “Rest in Power: Reham Yacoub’s assassination casts its long shadow over Iraq,” August 25, 2020, <https://www.newarab.com/opinion/rest-power-reham-yacoub>.

¹⁴⁵ Mahdi Jlassi, “Tunisie : L’Association des magistrats s’accroche à son indépendance,” Nawaat, <https://nawaat.org/2026/02/19/tunisie-lassociation-des-magistrats-saccroche-a-son-independance/>; Amnesty International, May 11, 2026, “Tunisia: Dozens of NGOs at risk of dissolution as crackdown on civil society intensifies,”

changing environment also made the research itself more difficult by narrowing the pool of digital experts willing or able to speak openly about their experiences.

Interviewees consistently pointed to the 2021 power grab as the most significant inflection point in Tunisia's trajectory towards digital authoritarianism. Existing research similarly traces the erosion of civic freedoms to this moment.¹⁴⁶ The period of genuine civic and digital openness brought on by the 2011 revolution and anchored by Decree-Law 115 on press freedom and Decree-Law 88 on associations has been systematically dismantled.

Since 2021, Kais Saied has installed an increasingly restrictive legal framework that gives the state sweeping authority over online life and the organizations and individuals who inhabit it. The most consequential element of Saied's legal toolbox is Decree-Law 54 on Combating Crimes Related to Information and Communication Systems of 2022 (Decree-Law 54 for short), a cybercrime decree weaponized against journalists, lawyers, judges, human rights defenders, and ordinary citizens alike. Laila, an Egyptian digital expert familiar with Tunisia, described the country as following "the same blueprint" that Egypt experienced between 2013 and 2019, particularly since Decree-Law 54 was adopted.¹⁴⁷

The 2015 Counterterrorism Law, financial crime investigations, asset freezes, administrative suspensions, and money laundering charges add to the "arsenal" of tools used to restrict civic space.¹⁴⁸ Dozens if not hundreds of Tunisian advocacy and civil society groups are at risk of forced closure, but that number is likely much higher due to some organizations choosing not to publicly disclose the current difficulties they're facing with the government.¹⁴⁹ Organizations working on migration, LGBTQ+ rights, and anti-corruption are especially exposed. Like their Egyptian peers, Tunisian civil society actors face online smear campaigns orchestrated by government officials or pro-government media.¹⁵⁰

<https://www.amnesty.org/en/latest/news/2026/05/tunisia-dozens-of-ngos-at-risk-of-dissolution-as-crackdown-on-civil-society-intensifies/>.

¹⁴⁶ International Center for Not-For-Profit Law, "Civic Freedom Monitor: Tunisia," August 2, 2026, <https://www.icnl.org/resources/civic-freedom-monitor/tunisia?do=pdf>; Human Rights Watch, "All Conspirators: How Tunisia Uses Arbitrary Detention to Crush Dissent," April 16, 2025, <https://www.hrw.org/report/2025/04/16/all-conspirators/how-tunisia-uses-arbitrary-detention-crush-dissent>.

¹⁴⁷ SMEX phone interview with "Laila," May 22, 2026.

¹⁴⁸ SMEX phone interview with "Adham," April 15, 2026.

¹⁴⁹ SMEX phone interview with "Nissaf," June 5, 2026; SMEX written correspondence with "Mona," June 11, 2026; L'Economiste Maghribin, "Tunisie : plus de 600 associations menacées de suspension," November 11, 2011, <https://www.leconomistemaghreb.com/2025/11/11/tunisie-plus-de-600-associations-menacees-de-suspension/>; Amnesty International, May 11, 2026, "Tunisia: Dozens of NGOs at risk of dissolution as crackdown on civil society intensifies," <https://www.amnesty.org/en/latest/news/2026/05/tunisia-dozens-of-ngos-at-risk-of-dissolution-as-crackdown-on-civil-society-intensifies/>.

¹⁵⁰ Haifa Mzalouat and Mathilde Warda, "'Civil Society', in the crosshairs of Kaïs Saïed," Inkyfada, March 15, 2022, <https://inkyfada.com/en/2022/03/15/kais-saied-threat-civil-society-tunisia/>; "Civil Society: Threats of dismantling and demonization," Inkyfada podcast, March 9, 2022, <https://inkyfada.com/en/podcast/inkytalk-english/3-civil-society-threats-of-dismantling-and-demonization/>.



Saied repeatedly paints these groups as “corrupt and illegitimate intermediaries” in his public appearances.¹⁵¹ His philosophy of direct rule paints these groups as standing between him and the Tunisian people, Rouba, a Tunisian journalist, explained.¹⁵²

Legal Architecture Governing Digital Speech and Activities

Tunisia’s crackdown on online speech using Decree-Law 54 marks a sharp departure from the legal framework that emerged after Tunisia’s 2011 revolution. Decree-Law 115 of 2011 governed freedom of the press, printing, and publishing, while Decree-Law 88 of 2011 established one of the region’s most enabling legal frameworks for civil society by protecting freedom of association and prohibiting state interference in CSO operations. Those laws did not fully resolve Tunisia’s free expression and association challenges, but they established a baseline that many digital rights and civil society actors still view as a workable legal framework for public-interest speech and organizing.

Decree-Law 54, issued by President Kais Saied on September 13, 2022, reversed much of that trajectory. Article 24 of the decree imposes penalties of up to five years in prison and a fine of up to 50,000 TND for using communication networks to spread “false news,” rumors, or information deemed to harm public security, national defense, or others’ rights; the prison sentence doubles if the targeted person is considered a public official. The decree has since become a central tool for policing public discourse.¹⁵³ Dozens of politicians, lawyers, media figures, artists, academics, and individual internet users have faced criminal charges under Decree-Law 54.¹⁵⁴

“Nissaf,” a Tunisian human rights advocate, said that civil society organizations did not initially grasp how far-reaching Decree-Law 54 would become.¹⁵⁵ She said the

¹⁵¹ Amnesty International, “Tunisie. Le durcissement de la répression contre les organisations de défense des droits humains atteint des niveaux critiques,” November 14, 2025, <https://www.amnesty.org/fr/latest/news/2025/11/tunisia-escalating-crackdown-on-human-rights-organizations-reaches-critical-levels/>.

¹⁵² SMEX phone interview with “Rouba,” May 19, 2026.

¹⁵³ Mahdi Jlassi, Rihab Boukhatia, Najla Ben Salah, “Criminalizing Dissent: Six Stories from Tunisia’s Political and Media Crackdown,” Nawaat, December 20, 2025, <https://nawaat.org/2025/12/20/criminalizing-dissent-six-stories-from-tunisias-political-and-media-crackdown/>.

¹⁵⁴ AlJazeera, “Tunisia sentences opposition leader Abir Moussi to 12 years in jail,” December 12, 2025, <https://www.aljazeera.com/news/2025/12/12/tunisia-sentences-opposition-leader-abir-moussi-to-12-years-in-jail>; Human Rights Watch, “Tunisia: Death Sentence for Facebook Posts,” October 8, 2025, <https://www.hrw.org/news/2025/10/08/tunisia-death-sentence-for-facebook-posts>; Wagdy Sawahel, “Academics, students call for release of political prisoners,” University World News, May 23, 2023, <https://www.universityworldnews.com/post.php?story=20230521180218178>; Amnesty International, “Tunisia: Artist Jailed for Criticizing President: Rached Ghabbour,” March 28, 2024, <https://www.amnesty.org/en/documents/mde30/7893/2024/en/>; Human Rights Watch, “Tunisia: Authorities Escalate Crackdown on Media, Freedom of Expression,” May 30, 2024, <https://www.hrw.org/news/2024/05/30/tunisia-authorities-escalate-crackdown-media-freedom-expression>; Human Rights Watch, “Tunisia: Prominent Lawyer Arbitrarily Detained,” February 10, 2026, <https://www.hrw.org/news/2026/02/10/tunisia-prominent-lawyer-arbitrarily-detained>.

¹⁵⁵ SMEX phone interview with “Nissaf,” June 5, 2026.



decree was adopted without meaningful CSO input and was presented by the government as a technical measure to regulate cybercrime, make the internet safer, and bring Tunisia closer to international cybercrime standards, including the Budapest Convention on Cybercrime.¹⁵⁶ At the time, civil society actors were already overwhelmed by Saïed's broader government overhaul and constitutional referendum and were not coordinated enough to respond forcefully.¹⁵⁷ Many initially assumed the decree would primarily impact freedom of expression organizations or the journalists' union. Instead, she said, it quickly became clear that political parties, judges, journalists, lawyers, and civil society organizations all had a stake in opposing it.

The 2015 Counterterrorism Law adds another layer to Tunisia's digital rights environment.¹⁵⁸ Rights groups warned upon its adoption that it expanded security powers while weakening due process safeguards.¹⁵⁹ Activists frequently face charges under this law, often together with Decree-Law 54.

Legal Architecture Impacting Digital Rights Organizations' Day-to-Day Activities

Tunisian authorities also rely on financial crime, money laundering, counterterrorism, and administrative regulations to pressure civil society organizations and independent media.¹⁶⁰ Rights groups and media repeatedly document arbitrary arrests, asset freezes, bank restrictions, financial investigations, and court-ordered suspensions imposed under the stated aim of combating "suspicious" foreign funding and protecting national interests.

These measures disrupt organizations' day-to-day operations by diverting staff time and resources from core work toward responding to investigations, managing financial restrictions, and defending their legal status. Organizations are sometimes unexpectedly asked to produce paperwork, registration renewals, and financial records from the past decade, and to return repeatedly to government offices to answer questions. Rouba, a Tunisian journalist, described

¹⁵⁶ Council of Europe, "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols," available <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

¹⁵⁷ Human Rights Watch, "Tunisia: Questions and Answers on the Draft Constitution," July 14, 2022, <https://www.hrw.org/news/2022/07/14/tunisia-questions-and-answers-draft-constitution>.

¹⁵⁸ Basic Law 2015-26 of 7 August 2015 dealing with combating terrorism and preventing money-laundering as amended by Basic Law 2019-09 of 23 January 2019, available <https://ctaf.gov.tn/data/uploads/pdf/6172e2e9284080.20621154.pdf>.

¹⁵⁹ Amnesty International, "Tunisia: Flaws in Revised Counterterrorism Bill," July 15, 2015, <https://www.amnesty.org/en/latest/news/2015/07/tunisia-flaws-in-revised-counterterrorism-bill>; International Commission of Jurists, "Position Paper: Tunisia's Law on Counter-Terrorism in light of international law and standards," August 6, 2015, <https://www.icj.org/wp-content/uploads/2015/08/Tunisia-CT-position-paper-Advocacy-PP-2015-ENG-REV.pdf>.

¹⁶⁰ Mahdi al-Ash, Legal Agenda, "المجتمع المدني في مواجهة الاستبداد," December 2025, https://legal-agenda.com/wp-content/uploads/2025/12/Legal-Agenda_TN_34_FILE_Web-1.pdf.

this as a form of “harassment” meant to exhaust organizations rather than resolve any specific legal issue.¹⁶¹

Every Tunisian interviewee described how their respective organizations have been summoned or are about to be summoned by financial crimes and money laundering authorities without clear charges. To date, dozens of civil society groups such as Amnesty International, Avocats Sans Frontières, Association Tunisienne des Femmes Démocrates, Tunisian Forum for Economic and Social Rights, and the Tunisian League for Human Rights, as well as independent media outlets including Inkyfada and Nawaat, have faced administrative suspensions.¹⁶² These administrative pressures compound the funding and capacity constraints discussed later in this report.

Targeting of Anti-Racist, Migrant and Refugee Rights Groups

Rights groups have documented particularly intense pressure on organizations working on migration, refugee protection, and anti-racism.¹⁶³ Nissaf emphasized that these groups are not alone. LGBTQ+ organizations, women’s rights, and media organizations also face government pressure, but authorities can more easily exploit existing racist and anti-migrant sentiment to legitimize an initial wave of repression against migration-focused groups and then expand the crackdown.¹⁶⁴ “Honestly, in this respect we are all equal,” she said.

In February 2023, President Saïed claimed that migration from sub-Saharan Africa was part of a plan to alter Tunisia’s demographic makeup, remarks widely condemned as racist and followed by intense waves of violence targeting Black

¹⁶¹ SMEX phone interview with “Rouba,” May 19, 2026.

¹⁶² Avocats Sin Fronteres, “ASF en Tunisie suspendue pendant 30 jours (français),” May 6, 2026, <https://asf.be/publication/asf-en-tunisie-suspendue-pendant-30-jours/?lang=fr>; International Federation for Human Rights, “Tunisia: Arbitrary suspension of ATFD and FTDES – Freedom of association under attack,” November 3, 2025, <https://www.fidh.org/en/region/north-africa-middle-east/tunisia/tunisia-arbitrary-suspension-of-atfd-and-ftdes-freedom-of-association>; International Federation for Human Rights, “Tunisia: The longest-standing human rights organisation suspended by the dictatorship of Kais Saïed,” April 27, 2026, <https://www.fidh.org/en/region/north-africa-middle-east/tunisia/tunisia-the-longest-standing-human-rights-organisation-suspended-by>; Amnesty International, “Tunisia: Escalating crackdown on human rights organizations reaches critical levels,” November 14, 2025, <https://www.amnesty.org/en/latest/news/2025/11/tunisia-escalating-crackdown-on-human-rights-organizations-reaches-critical-levels/>; Nawaat, “Nawaat will not be silenced,” October 31, 2025, <https://nawaat.org/2025/10/31/nawaat-will-not-be-silenced/>; Inkyfada, “Al Khatt, l’éditrice de inkyfada, est convoquée en dissolution. Nous continuons,” April 23, 2026, <https://inkyfada.com/fr/2026/04/23/alkhatt-inkyfada-dissolution-continue/>.

¹⁶³ Human Rights Watch, “Tunisia: Joint Statement Calling for End to Crackdown,” June 18, 2024, <https://www.hrw.org/news/2024/06/18/tunisia-joint-statement-calling-end-crackdown>; Amnesty International, “Tunisia: Repressive crackdown on civil society organizations following months of escalating violence against migrants and refugees,” May 16, 2024, <https://www.amnesty.org/en/latest/news/2024/05/tunisia-repressive-crackdown-on-civil-society-organizations-following-months-of-escalating-violence-against-migrants-and-refugees/>.

¹⁶⁴ SMEX phone interview with “Nissaf,” June 5, 2026; Najla Ben Salah, “Denigration, Kais Saïed’s political weapon of choice,” February 28, 2024, <https://nawaat.org/2024/02/28/denigration-kais-saieds-political-weapon-of-choice/>.

and migrant populations in Tunisia.¹⁶⁵ In May 2024, Saied again attacked civil society organizations working on migration, accusing them of being “traitors” and “foreign agents” and of seeking to facilitate the “settlement” of sub-Saharan migrants in Tunisia.¹⁶⁶

The case against Mnementy (“My Dream”), a Tunisian anti-racism group, reflects this broader dynamic. Its president, Saadia Mosbah, is a prominent Black Tunisian activist who helped push for Tunisia’s 2018 law on eliminating racial discrimination. In May 2024, amid a wider crackdown on organizations working on migration, asylum, and racial justice, security forces arrested Mosbah and Mnementy’s program coordinator, Zied Rouin, searched Mosbah’s home and the organization’s offices, and confiscated devices and documents. Rouin was released after questioning, but Mosbah was placed in custody as part of an investigation into alleged financial crimes. Pro-government social media accounts carried out an aggressive smear campaign against Mosbah in the days before her arrest. Mosbah remains arbitrarily detained since May 2024. In March 2026, authorities sentenced her to eight years in prison and fined her 122,000 TND on unsubstantiated charges of money laundering and “illicit enrichment.” Five other Mnementy staff and collaborators received prison sentences ranging from one to three years and fines of up to 64,000 TND. Tunisian authorities have sought to dissolve Mnementy, with dissolution proceedings opening in May 2026.

Authorities have also targeted other prominent migrant and refugee rights organizations, including the Association for the Promotion of the Right to Difference (ADD), Terre d’Asile Tunisie, the Tunisian Council for Refugees, Children of the Moon of Medenine, and the Tunisian Forum for Economic and Social Rights.¹⁶⁷

¹⁶⁵ Amnesty International, “Tunisia: President’s racist speech incites a wave of violence against Black Africans,” March 10, 2023, <https://www.amnesty.org/en/latest/news/2023/03/tunisia-presidents-racist-speech-incites-a-wave-of-violence-against-black-africans/>.

¹⁶⁶ Amnesty International, “Tunisia: Escalating crackdown on human rights organizations reaches critical levels,” November 14, 2025, <https://www.amnesty.org/en/latest/news/2025/11/tunisia-escalating-crackdown-on-human-rights-organizations-reaches-critical-levels/>.

¹⁶⁷ Human Rights Watch, “Tunisia: End Abusive Prosecution of Refugee Aid Workers,” May 11, 2026, <https://www.hrw.org/news/2026/05/11/tunisia-end-abusive-prosecution-of-refugee-aid-workers>.

II. Advocacy Strategies Employed by Digital Rights Groups in Egypt, Iraq and Tunisia

Despite the severe and outright debilitating restrictions in Egypt, Iraq, and Tunisia described in this report, digital rights organizations continue to develop strategies for operating within increasingly hostile environments.

A. “Cause Lawyering”: Offensive and Defensive Strategic Litigation

Rights groups with in-house lawyers sometimes use strategic litigation to challenge government restrictions on free expression and defend people criminally prosecuted for their peaceful speech. Strategic litigation is one tool of “cause lawyering,” a term used to describe lawyers who use legal work to support social movements or pursue broader rights-based change.¹⁶⁸ Cause lawyering has a long history in the SWANA region and continues today in Egypt, Iraq, and Tunisia, although lawyers in each country face distinct constraints on their ability to defend free expression.¹⁶⁹

Strategic litigation can take both offensive and defensive forms. Offensive strategic litigation proactively challenges an abusive law, policy, or government action.¹⁷⁰ Rather than responding to a prosecution, lawyers choose the legal claim, the plaintiff, and the remedy they seek. They may ask a court to strike down a law, stop an unlawful practice, or recognize a right that authorities have ignored. The goal is not only to secure relief for the people involved in the case, but to change the law or how it is applied more broadly.¹⁷¹

¹⁶⁸ Cause lawyering also includes research and public advocacy. It has also been referred to as “political lawyering” or “rights lawyering.”

¹⁶⁹ , “Challenging the Legal Ideology of the State: Cause Lawyering and Social Movements in Egypt,” May 24, 2019, Arab Reform Initiative, <https://www.arab-reform.net/publication/challenging-the-legal-ideology-of-the-state-cause-lawyerin-g-and-social-movements-in-egypt/>; “Lawyering for Change: Q&A with on Egypt,” The Tahrir Institute for Middle East Policy, April 19, 2021, <https://timep.org/2021/04/19/ga-with-ahmed-ezzat-on-egypt/>; Eric Gobe, “Tunisia. Lawyers: A Political Profession?” Lawyers in 21st Century Societies. Volume 1: National Reports, April 22, 2020, <https://shs.hal.science/halshs-02551329/document>,

¹⁷⁰ See *Pursuing the Public Interest: A Handbook for Legal Professionals and Activists*, chapter 3, “Strategic Litigation: Bringing Lawsuits in the Public Interest,” Columbia School of Law, 2001, available:

<https://www.pilnet.org/wp-content/uploads/2020/04/Pursuing-the-Public-Interest-Article.pdf>; International Commission of Jurists, *Strategic Litigation Handbook for Myanmar: First Edition*: September 2019, <https://www.ici.org/wp-content/uploads/2019/09/Myanmar-Strat-Litig-HB-Publications-Report-Thematic-reports-2019-ENG.pdf>.

¹⁷¹ See *Pursuing the Public Interest: A Handbook for Legal Professionals and Activists*, chapter 3, “Strategic Litigation: Bringing Lawsuits in the Public Interest,” Columbia School of Law, 2001, available:

<https://www.pilnet.org/wp-content/uploads/2020/04/Pursuing-the-Public-Interest-Article.pdf>; International Commission of Jurists, *Strategic Litigation Handbook for Myanmar: First Edition*: September 2019, <https://www.ici.org/wp-content/uploads/2019/09/Myanmar-Strat-Litig-HB-Publications-Report-Thematic-reports-2019-ENG.pdf>.



Defensive strategic litigation begins when state authorities criminally prosecute a person and lawyers respond by contesting the charges. Yet not every criminal defense case qualifies as strategic litigation. Criminal defense litigation becomes strategic when lawyers deliberately use one or more cases to pursue a broader legal or social justice goal. Lawyers may coordinate arguments across several similar prosecutions to demonstrate a pattern of abuse or reveal recurring misuse of a law. They may also connect the cases to a wider human rights campaign.

This report finds that rights groups in Egypt, Iraq, and Tunisia rely more heavily on defensive strategic litigation and other forms of cause lawyering than in offensive litigation to protect online expression. The approach to defensive litigation differs by country. Egyptian lawyers defend people prosecuted under cybercrime and morality provisions while pursuing some offensive litigation in less politically sensitive fields. Iraqi and Kurdish lawyers challenge the application of outdated penal, counterterrorism, and telecommunications laws in individual speech cases. In Tunisia, groups have focused primarily on documenting prosecutions, training defense lawyers, and protecting the legal profession rather than developing a coordinated strategic litigation agenda.

