Critical Policy Analysis | 2021-2025

On the Egyptian State's Policy of Blocking Websites

Mai Amer

March 2025

Introduction

Over the past ten years, Egyptian authorities have developed legal and technical mechanisms to block websites for the purposes of stifling political dissent, preventing the public from accessing certain information and opinions, or censoring certain types of content for religious or moral reasons. The authorities have developed and applied a range of legal strategies during this period. These include arbitrary interpretations of the telecommunications laws; conservative judicial interpretations of legal concepts such as national security; imposing censorship through exceptional legislation such as the Anti-Terrorism Law; and legalizing the permanent blocking of websites through ordinary legislation. This is the case of the Cybercrime Law, which allows websites to be blocked as part of investigative procedures, or the Law Regulating the Media and the Press, which gives the Supreme Council for Media Regulation broad powers to impose various forms of censorship as an administrative sanction against online journalism.

The development of the legislative environment to legalize website blocking has coincided with the development of blocking mechanisms, from simply relying on IP address and IP packet-blocking, or deep packet inspection-based blocking, to the use of sophisticated equipment such as Sandvine's. The authorities' interest in censoring the internet comes from a recognition of cyberspace as a new dimension of the public sphere. Activists have been able to use cyberspace as an alternative to all other spaces that were prohibited by the authorities for political, religious, or moral reasons. This decentralized nature of the internet and the difficulty of regulating online content have become a source of concern for the authorities. As a result, there is a direct correlation between the flare-up of political crises and the blocking of websites in Egypt. Website blocking is used by authorities to attack various outlets of expression, including newspapers, political parties, civil society organizations, and even peaceful anti-repression protest movements. Despite the continued effectiveness of the internet in Egyptian society, the State's censorship efforts, especially since 2017, have prevented users from accessing hundreds of journalistic, political, and cultural websites. In recent years, there has been an increase in the number

of violations faced by individuals with respect to the freedoms of information, opinion and expression, the press, and use of the internet.

A Decade of Legislative Developments Enabling the Blocking of Online Content

The Egyptian State is witnessing a pervasive crisis of freedom of opinion and expression on several levels. A number of legislations and judicial rulings in Egypt have set rules and principles related to imposing different forms of censorship of visual, audio, and written content over the years. Before 2015, there were no legal texts regulating the process of blocking websites, so the practice began with judicial jurisprudence based on existing telecommunications laws. A new anti-terrorism law issued in 2015 empowered judicial bodies to approve the blocking process through special controls. However, the exceptional nature of this law did not allow for large-scale blocking, so Egyptian authorities then began blocking online portals without legal cover or official announcements. Over time, blocking became something that users faced on a daily basis. Subsequently, the authorities issued a number of basic legislations and executive regulations governing the blocking process in 2018. The timeline of these developments is outlined in detail below.

Between 2011 and 2015, there was no legislation that explicitly addressed the possibility of blocking or clarified the authority of administrative and other law enforcement authorities to block websites. However, according to Masar's 2021 report "Website Blocking in Egypt: Tactics and Laws", Egyptian judicial authorities contributed to entrenching the practice of blocking carried out by the executive when adjudicating a petition raised by an Egyptian lawyer in 2012. The provisions of Law No. 10 of 2003 – the Telecommunications Regulation Law – require service providers to provide technical potentials, including equipment, systems, software, and communications to allow the armed forces and national security agencies to exercise their powers. It also allows these security agencies to take control of all services and networks of any service provider in the event of a natural or environmental disaster or during declared periods of general mobilization or any other cases related to national security. The law does not specify the nature of these technical potentials or the rules for their use, nor does it include a clear definition of the concept of national security. These broad and vague provisions allowed the Administrative Court to find a legal justification for blocking access to content. It did so by expanding the concept of national security to include "social national security" and emphasizing the need for its protection from possible threats. By doing so, it ended up setting a precedent that effectively required administrative authorities to take blocking measures under the Telecommunications Regulation Law.

In 2015, the Anti-Terrorism Law was issued, which for the first time regulated the process of blocking websites in Egypt. The law gave the public prosecution or the competent investigative authority the power to stop or block websites if the website was "established for the purpose of promoting ideas or beliefs calling for the perpetration of terrorist acts or broadcasting material intended to mislead security authorities, influence the course of

justice in any terrorist crime, exchange messages, issue assignments among terrorist groups or their members, or exchange information related to the actions or movements of terrorists or terrorist groups domestically and abroad." As mentioned before, this was the first law to allow blocking through a process of judicial review in exceptional cases.