Repressive laws, government pressure on lawyers and rights groups, and the erosion of judicial independence – particularly in Egypt and Tunisia – constrain both offensive and defensive strategic litigation.¹⁷² Egypt's surviving rights organizations have already adapted to years of consolidated repression and now operate in an environment with narrow legal openings. Tunisian groups are currently fighting to preserve their legal status and basic ability to operate amid an accelerating crackdown. Iraq's fragmented legal and political system leaves lawyers somewhat more room to engage with courts, but they must work with an outdated set of laws to litigate free expression cases. The country sections below examine the limited legal openings that remain.

Egypt

Since Abdel Fattah al-Sisi took power in 2013, Egyptian rights lawyers have relied mainly on defensive legal strategies to address free speech violations.¹⁷³ Strategic criminal defense has previously forced authorities to change how they prosecute online expression, but the state responded by shifting to broader and more punitive legal frameworks.¹⁷⁴

¹⁷² Ariq Hatibie, "Prospects and Obstacles of Strategic Human Rights Litigation Globally: A Spotlight on Egypt," Human Rights Program at Harvard Law School, March 21, 2024, <https://hrp.law.harvard.edu/prospects-and-obstacles-of-strategic-human-rights-litigation-globally-a-spotlight-on-egypt/>.

¹⁷³ , "Challenging the Legal Ideology of the State: Cause Lawyering and Social Movements in Egypt," May 24, 2019, Arab Reform Initiative, <https://www.arab-reform.net/publication/challenging-the-legal-ideology-of-the-state-cause-lawyerin-g-and-social-movements-in-egypt/>.

¹⁷⁴ , "Challenging the Legal Ideology of the State: Cause Lawyering and Social Movements in Egypt," May 24, 2019, Arab Reform Initiative,

Beginning around 2020, Egyptian authorities increasingly moved away from prosecuting LGBTQ+ people primarily under morality and prostitution laws and towards prosecuting them using cybercrime legislation in the Economic Court, according to documentation by Egyptian rights group Bedayaa and research by digital rights expert Afsaneh Rigot.¹⁷⁵ Rigot attributes this change to the work of skilled criminal defense teams. Egyptian lawyers repeatedly exposed evidentiary and procedural flaws in debauchery cases and argued that prosecutors had failed to establish the legal elements required for conviction. In several cases Rigot reviewed, these legal defense arguments successfully secured acquittals or reduced sentences for defendants.¹⁷⁶

As these defenses made debauchery prosecutions harder to sustain, authorities adapted rather than abandon them. Prosecutors increasingly relied instead on broad cybercrime provisions that were easier to apply to online conduct and had a lower evidentiary threshold. Authorities have since used the same framework against women and girls who publish content online, charging them with violating “family values” under the cybercrime law.¹⁷⁷

A May 2020 statement by Egypt’s Public Prosecution Office about Haneen Hossam, an Egyptian TikTok influencer charged with “undermining family values and principles,” explicitly acknowledges and justifies this turn to cybercrime enforcement:

It has now become a fact that, in addition to the three traditional land, sea and air borders, our nation is confronted with a fourth access point; one that necessitates the introduction of radical changes to the legislative policy as well as to the administrative and judicial controls.

<https://www.arab-reform.net/publication/challenging-the-legal-ideology-of-the-state-cause-lawyerin-g-and-social-movements-in-egypt/>; Afsaneh Rigot, “Egypt’s Dangerous New Strategy for Criminalizing Queerness,” December 30, 2020, <https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html>.

¹⁷⁵ Bedayaa, “Legal Aid Annual Report 2020,”

<https://bedayaa.org/wp-content/uploads/2023/02/Legal-Aid-Annual-Report-20201.pdf>; Afsaneh Rigot, “Digital Crime Scenes: The Role of Digital Evidence in the Persecution of LGBTQ People in Egypt, Lebanon, and Tunisia,” March 7, 2022, https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/Digital%20crime%20scenes%20.pdf.

¹⁷⁶ Afsaneh Rigot, “Digital Crime Scenes: The Role of Digital Evidence in the Persecution of LGBTQ People in Egypt, Lebanon, and Tunisia,” March 7, 2022,

https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/Digital%20crime%20scenes%20.pdf.

¹⁷⁷ Abed Kataya, “The TikTok Case: A New Platform to Oppress Women in Egypt,” August 28, 2020,

<https://smex.org/the-tiktok-case-a-new-platform-to-oppress-women-in-egypt/>; Human Rights Watch, “Egypt: Mass Crackdown Targets Online Content Creators,” September 10, 2025,

<https://www.hrw.org/news/2025/09/10/egypt-mass-crackdown-targets-online-content-creators>;

Human Rights Watch, “Egypt: Spate of ‘Morality’ Prosecutions of Women,” August 17, 2020,

<https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women>.



We are now faced with a new cyber border and websites that need full deterrence and prudence in protecting them, just as any border...¹⁷⁸

This shift illustrates both the possibilities and limitations of defensive strategic litigation. Rigot's research shows that police and prosecutors responded to the weaknesses exposed by defense lawyers by making charges that allowed them to bypass those arguments. Moving cases to the Economic Courts narrowed many of the legal openings lawyers had used to obtain acquittals or reduced sentences. Egyptian lawyers' successful criminal defense strategy produced an unintended, adverse result: it prompted authorities to develop a broader and more punitive framework for policing Egyptian queer life online.

When asked why digital free expression cases are particularly difficult to litigate, three Egyptian civil society representatives pointed to the unique role digital platforms play in public life.¹⁷⁹ Online spaces allow large numbers of people to communicate, organize, and express themselves outside traditional state-controlled channels. Unlike newspapers or television stations, major digital platforms connect millions of users and operate partly beyond the direct reach of Egyptian media regulations. Authorities therefore view these spaces as requiring heightened surveillance and control. Officials often justify such intervention by invoking the need to protect Egyptian values, national identity, or social cohesion. In practice, however, authorities frequently use these concepts to restrict discussion of politically sensitive issues, including the military, sexuality, Palestine, and criticism of government policy.¹⁸⁰

Egyptian cause lawyers retain somewhat more room to pursue offensive strategic litigation in other fields. One unnamed Egyptian group, for example, has proactively challenged government decisions involving the increased price of medication and brought cases concerning abuses against members of religious minorities. Yet even these offensive cases tend to result in limited and incremental change. Hassan, a member of the organization, said that "sometimes it takes years and years, and there's a black hole of regulations that we have to navigate." Still, he said that litigation involving the right to health, minority rights, and freedom of religion can produce "micro-improvements."¹⁸¹

Despite the limited scope of these victories, they remain meaningful for the affected communities, the expert said. The organization continues to pursue

¹⁷⁸ Youm7, "النابية العامة تنشر رسالتها بقضية الطالبة حنين حسام مترجمة بالغة الإنجليزية," May 2, 2020, https://www.youm7.com/story/2020/5/2/%D8%A7%D9%84%D9%86%D9%8A%D8%A7%D8%A8%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9-%D8%AA%D9%86%D8%B4%D8%B1-%D8%B1%D8%B3%D8%A7%D9%84%D8%AA%D9%87%D8%A7-%D8%A8%D9%82%D8%B6%D9%8A%D8%A9-%D8%A7%D9%84%D8%B7%D8%A7%D9%84%D8%A8%D8%A9-%D8%AD%D9%86%D9%8A%D9%86-%D8%AD%D8%B3%D8%A7%D9%85-%D9%85%D8%AA%D8%B1%D8%AC%D9%85%D8%A9-%D8%A8%D8%A7%D9%84%D9%84%D8%BA%D8%A9/4754263#goog_rewarded.

¹⁷⁹ SMEX phone interview with "Hassan," April 17, 2026; SMEX phone interview with "Laila," May 22, 2026; SMEX phone interview with "Fareid," May 14, 2026.

¹⁸⁰ SMEX phone interview with "Hassan," April 17, 2026.

¹⁸¹ SMEX phone interview with "Hassan," April 17, 2026.



other rights issues – including digital rights – as a matter of principle, but does so with the understanding that success is far less likely. The group's experience shows that offensive strategic litigation has not disappeared entirely in Egypt. Instead, cause lawyers select narrower issues where they believe courts may still provide some relief. Online expression offers far fewer such openings because the state treats control over digital spaces as a central political and security concern.

The state has also systematically weakened the very organizations and lawyers capable of pursuing either defensive or offensive cases. Representatives of legal rights groups and independent lawyers face the same travel bans, asset freezes, arrests, surveillance, smear campaigns, and legal harassment that target digital rights activists and civil society more broadly, reducing the number of legal experts available to litigate altogether.¹⁸²

Judicial independence presents another fundamental barrier. Gamal, an Egyptian legal expert, said that strategic litigation in Egypt now exists only on a “very limited scale” because it requires “a minimum of judicial independence to produce meaningful results for social movements.”¹⁸³

In Gamal's view, the problem is not simply that judges face pressure from the state, but that many judges understand themselves as part of the state's “ruling coalition.” He pointed to the president's role in judicial appointments, the politicization of courts, the punishment or removal of judges who issue rulings not aligned with state narratives, and the close professional and familial ties between the judiciary, security, and military as factors that make courts far less independent from the security apparatus.¹⁸⁴

¹⁸² Mada Masr, “Director of Hisham Mubarak Law Center released on bail in NGO case,” April 13, 2017, <https://www.madamasr.com/en/2017/04/13/news/u/director-of-hisham-mubarak-law-center-released-on-bail-in-ngo-case/>; Committee for Justice, “Egypt: Committee for Justice Documents the Targeting of Lawyers and Human Rights Defenders and Calls for the Protection of Human Rights Work,” June 9, 2026, <https://www.cfjustice.org/egypt-committee-for-justice-documents-the-targeting-of-lawyers-and-human-rights-defenders-and-calls-for-the-protection-of-human-rights-work/>; Amnesty International, “Egypt: Lift travel bans imposed on two human rights lawyers,” July 9, 2024, <https://www.amnesty.org/en/latest/news/2024/07/egypt-lift-travel-bans-imposed-on-two-human-rights-lawyers/>.

¹⁸³ SMEX phone interview with “Gamal,” June 18, 2026.

¹⁸⁴ Reuters, “Egypt issues law allowing president to appoint judges,” April 28, 2017, <https://www.reuters.com/article/world/egypt-issues-law-allowing-president-to-appoint-judges-idUSKBN17U18T/>; Youssef Auf, Carnegie Endowment for Peace, “The Battle Over Appointing Judges in Egypt,” January 16, 2018, <https://carnegieendowment.org/sada/2018/01/the-battle-over-appointing-judges-in-egypt/>; International Commission of Jurists, “Egypt: authorities must end politicization of the judiciary and ensure its independence and accountability,” October 12, 2016, <https://www.ici.org/wp-content/uploads/2016/10/Egypt-Tool-of-repression-report-launch-News-Press-release-2016-ENG.pdf>; Moataz El Fegieri, “Egypt's Fragile Stability: Erosion of the Rule of Law and Institutions of Governance,” Arab Center Washington DC, <https://arabcenterdc.org/resource/egypts-fragile-stability-erosion-of-the-rule-of-law-and-institutions-of-governance/>; The New Arab, “Senior Egyptian judge dropped from elite council after drafting anti-torture law,” June 29, 2020, <https://www.newarab.com/news/egyptian-judge-who-drafted-anti-torture-law-dismissed-council/>; Ahmed Aboulenein, “How Egypt's crackdown on dissent ensnared some of the country's top

“The vast majority of judges believe in the project of the current state. The collapse of the state would negatively impact them as privileged members of the ruling class, so...they [consider themselves] part of the state too and have an interest in upholding the status quo.”¹⁸⁵

Taken together, these conditions have made cause lawyering in Egypt predominantly defensive under al-Sisi. Some defense efforts have produced wider effects and qualify as defensive strategic litigation. Offensive cases continue in fields such as health and freedom of religion, but these cases rarely provide a viable route for challenging restrictions on online expression or transforming Egypt’s digital rights framework.

Iraq/Kurdistan Region of Iraq (KRI)

Iraqi civil society has occasionally pursued offensive strategic litigation to challenge laws directly. In 2012, for example, the Society for Defending Press Freedom in Iraq challenged the Journalists’ Rights Law before the Federal Supreme Court, arguing that it restricted media freedom.¹⁸⁶ The court ultimately upheld the law. This proactive challenge differs from the defensive criminal work that now dominates the legal strategies described by the Iraqi and Kurdish interviewees in this report. Today, defensive strategic litigation remains their most viable, if constrained, tool for contesting restrictions expression, including online speech.

“Diyar,” a Kurdish human rights expert and lawyer, described legal defense as one of his organization’s principal strengths, despite the deeply flawed legal environment in which it operates. In his view, even an imperfect legal framework is preferable to arbitrary repression because it gives defense lawyers a set of laws, procedures, and institutions through which they can challenge abuses.

Diyar contrasted the current environment with the KRI of the 1990s and early 2000s, when authorities often silenced journalists and critics through

judges,” Reuters, October 18, 2016, <https://www.reuters.com/investigates/special-report/egypt-judges/>; Egyptian Front for Human Rights, “Subjecting the Judiciary to Military Selection and Training: Further Militarization of the State and a Violation of What Remains of Judicial Independence in Egypt,” February 5, 2026, <https://egyptianfront.org/2026/02/subjecting-the-judiciary-to-military-selection-and-training-further-militarization-of-the-state-and-a-violation-of-what-remains-of-judicial-independence-in-egypt/>; Noon Post, “Egypt: How the Military Academy Is Reengineering the Judiciary and Religious Preaching,” January 30, 2026, <https://www.noonpost.com/en/363144/>.

¹⁸⁵ SMEX phone interview with “Gamal,” June 18, 2026.

¹⁸⁶ Press Freedom Advocacy Association, “جمعية الدفاع عن حرية الصحافة تعيد رفع دعوى الطعن بـ”قانون حقوق الصحفيين“,” April 26, 2012, <https://pfaa-iq.com/?p=182>; Alaa Youssef, “طعون بقانون حقوق الصحفيين بالعراق,” Al Jazeera, June 24, 2012, <https://www.aljazeera.net/news/2012/6/24/%D8%B7%D8%B9%D9%88%D9%86-%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AD%D9%82%D9%88%D9%82-%D8%A7%D9%84%D8%B5%D8%AD%D9%81%D9%8A%D9%8A%D9%86-%D8%A8%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82>; Committee to Protect Journalists, “Iraq’s journalist protection law doesn’t protect them,” January 24, 2012, <https://cpj.org/2012/01/iraqs-journalist-protection-law-doesnt-protect-the/>.

intimidation, physical violence, or arbitrary detention – sometimes resulting in death.¹⁸⁷ Today, he said, authorities are more likely to rely on courts and criminal prosecutions. This does not eliminate repression or the threat of physical retaliation, but it creates more opportunities for defensive legal advocacy.¹⁸⁸ "At least there's a court, a judge. It's different than when they would only send people to your house to beat you up and intimidate you into silence. It's 'progress' in the historical sense."¹⁸⁹

As previously discussed, KRI authorities frequently manipulate this legal framework to achieve political ends. Rather than handling speech-related offenses under the KRI's Press Law No. 35 of 2007, which provides protections and procedures specific to journalists, authorities often pursue charges under the federal penal code, KRI Counterterrorism Law No. 21 of 2003, or KRI Law No. 6 of 2008 to Prevent the Misuse of Telecommunications Equipment.¹⁹⁰ Their broad provisions allow authorities to frame speech as a threat to state security, public morality, religion, or social values, a trend seen in Egypt as well.¹⁹¹ They also give prosecutors greater flexibility and expose defendants to harsher penalties than the Press Law.

For organizations such as Diyar's, defensive strategic litigation offers little prospect of sweeping legal victories. Instead, lawyers use individual cases to contest how authorities interpret and apply the law. "Of course we have feedback for how the government applies these laws," Diyar said, "but at least it's a framework for me as a lawyer to engage with." Formal proceedings give lawyers in Iraq and the KRI repeated opportunities to challenge abusive interpretations, document patterns of misuse, and push for incremental reform.

A different challenge arises when rights groups support survivors of online gender-based violence.¹⁹² In these cases, organizations are not defending a client against state prosecution. They are helping a survivor pursue a complaint against a private actor who may be anonymous or difficult to identify. Even when the

¹⁸⁷ Committee to Protect Journalists, "Sardasht Osman," n.d., <https://cpj.org/data/people/sardasht-osman/>; Human Rights Watch, "Iraqi Kurdistan: Journalists Under Threat," October 29, 2010, <https://www.hrw.org/news/2010/10/29/iraqi-kurdistan-journalists-under-threat>.

¹⁸⁸ Zainab Al-Mashat, Jummar Media, "'My questions are turned into a weapon to kill me': the deadly war against Iraq's journalists," March 23, 2023, <https://jummar.media/en/2023/03/23/my-questions-are-turned-into-a-weapon-to-kill-me-the-deadly-war-against-irags-journalists/>; Iraqi Organization for Human Rights, "Press Freedom in Iraq: The Return to Intimidation," May 3, 2026, <https://iohriq.org/195.html#>; Amnesty International, "Kurdistan Region of Iraq: Arbitrary arrests and enforced disappearance of activists and journalists," June 15, 2021, <https://www.amnesty.org/en/latest/press-release/2021/06/kurdistan-region-of-iraq-arbitrary-arrests-and-enforced-disappearance-of-activists-and-journalists/>.

¹⁸⁹ SMEX phone interview with "Diyar," May 9, 2026.

¹⁹⁰ Press Law No. 35 of 2007, available at <https://presidency.gov.krd/krp/docs/PressLaw-KRI.pdf>.

¹⁹¹ Human Rights Watch, "'We Might Call You in at Any Time': Free Speech Under Threat in Iraq," June 15, 2020, <https://www.hrw.org/report/2020/06/15/we-might-call-you-any-time/free-speech-under-threat-iraq>.

¹⁹² Asia Abdulkareem, "Dina Sparks a Movement Against Digital Violence," May 21, 2025, <https://insm-iq.org/en/?p=1639>.



perpetrator is known, existing criminal laws may not clearly capture the digital harm. Survivors can file complaints, but investigators and prosecutors determine whether and how those complaints proceed.

This work is proactive, but it has not developed into a coordinated offensive strategic litigation campaign. Iraqi and Kurdish organizations instead provide ad hoc legal aid. They help survivors document abuse, understand their rights, seek content removal, file complaints, and approach local authorities. Selected cases could, in principle, clarify how existing laws apply, improve investigative and evidentiary practices, or support legislative reform. In practice, however, Iraqi groups often lack the resources and legal tools needed to sustain such a strategy.

Yasmine, an Iraqi digital rights and gender expert, said that harassment and blackmail cases are especially difficult to prosecute because Iraq continues to rely on Penal Code provisions that were not designed for digital abuse.¹⁹³ Bots and social media channels created to harass and exploit women and girls “are proliferating at an increasingly high rate because there is no one controlling them and there are no clear penalties for their behavior,” she said, a phenomenon even the interior ministry acknowledges.¹⁹⁴

Daria, a Kurdish expert on digital rights and online gender-based violence, similarly described a widening gap between the severity of the harms women face online and the ability of existing institutions to respond.¹⁹⁵ Many women and girls do not know that they can report online harassment or blackmail. Others hesitate to approach the police or civil society organizations because they fear breaches of confidentiality, stigma, or retaliation from their families and communities. Legal support must begin by building trust and explaining available options before litigation becomes possible.¹⁹⁶

These accounts reveal two distinct legal challenges. In speech cases, defense lawyers can contest the state’s misuse of existing criminal laws. In digital violence cases, rights groups must first identify a responsible actor, find a legal provision that reflects the harm, and persuade state institutions to respond. This gap does not reflect a failure of defensive strategic litigation. It reflects the absence of effective remedies and the difficulty of building a proactive test-case strategy from individual complaints.

¹⁹³ SMEX phone interview with “Yasmine,” June 5, 2026.

¹⁹⁴ SMEX phone interview with “Yasmine,” June 5, 2026; Asia Abdelkarim Anwar, Walaa Ali Farhan, Tara Aziz, “Digital violence against women in Iraq,” SecDev Foundation, October 2023, <https://portal.salamatmena.org/wp-content/uploads/2024/01/Iraq-DVAW-2023-EN.pdf>; Ideas Beyond Borders, “Money, Sex, Revenge: The Forces Driving Online Violence in Kurdistan,” January 4, 2023, <https://ideasbeyondborders.org/money-sex-revenge-the-forces-driving-online-violence-in-kurdistan/>; Rudaw English, YouTube, “Social media harassment on the rise: interior ministry,” June 28, 2021, <https://www.youtube.com/watch?v=aALQW4qfmA4&t=7s>.

¹⁹⁵ SMEX phone interview with “Daria,” June 3, 2026.

¹⁹⁶ Asia Abdulkareem, “Dina Sparks a Movement Against Digital Violence,” May 21, 2025, <https://insm-iq.org/en/?p=1639>; IDRC, “From online harm to hopeful responses in the Middle East and North Africa,” November 14, 2025, <https://idrc-crds.ca/en/research-in-action/online-harm-hopeful-responses-middle-east-and-north-africa>.

This does not mean that broad cybercrime legislation would necessarily resolve the problem. Iraq's previous draft cybercrime laws have drawn serious criticism precisely because their broad, vague provisions on morality and national security could criminalize protected expression rather than protect people from abuse or provide meaningful remedy.¹⁹⁷ Egypt's cybercrime law demonstrates this danger.¹⁹⁸

Aiman said that his organization helped review Iraq's draft cybercrime law and contributed to scaling back some of its most egregious provisions. However, he said legislators still have significant gaps in their understanding of cybercrime. "Financial extortion, blackmail, hackers – these are good things to fight against with a cybercrime law...[but legislators] have political agendas divorced from the free expression ideals of the Iraqi constitution," he said, speaking to legislators' efforts to insert morality clauses into the law.¹⁹⁹

The challenge, then, is not simply the absence of a cybercrime law. Iraq lacks a rights-respecting legal framework that distinguishes genuine digital harms from protected expression and gives survivors a usable path from complaint to investigation and remedy. Effective legal strategies require laws that allow defense lawyers to challenge abusive prosecutions while enabling survivors to pursue accountability without expanding the state's already broad power to police expression.

Tunisia

Unlike their counterparts in Egypt and Iraq, the Tunisian groups interviewed by SMEX did not describe a formalized offensive or defensive strategic litigation strategy around online expression. They have instead responded to Decree-Law 54 by documenting prosecutions, training lawyers on cybercrime and digital rights, and defending their professional space. Their focus on Decree-Law 54 reflects its central role in Tunisia's digital repression.

This approach reflects the severe squeeze on Tunisia's advocacy landscape. Civil society organizations must make immediate decisions about where to direct limited staff and resources while facing mounting and administrative pressure. Nissaf, a Tunisian human rights advocate, described civil society in Tunisia as "fragmented," noting that "when you need to ensure your survival, it affects what you can advocate for."²⁰⁰ She said that the constant threat of government

¹⁹⁷ Zeinab Ismail, "More Control: Iraq's Alarming Cybercrime Law," August 3, 2023, <https://smex.org/more-control-iraqs-alarming-cybercrime-law/>; Safaa Ayyad, "Iraqi Cybercrime Draft Law: In Suspension," July 6, 2022, <https://smex.org/iraqi-cybercrime-draft-law-in-suspension/>.

¹⁹⁸ SpeakUp, "Reality of cyberbullying and blackmail crimes in Egypt," March 2024, <https://speakupeg.com/2024/03/25/reality-of-cyberbullying-and-blackmail-crimes-in-egypt/>.

¹⁹⁹ SMEX phone interview with "Aiman," May 22, 2026

²⁰⁰ SMEX phone interview with "Nissaf," June 5, 2026; Karim Elmarzouky, Legal Agenda, "تعليق نشاط: الجمعيات في تونس: تصعيد جديد ضد العمل المدني," December 5, 2025, <https://legal-agenda.com/%d8%aa%d8%b9%d9%84%d9%8a%d9%82-%d9%86%d8%b4%d8%a7%d8%>

summonses and pending investigations is “exhausting,” and leaves organizations with little capacity to pursue litigation opportunities. Mona, also a human rights expert, said staff at her organization wait with “bated breath” wondering if they will be targeted next, while Youssef described a “sustained climate of pressure.”²⁰¹

Under these conditions, digital rights groups have prioritized building the capacity of criminal defense lawyers rather than selecting cases for a broader litigation campaign. Prosecutions involving cybercrime and digital evidence remain relatively new and technically complex, leaving many lawyers without specialized experience. At the same time, defendants are often reluctant to work directly with Tunisian digital rights society organizations because authorities and their supporters stigmatize these groups as “foreign agents” or “traitors.” As a result, Nissaf said, defendants sometimes “find themselves with lawyers who aren’t as qualified because cybercrime is a newer subject for them.”²⁰² Training lawyers allows digital rights organizations to strengthen individual criminal defenses without requiring defendants to associate publicly with a targeted civil society group.

This strategy still depends on lawyers being willing and able to accept sensitive cases. Yet, like their Egyptian counterparts, Tunisian lawyers are constantly under threat, as is the judiciary’s independence.²⁰³ Three out of four Tunisian experts interviewed for this report pointed specifically to lawyer Sonia Dahmani’s arrest as a “pivotal” moment in Tunisia’s escalation against its legal experts.²⁰⁴ In June 2026, a coalition of 40 legal and human rights organizations warned that widespread reprisals against Tunisian lawyers were deterring them from working on sensitive cases and undermining the public’s access to legal representation and justice.²⁰⁵

[b7-%d8%a7%d9%84%d8%ac%d9%85%d8%b9%d9%8a%d8%a7%d8%aa-%d9%81%d9%8a-%d8%aa%d9%88%d9%86%d8%b3-%d8%aa%d8%b5%d8%b9%d9%8a%d8%af%d9%8c-%d8%ac%d8%af%d9%8a/](https://www.ohchr.org/en/press-releases/2025/07/tunisia-un-experts-alarmed-deteriorating-human-rights-situation-lawyers)

²⁰¹ SMEX written correspondence with “Mona,” June 11, 2026; SMEX phone interview with “Youssef,” May 14, 2026.

²⁰² SMEX phone interview with “Nissaf,” June 5, 2026.

²⁰³ Nawaat, “إضراب عام المحامين: مطالبة باستقالة وزيرة العدل ورفض التضيق والترهيب,” June 18, 2026,

<https://nawaat.org/2026/06/18/%D8%A5%D8%B6%D8%B1%D8%A7%D8%A8-%D8%B9%D8%A7%D9%85-%D8%A7%D9%84%D9%85%D8%AD%D8%A7%D9%85%D9%8A%D9%86-%D9%85%D8%B7%D8%A7%D9%84%D8%A8%D8%A9-%D8%A8%D8%A7%D8%B3%D8%AA%D9%82%D8%A7%D9%84%D8%A9-%D9%88%D8%B2/>; UN press release, “Tunisia: UN experts alarmed by deteriorating human rights situation of lawyers,” July 15, 2025, <https://www.ohchr.org/en/press-releases/2025/07/tunisia-un-experts-alarmed-deteriorating-human-rights-situation-lawyers>.

²⁰⁴ In May 2024, security forces raided the Tunisian Bar Association’s offices to arrest Sonia Dahmani under article 24 of Decree-Law 54, prompting lawyers to launch a nationwide strike. See: “Tunisia extends the detention of two journalists, lawyers begin a strike,” May 13, 2024, Reuters, <https://www.reuters.com/world/africa/tunisia-extends-detention-two-journalists-lawyers-begin-strike-2024-05-13/>; SMEX phone interview with “Rouba,” May 19, 2026; SMEX phone interview with “Adham,” April 15, 2026; SMEX phone interview with “Youssef,” May 14, 2026; Human Rights Watch, “Tunisia: Authorities Escalate Clampdown on Media, Freedom of Expression,” May 30, 2024, <https://www.hrw.org/news/2024/05/30/tunisia-authorities-escalate-clampdown-media-freedom-expression>.

²⁰⁵ International Commission of Journalists, “International legal and human rights organizations condemn the Tunisian Authorities’ escalating attacks on the legal profession, the independence of the judiciary and civil society,” June 9, 2026, <https://www.icj.org/international-legal-and-human-rights-organizations-condemn-the-tunisian-aut>

Tunisian digital rights organizations practice cause lawyering in emergency conditions. Their immediate priorities are documenting abuses, equipping defense lawyers, and protecting the organizations and professional bodies that make future litigation possible.²⁰⁶ Under these conditions, building an offensive or coordinated defensive litigation strategy remains secondary to keeping Tunisia's lawyers, rights organizations, and civic space intact.

B. Deepening Government Relationships

Digital rights advocates in Egypt, Iraq, and Tunisia expressed mixed views about the value of engaging directly with their respective governments. Interviewees generally agreed, however, that the effectiveness of their engagement depends heavily on the individuals involved, that more-accessible parliamentary figures exercise limited influence over the executive branch, and that security concerns often discourage organizations from publicizing their government engagement at all.

Both sides often keep these relationships private. Government officials remain reluctant to engage openly with civil society organizations because of the political sensitivities surrounding their work (especially if related to women, LGBTQ+ people, or other marginalized communities), while civil society actors themselves frequently question the value of such engagement and avoid publicizing it because of the stigma associated with working closely with government figures.

Hassan, an Egyptian digital rights expert, described these relationships as highly dependent on the official's interest in the issue at hand and their risk appetite:

Some people in parliament take us seriously, and we try to be proactive with MPs. Sometimes people speak with us, sometimes they don't. [Government representatives] understand there is continuous retaliation against [group name withheld], so they don't engage with us so they don't get in trouble. Some people are brave enough to take our opinion, though. But overall, talking with CSOs isn't really a practice that [government officials] get into all that much.”²⁰⁷

[horities-escalating-attacks-on-the-legal-profession-the-independence-of-the-judiciary-and-civil-society.](#)

²⁰⁶ ASF, “International legal and human rights organisations condemn the Tunisian authorities’s escalating attacks on the legal profession, the independence of the judiciary and civil society,” June 5, 2026,

<https://asf.be/publication/international-legal-and-human-rights-organisations-condemn-the-tunisia-n-authoritiess-escalating-attacks-on-the-legal-profession-the-independence-of-the-judiciary-and-civil-society/>.

²⁰⁷ SMEX phone interview with “Hassan,” April 17, 2026.



Fareid, another Egyptian digital rights representative, also said that his organization engages with parliament primarily through personal relationships with individual members, but that even these connections rarely produce significant results. As he put it, “you don’t really get far.”²⁰⁸

Hassan attributed this limited influence to the Egyptian parliament's institutional weakness.²⁰⁹ When asked how successful these collaborative relationships with MPs are in shaping government policy on digital rights issues, he said: “Parliament is weak and it’s not strong nor independent, and many parts of parliament are in the dark themselves...We don’t have access to information all the time and neither do they sometimes.”²¹⁰

Interviewees also described significant security concerns surrounding engagement with government officials. Amr, an Egyptian digital rights activist, told SMEX, “If someone asks me, ‘are you engaging with anyone from the government?’ Of course I’m going to say no. I’m going to deny it.”²¹¹

In the Tunisian context, the balancing act is much the same. “Adham,” a Tunisian digital rights advocate told SMEX: “Civil society and MPs have varying relationships. The risk appetite is dependent on the organization itself, and anyone who is actually working with parliament will deny it publicly.”²¹²

Adham said he reviewed a draft of Tunisia’s forthcoming data protection law, which is expected to replace Law No. 63 of 2004 that currently governs data protection practices.²¹³ In his view, the draft includes some improvements and attempts to align with international standards, including the European Union’s General Data Protection Regulation.²¹⁴ But his influence as a digital expert remains limited. He said he does not know what the law will look like after parliamentary deliberations, which he will not participate in directly. Instead, his review and substantive feedback take place bilaterally through individual MPs with whom he has existing relationships. Still, he’s not sure how successful those MPs will be in determining the final outcome. “Some [MPs] are trying to come up with good legislation, but at the end of the day, it [often] becomes a game of politics.”²¹⁵

²⁰⁸ SMEX phone interview with “Fareid,” May 14, 2026.

²⁰⁹ SMEX phone interview with “Hassan,” April 17, 2026; Egyptian Front for Human Rights, “ترشيعات سلطوية، ورقابسة غائبة,” September 2025, <https://egyptianfront.org/wp-content/uploads/2025/09/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1-%D9%83%D8%B4%D9%81-%D8%AD%D8%B3%D8%A7%D8%A8-%D8%A8%D8%B1%D9%84%D9%85%D8%A7%D9%86-2020-2025.pdf>.

²¹⁰ SMEX phone interview with “Hassan,” April 17, 2026.

²¹¹ SMEX phone interview with “Amr,” June 8, 2026.

²¹² SMEX phone interview with “Adham,” April 15, 2026.

²¹³ Law No. 63 of 2004 on the Protection of Personal Data, available <https://www.ins.tn/sites/default/files/2020-04/Loi%2063-2004%20Fr.pdf>

²¹⁴ General Data Protection Regulations, available <https://gdpr-info.eu/>.

²¹⁵ SMEX phone interview with “Adham,” April 15, 2026.

Like Egypt, Tunisia's parliament under President Kais Saied functions as a severely weakened body, stripped of meaningful legislative power and subordinate to the executive – a “dissident-free parliament,” as Samir Bouaziz, Advocacy Officer at Reporters Without Borders, previously told SMEX.²¹⁶

Like their Tunisian counterparts, many Iraqi and Kurdish organizations are navigating “burdensome” registration requirements, administrative reviews, and government oversight that makes engagement with officials less a source of influence than a condition of survival.²¹⁷ Many groups remain reluctant to discuss these pressures publicly.

Yet interviewees also identified limited areas in which government–civil society coordination has produced meaningful results. One OGBV expert, Daria, said her organization maintains a “very successful” relationship with the Directorate of Combating Violence Against Women and Girls in Dohuk (DCVAW).²¹⁸ Daria said the relationship has strengthened as government officials have come to understand the severity of digital violence against women and its potential consequences. In her view, the high number of suicides and killings by family members associated with online abuse and blackmail compelled authorities to take the issue more seriously over the past two to three years.

This example does not erase the broader constraints organizations face when engaging with the state. It does, however, suggest that sustained collaboration becomes more possible when officials recognize digital harms as immediate threats to physical safety and view civil society organizations as necessary partners in responding to them.

C. Maintaining Low Profiles and Adopting Digital Security Measures

The difficult security challenges associated with speaking openly about the human rights records of Egypt, Tunisia, and Iraq were reflected in the interview process itself. Every Egypt and Tunisia expert interviewed for this report requested

²¹⁶ Najla ben Salah, SMEX, “Tunisian Government Tightens Grip on Journalistic Sources,” December 23, 2022, <https://smex.org/tunisian-government-tightens-grip-on-journalistic-sources/>; “Human Rights Watch, “Tunisia: Questions and Answers on the Draft Constitution,” July 14, 2022, <https://www.hrw.org/news/2022/07/14/tunisia-questions-and-answers-draft-constitution>

²¹⁷ Marsin Alshamary and Sura Maqsood, “The Landscape of Civil Society in Iraq,” June 2022, Konrad Adenauer Stiftung, <https://cnxus.org/the-iraqi-knowledge-sharing-platform/wp-content/uploads/2022/07/The-Landscape-of-Civil-Society-in-Iraq.pdf>; USAID, “2020 Civil Society Organization Sustainability Index For the Middle East and North Africa,” October 2021, <https://www.fhi360.org/wp-content/uploads/drupal/documents/csosi-mena-2020-report.pdf>; Amnesty International, “Iraq: 2025,” n.d., <https://www.amnesty.org/en/location/middle-east-and-north-africa/middle-east/iraq/report-iraq/>; Ghamgin Mohammad, “Registering an NGO in the Kurdistan Region plagued by delays and bureaucracy,” Paragraph, May 21, 2023, <https://peregraf.com/en/investigation/5644>.

²¹⁸ SMEX phone interview with “Daria,” June 3, 2026.



anonymity in SMEX's reporting, while interviewees based in or working on Iraq and the KRI were generally more comfortable with the prospect being named. This distinction does not mean that Iraqi civil society actors face fewer risks. Rather, it reflects the different configurations of risk across the three contexts, including the heightened sensitivity of public attribution in Egypt and Tunisia and the varied ways that state and non-state actors retaliate against critics across these countries.

These precautions demonstrate how some experienced organizations have adapted to sustained threats. Their adoption remains uneven, however, and many organizations have not institutionalized digital security as a routine organizational practice, as discussed below.

Digital Security Precautions

Interviewees described how they developed stricter habits around their digital hygiene, often in response to a traumatic or significant incident that threatened their or their colleagues' safety.

Rouba, a Tunisian journalist, said that after the government began targeting her place of work, she and her colleagues "moved all our communications to Signal and Whatsapp, even casual conversations... we always use disappearing messages," amongst other digital security measures.²¹⁹

Interviewees also described removing staff names and office addresses from their organizational websites and social media pages to protect themselves and their colleagues. Several provided SMEX with examples of times when staff members were mentioned by name on social media when members of the general public disapproved of their work.

When authorities banned the use of the word "gender" in Iraq in 2023, digital rights actors documenting online gender-based violence faced overlapping risks due to intense smear campaigns (something women's rights activists have been dealing with more prominently since the 2019 Tishreen protests).²²⁰ Yasmine, an Iraqi digital rights and gender expert, described how Telegram channels published the names of workers and institutions involved in online gender-based violence work. "It was a really scary time. People had to stay home, wear their

²¹⁹ SMEX phone interview with "Rouba," May 19, 2026.

²²⁰ Independent Arabia, "غير المحجبات في العراق في قلب عاصفة التحريض," February 8, 2025,

<https://www.independentarabia.com/node/617324/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A9/%D8%AA%D9%82%D8%A7%D8%B1%D9%8A%D8%B1/%D8%BA%D9%8A%D8%B1-%D8%A7%D9%84%D9%85%D8%AD%D8%AC%D8%A8%D8%A7%D8%AA-%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D8%B1%D8%A7%D9%82-%D9%81%D9%8A-%D9%82%D9%84%D8%A8-%D8%B9%D8%A7%D8%B5%D9%81%D8%A9-%D8%A7%D9%84%D8%AA%D8%AD%D8%B1%D9%8A%D8%B6>; Balsam Mustafa, "GENDER FOUND GUILTY: Anti-Gender Backlash and (Dis)Translation Politics in Iraq," Cardiff University, 2025, <https://orca.cardiff.ac.uk/id/eprint/177268/9/mustafa-2025-gender-found-guilty-anti-gender-backlash-and-%28dis%29translation-politics-in-iraq.pdf>.

masks when they went outside, avoid doing public events, and shut down their websites,” she said.²²¹

More recently, Yasmine said her organization faced coordinated online backlash after publishing a resource related to a marginalized community. Its website was attacked, its social media pages were flooded with hostile comments, and staff temporarily took the website offline.²²² Daria similarly described removing online content and taking down her organization's website after it received serious threats amid a broader wave of online harassment targeting civil society organizations, including death threats to the organization's senior leadership.²²³

Another Iraqi digital rights organization faced online harassment after publishing content challenging misinformation. A widely circulated post by someone affiliated with a militia disclosed identifying information about the organization and its staff, prompting Meta to remove it and staff members to remain home for several days out of concern that the online incitement could lead to arrest or physical violence.²²⁴

Rouba, the Tunisian journalist, pointed to a recurring concern across interviews: digital security measures are only as strong as the weakest participant in a communication chain. “If I take all these precautions to protect someone's identity, chatting only on Signal, using pseudonyms, etcetera, but the other person doesn't reciprocate, it's like I didn't do anything,” she said. “It defeats the purpose of the precautions.”²²⁵ This concern was echoed by Aiman, an Iraqi digital rights advocate, who said, “If both people don't have good digital hygiene, it blows up the whole interaction.”²²⁶

Self-Censoring Online

Self-censorship online functions as both personal and organizational protection. For example, one interviewee said:

Even though I am a respected lawyer, I cannot say all the things I want to say online. I am very careful because [the authorities] can use it against me. I have some political ambitions and ideas, as do some of my friends, and so we cannot express our opinions freely on digital platforms because of fear – fear of the regime, fear they will make any excuse to take revenge on you or your family.

In Iraq, self-censorship is also driven by government efforts to police the language civil society organizations use to describe their work on women and gender. After

²²¹ SMEX phone interview with “Yasmine,” June 5, 2026.

²²² SMEX phone interview with “Yasmine,” June 5, 2026.

²²³ SMEX phone interview with “Daria,” June 3, 2026.

²²⁴ SMEX phone interview with “Omar,” April 16, 2026.

²²⁵ SMEX phone interview with “Rouba,” May 19, 2026.

²²⁶ SMEX phone interview with “Aiman,” May 22, 2026



the government banned the use of the term “gender,” Daria, a Kurdish OGBV expert, said, “We removed our posts, deleted our posts on Facebook, deleted our website. The government forbade us to use this term, so we removed everything. Our main mission did not change, but we now have a lot of limits and a lot of filters before we post about any activities online.”²²⁷

This pressure to sanitize public language in Iraq is even more pronounced around LGBTQ+-related issues. Several interviewees said they fear speaking out about LGBTQ+ issues online for fear of repression. For some organizations, this means avoiding LGBTQ+-related speech altogether. For others, it means folding the issue into broader language about risks to “vulnerable” or “marginalized” groups. In both cases, the fear of retaliation limits the ability of digital rights groups to publicly defend LGBTQ+ people, who sit at the intersection of the most violent and repressive tactics of digital surveillance.

One Iraqi interviewee said he withdrew from a televised discussion about LGBTQ+ people in Iraq with a prominent media outlet based outside of Iraq despite believing the issue fell squarely within his organization’s human rights mandate.²²⁸ However, after consulting with his team, he decided not to participate because of the possible consequences for his reputation, his organization, and its registration and renewal processes in Baghdad.

Speech about the Regional Escalation

The genocide in Gaza coupled with the regional escalation led by Israel and US in Iran has led governments throughout the SWANA region to crack down on peaceful online speech and media coverage as a matter of “national security.”²²⁹ Interviewees from all three countries spoke to the heightened sensitivities surrounding online speech and media coverage about Gaza, Iran, and Israel.