Despite this, Egypt's legal environment lacked a legal cover for the practice of large-scale blocking, until August 2018 when President Abdel Fattah al-Sisi ratified Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes and Law No. 180 of 2018 on Press, Media, and the Supreme Council for Media Regulation, two laws that explicitly authorize the practice of website blocking and communications surveillance in Egypt. The enactment of these laws and their loose wording constituted a legal entitlement to judicial violations. As a result, several websites, including news and educational outlets, were blocked, media organizations were shut down, and many journalists, writers, and content creators on social media were subjected to arrest campaigns that ended with judgments being issued against them.

The two laws blatantly contradict multiple articles of the Egyptian Constitution. For instance, Article 68 of the 2014 constitution states: "Information, data, statistics and official documents are owned by the people. Disclosure thereof from various sources is a right guaranteed by the state to all citizens. The state shall provide and make them available to citizens transparently. The law shall regulate rules for obtaining such, rules of availability and confidentiality, rules for depositing and preserving such, and lodging complaints against refusals to grant access thereto. The law shall also specify penalties for withholding information or deliberately providing false information."

Similarly, Article 57 of the Constitution states: "The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law." Article 71 further adds: "It is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers and media outlets in any way. Exception may be made for limited censorship in time of war or general mobilization."

Although all the aforementioned constitutional articles emphasize the citizen's right to access knowledge from all sources, we find that the information circulation laws contain restrictive texts and provide for bureaucratic procedures without guarantees. This effectively translates a contrary principle of withholding information into legislation, with disclosure by State institutions becoming the exception rather than the rule. The expansion of publication bans, prohibiting the circulation of publications, and censorship of the Internet all point to this. Moreover, these laws impose custodial penalties on both citizens and institutions in this regard. This stems from a mutually exclusive view of national security and the people's right to information, whereas a careful review of recent history would show that, in practice, the legality of national security interests is better protected when the public is well informed about state activities, including those designed to protect national security.

All these aforementioned developments were an attempt to restrict the digital revolution that has given Egyptian citizens open access to knowledge. The January 2011 revolution confronted the Egyptian State with millions of people demanding change, gathered in the squares on the ground or critical of the government online. As the internet, media, and civil society organizations played a key role in toppling the Mubarak regime, the security and judicial agencies have moved to keep these voices in check under Sisi.

The General Environment of Censorship in Egypt

The mentality of the state of Egypt regarding censorship is evident in its actions to block websites even before the enactment of the 2018 laws, as well as in the discussions that preceded them. On 24 May 2017, for instance, Egyptian authorities blocked 21 websites, mostly news sites. No official decision was announced and no explanation from government agencies or telecommunications companies was provided. All that was issued in connection with the matter was a report circulated by various newspapers, claiming that it came from a sovereign authority that considered "state censorship of social media networks [as] a legal right," based on monitoring the experiences of foreign and Arab countries in blocking websites. Subsequently, the authorities expanded the blocking of websites to a huge number of portals offering different types of content and services.

The Association for Freedom of Opinion and Expression (ATFE) issued a report on 4 June 2017 titled "Decision from an Unknown Body: On blocking websites in Egypt". The report emphasized that there was no legal umbrella that allowed blocking and considered it a clear violation of the freedom of work of media outlets. The report also explained that while the decision to block seemed to be based on three laws: the Anti-Terrorism Law, the Emergency Law, and the Telecommunications Regulation Law, these were not clearly addressed to regulate digital communication, but all included broad formulations such as preserving public morals and protecting national security or citizens' interest, which invite subjective interpretation. ATFE continued to monitor websites blocked by the authorities and issued its report entitled "Occasionally by Decree.. Update on the Block of Websites in Egypt." According to this report, the number of temporarily or permanently blocked websites shot up to at least 496 sites by February 1, 2018, that is, in less than eight months.

Blocking websites was already present in the draft cybercrime law proposed by MP Tamer al-Shahawi, a former officer and member of the Egyptian House of Representatives in May 2016. The draft law contains 30 articles that did not aim to combat cybercrime, but rather to control digital and social media users by imposing self-censorship practices and threatening harsh penalties for offences. A member of the House of Representatives proposed issuing a law that obliges Egyptian users to obtain a license to use social networks. Other parliamentary demands to block websites and impose censorship on the Internet have emerged, with members of the Egyptian Parliament announcing that they wished to issue a law to block pornographic websites and websites affiliated with armed organizations. One of the strangest proposals issued by members of the House of Representatives in April 2017 was a call by some members to enact a law requiring users of social networks in Egypt to pay a monthly fee for using Facebook.