In Iraq, censorship related to the regional escalation took a sharp turn in January 2025 when the CMC issued a directive to “all [Iraqi] media organizations” with broad and vague instructions for how they should carry out their media coverage about the escalation.²³⁰ The CMC has also allegedly pressured social media

²²⁷ SMEX phone interview with “Daria,” June 3, 2026.

²²⁸ SMEX phone interview with “Diyar,” May 9, 2026,

²²⁹ Middle East Eye, YouTube, “UAE geoblocks social media accounts over Iran war footage,” April 24, 2026, <https://www.youtube.com/watch?v=ROkAbedOPg>; Committee to Protect Journalists, “Global press freedom violations during the Iran war,” March 19, 2026, <https://cpj.org/2026/03/press-freedom-violations-in-the-middle-east-during-the-iran-war/>; Jillian York, “War as a Pretext: Gulf States Are Tightening the Screws on Speech—Again,” Electronic Frontier Foundation, April 13, 2026, <https://www.eff.org/deeplinks/2026/04/war-pretext-gulf-states-are-tightening-screws-speech-again>; Human Rights Watch, “Gulf States: Repression of Migrant Workers During Conflict,” June 11, 2026, <https://www.hrw.org/news/2026/06/11/gulf-states-repression-of-migrant-workers-during-conflict>.

²³⁰ Communication and Media Commission of Iraq, “Framework Regulations for Digital Platforms and Services,” available <https://cmc.iq/ar/wp-content/uploads/2025/03/Framework-regulations-for-digital-platforms-and-serv>

platforms to remove content criticizing Iraq.²³¹ Now, interviewees say, the risk of retaliation is so high that they self-censor.

"If someone posts something online saying, 'this isn't our war,' or 'this is not a sectarian issue,' they can find themselves in jail," said Aiman, an Iraq digital rights activist. "Or if someone simply asks, 'why is this Iraq's fight?' again, jail. There isn't any freedom of expression. It's a very sensitive topic."²³²

"In wartime, it's even harder to speak," Diyar, a Kurdish human rights expert, said. "The red lines become bolder, wider. Before the war, we were able to criticize Iran online ... but now that the war has broken out, I won't dare to speak about this."²³³

However, "pro-Iran" online speech or media reporting is not censored in the same way. "I don't see pro-Iran content removed even when it clearly violates [social media platforms'] community standards or Iraqi law," said Omar, an Iraqi digital rights activist.²³⁴ A group of Iraqi CSOs under the Social Media 4 Peace Initiative launched a monitoring campaign in response to the "surge" of abusive content related to the escalation.²³⁵

Egyptian authorities appear less discerning about who posts what. "It doesn't matter how close you are to the government or if you wear an MP or religious establishment hat. Regarding Palestine...you cannot criticize the government," Hassan, an Egyptian digital rights activist said.²³⁶

In Tunisia, the government has monitored and restricted some forms of Palestine-related organizing and peaceful online speech for years.²³⁷ Most recently, authorities detained at least three pro-Palestinian activists involved in preparations for the Global Sumud Flotilla. The case has made online speech

[ices-en.pdf](#); Iraqi National News Agency, "بالوثيقة.. هيئة الاعلام والاتصالات توجه وسائل الاعلام بعدم استخدام عدد من المفردات," August 8, 2023, <https://ninanews.com/website/News/Details?key=1069633>.

²³¹ Dana Tlaib Mnemy, "Facebook, X, and TikTok restrict Iraqi accounts after state pressure," The New Arab, October 22, 2025, <https://www.newarab.com/news/social-media-giants-restrict-iraqi-accounts-after-state-pressure>.

²³² SMEX phone interview with "Aiman," May 22, 2026

²³³ SMEX phone interview with "Diyar," May 9, 2026,

²³⁴ SMEX phone interview with "Omar," April 16, 2026.

²³⁵ UNESCO, "Iraqi CSOs Respond to Surge in Harmful Online Content with Coordinated Monitoring Initiative," April 28, 2026, <https://www.unesco.org/en/articles/iraqi-csos-respond-surge-harmful-online-content-coordinated-monitoring-initiative>.

²³⁶ SMEX phone interview with "Hassan," April 17, 2026.

²³⁷ Nesrin Zribi, "Ce sera votre dernière manifestation" : la répression des activistes pro-Palestine en Tunisie," Inkyfada, November 29, 2024, <https://inkyfada.com/fr/2024/11/29/repression-activiste-palestine-tunisie/>; Bassma al Atti, "Tunisia arrests pro-Palestine activist over 'terrorism' charges," The New Arab, October 15, 2024, <https://www.newarab.com/news/tunisia-arrests-pro-palestine-activist-over-terrorism>; Bassma al Atti, "Tunisia investigates activists amid crackdown on the pro-Palestine movement," The New Arab, November 12, 2024, <https://www.newarab.com/news/tunisia-investigates-3-pro-palestine-activists-over-7-oct-rally>.

around Palestine and solidarity organizing even more sensitive for civil society groups, according to Adham, one of the Tunisian digital rights activists.²³⁸

Physical Safety Precautions

Interviewees described physical safety precautions as part of a broader risk management strategy that extends from how they speak in public and how they move through cities to whether remaining in their country of origin is worth the risk at all.

Public affiliation with an organization non-grata carries a danger of being publicly recognized, a situation several people interviewed by SMEX manage on a daily basis. “Youssef” works at a targeted rights organization in Tunisia and is publicly affiliated with it. He said he always feels scared when he goes out in public: “I’ve received threats made out to my family. In stores, the public areas, in the train stations – I am looking over my shoulder as I go about my day.”²³⁹ Rouba, a Tunisian journalist affiliated with a targeted media organization, echoed those feelings when she said, “You don’t feel safe. You can’t imagine the fear that’s palpable in the air. Every time I travel, I try to have someone with a connection in the police on standby that I can call so I don’t get into trouble.”²⁴⁰

Multiple interviewees familiar with or working in Tunisia said that their organizations conduct extensive risk assessments before publishing certain products, especially when Tunisia-based staff or local civil society groups are involved.²⁴¹

In Egypt, similar calculations affect who receives public credit for research. Staff of Egyptian origin working with human rights organizations outside of Egypt may have to decide whether public association with an organization is worth the risk of harassment, arbitrary detention, or losing the ability to travel to Egypt due to their affiliation with the rights group, according to an interviewee who has not published research on Egypt using her real name for this very reason.²⁴²

For some interviewees, these physical safety assessments led not only to modified daily routines, but to self-exile. Four interviewed staff members are in self-exile due to the overwhelming security risks associated with remaining in their countries of origin.²⁴³ One person relocated from one part of the country to another hoping that would lessen the targeting but eventually left the country altogether. He now has a new passport from a European country.²⁴⁴ When he

²³⁸ SMEX phone interview with “Adham,” April 15, 2026.

²³⁹ SMEX phone interview with “Youssef,” May 14, 2026.

²⁴⁰ SMEX phone interview with “Rouba,” May 19, 2026.

²⁴¹ SMEX written correspondence with “Mona,” June 11, 2026; SMEX phone interview with “Nissaf,” June 5, 2026.

²⁴² SMEX written correspondence with “Mona,” June 11, 2026.

²⁴³ SMEX phone interview with “Omar,” April 16, 2026; SMEX phone interview with “Hassan,” April 17, 2026; SMEX phone interview with “Aiman,” May 22, 2026; SMEX phone interview with “Gamal,” June 18, 2026.

²⁴⁴ SMEX phone interview with “Omar,” April 16, 2026.



does go back, however, he alerts the European country's embassy and discusses his itinerary at length as part of the security measures he takes before going.

Hundreds of dissidents between Egypt, Iraq, and Tunisia live in self-exile to avoid repression at home, at grave cost to their mental health and family lives.²⁴⁵

Amr, an Egyptian digital rights expert who lives in Egypt says he does not use his real name when he works because he works with marginalized and at-risk populations like LGBTQ+ people, sex workers, and rights advocates. "I work with a different name each time, nobody knows my real identity."²⁴⁶ He said this measure is to protect him as much as it is to protect the people he works with. He also avoids using overtly human rights-oriented language in public-facing digital rights workshops, concerned that it could lead participants to make assumptions about his affiliations or professional background."²⁴⁷

Checkpoints

Checkpoints in Egypt and Iraq, concentrated in urban areas, carry especially serious risks for people whose digital and social media footprints may become liabilities once officers seize and search their phone and interpret something as incriminating or morally objectionable.²⁴⁸

Interviewees described checkpoint searches as well-defined opportunities for officers to exert sweeping and arbitrary power over the people they stop, though phone searches take place outside the context of checkpoints, too.²⁴⁹

²⁴⁵ Hossam el-Hamalawy, "City of Exile: The Egyptian Diaspora in Berlin," DAWN, October 21, 2021, <https://dawnmena.org/city-of-exile-the-egyptian-diaspora-in-berlin/>; Human Rights Watch, "Egypt: Dissidents Abroad Denied Identity Documents," March 13, 2023, <https://www.hrw.org/news/2023/03/13/egypt-dissidents-abroad-denied-identity-documents>; GC4HR, "دع ب قار علا يف ناسنلا قوقح نع تاغاداملاو نيعفاداملا تايدحت كارج نيرشت بيعشلا" February 2023, https://www.gc4hr.org/wp-content/uploads/2023/02/GCHR_Report_on_Iraq_05_May_2022_Ar_FF.pdf; Yousra Bilali, "على خطى اللاجئين.. خرائط المنفيات التونسيات في فرنسا عبر الأجيال," Hounna, December 24, 2025, <https://hounna.net/%D8%B9%D9%84%D9%89-%D8%AE%D8%B7%D9%89-%D8%A7%D9%84%D9%84%D8%A7%D8%AC%D8%A6%D8%A7%D8%AA-%D8%AE%D8%B1%D8%A7%D8%A6%D8%B7-%D8%A7%D9%84%D9%85%D9%86%D9%81%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%AA%D9%88%D9%86/>; Méline Laffabry, "You either cooperate or you end up in prison,' says Tunisian journalist in exile," Aidóni, May 24, 2024, <https://aidoni.org/2024/05/24/you-either-cooperate-or-you-end-up-in-prison-says-tunisian-journalist-in-exile/>.

²⁴⁶ SMEX phone interview with "Amr," June 8, 2026.

²⁴⁷ SMEX phone interview with "Amr," June 8, 2026.

²⁴⁸ Mahdi Ahmed, "Digital Rights Violations of Iraqis During the October (Tishreen) Protests: Internet Shutdowns, Platform Blocking, and Phone Searches," INSM, October 2, 2025, <https://insm-iq.org/en/?p=1711>; Human Rights Watch, "'Everyone Wants Me Dead' Killings, Abductions, Torture, and Sexual Violence Against LGBT People by Armed Groups in Iraq," March 23, 2022, <https://www.hrw.org/report/2022/03/23/everyone-wants-me-dead/killings-abductions-torture-and-sexual-violence-against>.

²⁴⁹ Mahdi Ahmed, "Digital Rights Violations of Iraqis During the October (Tishreen) Protests: Internet Shutdowns, Platform Blocking, and Phone Searches," INSM, October 2, 2025, <https://insm-iq.org/en/?p=1711>; France24, "مصر: المجلس القومي لحقوق الإنسان ينتقد تفتيش هواتف المواطنين بالقوة في الشارع," October 4, 2019, <https://www.france24.com/ar/20191004-%D9%85%D8%B5%D8%B1-%D8%AD%D9%82%D9%88%D9%82-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86-%D9%85%D8%AC%D9%84%D8%B3->

Egypt has a well-established pattern of setting up ad hoc, location or event-specific checkpoints at which officers conduct unauthorized phone searches and detentions.²⁵⁰ For example, churches in Egypt always look like “war zones,” according to one interviewee, while events such as the 2022 UN Climate Conference (COP27) often result in a surge of additional temporary checkpoints.²⁵¹ In Iraq, checkpoints are a vestige of US invasion that continue to be maintained by Iraqi, Kurdish, and militia security personnel, and are mainstays of daily life for Iraqis.

In both countries, checkpoints are places where officers can seize and search your phone without warrants, and where arbitrary arrests can be made based on what officers deem inappropriate content. People are often threatened by officers into compliance. “If you refuse to open your phone, they assume the worst of you,” Hassan, an Egyptian digital rights activist said.²⁵² He continued:

“The police have the right to ask you for your phone [at checkpoints], and once it’s in their hand, they check your Facebook, your WhatsApp, your photos. And that’s how it starts. You could be a member of the Muslim Brotherhood, a lesbian – anyone with something on their phone that doesn’t match the officer’s personal social values. If they see something they don’t like, it’s over.”

For this reason, interviewees described limiting the number of devices they carry on their person and what information they keep stored on them (photos, messages, etc.) and treating domestic and international travel and checkpoint preparation as part of their broader digital hygiene routines.

Office-Related Precautions

In Tunisia, interviewees described the crackdown as both imminent and already underway. Mona, an Egyptian human rights expert, said that her organization’s office in Tunis is “bracing itself every day” for a summons from the government and that it had developed “contingency plans and pre-emptive security measures” to mitigate the oncoming storm.²⁵³ Two interviewees said they placed additional security cameras at the entrances of their respective offices in Tunis.²⁵⁴ In Egypt, by contrast, many of the most severe organizational security decisions – such as closing offices or moving programming outside the country – were made

[%D8%AA%D9%81%D8%AA%D9%8A%D8%B4-%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D9%88%D8%B2%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%AF%D8%A7%D8%AE%D9%84%D9%8A%D8%A9-%D9%85%D8%B8%D8%A7%D9%87%D8%B1%D8%A7%D8%AA.](#)

²⁵⁰ Human Rights Watch, “All This Terror Because of A Photo: Digital Targeting and Its Offline Consequences,” February 21, 2023, <https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt>.

²⁵¹ SMEX phone interview with “Hassan,” April 17, 2026; Ragheb Malli, SMEX, “Heightened Digital Oppression in Egypt,” January 27, 2023, <https://smex.org/heightened-digital-oppression-in-egypt/>.

²⁵² SMEX phone interview with “Hassan,” April 17, 2026.

²⁵³ SMEX written correspondence with “Mona,” June 11, 2026.

²⁵⁴ SMEX written correspondence with “Mona,” June 11, 2026; SMEX phone interview with “Rouba,” May 19, 2026.



years earlier. Most digital rights organizations no longer have offices in Egypt to manage. In Iraq and the KRI, interviewees described physical security threats as more diffuse and less reducible to direct government retaliation alone due to the presence of militias.

D. Increasing Awareness of Digital Safety Practices, Media Literacy Campaigns, Fact-Checking

A capacity challenge digital rights groups face is who to focus their media literacy efforts on. Often, if a group runs media literacy campaigns and digital hygiene campaigns, they are geared for the human rights defenders with the biggest profiles. But, as Amr pointed out, if government figures, hackers, or other actors want to harm a prominent figure, they won't necessarily target the prominent figure first, or even directly. They may target "their mom, their sister, their father – people who aren't working in a high risk environment and whose devices and practices are far more rudimentary."²⁵⁵

Laila, also an Egyptian digital rights expert, echoed a similar sentiment when she said that digital rights "need to connect more directly with the digital needs for the public by speaking to the 'normal citizen' and discuss with them questions like why are digital rights important, what is digital security, and why does it matter for you?"²⁵⁶

Some organizations respond to this gap by running public education campaigns that teach people the basics of the principles of free expression, things to look out for when engaging with others online, and how to protect oneself online. Salam@, an initiative launched by the SecDev Foundation, focuses its media literacy efforts on women and girls throughout the SWANA region to help protect them against online harassment, blackmail, and other digital harms.²⁵⁷ An individual familiar with the project described it as a "guerilla awareness campaign for digital safety. We did not make this product for human rights defenders, we made it for your local coiffeur, your grocery store cashier – your everyday women – and students too."²⁵⁸ Masaar, an Egyptian digital rights group, takes a similar open-access approach by publishing resource guides that are not limited to Egypt or formal civil society actors.²⁵⁹ The Baghdad Women's Association runs digital clinics at

²⁵⁵ SMEX phone interview with "Amr," June 8, 2026.

²⁵⁶ SMEX phone interview with "Laila," May 22, 2026.

²⁵⁷ SecDev Foundation, "Salam@: Promoting digital resilience for women and girls across the Middle East and North Africa (MENA)," n.d., <https://secdev-foundation.org/salamat/>.

²⁵⁸ SMEX phone interview with "Amr," June 8, 2026.

²⁵⁹ Masaar, "Tools and Applications for Digital Security and Privacy Protection," December 18, 2023, <https://masaar.net/en/digital-security-tools-and-applications/>; Masaar, "Digital Security for Women: Initiatives and Training Guides," September 12, 2022, <https://masaar.net/en/digital-security-for-women-initiatives-and-training-guides/>.

university campuses throughout Iraq and the KRI.²⁶⁰ civil society actors.²⁶¹ The Baghdad Women's Association runs digital clinics at university campuses throughout Iraq and the KRI.²⁶²

Offering a direct public service element is also important because awareness campaigns alone do not address urgent harm once it occurs. Digital Citizenship Tunisia, a project housed within the Salam@ initiative, manages a free hotline that supports individuals in Tunisia who report instances of online violence, with a focus on digital safety support such as fighting identity theft, removing harmful content, and recovering or reactivating accounts and pages wrongly taken down.²⁶³ INSM manages a similar effort called the Digital Emergency Helpdesk, and Access Now runs a Digital Security Helpline.²⁶⁴

These emergency response desks fill an urgent need, but they are difficult to sustain, as interviewees described. Emergency desks require trained staff who are available to respond to requests quickly, stable funding, and technical training. That need becomes more acute during moments of acute crisis, yet the crises that increase demand for emergency support also strain the organizations providing it.

Fact-checking platforms exist within this broader media literacy ecosystem because the ability to identify misleading or manipulated information is itself a digital safety practice – especially in contexts where disinformation is often used to smear activists, discredit political opponents, or justify repression.²⁶⁵ Digital

²⁶⁰ Baghdad Women's Association, "Baghdad Women Association Implements 'Digital Clinic' Activity to Combat Digital Violence at Nawroz University," December 31, 2025, <https://bwa-iraq.org/baghdad-women-association-implements-digital-clinic-activity-to-combat-digital-violence-at-nawroz-university/>; Baghdad Women's Association, "Empowering Students Against Digital Violence: BWA Marks 16 Days of Activism with Digital Clinic in Zakho University," December 31, 2025, <https://bwa-iraq.org/empowering-students-against-digital-violence-bwa-marks-16-days-of-activism-with-digital-clinic-in-zakho-university/>.

²⁶¹ Masaar, "Tools and Applications for Digital Security and Privacy Protection," December 18, 2023, <https://masaar.net/en/digital-security-tools-and-applications/>; Masaar, "Digital Security for Women: Initiatives and Training Guides," September 12, 2022, <https://masaar.net/en/digital-security-for-women-initiatives-and-training-guides/>.

²⁶² Baghdad Women's Association, "Baghdad Women Association Implements 'Digital Clinic' Activity to Combat Digital Violence at Nawroz University," December 31, 2025, <https://bwa-iraq.org/baghdad-women-association-implements-digital-clinic-activity-to-combat-digital-violence-at-nawroz-university/>; Baghdad Women's Association, "Empowering Students Against Digital Violence: BWA Marks 16 Days of Activism with Digital Clinic in Zakho University," December 31, 2025, <https://bwa-iraq.org/empowering-students-against-digital-violence-bwa-marks-16-days-of-activism-with-digital-clinic-in-zakho-university/>.

²⁶³ Digital Citizenship Tunisia, "Our Work," n.d., <https://dco-tn.org/our-work>.

²⁶⁴ INSM, "INSM Digital Emergency HelpDesk," n.d., https://insm-iq.org/en/?page_id=1540; Access Now, "Digital Security Helpline," n.d., <https://www.accessnow.org/help/>.

²⁶⁵ Duke Reporters' Lab at Duke University's Sanford School of Public Policy, "Fact Checking Sites Around the World," n.d., <https://reporterslab.org/fact-checking/>; Ian Dehaven, "Disinformation as a Tool of Regime Survival in Tunisia," Arab Center of Washington DC, July 21, 2023, <https://arabcenterdc.org/resource/disinformation-as-a-tool-of-regime-survival-in-tunisia/>; Mohammed Salih, "Much Ado About Nothing: Disinformation Campaigns and Foreign Policy in Iraq," Carnegie Endowment for Peace, October 3, 2023, <https://carnegieendowment.org/sada/2023/10/much-ado-about-nothing-disinformation-campaigns->

rights groups in Egypt, Iraq, and Tunisia work in the fact-checking space, but not without risks. For example, in Egypt, after Saheeh Masr published an investigation alleging domestic media censorship of Egypt's 2023 presidential election, the Supreme Council for Media Regulation accused it of violating media codes and launched a legal investigation for "spreading false news."²⁶⁶ Also in 2023, Egyptian authorities violently raided the home of journalist Karim Asaad of Matsadaash, another independent fact-checking group, just hours after the group posted an investigation implicating the Egyptian government in a gold smuggling scheme.²⁶⁷

In Iraq, INSM does both public education and fact-checking. In partnership with UNAMI, INSM launched a digital security guide for Iraqi human rights defenders, journalists, activists, and civil society groups, and has held over 200 digital security trainings for these actors since 2021.²⁶⁸ INSM also developed The Checker, a free, public fact checking and digital media literacy platform focused on promoting an online environment free from hate speech and disinformation.²⁶⁹

INSM is one among many groups trying to balance the digital needs of civil society actors and those of the general public.²⁷⁰ That balance, however, is difficult to strike. Digital rights organizations are expected to train high-risk actors, respond to individual emergencies, monitor digital threats, correct false information, and sustain public education campaigns, often with limited staff and short-term funding reliant on external donors (and by extension, external political shifts).²⁷¹

Media education and fact-checking initiatives across the SWANA region also suffer from severe funding restrictions, most noticeably after the 2025 U.S. foreign

[and-foreign-policy-in-iraq](#); Dina Sadek, Layla Mashkour, Iain Robertson, and Andy Carvin, "Intentionally vague: How Saudi Arabia and Egypt abuse legal systems to suppress online speech," Atlantic Council, June 12, 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/intentionally-vague-how-saudi-arabia-and-egypt-abuse-legal-systems-to-suppress-online-speech/>.

²⁶⁶ Saheeh Masr X post, @saheehmasr; "أصدرت الشركة المتحدة للخدمات الإعلامية المملوكة للدولة، نشرة بـ"المحظورات" خلال الانتخابات الرئاسية المصرية، وأرسلتها إلى إدارات القنوات التلفزيونية والمواقع الإلكترونية التابعة لها....تغطية##الانتخابات_الرئاسية_المصرية،" December 10, 2023, <https://x.com/SaheehMasr/status/1733799668843245606>; Salma Hindy, "Saheeh Masr under investigation for exposing electoral media censorship," Mada Masr, December 11, 2023, https://www.madamasr.com/en/2023/12/11/news/u/saheeh-masr-under-investigation-for-exposing-electoral-media-censorship/?mc_cid=f785df730e&mc_eid=de4blae238.

²⁶⁷ PEN America, "In Solidarity with Egyptian Fact-Checking and Independent Media Platform Matsadaash," August 25, 2023, <https://pen.org/in-solidarity-with-egyptian-fact-checking-and-independent-media-platform-matsadaash/>.

²⁶⁸ UNAMI, "UNAMI Human Rights and INSM for Digital Rights in Iraq launch user guide on digital security for Iraqi human rights defenders," October 31, 2022, <https://iraq.un.org/en/205342-unami-human-rights-and-insm-digital-rights-iraq-launch-user-guide-digital-security-iraqi>.

²⁶⁹ INSM, "TheChecker' Platform for Fact-Checking and Digital Media Literacy," n.d., https://insm-iq.org/en/?page_id=1547.

²⁷⁰ NDI, "Information Disorder in Iraq: Trends, Perceptions, and Implications," https://www.ndi.org/sites/default/files/Information%20Disorder%20in%20Iraq_EN%20%28v.1%29.pdf.

²⁷¹ NDI, "Information Disorder in Iraq: Trends, Perceptions, and Implications," https://www.ndi.org/sites/default/files/Information%20Disorder%20in%20Iraq_EN%20%28v.1%29.pdf.

assistance cuts and proposals to terminate nearly all State Department Bureau of Democracy, Human Rights, and Labor (DRL) grants.²⁷² The source familiar with the Salam@ initiative said that after the DRL cuts, Salam@’s SWANA-based operations drastically slowed.²⁷³

“Yasir,” a Kurdish journalist and independent fact-checker similarly told SMEX that he could not find consistent work after the DRL cuts because many of the NGOs he had worked with were no longer prioritizing fact-checking initiatives, much less in the Kurdish language.²⁷⁴ “Because of the lack of funding, there isn’t a consistent focus on fact-checking in Kurdistan,” even though “there is a lack of these platforms in Iraq and there is a lot of misinformation in general online in the KRI and Iraq,” he said.

This funding instability underscores the central tension of public-facing digital safety work generally. The risks are continuous, but the resources available to respond to them are often temporary (described further below). Interviewees also emphasized that in addition to capacity and funding constraints, the cultural landscape in which fact-checkers operate makes the work harder. Fact-checking initiatives do not operate in a neutral information environment; rather, they work in polarized settings where people may reject corrections that don’t align with their social, political, or religious views.²⁷⁵

Trust is another barrier. Without an established reputation, it’s easy for people to dismiss the person or entity doing the fact-checking. Yasir said of the Iraqi landscape:

Fact-checking in Iraq needs a lot of funding and technical capacity to be trusted. Tech4Peace is really the only group that has this funding. They also have an established reputation such that when they say something is true or not, people know to trust them – even if they disagree or are angered by the results of the fact-check itself.

However, I’m not trustworthy as a fact-checker in KRI. If I go online and post something on my personal social media accounts that something is not true, people will be like, ‘Who are you? What are your credentials?’²⁷⁶

²⁷² Arab Fact-Checkers Network, “Summary of the Regional Meetings for the Arab Fact-Checkers Network (AFCN) from ARIJ 2022 - 2025,”

<https://arabfcn.net/regional-meetings-summary/2022-2024/en/>; Mohammed al-Maskati and Luis Barrueto, “How U.S. funding cuts expose civil society to digital attacks,” April 9, 2025, Access Now, <https://www.accessnow.org/u-s-funding-cuts/>.

²⁷³ SMEX phone interview with “Amr,” June 8, 2026.

²⁷⁴ SMEX phone interview with “Yasir,” June 9, 2026,

²⁷⁵ SMEX phone interview with “Omar,” April 16, 2026; SMEX phone interview with “Yasir,” June 9, 2026; SMEX phone interview with “Diyar,” May 9, 2026; Saheeh Masr, “Fact Checking in a Polarized Egyptian Public Opinion,” Arab Fact Checkers Network, October 4, 2021, <https://arabfcn.net/en/blog/2021/10/04/fact-checking-in-a-polarized-egyptian-public-opinion/>.

²⁷⁶ SMEX phone interview with “Yasir,” June 9, 2026,



A Tunisian civil society representative said her organization is shifting its priorities to media literacy and education campaigns precisely to continue building trust with the public, amid a time when avenues for other advocacy opportunities are shrinking. She said that legal advocacy has limited reach without public support, and that helping people better understand digital media, emerging technologies, and how online information is shaped offers civil society organizations a safer way to maintain public engagement and rebuild trust.

E. Conducting and Publishing Research in Coalitions

A key aspect of digital rights organizations' work in Egypt, Iraq, and Tunisia is conducting research that feeds into initiatives owned by broader coalitions or published in partnership with larger international organizations, especially when a group cannot litigate or conduct public advocacy alone due to security risks.

A benefit to this approach is that smaller organizations often have stronger local networks, language skills, and context-specific knowledge, while larger organizations are better positioned to absorb public or governmental pressure and attract public support. Joint work between them allows local groups to shape the analysis while sharing the burden of publication and potential retaliation with larger ones. For example, one Iraqi organization told SMEX that it has ghost-written statements published by international rights groups that include the use of the term “gender” so as to continue supporting this stream of work while avoiding government retaliation for using the term.²⁷⁷ In Tunisia, coalition work is often the only way to publish sensitive material due to the active crackdown and fragmentation of CSOs attention, according Nissaf, a Tunisian human rights advocate.²⁷⁸

However, joint work is resource-intensive and difficult to manage in an environment beset with security challenges and competing mandates. It generally requires a main interlocutor, and the burden of work is almost never evenly shared among partners. Two regional digital rights experts described the “constant conundrum of shared work between local, regional, and international NGOs,” noting that international organizations often have specific ways of describing abuses that can be useful for global advocacy but constraining for local partners.²⁷⁹

Both experts also noted that joint research also often depends on unpaid work by volunteers or smaller NGOs based in conflict zones who may struggle with internet connectivity and face other acute security challenges. As such, while coalition work can be protective, it can also reproduce inequities between

²⁷⁷ SMEX phone interview with “Yasmine,” June 5, 2026.

²⁷⁸ SMEX phone interview with “Nissaf,” June 5, 2026.

²⁷⁹ SMEX phone interview with Dia Kayyali, June 15, 2026; SMEX written correspondence with “Mona,” June 11, 2026.



organizations that supply local organizations and those with the resources to coordinate, edit, publish, and promote the final product.²⁸⁰

Competing for media attention also shapes coalition priorities. One expert commented that digital rights issues in Egypt, Iraq, and Tunisia “don’t get enough attention, even at the regional level,” in coalition settings in part because coalition work is often pulled towards the crises that already command the most media, funding, and platform attention.²⁸¹ They noted that a large share of regional digital rights coalition work in recent years has focused on Palestine, particularly amid the escalation in Gaza, a topic that draws wide attention from Western activists, journalists, and policymakers. While the attention increases engagement for the coalition’s material, it means other issues such as hate speech targeting women and LGBTQ+ people in less visible countries receive less attention.

These challenges have not prevented civil society actors from coordinating widely around especially urgent issues. In 2023, more than 1,000 Iraqi academics, journalists, activists, lawyers, civil society representatives, and other public figures signed the statement “On Gender, Freedoms, and Social Justice,” condemning a politically driven campaign against the use of the term “gender” and defending it as consistent with Iraq’s constitutional and international obligations.²⁸² The initiative brought together participants from across sectors at a time when many organizations feared addressing the campaign publicly.²⁸³

F. Engaging in Platform Accountability Efforts

Across the SWANA region, local digital rights organizations do not treat social media platforms only as spaces where censorship, harassment, and disinformation unfold. They also treat them as governance actors whose policies help determine what people can say online, what content stays up, what content disappears, and whose abuse gets taken seriously. Platform engagement therefore forms a distinct civil society strategy. Digital rights groups meet with companies, raise concerns about content moderation and takedown practices, push for stronger protections for users at risk, and advocate for policies that better reflect the political and linguistic realities of the region.

The organizations consulted for this report discussed Meta platforms at length, particularly Facebook, Instagram, and WhatsApp, because of their wide reach in Egypt, Iraq, and Tunisia. They also raised concerns about Telegram, TikTok, X,

²⁸⁰ SMEX phone interview with Dia Kayyali, June 15, 2026; SMEX written correspondence with “Mona,” June 11, 2026.

²⁸¹ SMEX phone interview with Dia Kayyali, June 15, 2026.

²⁸² “عن الجندر والحريات والعدالة الاجتماعية,” available <https://docs.google.com/forms/d/e/1FAIpQLSd6URKP0BkZrMT8fHoYD88LBjhMaVgw7r5RxWZIKl-qEZrRRw/viewform>.

²⁸³ Zahra Ali, “In Iraq, To Defend Gender Is to Refuse Violence,” Jadaliyya, August 31, 2023, <https://www.jadaliyya.com/Details/45269>.

YouTube, though their ability to engage with these companies varies and remains far more limited than their engagement with Meta.²⁸⁴

SMEX found that digital rights organizations' ability to influence social media platforms has narrowed in recent years, brought on in large part by the Covid-19 pandemic and the second election of US President Donald Trump. A SWANA digital rights expert described how, before relations began to deteriorate around 2020, regional civil society groups generally had greater access to company representatives and more opportunities to raise concerns about government overreach and restrictions on peaceful content.²⁸⁵ These channels never offered a reliable accountability mechanism because they depended on company willingness, staff relationships, and internal platform priorities. Still, they gave digital rights organizations a way to push companies toward stronger free expression and human rights commitments.

That landscape changed considerably. The expert traced the first major shift to around 2020, when the Covid-19 pandemic disrupted the in-person meetings through which platforms had often engaged civil society organizations. Staffing changes introduced during this period later hardened into long-term cuts, while companies increasingly replaced or supplemented human review with artificial intelligence. The gap deepened after Elon Musk acquired X (formerly Twitter) in 2022 and moved the platform sharply away from the trust-and-safety and civil society engagement efforts that had previously supported parts of platform accountability work in the region.²⁸⁶ The relationship deteriorated further when US President Donald Trump began his second term, as major technology companies increasingly aligned themselves with a political environment hostile to content moderation, diversity initiatives, and other rights-based safeguards. The effect was not limited to X and includes Meta.²⁸⁷

Much of the region's platform accountability work depends on relationships. Organizations have used coalitions – including the Middle East and North Africa (MENA) Alliance for Digital Rights (MADR), in which SMEX participates and serves as secretariat – to approach platforms collectively.²⁸⁸ Organizations nevertheless must rely on personal relationships to get meetings, escalate urgent cases, or obtain responses.²⁸⁹ That makes the work vulnerable. When a trusted employee

²⁸⁴ MADR Network, "FAQ: Content Moderation Policies," n.d., <https://madr.network/faq-content-moderation-policies/>.

²⁸⁵ SMEX interview with Dia Kayyali, June 15, 2026.

²⁸⁶ NPR, "Musk's Twitter has dissolved its Trust and Safety Council," December 12, 2022, <https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk>; Thomas Brewster, "Musk's X Fired 80% Of Engineers Working On Trust And Safety, Australian Government Says," Forbes, January 10, 2024, <https://www.forbes.com/sites/thomasbrewster/2024/01/10/elon-musk-fired-80-per-cent-of-twitter-x-engineers-working-on-trust-and-safety/>.

²⁸⁷ Dionysia Peppas, SMEX, "Meta in X's steps: how new content moderation policy changes endanger the digital space in WANA and abroad," January 9, 2025, <https://smex.org/meta-in-xs-steps-how-new-content-moderation-policy-changes-endanger-the-digital-space-in-wana-and-abroad/>.

²⁸⁸ See MADR Network website, <https://madr.network/>.

²⁸⁹ SMEX phone interview with "Yasmine," June 5, 2026.



leaves a company, when a civil society contact loses capacity, or when a platform dissolves the relevant team, the channel can disappear.

This fragility reflects a broader retreat from rights-based platform governance, leaving SWANA-based organizations with fewer reliable tools to challenge company decisions just as digital repression and online abuse are becoming more consequential. Digital rights organizations continue to press companies to uphold free expression principles, resist government overreach, and address online abuse. They do so, however, in an environment where engagement channels have weakened, trust-and-safety teams have shrunk, and major platforms often ask civil society organizations for documentation without providing clear remedies. As one digital rights expert summarized, “It’s always about them asking for reports and promising they’ll do their best.”

Iraqi Digital Rights Organizations’ Engagement with Platforms

Iraqi digital rights organizations provided the most detailed examples of direct platform accountability work for this report. Egyptian and Tunisian organizations face more decimated or tightly restricted civil society landscapes, while Iraqi organizations described having more room to engage platforms and government bodies, even under serious political pressure.

Yasmine said her organization has sent platforms detailed research and reports showing that digital violence against women continues to rise in Iraq.²⁹⁰ She described some recent progress with TikTok. “We have had a good response from TikTok in the past few months because they are interacting with us,” she said. “We did a lot of presentations with them, we also developed a specific lexicon for them that people are using on TikTok and Meta.” Her organization developed this lexicon to help platforms understand the coded language people use to threaten women in Iraqi Arabic and Kurdish Sorani and Kurmanji.

One example captures why local language expertise matters. Yasmine described the Iraqi phrase “ijaj abu delivery,” which might sound to a non-Iraqi reviewer like a harmless reference to a delivery driver. In Iraqi online spaces, she said, users now deploy the phrase as a death threat against women. The phrase refers to the killing of Iraqi influencer Um Fahad, who was shot by a person dressed as a delivery worker in April 2024.²⁹¹ Yasmine’s organization added the phrase to the lexicon it shared with TikTok. According to her, TikTok promised to control the term on its platform, though she said “until now nothing is really happening.” Still, she described TikTok’s response as more serious than usual: “They at least took our presentation seriously and engaged with it seriously.”²⁹²

²⁹⁰ SMEX phone interview with “Yasmine,” June 5, 2026.

²⁹¹ NBC, “Iraqi authorities investigating killing of social media influencer Um Fahad,” April 27, 2024, <https://www.nbcnews.com/news/world/iraqi-authorities-investigating-killing-social-media-influencer-um-fah-rcna149671>.

²⁹² SMEX phone interview with “Yasmine,” June 5, 2026.



The lexicon identifies a broader vocabulary of coded misogyny in Iraqi online spaces, including phrases that draw on car culture, pandemic terminology, national geography, household objects, gaming language, and women's rights terminology to sexualize, threaten, or delegitimize women while preserving plausible deniability.²⁹³ In literal translation, these phrases can look like ordinary references to the Mercedes Benz logo, an engine size, or the Tigris and Euphrates rivers. In Iraqi digital culture, however, they are understood as sexual insults, threats of assault, or accusations that women activists are immoral, foreign-backed, or linked to LGBTQ+ activism. Yasmine emphasizes that this vocabulary is designed to "operate beneath the radar of platform safety systems while inflicting maximum social damage," which is precisely why platform escalation depends on local experts who can explain not only what a term means, but when and how it becomes a threat.

Yasmine's organization's platform engagement has produced results in urgent cases. She described one case involving a girl whose private photos were leaked online and who faced blackmail. The girl told Yasmine that if the content did not come down within 24 hours, she would kill herself. Yasmine escalated the case to Meta. "They responded really quickly and resolved the situation within hours," she said. "Her photos were removed." She added that platforms do not respond in every case, but Meta and TikTok understand that cases from Iraq can carry immediate risks. "They are aware that there is a different context in our region and that they need to respond quickly whenever they can, especially if we flag a case," she said.

But the case also exposed the fragility of the relationship model. "If [redacted organization] wasn't a trusted partner, this problem would never be solved," she said. Platform accountability in Iraq often depends on whether a specific organization has enough trust, staff capacity, and personal relationships to escalate urgent cases. If her organization could no longer play that role, she warned, similar cases might go unanswered. Platforms now reach out to her organization when online harassment cases arise. The organization takes that responsibility seriously, but the work has also become overwhelming.

That platform relationship became more complicated as Meta increased its engagement with the CMC. Yasmine said recent restrictions and geoblocking measures have made advocacy with Meta more difficult and raised transparency and accountability concerns.²⁹⁴ Meta apparently told her organization that it blocks content at the government's request because the government frames the

²⁹³ Information on file with SMEX.

²⁹⁴ In October 2025, ARTICLE 19 reported that the CMC had repeatedly asked Meta to georestrict posts and accounts under broad legal provisions, including provisions that criminalized insulting or defamation of public officials. Meta acknowledged restricting such content but said that it did not violate its Community Standards when responding to Iraqi legal requests. See: ARTICLE 19, "Iraq: Cooperation with Big Tech must not put freedom of expression at risk," October 23, 2025, <https://www.article19.org/resources/iraq-cooperation-with-big-tech-must-not-put-freedom-of-expression-at-risk/>.

content as unlawful and because Meta wants to maintain a workable relationship with Iraqi authorities so the platform does not face broader restrictions. Her organization views much of this content removal as freedom of expression violations, but Meta has responded by asking civil society to pressure the government to reduce geoblocking requests.

This places the organization in a difficult intermediary position. It maintains a good working relationship with the CMC, which invites her to workshops, asks her to speak about online gender-based violence and cybersecurity. The CMC, however, no longer engages it on policy questions such as geoblocking. Yasmine contrasted this with 2023, when her organization reviewed and successfully pushed back against the CMC's proposed digital content regulation guidelines. That kind of policy engagement, however, "is not happening anymore."

Yasmine attributed the difference to political sensitivity. Online gender-based violence can be framed as a user safety issue; geoblocking, by contrast, primarily affects political content, including election-related content, commentary about candidates or parliament, and even political humor. "Political content is way more sensitive than online gender based violence," she said, because "it's ultimately about control and order." This distinction helps explain why engagement can succeed in urgent safety cases while failing when restrictions serve political interests.