In the second quarter of 2017, American cloud services company Akamai's quarterly State of the Internet report revealed that Egypt ranked first globally as the largest source of blocked IP addresses. Since the enactment of the 2018 laws, the situation has only become worse. A statement issued by six civil society organizations in September 2018 called the new laws an attempt by the authority to legalize the repressive steps it had taken with regard to internet censorship for more than a year. As such, they called for the repeal of the Cybercrime Law, as well as a review of the articles related to internet surveillance and website blocking in the Press and Media Regulation Law.

On May 15, 2019, AFTE submitted a report entitled "Thousands of Websites are collaterally blocked in Egypt," in which it addressed the method of blocking websites based on blocking the Internet protocol package (TCP/IP) and data traffic between users and a specific IP address of a specific server. When multiple sites are hosted on the same server, all the sites on the server are blocked along with the targeted site. For example, when the State moved to block the website Fakartany.com, all 279 domains hosted on its IP address 188.121.43.37 ended up being blocked. AFTE continues to monitor blocked sites and has an updated report that includes a list of all blocked sites, which so far includes 549 websites. As a result of the repressive practices against journalists and website blocking in particular, Egypt ranked 163rd on the Press Freedom Index out of 180 countries for 2018, according to Reporters Without Borders' April 2020 report.

In June 2023, the Board of Trustees of the National Dialogue held a session titled "The Case of the Freedom of Information Law." Journalist Khaled Elbashy referred to the issue of blocking websites and received a response from Counselor Mahmoud Fawzy, head of the Technical Secretariat of the National Dialogue and Secretary General of the Supreme Council for Media Regulation, stating that blocking is mostly an administrative procedure imposed due to issues with the licensing procedures of these websites. Fawzy responded by asking "If the reasons for blocking are administrative and related to licenses inside Egypt, why are websites operating abroad blocked?" This exchange demonstrates the Egyptian regime's desire to block information and opinions that oppose or critically analyze the state's policies.

Websites like Al-Manassa have reported that they have been blocked within Egypt 13 times by the Egyptian authorities between 2017 and 2022. The blocking was carried out without a legal basis and without any official or security body clearly claiming responsibility for it. 28 civil society organizations working inside and outside Egypt signed a statement issued in August 2022, titled "28 Civil society organizations condemn the continued blocking of Al-Manassa's website and call on the Egyptian authorities to lift the blocking of dozens of news websites," arguing that the continued blocking of websites exacerbates the violation of the right to media freedoms and citizens' right to knowledge, access to information and use of the internet, all rights protected by Articles 57, 65, 68 and 71 of the Egyptian Constitution. The signatory organizations also called on the Egyptian authorities to immediately stop censoring the internet, end the blocking of news websites, and guarantee press freedom.

Representatives of many such blocked websites have filed complaints with the Journalists'

Syndicate, the Supreme Media Council, the Ministry of Transportation, and the Public Prosecutor, but have yet to receive a response. The Egyptian online newspaper Mada Masr filed a lawsuit challenging the decision to block its website before the Administrative Court, but the case has not been heard even after five years. As for the blocking of websites operating outside Egypt, the liberal Arab media network Raseef22 was blocked in Egypt and Saudi Arabia for four years, during which the website launched an "I am not afraid" campaign on social media in 2019, releasing a video featuring all the pervasive issues that the censorship and security authorities prevent it from raising.

The latest incident of blocking a news website was Cairo24, which was blocked inside Egypt in November 2024. While the website's administration has not yet engaged publicly with the blocking, no decision has been issued by the Supreme Council for Media Regulation in this regard, despite many previously blocked websites such as Raseef22, Al-Manassa, and Gem being unblocked during this time. All these instances of blocking combine to outline a general picture of the type and forms of censorship pressures they are subject to in Egypt, and their weak access to legal recourse.

Towards a New Egyptian Information Circulation Law: Lessons from the Jordan and Tunisian experience

In a report titled "Open Access.. Arab regional lessons drawn from information access laws in Jordan and Tunisia" in December 2021, ATFE presented a reading and analysis of the Right to Access to Information Law in Jordan No. 47 of 2007, and a number of laws that impact on the right to circulate information, such as the Law on the Protection of State Secrets and Documents No. 50 of 1971, and the Cybercrime Law issued in 2015.