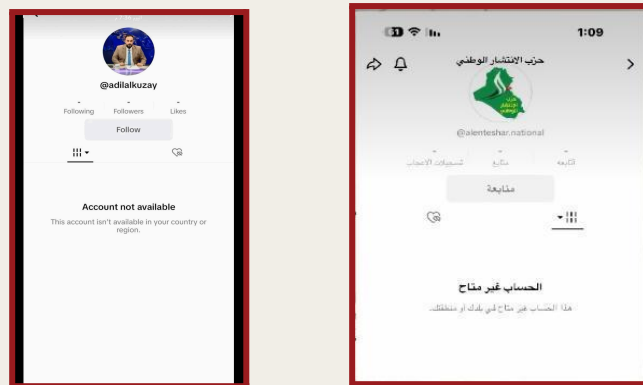
Omar, an Iraqi digital rights expert, explained that the government pressures technology companies with the threat of broader restrictions if they do not comply with geoblocking and takedown requests. He said these requests disproportionately target political content posted by adversaries of the government or political rivals. According to him, the two biggest entities for regulating media in Iraq (the National Contact Point of Iraq and the CMC) coordinate their efforts to flag content they consider inappropriate and ask Meta and other platforms to block or remove it. He said one person familiar with the monitoring process told him the takedown requests were "coming from above" and from "a really high level."²⁹⁵ According to Meta's most recent public reporting, between July and December 2025, it restricted 1,400 items reported by National Contact of Iraq for allegedly violating various Iraqi laws.²⁹⁶

The result is a platform environment in which peaceful political content gets taken down while abusive content remains available. Omar told SMEX that Arabic-language posts on Meta platforms about US-sanctioned figures or armed groups are often geoblocked within Iraq and the KRI, even if 1) those posts discuss these figures in a purely academic or factual manner, 2) they are posted by trusted Iraqi media outlets, and 3) even when the post does not praise or support

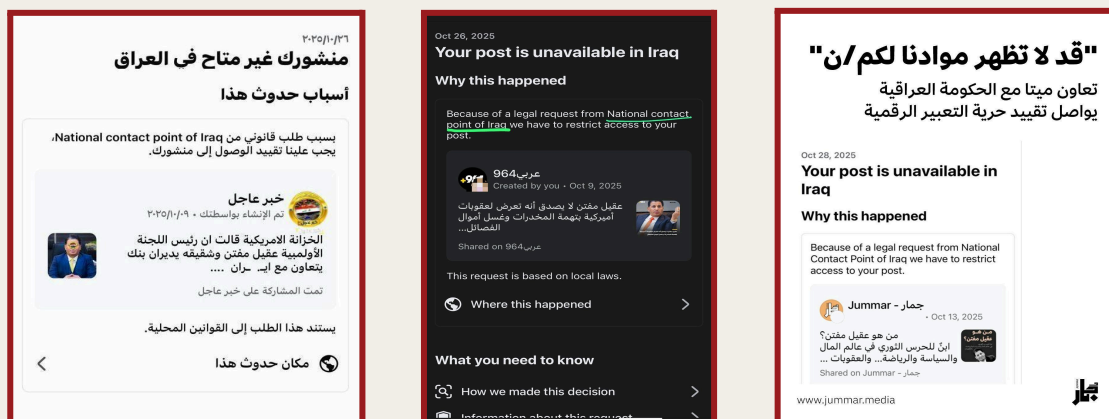
²⁹⁵ SMEX phone interview with "Omar," April 16, 2026.

²⁹⁶ Meta Transparency Center, Case Studies, available <https://transparency.meta.com/reports/content-restrictions/case-studies/>.

the group.²⁹⁷ SMEX reviewed several screenshots provided by the interviewee supporting this claim.



Omar also pointed out that TikTok geoblocked the account of the political party “Hezb Al-Intishar Al-Watany” during the 2025 elections after the party criticized the prime minister and discussed corruption in a video. The TikTok page and content of Adil al-Kuzay, Director of the Iraqi Observatory for Rights and Freedom, is also geoblocked. He provided screenshots of the pages from inside Iraq; the SMEX researcher, who is based outside of Iraq, could view the TikTok profiles and content without issue at the time of writing.



Persistent Platform Gaps

The research also identified platform problems that extend beyond takedown and geoblocking disputes. These include weak child safety mechanisms, WhatsApp and Facebook groups where racist and abusive content runs rampant, violent gaming content, sports betting, human trafficking schemes, data leaks, and online harassment in closed or hard-to-monitor spaces. These issues matter because civil society organizations often can document only the most visible harms. Private groups, closed chats, and platform features designed for rapid sharing can hide abuse from researchers while still exposing users to serious risk. Laila described several child safety concerns on social media platforms more generally.²⁹⁸ She said children can access age-inappropriate material and open social media accounts without effective safeguards. WhatsApp creates particular

²⁹⁷ SMEX phone interview with “Omar,” April 16, 2026.

²⁹⁸ SMEX phone interview with “Laila,” May 22, 2026.

risks because a child with a phone number can be added to groups without knowing how to leave them, exposing them to harassment or harmful content. She also raised concerns about violent games, sports betting, and financial activity by young teens online without adult oversight. These examples show that platform accountability work cannot focus only on political speech. It also requires attention to choices that can potentially expose children and young people to abuse, exploitation, or financial harm.

Private Facebook groups create another gap. The same Egyptian expert described local neighborhood groups in Egypt where racist hate speech about Black Sudanese people circulates with little outside scrutiny. Civil society organizations struggle to research these spaces because access depends on membership and trust, but the harm still impacts large numbers of people.

Amr described a severe abuse pattern involving human trafficking schemes that begin through Facebook advertisements or closed groups targeting economically disadvantaged women.²⁹⁹ Traffickers post remote work offers, flexible work opportunities, or home-based sales jobs. They then collect Facebook information, family contacts, and sometimes private photos of women under the pretext of reviewing applications. According to the expert, traffickers then manipulate these photos with AI and use them for blackmail.

Telegram

Telegram represents a distinct accountability gap across the three country contexts examined in this report, although comparable public data do not establish its relative penetration in Egypt, Iraq, and Tunisia. The problem, however, emerged most prominently in the report's Iraq research. Yasmine identified three particularly harmful types of Telegram channels: channels that publish hate speech and incite violence against political candidates, especially women; channels that leak people's private photos and information; and channels or bots that manipulate images for use in blackmail.³⁰⁰ Comparable forms of abuse have also been documented on Telegram in Egypt and Tunisia, often targeting women and girls.³⁰¹

²⁹⁹ SMEX phone interview with "Amr," June 8, 2026.

³⁰⁰ The Iraq Foundation, "Election Watch: Assisting Women Candidates to Counter Gender-Based Violence and Hate Speech During the Election Campaign," January 2022, <https://iraqfoundation.org/wp-content/uploads/2022/08/UNAMI-Final-Narrative-Report-Phase-3.pdf>; Frontline Defenders, "Open Letter: Social media companies must take urgent action to protect women human rights defenders," August 4, 2023, <https://www.frontlinedefenders.org/en/statement-report/open-letter-social-media-companies-must-take-urgent-action-protect-women-human>; Matt Burgess, "Millions of People Are Using Abusive AI 'Nudify' Bots on Telegram," Wired Magazine, October 15, 2024, <https://www.wired.com/story/ai-deepfake-nudify-bots-telegram/>; Aida al-Kaisy, "Online Violence Towards Women in Iraq," February 2022, <https://elbarlament.org/wp-content/uploads/2022/03/Aida-2.pdf>.

³⁰¹ Asmaa Fathy, SMEX, "Egypt Online Violence Against Women on the Rise," January 30, 2024, <https://smex.org/egypt-online-violence-against-women-on-the-rise/>; Yasmina Shabana, Arab Reporters for Investigative Journalism's I Will Not Stay Silent program, "Cyberterrorism: The Spread

Despite the severity of these harms, Telegram remains difficult for civil society organizations to reach. This limited responsiveness extends beyond civil society. Authorities in several countries report repeated failures or lengthy delays by Telegram in responding to court orders, regulatory notices, and official requests, with cooperation sometimes occurring only after issuing fines, blocking orders, or threats of suspension.³⁰²

Yasmine said Telegram shows little interest in engaging with civil society organizations on online gender-based violence or geoblocking. “It’s not an [us] issue,” she said, noting that other digital rights groups face similar barriers and that they often lack a Telegram contact to which they can escalate cases. Yasir, a Kurdish journalist who works as an independent fact-checker, made a similar point about Telegram. In his experience, Telegram responds quickly to reports involving suspected ISIS groups. For other problems, it often takes little or no action, especially for content in the Kurdish language.³⁰³

Content Moderation Efforts are not Language-Responsive

Platform failures are compounded by the companies’ limited local presence and lack of language expertise needed to identify harmful content in Arabic dialects, Sorani, and Kurmanji. The issue does not only involve translation. Users often rely on emojis, stickers, flags, hashtags, and jokes to communicate threatening or harmful messages that automated systems likely cannot pick up on. The “ijaj abu delivery” example discussed above shows how dangerous this gap can become – a phrase that appears harmless to outsiders can carry a locally understood threat.

Civil society organizations try to fill this gap themselves. An Egyptian digital rights expert with a background in OGBV said she was working on a machine learning project addressing OGBV terminology in different Arabic dialects.³⁰⁴ INSM has also started developing an AI model called SAFA, or Safer Access for All, to detect

of Digital Violence Against Egyptian Women Activists,” September 7, 2025, <https://iwnss.arij.net/cyberterrorism-the-spread-of-digital-violence-against-egyptian-women-activist/>; Alia Taalat, Arab Reporters for Investigative Journalism’s I Will Not Stay Silent program, “Egypt’s Personal Status Law Fuels Digital Violence,” August 19, 2025, <https://iwnss.arij.net/digital-violence-an-obstacle-for-women-in-expressing-their-personal-lives/>; al-Hadath Tunisia, “انتهاك خصوصية فتيات تونسيات عبر تلغرام,” August 29, 2025, <https://www.facebook.com/watch/?v=1417848619518457>; Diwan FM Live, “و instagram شنوة صاير في,” August 18, 2023, <https://www.youtube.com/watch?v=WkipwfiwR6s>.

³⁰² Sarah McLaughlin, “Australia Targets Telegram as Russia Charges Its Founder with Terrorism,” August 4, 2026, Foundation for Individual Rights and Expression, <https://www.fire.org/news/blogs/free-speech-dispatch/australia-targets-telegram-russia-charges-its-founder-terrorism>; Ulisses Levy Silvério dos Reis, “Brazilian Judicial Branch v. Telegram (and Bolsonaro),” Verfassungsblog, March 25, 2022, <https://verfassungsblog.de/brazilian-judicial-branch-versus-telegram-and-bolsonaro/>; “Germany slaps messaging app Telegram with \$5 million fine,” AP News, October 17, 2022, <https://apnews.com/article/technology-middle-east-business-germany-dubai-aeff487f20d5b2da2bf73b76a32310f8>; Stephen Wright, “Telegram blocks terror content after Indonesia threatens ban,” AP News, July 16, 2017, <https://apnews.com/general-news-d04f02ec859f40fa98bbe5b11f455eac>.

³⁰³ SMEX phone interview with “Yasir,” June 9, 2026.

³⁰⁴ SMEX phone interview with “Laila,” May 22, 2026.



harmful content online.³⁰⁵ The model remains under development, but it reflects a broader civil society effort to build tools that platforms have not adequately invested in themselves. Regional digital rights groups should develop a shared lexicon or glossary and deliver it to platforms so companies can better understand local forms of abuse.

Yasir described similar problems with Kurdish content.³⁰⁶ He said Meta previously asked his team for a list of Kurdish swear words and racist epithets that users deployed freely without restrictions. His team sent the list, and Meta restricted those terms. “That was good,” he said. But he also said the Kurdish community remains largely unrecognized on social media platforms and that Kurdish language moderation still falls short. Kurdish content creates additional challenges because users write Kurmanji in Latin script and Sorani in Arabic script.

Yasir also described how language gaps affect the moderation of sexualized content involving children. He said Meta used to hold frequent meetings with the digital rights organization he was formerly affiliated with. The organization raised concerns about Instagram reels portraying underage girls with unmoderated sexual comments. Part of the problem, he said, came from ambiguity in the captions. Content moderators could not always tell whether a parent had posted the video, whether the girl had posted it herself, or whether someone else had posted sexualized content involving a minor. “But in Kurdish this is all hard to find and flag,” he said.

Another digital rights activist who focuses on the KRI further described difficulties with content moderation efforts for Kurdish-language material.³⁰⁷ Some harmful content disappears without clear explanation, making it difficult to know whether platforms removed it, users reported it, political actors targeted it, or coordinated campaigns pushed it offline. Other harmful posts circulate on platforms with weaker moderation, including Snapchat. Some accounts move between public and private settings to make posts go viral and then avoid public censure by privatizing their account. Other users place text, emojis, symbols, flags, and hashtags directly on images to evade platform detection. These tactics complicate both civil society monitoring and platform enforcement.

Artificial Intelligence, Disinformation, and Platform Responsibility

Artificial intelligence-generated (AI) content, manipulated images, and disinformation spread quickly and carry offline consequences. “Tarek,” an AI expert, described the rise of “AI slop” across the SWANA region and said people feel overwhelmed by the difficulty of determining what content is real before it gets manipulated. He argued that platforms should take more responsibility for

³⁰⁵ INSM, “Understanding and Analyzing Tactics and narratives of TFGBV during the Iraqi Parliament Elections November 2025,” June 15, 2026, <https://insm-iq.org/en/?p=1789>.

³⁰⁶ SMEX phone interview with “Yasir,” June 9, 2026.

³⁰⁷ Written correspondence with a Kurdish digital rights activist, relayed by “Yasmine.” SMEX written correspondence with “Yasmine,” June 5, 2026.



supporting communities and that governments should create a legal landscape requiring companies to act responsibly. “A landscape where nobody knows what’s real and what’s not is not benefitting anyone,” he said.³⁰⁸

He also emphasized that “it’s not the most vulnerable people who are the most susceptible to disinformation. It is the ‘normal’ people - those who are educated, young.” Yasir, the Kurdish journalist, said that he reposted a video on social media that he didn’t realize was AI-generated until his friend pointed it out to him.³⁰⁹ Daria, a Kurdish OGBV expert, reinforced this danger too. When it comes to digital blackmail, she sees “really advanced AI, not simple stuff.”³¹⁰

In Iraq, Egypt, and Tunisia, politicians or their supporters often pay social media pages to circulate rumors, smear campaigns, and disinformation about political opponents or other figures.³¹¹ During elections, these campaigns often target candidates using doctored images designed to damage their credibility and push them out of public life.³¹² Women who run for office routinely face rumors and manipulated images portraying them as drinking alcohol, behaving promiscuously, or otherwise violating social norms, making gendered disinformation a recurring focus of election-related fact-checking work.³¹³

The case of Zeinab Bijawat, known online as Zeinab “CEDAW,” shows how digital abuse and platform inaction can reinforce one another. Bijawat was targeted by militia actors for her work as a women’s rights activist and lawyer. After PMF-linked actors stopped her at a checkpoint in Baghdad, they seized her phone. Soon after, AI-generated and doctored photos of Bijawat were leaked online, including photos of her consuming alcohol and not wearing the hijab. According to “Omar,” an interviewee familiar with the case, Bijawat now lives in Erbil because she risks arrest if she travels through other governorates.³¹⁴ The interviewee said PMF-linked actors have brought a case against her, and that passport control could detain her if she leaves the KRI.

³⁰⁸ SMEX phone interview with “Tarek,” May 22, 2026.

³⁰⁹ SMEX phone interview with “Yasir,” June 9, 2026.

³¹⁰ SMEX phone interview with “Daria,” June 3, 2026.

³¹¹ Sheref Morad, “One million US Dollars spent on Iraqi election ads: Tracking three months of costly social media campaigning,” Jummar Media, November 3, 2025, <https://jummar.media/en/2025/11/03/one-million-us-dollars-spent-on-iraqi-election-ads-tracking-three-months-of-costly-social-media-campaigning/>; SMEX phone interview with “Yasir,” June 9, 2026; DFR Lab, “OPERATION CARTHAGE How a Tunisian company conducted influence operations in African presidential elections,” June 5, 2020, <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/operation-carthage-002.pdf>; Najla Ben Salah, “Tunisia: Defamation as a Way of Discrediting Opponents,” March 23, 2022, <https://smex.org/tunisia-defamation-as-a-way-of-discrediting-opponents/>.

³¹² SMEX phone interview with “Daria,” June 3, 2026; Hisham al Aqrabi, SMEX phone interview with “Diyar,” May 9, 2026; SMEX phone interview with “Yasmine,” June 5, 2026.

³¹³ SMEX phone interview with “Yasir,” June 9, 2026,

³¹⁴ SMEX phone interview with “Omar,” April 16, 2026.

III. Constraints on Digital Rights Groups Across Egypt, Iraq and Tunisia

A. Mental Health Struggles

Several interviewees described their struggles with mental health due to targeting by the government and absorbing second-hand trauma.

Aiman, an Iraqi digital rights expert, said the difficult legal landscape, personal security risks, and critical lack of resources while doing digital rights work in Iraq forces him to self-censor to avoid targeting by the government, causing a “psychological crisis” (*azmah nafsia*).³¹⁵

Amr, an Egyptian digital rights expert, described the kinds of cases he works on, including cases involving human trafficking and women driven to self-harm or suicide due to blackmail by anonymous Facebook profiles. When asked by the SMEX researcher what he thinks digital rights organizations should prioritize when supporting survivors of these abuses, the expert paused. He said, “I really don’t know what to tell you honestly. It’s all very depressing, and I don’t know how to deal with it...have I depressed you too yet?”³¹⁶

Daria, a Kurdish OGBV expert, echoed similar sentiment about digital violence cases involving women. She said: “It’s not easy to fight these things. Mentally and physically, it’s really difficult [for staff].”³¹⁷ She emphasized that survivors need better mental health resources too. “I think women [survivors] need more mental health support so they can know how to deal with this kind of hate, and the emotions that come with this experience, this new kind of violence.”

Some interviewees organize psychosocial support for their colleagues in the field, including consultations with licensed psychiatrists and mental health professionals.³¹⁸ Still, Hassan says, it’s not enough support. “Our funders and donors need to find creative methods to take care of our mental health and wellbeing.”³¹⁹

Hassan continued: the “mental burnout and mental health impact” of government repression on digital rights civil society “is huge.”³²⁰

Yet he ended on a positive note. “Even in our darkest moments, we have hope. We believe we are stronger than them. We have survived police kidnappings, traumas, arrests, but we are still here.”

³¹⁵ SMEX phone interview with “Aiman,” May 22, 2026.

³¹⁶ SMEX phone interview with “Amr,” June 8, 2026.

³¹⁷ SMEX phone interview with “Daria,” June 3, 2026.

³¹⁸ SMEX phone interview with “Yasir,” June 9, 2026; SMEX phone interview with “Amr,” June 8, 2026.

³¹⁹ SMEX phone interview with “Hassan,” April 17, 2026.

³²⁰ SMEX phone interview with “Hassan,” April 17, 2026.



B. Weak Institutionalization of Digital Security Practices

Interviewees repeatedly described a paradox in the digital rights field: that the people most familiar with surveillance, hacking, device seizures, and digital harassment often maintain inconsistent digital hygiene practices themselves.

The problem was most acute in interviews about Iraq. Several interviewees said that digital security is still not treated as a routine part of civil society work. Aiman, an Iraqi digital rights expert, said there is “no culture of digital security awareness in Iraq – not among the public, civil society, or the government.”³²¹ Yasir, the Kurdish journalist and fact-checker, estimated that “95 percent of journalists in Iraq don’t have a good idea of digital safety,” including basic tools like password managers.³²²

The interviews suggest that this gap is due in part to weak institutionalization of digital safety practices. Smaller NGOs, media outlets, and civil society groups often do not have the internal expertise, policies, or resources to train staff on digital security. Yasir said that larger media channels may have some awareness of these issues, but smaller outlets and civil society organizations often do not provide staff with proper training before sending them into risky reporting environments. As he put it, organizations often “just want to cover as much as they can” without developing procedures for covering investigations safely or preparing staff for worst-case scenarios.³²³

This reflects a broader problem – that digital safety is still often treated as a workshop topic rather than an organizational practice. Several interviewees said that staff may attend digital security trainings, but the lessons do not necessarily translate into sustained behavioral change. Yasir, drawing on his experience organizing digital trainings for civil society actors, said some participants were motivated less by the substance of the training than by the opportunity to travel, network, or take part in a funded activity.³²⁴ That does not mean digital security trainings are useless. Rather, it shows why one-off trainings are insufficient unless they are paired with institutional policies, staff accountability, follow-up audits, and clear procedures for high-risk work.

SMEX’s interviews also suggest that the problem should not be reduced to whether activists “care” enough about their digital hygiene. In many cases, the issue is that people do not perceive the threat as immediate enough to justify changing their routines.

³²¹ SMEX phone interview with “Aiman,” May 22, 2026.

³²² SMEX phone interview with “Yasir,” June 9, 2026.

³²³ SMEX phone interview with “Yasir,” June 9, 2026.

³²⁴ SMEX phone interview with “Yasir,” June 9, 2026.



Digital threats can feel abstract, even in environments where surveillance is widespread. This is especially true when activists and journalists are already dealing with urgent legal, political, financial, and personal threats.

A regional digital rights expert connected this discrepancy to the mental health struggles described earlier.³²⁵ Chronic exposure to state repression, threats, harassment, and second-hand trauma can affect activists' ability to assess risk and take protective action, the expert said. Medical literature recognizes that exposure to trauma and PTSD shape decision-making and threat appraisal.³²⁶ In a region where surveillance is already normalized, it can be difficult to persuade people that privacy is something they should care about or have a right to demand. That dynamic is intensified by trauma, which can change how people analyze risk. Abstract digital threats can be harder to visualize than the immediate repression activists and survivors are already facing.

This helps explain why digital hygiene practices may remain inconsistent, even among people who understand the risks.

In 2023, UNAMI and INSM launched a digital training program for human rights defenders, activists, journalists, bloggers, and lawyers. Before the program began, INSM conducted a "wellness check" of 25 civil society organizations and found that 70 percent were at "high risk" because of their poor digital practices.³²⁷ A separate 2023 study by OpenArchive and INSM similarly found that Iraqi human rights defenders commonly face hacking and surveillance threats by external actors despite having outdated devices and poor storage practices for the sensitive research material they collect.³²⁸

Interviewees described similar problems in Egypt. Amr conducts digital audits for organizations and said he had seen things that "made me want to rip my eyes out, I was so shocked."³²⁹ He described serious lapses in how civil society organizations and staff protected sensitive information, even when they understood the risks of state repression.

The Baghdad Women's Association (BWA) experienced a hacking incident in 2024 that required a professional digital audit and serious investment in its digital security practices.³³⁰ A hacker impersonated Liza Hido, BWA's director, and intercepted incoming email that could have alerted staff to the attack. After the

³²⁵ SMEX interview with Dia Kayyali, June 15, 2026.

³²⁶ Porcelli AJ, Delgado MR, "Stress and Decision Making: Effects on Valuation, Learning, and Risk-taking," PMCID: PMC5201132, <https://pubmed.ncbi.nlm.nih.gov/28044144/>; Starcke K, Brand M, "Effects of stress on decisions under uncertainty: A meta-analysis," PMID: 27213236, <https://pubmed.ncbi.nlm.nih.gov/27213236/>.

³²⁷ UN, "Mapping and addressing threats to civic space online," June 20, 2023, <https://www.ohchr.org/en/stories/2023/06/mapping-and-addressing-threats-civic-space-online>.

³²⁸ INSM, "Memo from Baghdad: Identifying and Addressing the Needs of Iraqi Documenters," May 11, 2023, <https://insm-iq.org/en/?p=918>.

³²⁹ SMEX phone interview with "Amr," June 8, 2026.

³³⁰ SecDev Foundation, "Patchwork To Pathways: Learning to Support Iraqi Women Facing Digital Violence," February 3, 2026, <https://secdev-foundation.org/dvaw-support-bwa-2026/>.



incident and with support from SecDev Foundation (which also supports Salam@), BWA immediately introduced new safety measures alongside digital security improvements that all staff are held to.³³¹ BWA's response illustrates what stronger digital hygiene practices look like when they are made an institutional priority.

To this point, Amr emphasized that digital security cannot be treated as a one-time thing for individuals and organizations. He recommended regular digital security audits every three years, unless an exceptional circumstance necessitates it sooner.³³² He also noted that organizations may receive donor funding to conduct audits without sufficient accountability to ensure that recommended practices are actually implemented over time by all staff. Without accountability measures, digital security remains dependent on individual habits rather than organizational systems.

C. Low Public Trust Undermining Efficacy

Several individuals said that the efficacy of their work and their services relies heavily if not solely on trust networks and word of mouth. This becomes more challenging, however, when the perception of digital rights organizations is so poor among the general public. In environments where public trust in civil society has weakened – as they have in Egypt, Iraq, and Tunisia – digital rights groups must spend significant time proving their legitimacy before they can begin the work itself.

Nissaf, a human rights advocate, described this as part of a broader crisis of legitimacy facing the human rights sector. “That legitimacy that we once had as a CSO, I feel it might be diminishing,” she said.³³³ It keeps many groups from speaking out publicly about government targeting because “it’s hard to garner sympathy.” She linked this decline not only to domestic political pressures, but also to the wider erosion of faith in human rights advocacy. She said the war in Palestine and the double standards it exposed have made the human rights landscape more difficult, because many people “don’t really believe in CSOs, their effectiveness, [or] their ability to influence change.”

In this context, digital rights organizations face a double challenge in that they must respond to immediate harms while also persuading communities that their interventions matter.

Interviewees in Iraq described similar pressures after the “anti-gender” campaign portrayed civil society organizations, especially gender and women’s rights groups, as suspicious or foreign. Daria, the Kurdish OGBV expert, responded by

³³¹ SecDev Foundation, “Patchwork To Pathways: Learning to Support Iraqi Women Facing Digital Violence,” February 3, 2026, <https://secdev-foundation.org/dvaw-support-bwa-2026/>.

³³² SMEX phone interview with “Amr,” June 8, 2026.

³³³ SMEX phone interview with “Nissaf,” June 5, 2026.



taking time to explain its work to stakeholders and the public.³³⁴ Existing government partners understood the organization's mandate, but in areas where her organization had less established relationships, staff provided local officials with documentation proving what they did, that they worked with government approval, and that they complied with relevant rules and regulations. Daria's organization also increased coordination with other CSOs so they could identify shared challenges and develop a collective response.

Trust also shapes whether organizations feel safe enough to request digital security support. Amr said that, to build his client network of audited organizations, he started by reaching out proactively to a small group of rights organizations in Egypt.³³⁵ Once he established trust with the smaller group, his work then expanded through referrals from these organizations. Now, organizations reach out to him proactively, though unfortunately often only after experiencing serious incidents such as hacks or asset freezes.

Tarek, an Egyptian digital rights and AI expert builds his clientele largely via the snowball method, too, to protect the identity of the participants and practitioners in his AI workshops.³³⁶

Fact-checking also demonstrates how public trust impacts digital rights organizations' work. As discussed earlier, a Kurdish journalist noted that people overwhelmingly trust Tech4Peace's corrections but would not trust him if he did the same on his own personal page because he is not as recognizable to them.

Across these examples, low public trust emerges as a structural constraint on digital rights work. Digital rights organizations therefore cannot treat trust-building as secondary to their technical work. In many cases, trust-building is the condition that makes the technical work possible.

D. Struggles with Regional Coordination

Interviewees repeatedly described regional coordination among digital rights organizations and allied civil society groups as "fragmented" and underresourced. Across interviews, the problem that emerged is that organizations lack a durable SWANA-based structure through which they can regularly compare threats, develop shared advocacy strategies, and coordinate responses that reflect the region's specific political realities.

Hassan, an Egyptian digital rights expert, framed this fragmentation as both a coordination and resilience challenge for digital rights organizations. As Egypt's

³³⁴ SMEX phone interview with "Daria," June 3, 2026.

³³⁵ SMEX phone interview with "Amr," June 8, 2026.

³³⁶ SMEX phone interview with "Tarek," May 22, 2026.

civic space continues to shrink, he asked: “How can we exist efficiently and effectively without having to give up on our work?”³³⁷

Hassan said Egyptian civil society’s rapid decline makes “south to south” coordination and ideas exchanges more urgent and simultaneously more difficult. Yet existing convening spaces often fail to meet that need. “We either meet at European events, but half of us isn’t able to go,” he continued. “These [events] are often too global to address our specific region.” A representative from another regional digital rights group, Saleh, similarly pointed to the lack of appropriate regional convening spaces. He noted that major journalism and media conferences exist in Latin America and Southeast Asia where “global players and media stakeholders” regularly gather. By contrast, Saleh said comparable events are rarely hosted in SWANA, and existing ones like the Arab Reporters for Investigative Journalism (ARIJ) do not necessarily fill the gap. “Our major journalism conference is in Jordan, but what are you going to say about human rights there?”³³⁸ Smaller gatherings, such as Nawaat Festival in Tunisia, provide important but limited spaces for exchange.³³⁹

A cautioning against flattening regional experience came through clearly in Iraq as well. Daria, the Kurdish OGBV expert, said that even within a single country – such as Iraq – organizations can face strikingly different obstacles. Her workplace collaborates with a collective of 45 organizations across Iraq, and she said their internal discussions showed that “each group has a unique and different set of challenges as if we are all operating in a different environment, honestly.”³⁴⁰

As such, organizations need more collective infrastructure, but effective coordination cannot rely on a single template. It has to create space for groups to identify common patterns without erasing the local legal, political, linguistic, and security conditions that shape their work.

Where coordination does happen, it often depends on whichever organization has the capacity to take the lead. Nissaf, a Tunisian civil society representative described efforts around amending Decree-Law 54 as an example of this ad hoc model.³⁴¹ The initiative brought together national and international groups. They focused on a “small wins” strategy and narrowed their demands from a broader overhaul of the law to just the removal of article 24. Not everyone agreed with that approach, she said, but the discussions themselves showed how coordination currently works. “Usually one organization takes initiative and calls the others up,” Nissaf explained. From there, coordination may happen in person, over email, Signal, or WhatsApp.

³³⁷ SMEX phone interview with “Hassan,” April 17, 2026.

³³⁸ SMEX phone interview with “Saleh,” June 25, 2026.

³³⁹ Moussa Archerchour, “Nawaat Festival : Trois jours de résistance artistique, d’amour et de liberté,” Nawaat, October 8, 2025, <https://nawaat.org/2025/10/08/nawaat-festival-trois-jours-de-resistance-artistique-damour-et-de-liberte/>.

³⁴⁰ SMEX phone interview with “Daria,” June 3, 2026.

³⁴¹ SMEX phone interview with “Nissaf,” June 5, 2026.



Nissaf emphasized that this fragmentation reflects the pressure organizations themselves face. “It can be exhausting,” she said. For many organizations, the same conditions that make coordination necessary also make it difficult to sustain.

Taken together, the interviews suggest that SWANA digital rights groups do not need coordination for its own sake. They need accessible, regionally grounded spaces where organizations can identify shared patterns of digital repression and develop collective responses without overlooking the different legal, political, linguistic, and security conditions they face across and within countries.

E. Challenges in Fundraising

Global Funding Squeeze

Funding is one of the most immediate constraints on digital rights work across Egypt, Iraq, and Tunisia.³⁴² Authorities in all three countries place restrictions on civil society organizations’ ability to fundraise.³⁴³ These pressures exist alongside a wider global contraction in funding, sharply intensified when the US Trump administration terminated 85 percent of its USAID programs in March 2025 and a slew of foreign-assistance State Department grants.³⁴⁴ Remaining available grants tend to reflect donor priorities, leaving digital rights organizations with little flexibility to respond to urgent local needs.³⁴⁵

Omar, an Iraqi digital rights activist, said scarce funding keeps organizations in “survival mode,” leaving them with little time or staff to build regional networks or pursue long-term strategies.³⁴⁶ He also criticized a system that directs much of

³⁴² Winthrop Rodgers, “US Foreign Aid Cuts Hobble Independent Media in Iraqi Kurdistan,” Inkstick Media, March 20, 2025,

<https://inkstickmedia.com/us-foreign-aid-cuts-hobble-independent-media-in-iraqi-kurdistan/>.

³⁴³ Mia Crochot, Maharat Foundation, “Media Viability Best: Practices in The MENA Region,” March 13, 2025, <https://maharatfoundation.org/media/2939/media-viability-report-2025-final.pdf>; USAID, “2020 Civil Society Organization Sustainability Index For the Middle East and North Africa,” October 2021, <https://www.fhi360.org/wp-content/uploads/drupal/documents/csosi-mena-2020-report.pdf>; Digital Democracy Initiative, “Strengthening Support Ecosystems for Digital Democracy in Egypt: A Case Study Assessment Report,” March 2025,

https://www.civicus.org/documents/ddi/ddi_case-study-report_egypt.pdf.

³⁴⁴ OECD, “Cuts in official development assistance,” June 26, 2025,

https://www.oecd.org/en/publications/cuts-in-official-development-assistance_8c530629-en/full-report.html; OECD, “A historic decline in foreign aid: Preliminary 2025 ODA data,” April 9, 2026,

<https://www.oecd.org/en/data/insights/data-explainers/2026/04/a-historic-decline-in-foreign-aid-preliminary-2025-oda-data.html>; Oxfam, “What USAID did, and the effects of Trump’s cuts on lifesaving aid,” January 27, 2026,

<https://www.oxfamamerica.org/explore/issues/making-foreign-aid-work/what-do-trumps-proposed-foreign-aid-cuts-mean/>.

³⁴⁵ CIVICUS, “2025 State of Civil Society Report,” March 2025,

https://www.civicus.org/documents/reports-and-publications/SOCS/2025/state-of-civil-society-report-2025_en.pdf.

³⁴⁶ SMEX phone interview with “Omar,” April 16, 2026.



the available funding through Global North organizations rather than directly to groups in the region, a widely documented dynamic.³⁴⁷

Diyar, a Kurdish human rights expert, said his organization had operated three programs related to protecting freedom of assembly in Iraq as well as a community center providing pro-bono legal support for refugees before the USAID cuts. The center employed almost 30 social workers and lawyers and handled more than 200 cases within its first month, January 2025. Just three months later, in March, the organization learned that it needed to shut down by June. “In one day, everything was cut...We had to fire everyone,” he said.³⁴⁸ The loss was especially damaging because the clinic filled a critical service gap for a highly vulnerable group in Iraq.³⁴⁹

Nissaf, a Tunisian human rights advocate, said her organization lost projects that it expected to sustain its work for the next two to three years.³⁵⁰ Some of the funding had already been incorporated into budgets for ongoing projects, forcing the organization to seek replacement support. These cuts also affect smaller organizations that rely on larger organizations for financial support.³⁵¹ This makes collaboration harder and reduces their capacity to produce joint research.

European funders have since begun to fill some of the support lost through the USAID and State Department cuts, but interviewees said that the available support is often smaller, more restrictive, and accompanied by less technical assistance. For some organizations, this shift has meant losing not only funding but also control over the direction of their work. Diyar said US grants had given his organization greater freedom to design programs around locally identified needs. European grants, by contrast, often prescribe narrow projects that fall outside the organization’s most urgent priorities. His organization has accepted some of this funding because it has few alternatives.³⁵²

The funding landscape generally overlooks other topics that digital rights organizations and experts consider urgent, such as child safety measures.³⁵³ These gaps affect the basic infrastructure of digital rights work. Yasir, a Kurdish journalist and independent fact-checker, said the broader funding squeeze has weakened Kurdish-language fact-checking.³⁵⁴ Unlike the more established Arabic-language

³⁴⁷ #ShiftThePower, “Too Southern to be Funded: The Funding Bias Against the Global South,” May 2024, <https://drive.google.com/file/d/1F4rH1v7YAU1sds1Z1XF3btAIRRtFijeo/view>; OECD, “Foreign aid surges due to spending on refugees and aid for Ukraine,” April 12, 2023, <https://www.oecd.org/en/about/news/press-releases/2023/04/foreign-aid-surges-due-to-spending-on-refugees-and-aid-for-ukraine.html>.

³⁴⁸ SMEX phone interview with “Diyar,” May 9, 2026.

³⁴⁹ INTERSOS, “Iraq: Providing legal assistance for the most vulnerable,” February 25, 2026, <https://www.intersos.org/en/iraq-providing-legal-protection-for-the-most-vulnerable/>.

³⁵⁰ SMEX phone interview with “Nissaf,” June 5, 2026.

³⁵¹ SMEX phone interview with “Nissaf,” June 5, 2026.

³⁵² SMEX phone interview with “Diyar,” May 9, 2026.

³⁵³ SMEX phone interview with “Tarek,” May 22, 2026; SMEX phone interview with “Laila,” May 22, 2026.

³⁵⁴ SMEX phone interview with “Yasir,” June 9, 2026.

ecosystem, Kurdish initiatives have fewer resources to hire staff, engage consistently with users, and build their reputations. Without sustained investment, organizations struggle to establish the public trust needed to challenge misinformation.

Funding constraints also intersect with a broader economy of digital exploitation. Yasir described how peer journalists and content creators who had once worked on NGO-funded peacebuilding and media projects became vulnerable to political and militia-linked patronage after those funds disappeared. “He changed his skin completely,” he said of a peer journalist who began posting increasingly violent political messaging after his ability to find work dried up. “But I know he makes so much more money doing this than the NGO work he used to do.”³⁵⁵

His account illustrates a broader consequence of the funding squeeze. When civil society and independent media cannot provide stable employment, political actors with greater resources gain more power to shape the information environment. Funding cuts do not only reduce the number of projects organizations can undertake. They can also weaken independent voices while making inflammatory, partisan, or abusive content more financially attractive.

Organizations Struggle to Fundraise for Themselves and Funder Affiliations Put Them at Risk

Digital rights organizations in Egypt, Iraq, and Tunisia struggle to fundraise for themselves because visibility can create risks for harassment and smear campaigns from the government and general public.

In Egypt, restrictive NGO laws and security scrutiny limit how organizations can receive and report funding, while broader pressure from “police, army, and the state” constrains their operating space.³⁵⁶ Comparable constraints exist in Tunisia and Iraq, although they take different forms. Tunisian authorities have increasingly used allegations surrounding foreign funding to subject civil society groups to financial investigations, bank-account freezes, and suspensions, while Iraqi organizations face mandatory financial reporting requirements and practical obstacles to opening bank accounts and receiving funds from abroad.³⁵⁷

However, as Daria, a Kurdish OBGV expert, noted, the need to keep a low profile online can create tension with funders who equate visibility with credibility,

³⁵⁵ SMEX phone interview with “Yasir,” June 9, 2026.

³⁵⁶ SMEX phone interview with “Hassan,” April 17, 2026; Human Rights Watch, “Q&A: Legal Framework and Environment for Nongovernmental Groups (NGOs) in Egypt,” July 15, 2021, <https://www.hrw.org/news/2021/07/15/ga-legal-framework-and-environment-nongovernmental-groups-ngos-egypt>.

³⁵⁷ Amnesty International, May 11, 2026, “Tunisia: Dozens of NGOs at risk of dissolution as crackdown on civil society intensifies,” <https://www.amnesty.org/en/latest/news/2026/05/tunisia-dozens-of-ngos-at-risk-of-dissolution-as-crackdown-on-civil-society-intensifies/>; International Center For Not-For-Profit Law, “Civic Freedom Monitor: Iraq,” n.d., <https://www.icnl.org/resources/civic-freedom-monitor/iraq>.

impact, or institutional seriousness.³⁵⁸ For digital rights groups, this creates a difficult situation because the safer they are, the less fundable they appear.

In some cases, the visibility of donor relationships can be weaponized against civil society groups. Kohl Journal detailed the smear campaigns Iraqi women's rights organizations faced at the height of the "anti-gender campaign" after a Telegram channel leaked their financial statements and revealed entities based in the Global North on their statements.³⁵⁹

One rights activist said restrictions on foreign funding pose a more immediate threat than cybercrime laws because they can prevent organizations from paying staff, maintaining offices, and continuing their work.³⁶⁰ Although dependence on grants is not sustainable, many groups have few alternative sources of funding.

Funding as a Moral and Political Choice

Interviewees described facing a moral and political dilemma about receiving money from the same governments that maintain security partnerships, migration-control deals, arms sales, or surveillance export regimes with the states repressing them.

Saleh, a regional digital rights activist, described this as a "structural issue" in the region. He said that independent media and civil society groups may receive European funding for human rights work, only to see European or other "Western" governments later redirect money, attention, or commercial relationships toward the very governments and security sectors that undermine those rights. Yet Saleh also noted that governments from outside the region remain important advocacy targets precisely because they always have a choice to make about whether to continue or condition this support, and political alliances can change. "I probably cannot force the UAE not to use spyware," he said, "but I can try to force the UK to not allow the export of those technologies."³⁶¹

Hassan, an Egyptian digital rights expert, argued that President Abdel Fattah al-Sisi has maintained international support in part because European governments prioritize migration containment and security cooperation over human rights concerns. European institutions may finance civil society initiatives, he said, while simultaneously providing the Egyptian government with large grants and supporting the transfer of surveillance and security technologies that strengthen its repressive capacity.³⁶²

³⁵⁸ SMEX phone interview with "Daria," June 3, 2026.

³⁵⁹ Manal Hameed, Kohl Journal, "The Spectre of Feminism in Post-October Iraq: on Political Absence and the Paralysis of Organising," Vol. 11 No. 2, Fall 2025, <https://kohljournal.press/spectre-feminism-post-october-iraq>.

³⁶⁰ SMEX phone interview with "Saleh," June 25, 2026.

³⁶¹ SMEX phone interview with "Saleh," June 25, 2026.

³⁶² SMEX phone interview with "Hassan," April 17, 2026.



Saleh described a similar cycle across the region. European donors may fund independent media through projects framed around human rights, only to later prioritize gas agreements or arms sales with regional governments.³⁶³

These contradictions have pushed some organizations to treat fundraising itself as an expression of political solidarity. Saleh said he knows of many organizations across the SWANA region who returned donor money “in response to those governments’ positions on Palestine.”³⁶⁴ Hassan also described how his own organization returned a European government’s funding after concluding that the funder’s’ positions no longer aligned with the organization’s own moral and social compass. “The past couple of years have forced us to be more aware about who we take our money from. We have to honor our people and our partners because we are part of a wider human rights movement... we have to practice solidarity.”³⁶⁵

³⁶³ SMEX phone interview with “Saleh,” June 25, 2026.

³⁶⁴ SMEX phone interview with “Saleh,” June 25, 2026.

³⁶⁵ SMEX phone interview with “Hassan,” April 17, 2026.



IV. Recommendations

To All Rights and Civil Society Organizations

Regarding digital and physical safety practices for staff members

- Ensure digital hygiene practices among staff are up to date. Develop or refresh digital hygiene policies and make training mandatory for all current management, employees, and new hires.
- Treat digital security as a core organizational responsibility rather than an optional or purely technical practice.
- Develop clear policies related to safe travel practices and ensure any staff member who travels on behalf of the organization complies with these policies.
- Develop security policies that govern internal communications that prioritize the safety and security of colleagues. Ensure personal devices aren't used for organizational work, standardize VPN usage, require communication take place only over encrypted platforms, and oblige staff to utilize password managers and two-factor authentication whenever possible.
- Establish clear internal procedures for reporting suspected security incidents and conduct a review after each significant incident to identify necessary changes.
- Conduct holistic digital audits of your internal and external digital and physical security practices at least every 3-5 years.
- Include psychosocial support and recovery planning in organizational responses to arrests, threats, hacking, doxxing, smear campaigns, and other serious security incidents.
- Conduct risk assessments before beginning projects involving politically sensitive subjects or vulnerable populations, including women and girls, LGBTQ+ people, migrants and refugees, journalists, and people documenting abuses by security forces or armed groups.
- Review the names, photographs, office addresses, staff biographies, partner information, and other identifying details published on websites and social media accounts. Obtain informed consent and conduct a security assessment before publicly disclosing this kind of information.
- Develop internal policies that clearly govern staff use of AI and generative AI to minimize the sharing of sensitive information.
- Invest in training for staff about AI including how to better identify it in visual and written content to improve fact-checking practices.



Regarding improving social media platform responsiveness to abusive, non-English online content

- Develop a localized glossary of terms and phrases in Arabic, Kurdish, and other relevant languages (including for specific dialects) that are racist, sexist, and abusive. Continuously monitor social media trends to ensure this glossary is responsive to current times. Share these lists with social media platforms and other digital rights groups in the SWANA region periodically and advocate that they are referenced by platforms' content regulators.

Regarding addressing gaps in research

- Invest in research that focuses on the exploitation of children online.
- Invest in research that investigates abuses on less-regulated platforms such as on Telegram and online neighborhood bulletins.

Regarding improving regional coordination within the SWANA region

- Create regional coalitions that connect digital rights work with gender justice, labor rights, migrant rights, media freedom, and anti-corruption advocacy.

Regarding digital rights initiatives

- Normalize digital and physical security and media literacy for the general public through multi-faceted campaigns and education initiatives that meet people where they are.
- Consistently engage in public outreach initiatives and develop relationships with local communities, such as in schools, community and recreation centers, libraries, and similar spaces to improve trust and expand awareness of digital safety, the importance of fact-checking, and of your services.
- Establish secure referral networks connecting survivors of online violence with digital security specialists, lawyers, mental health professionals, shelters, emergency protection services, and trusted government bodies where engagement does not expose the survivor to further harm.

To Donors Who Fund Digital Civil Society Organizations and Initiatives

- Fund sustained SWANA-wide networking and learning spaces that help civil society actors identify shared digital governance challenges and coordinate regional responses.
- Prioritize funding digital security audits for the organizations you support to ensure they can carry out their activities safely without fear of surveillance.



- Develop sustainability measures to ensure the longevity of digital security practices beyond the time period immediately following training.
- Conduct a review of current programs funded and evaluate them with an eye for identifying groups or language support gaps (i.e allocating resources towards minority language fact-checking programs such as in Kurdish).
- Permit organizations to reallocate funds when political conditions, security threats, government crackdowns, or community needs change during the grant period.
- Conduct audits of your own digital security practices and ensure they are implemented when speaking with members of digital society organizations and especially with groups who work with marginalized, at-risk populations.
- Invest in capacity building and technical training for all the people who are directly in touch with survivors of digital violence, especially for emergency and frontline responders.
- Prioritize mental health funding for civil society workers who regularly document abuse to improve their access to confidential and culturally appropriate mental health services, adequate leave, and opportunities to rotate out of high-intensity casework.
- Assess the legal, reputational, and security risks of publicly disclosing donor relationships and agree with partners in advance on whether and how the relationship will be publicized.
- Permit organizations to conduct low-profile, anonymous, or indirectly attributed work when publicity would expose staff members, partners, survivors, or beneficiaries to retaliation.
- Allow grantees to remove donor names and logos from public materials where disclosure could trigger legal action, financial investigations, smear campaigns, or physical threats.

To Social Media Companies

Meta (Instagram, Facebook, WhatsApp), TikTok, X, and YouTube

- Invest in resources to improve the labelling of uploaded AI content and ensure these labels are clear for all users.
- Invest in language-specific fact-checking and content regulation initiatives, especially for minority languages. Partner with local NGOs to do this.
- Prioritize hiring staff with specific language expertise, especially in Kurdish (Latin and Arabic script), to review content.
- Improve filtration systems to prevent the spread of non-consensual pornographic material.
- Partner with local digital rights organizations and journalists as independent third parties to act as fact-checkers for posted content.



- Improve communication with and responsiveness to requests from helpdesks supporting human rights defenders.

Telegram

- Create a clear channel for users and digital rights organizations to flag content that includes sexual exploitation and harassment of women and girls, especially in the Iraqi context.
- Work with digital rights organizations to develop a reference list of abusive words and phrases that are localized for different Arabic language dialects as well as Kurmanji and Sorani Kurdish.
- Improve filtration systems to prevent the spread of non-consensual pornographic material.

To the Government of Egypt

Regarding the 2018 Law on Combating Information Technology Crimes and the Criminalization of Online Expression

- Amend Law No. 175 of 2018 on Combating Information Technology Crimes to repeal or narrowly define provisions criminalizing content that allegedly violates “family principles or values,” “incites debauchery,” or threatens broadly defined concepts of national security or public order.
- Ensure that the Cybercrime Law does not criminalize peaceful criticism, journalism, human rights advocacy, artistic expression, discussion of gender or sexuality, or other expression protected under international human rights law.
- Review all criminal cases brought under the Cybercrime Law against people solely for peaceful online expression; drop the charges, quash resulting convictions, release anyone detained on this basis, and remove associated restrictions, including travel bans and asset freezes.
- Amend the law’s website-blocking provisions to require a prior order from an independent court. Any blocking order should identify the specific unlawful content, explain why blocking the entire website is necessary and proportionate, remain limited in duration and scope, and provide the affected party with notice and a meaningful right of appeal.
- Unblock independent media, civil society, and human rights websites unless the government can demonstrate before an independent court that restricting access satisfies the requirements of legality, necessity, and proportionality under Article 20 of the International Covenant on Civil and Political Rights (ICCPR).

Regarding the 2018 Press, Media, and Supreme Council for Media Regulation Law and the Supreme Council for Media Regulation



- Amend the 2018 Press, Media, and Supreme Council for Media Regulation Law to remove the designation of personal websites, blogs, and social media accounts with 5,000 or more followers as “media outlets.”
- Remove the SCMR’s authority to block websites, suspend publications, or impose penalties without prior authorization from an independent court.
- Establish transparent, merit-based procedures for appointing SCMR members and guarantee the council’s institutional, administrative, and financial independence from the presidency, security agencies, and government-controlled media bodies.
- Require the SCMR to publish regular reports identifying all content-removal, website-blocking, account-restriction, licensing, and sanctioning decisions, as well as the legal basis for each decision, the requesting authority, and the outcome of any appeal.
- Establish an accessible and independent appeals mechanism through which individuals, media organizations, and civil society groups can challenge SCMR decisions, including decisions involving blocking, licensing, fines, or alleged abuse of authority.
- Prohibit the SCMR from imposing sanctions based on vague concepts of morality, family values, or national unity that can be used to suppress protected expression.

Regarding the NGO Law and Restrictions on NGO Funding

- Amend Law No. 149 of 2019 to establish a notification-based system for the formation and registration of civil society organizations rather than requiring advance government authorization.
- Repeal provisions that require civil society organizations to obtain government approval before conducting field research, surveys, public-interest studies, partnerships, or other ordinary organizational activities.
- Permit organizations to seek, receive, and use domestic and foreign funding without prior government approval, subject only to transparent financial-reporting requirements that are necessary, proportionate, and equally applied to all organizations.
- Permit the suspension or dissolution of an organization only through a final order issued by an independent court, based on clear evidence of serious unlawful conduct, after the organization has received notice and an opportunity to respond.
- End the use of criminal investigations and administrative punishments such as asset freezes, travel bans, office raids, and long-running legal cases to punish organizations or staff members for legitimate human rights work or lawful international cooperation.
- Review and lift arbitrary travel bans and asset freezes imposed on civil society workers and lawyers, close politically motivated investigations, and return organizational property seized without a lawful basis.



Regarding Telecommunications, Surveillance, and Device Searches

- Amend the Telecommunications Law to expressly protect the use of virtual private networks, end-to-end encryption, and encrypted messaging applications for lawful purposes.
- Require security agencies and other government bodies to obtain an individualized judicial warrant before intercepting communications, accessing user information, searching a digital device, or compelling a telecommunications company to disclose data.
- Prohibit police, military, intelligence, and security personnel from compelling people to unlock or surrender their phones at checkpoints or during street stops without a judicial warrant and a lawful basis for the search.
- Exclude information obtained through an unlawful device search from criminal proceedings and establish disciplinary and criminal accountability for officials who conduct coercive or unauthorized searches.
- Require the National Telecom Regulatory Authority and all telecommunications providers to publish regular transparency reports detailing government requests for user information, surveillance assistance, content restrictions, service disruptions, and geoblocking.
- Publish the legal and contractual frameworks governing state access to telecommunications infrastructure and establish independent oversight of surveillance procurement and deployment.
- Conduct transparent human rights assessments before acquiring or deploying surveillance technology and prohibit its use against journalists, lawyers, human rights defenders, political opponents, and peaceful civil society organizations.

To the Federal Government of Iraq and the Kurdistan Regional Government

Regarding Pending Cybercrime Legislation and Online Expression

- Refrain from adopting any cybercrime bill containing vague or overbroad restrictions based on morality, governmental interests, religious interests, national security, social stability, public order, or similar concepts that could criminalize peaceful expression.
- Publish the full text of any proposed cybercrime legislation and provide sufficient time for meaningful public consultation with digital rights organizations, journalists, lawyers, women's rights groups, minority-language communities, technical experts, and organizations representing survivors of online violence.
- Limit criminal cybercrime offenses to clearly defined conduct involving demonstrable harm and wrongful intent, such as identity theft, doxxing, and the non-consensual distribution of private material.



- Ensure that penalties are proportionate to the harm caused and that no person faces imprisonment merely for criticizing public officials, institutions, political parties, religious authorities, or armed groups.
- Review the penal code, counterterrorism laws, and telecommunications laws to repeal or narrowly amend provisions concerning insults, false information, immorality, national unity, and national security that authorities use against protected expression.
- In the Kurdistan Region, ensure that Press Law No. 35 of 2007 governs journalism and publication-related cases and end the practice of using harsher penal code, counterterrorism, or telecommunications provisions against journalists for their professional work.

Regarding Online Violence Against Women and Girls

- Enact survivor-centered legislation that clearly defines and penalizes digital blackmail, doxxing, stalking, threats, non-consensual distribution of private images, and malicious AI-generated sexualized content.
- Ensure that the legislation protects survivors' confidentiality, prohibits officials from blaming or prosecuting them for the underlying images or communications, and allows them to seek remedies without notifying family members or other people who could place them at risk.
- Establish confidential, accessible reporting channels staffed by personnel trained in online gender-based violence, digital evidence, trauma-informed interviewing, and the risks survivors may face from family, community, political, or armed actors.
- Provide survivors with timely access to legal assistance, psychosocial support, emergency protection, digital-security assistance, and referrals to trusted civil society organizations.
- Collect and publish disaggregated data on complaints, investigations, prosecutions, case outcomes, and support provided to survivors without publishing information that could identify or endanger them.

Regarding Women's Participation During Elections

- Establish, before and during election periods, an independent rapid-response mechanism to receive and investigate threats, doxxing, blackmail, manipulated images, sexualized disinformation, and coordinated harassment targeting women candidates, campaign workers, journalists, and election observers.
- Ensure that election authorities, police, and prosecutors receive training on disinformation and the offline risks created by sexualized allegations and manipulated content.
- Publicly condemn campaigns designed to drive women out of political life and promptly investigate credible threats, including campaigns involving paid social media pages, party-affiliated actors, or armed groups.

- Publish regular, anonymized information about election-related online violence and the authorities' response, including the number of complaints received and investigations opened.
- Ensure that efforts to combat election-related abuse target threatening or deceptive conduct rather than legitimate political criticism, journalism, satire, or debate.

Regarding the Communications and Media Commission (CMC)

- Reform the appointment process for the CMC's leadership and board to protect its institutional, financial, and administrative independence from political parties, armed groups, and government officials.
- Withdraw the 2023 draft digital content regulation and refrain from adopting any comparable framework that gives the CMC general authority to monitor all online content, refer broadly defined speech to security bodies, or order pages blocked or deleted.
- Limit the CMC's content-related authority to functions clearly established by law and prohibit it from imposing criminal penalties or requesting content restrictions without an independent judicial order.
- Require the CMC to publish all requests to platforms involving content removal, account restriction, geoblocking, or user information, together with the legal basis, requesting authority, duration, and available appeal procedure.
- Establish an independent process through which users, journalists, political actors, and civil society organizations can challenge CMC licensing, sanctioning, geoblocking, and content-removal decisions.
- Include civil society organizations in substantive policy consultations, rather than limiting engagement to awareness-raising workshops or technical training.
- Suspend or substantially reform public-reporting initiatives such as Ballegh unless they operate under clear legal standards, protect against malicious or discriminatory reporting, provide notice and appeal, and exclude vague categories such as "indecent" content or threats to social stability.

Regarding Internet Shutdowns, Platform Blocking, and Access to Information

- End internet shutdowns during examinations and refrain from restricting internet access, social media platforms, messaging applications, DNS services, or information archives as a general response to cheating, data leaks, or protests.
- Ensure that any proposed restriction on a website or service has a clear basis in law, addresses a specific and demonstrable harm, is necessary and proportionate, remains limited in duration and geographic scope, and receives prior authorization from an independent court.



- Develop less intrusive responses to examination fraud, data breaches, and individual unlawful content that do not deprive the wider population of access to communications and information.

Regarding Armed Groups, Checkpoints, and Protection of Activists

- Promptly investigate militia and political party-linked online threats, doxxing, blackmail, smear campaigns, abductions, and physical attacks against journalists, women's rights activists, lawyers, and civil society workers.
- Prosecute those responsible where sufficient evidence exists, regardless of political affiliation, party membership, institutional position, or connection to armed groups.
- Establish effective protection measures for people facing credible online threats, including emergency contact points, risk assessments, relocation assistance, and coordination with trusted civil society organizations.
- Prohibit federal, Kurdish, and militia-affiliated security personnel from searching digital devices at checkpoints without a judicial warrant or lawful basis.

To the Government of Tunisia

Regarding Decree-Law 54 of 2022

- Repeal Decree-Law 54 of 2022 and replace it, following meaningful public consultation, with narrowly tailored legislation addressing genuine cybercrime rather than peaceful online expression.
- Ensure that any replacement cybercrime law clearly defines prohibited conduct, requires proof of wrongful intent and demonstrable harm, provides necessity and proportionality safeguards, and protects journalism, public-interest reporting, criticism, satire, advocacy, and political debate.
- Pending repeal, immediately suspend the application of article 24 and other provisions criminalizing "false news," rumors, or broadly defined harm to public security, national defense, or the rights of others.
- Drop charges, quash convictions, and release anyone detained solely for peaceful expression under Decree-Law 54, including journalists, lawyers, judges, artists, academics, political figures, human rights defenders, and other internet users.

Regarding Counterterrorism Legislation and Security Powers

- Amend the 2015 Counterterrorism Law to define terrorist acts narrowly and exclude peaceful political opposition, journalism, human rights advocacy, protest, and online organizing.



- End the practice of combining counterterrorism charges with Decree-Law 54, financial-crimes, or other charges to punish peaceful critics and civil society organizations.

Regarding Freedom of Association, Administrative Suspensions, and NGO Funding

- Reaffirm and fully implement Decree-Law 88 of 2011 as the principal framework governing associations, including its protections against state interference in lawful civil society activity.
- Permit civil society organizations to receive domestic and foreign funding without prior authorization, subject to transparent and proportionate reporting requirements applied without discrimination.
- End the use of foreign-funding allegations, financial-crimes investigations, money-laundering accusations, and demands for years of records as tools to punish or exhaust organizations engaged in lawful work.
- Lift administrative suspensions and unfreeze the bank accounts and assets of organizations where the authorities cannot present specific, credible evidence of a recognizable criminal offense before an independent court.
- Prohibit the suspension or dissolution of an association or independent media organization by administrative order. Any such measure should require a final judicial decision, clear evidence, prior notice, an opportunity to respond, and a right of appeal.
- Establish clear statutory deadlines for financial and administrative investigations so organizations are not subjected indefinitely to repeated summonses, document requests, or unresolved legal exposure.
- Protect Decree-Law 115 of 2011 as the principal framework for press and publication matters and refrain from prosecuting journalists under cybercrime or counterterrorism provisions for their professional work.

Regarding Official Smear Campaigns and Organizations Supporting Marginalized Communities

- End statements by senior officials that portray civil society organizations, independent media, migrant and refugee assistance groups, anti-racism organizations, women's rights groups, or LGBTQ+ rights advocates as traitors, foreign agents, corrupt intermediaries, or demographic threats.
- Publicly condemn racist, xenophobic, misogynistic, and anti-LGBTQ+ incitement and make clear that providing humanitarian assistance, legal advice, research, or advocacy does not constitute foreign interference or a criminal offense.
- Promptly investigate threats, doxxing, incitement, and coordinated online harassment against civil society workers and ensure that investigations include any potential involvement by public officials or government-aligned accounts.



- End dissolution proceedings, prosecutions, and administrative measures based solely on an organization's work with migrants, refugees, Black Tunisians, women, LGBTQ+ people, or other marginalized communities.

Regarding Lawyers and Judicial Independence

- End the arrest, prosecution, surveillance, and intimidation of lawyers for statements made in the course of their professional work or for representing government critics and human rights defenders.
- Drop charges and release lawyers detained solely for peaceful expression or legitimate professional activity.
- Guarantee lawyers confidential access to clients, case files, and places of detention and ensure they can participate in cybercrime and freedom-of-expression cases without retaliation.
- Establish transparent, objective, and reviewable procedures governing the appointment, discipline, suspension, and removal of judges and prosecutors.

To The Governments of Egypt, Tunisia, and Iraq

Regarding the Protection of Human Rights Defenders, Lawyers, and Judicial Independence

- End official and state-aligned media campaigns that portray peaceful civil society organizations, lawyers, journalists, and human rights defenders as terrorists, foreign agents, or threats to national security.
- Promptly and impartially investigate online threats, doxxing, physical assaults, unlawful surveillance, and smear campaigns against human rights defenders, including allegations that officials or state-aligned actors participated in or coordinated the abuse.
- Guarantee that lawyers can communicate confidentially with clients, litigate cybercrime and human rights cases, travel, and conduct their professional work without arrest, surveillance, asset freezes, or retaliation.
- Safeguard the independence of prosecutors and judges handling online-expression, media, and civil society cases, and prohibit security agencies or executive authorities from directing investigations or judicial outcomes.

Regarding Artificial Intelligence

- Develop, through meaningful consultation with local digital rights organizations, journalists, technologists, women's rights groups, and communities most affected by digital surveillance, legislation regulating the development and use of artificial intelligence.
- Criminalize the malicious creation or distribution of non-consensual intimate imagery and deceptive AI-generated sexualized content while



ensuring that such provisions cannot be used to prosecute lawful journalism, satire, artistic work, or peaceful political expression.

- Establish an independent data-protection authority with powers to investigate government agencies, order corrective measures, and provide remedies to affected individuals.
- Regulate AI-generated impersonation, deepfakes, and non-consensual sexualized imagery through narrowly defined harm-based provisions rather than broad prohibitions on false or immoral content.

To the Public

- Practice good digital hygiene including by using two-factor authentication on apps that require log-ins and speaking with friends and family exclusively over encrypted platforms.
- If attending a protest or a similarly sensitive event or location, be mindful of what information is stored on your phone before deciding to bring it with you.



Methodology

This report reflects interviews and written correspondence with 20 adult individuals with deep knowledge on digital and human rights in the SWANA region. Seven of those individuals focus on Iraq, six focus on Egypt, four focus on Tunisia, and three are general SWANA experts who spoke to regional trends.

Fourteen of those people represent local or international civil society organizations, six of which are exclusively focused on digital rights; one person represents a media organization; two are independent journalists; two are independent researchers; one is a lawyer.

Protection of interviewees' safety is SMEX's number one priority. For that reason, this report withholds identifying details about interviewees and uses pseudonyms unless the interviewee provided affirmative and explicit consent. Inclusion of publicly available information about specific organizations in this report does not necessarily mean that a person from that organization was interviewed.

The researcher corresponded and conducted interviews in Arabic and English between April and June 2026 remotely over encrypted platforms. Every interviewee was informed of the purpose of the interview and did not receive monetary compensation or other incentives for participating in the interview. Quotes included in this report are lightly edited for clarity and flow.

The researcher also conducted desk research to complement the interviews including by reviewing applicable laws and media regulations, news media, and other relevant data. The report builds on published research conducted by SMEX and other reputable digital rights and media organizations, cited throughout.



Acknowledgements

Asma Elgamal, research consultant for SMEX, conducted the research and wrote the report. **Zeinab Ismail**, Project Lead and Senior Policy Analyst, together with **Dia Kayyali**, Senior Policy Analyst, supervised the research and writing.

SMEX thanks the digital rights experts from Egypt, Iraq, and Tunisia who shared their experiences and continue their advocacy.

SMEX thanks the National Endowment for Democracy for financially supporting this project.