Article 12 of the 2015 Cybercrime Law in Jordan states: "Whoever intentionally accesses an information network or information system or any part thereof by any means without authorization or in violation or excess of an authorization with the aim of accessing data or information not available to the public that affects national security, foreign relations of the Kingdom, public safety or the national economy shall be punished with a term of imprisonment of not less than 4 months and a fine of not less than 500 dinars and not more than 5,000 dinars."

Article 4 of the same law further stated: "Anyone who intentionally introduces, publishes or uses a program through an information network or an information system to cancel, delete, add, destroy, disclose, damage, withhold, block, modify, change, transfer, copy, capture or enabling others to access data or information, obstructing, disrupting, stopping or disabling the functioning of the information system or accessing it, changing the location of any cartoons, canceling, destroying or modifying its contents or occupying it without authorization or in violation of that authorization or impersonating its identity or the identity of its owner shall be punished with a term of imprisonment for a period of not less than 3 months and not more than 1 year, and a fine of not less than 200 dinars and not more than 1000 dinars."

By prescribing penalties for specific offenses, the 2015 Law placed relative restrictions on the circulation and availability of information, but did not touch the freedom of publication. However, the adoption of a controversial new Cybercrime Law in 2023 in Jordan has caused a crisis of freedom of opinion and expression due to the presence of authoritarian formulations in its text. Article 15 of this law states: "Whoever intentionally sends, resends, or publishes data or information through an information network […] that includes fake e news targeting the national security and community peace, or defames, slanders, or contempt any person shall be imprisoned for a period of not less than three months or a fine of not less than (5000) five thousand Dinars and no more than (20000) twenty thousand Dinars." In addition, Article 16 of the same law punishes "acts that would assassinate [a person's] personality" with a penalty of 3 months to 3 years in prison and a fine ranging from 5,000 dinars (7,000 USD) to 20,000 dinars (28,000 USD). 14 human rights organizations, led by Access Now and Human Rights Watch, criticized the law in a statement saying that it "threatens" digital rights, freedom of expression, and access to information.

This is in addition to an analytical reading of parallel laws in the Tunisian experience, especially Decree No. 41 of 2011, which was amended by Decree Law 54 of 2011. Article 24 of this decree states: "Anyone who deliberately uses information and communication networks and systems to produce, promote, publish, send or prepare false news, data, rumors, or documents that are fabricated, forged or attributed falsely with the aim of infringing on the rights of others, harming public security or national defense, or spreading terror among the population will be punished with 5 years of prison and a fine of 50 000 dinars". The Right of Access to Information Law No. 22 of 2016 and the Tunisian Archive Law No. 95 of 1988 led to the establishment of an independent body to consider and investigate all matters related to the freedom of circulation and dissemination of information, including citizens' access to official reports and statistics, complaints and reports of dissemination of falsehoods. This body is called the 'Access to Information Commission' and consists of a group of independent experts in various fields.

Analyzing the above two experiences and comparing the Jordanian and Tunisian laws in principle, we find that both of these laws acknowledge that regulating the freedom of information may be the only way to attain transparency, reduce corruption, and provide a clear platform to faithfully present voices of both the regime and the opposition. In neither of these cases was the right to arbitrarily block websites recognized; rather, instances in which publishers of information could be prosecuted were clearly defined.

In light of this analysis, the Association for Freedom of Opinion and Expression (AFTE) submitted a draft proposal for the Information Circulation Law of 2023 to Egypt's National Dialogue. This draft aims to recognize the right of access to information in accordance with international standards and the principle that information should be made public in the absence of a reason for confidentiality that overrides this right, while establishing mechanisms and procedures to promote the disclosure of information to contribute to meeting the needs of society to solve economic and social issues; fulfil the requirements of planning and development; promote an effective, open, and accountable government; and

encourage participation in governance. It also aims to achieve its objectives while maintaining security, safety, and without infringing on public and personal interests and rights, such as the right to privacy.

Blocking Has Effects of Different Dimensions

Experts in the fields of journalism, media and information technology have noted the serious effects of blocking, including the technical aspects of the State's control over the exchange of news and information over the Internet through the deliberate blocking of specific websites, and the collateral and arbitrary blocking of hundreds of websites that occurs as a result of blocking the host domain of targeted websites, which we have described earlier in this paper.

There is also an economic impact to blocking, which includes the closure of platforms and the displacement of their employees, in addition to the fact that blocking practices abort any desire to invest in supporting digital journalism experiences. These effects can be estimated in light of the journalistic context in Egypt, where the print press is suffering from severe crises that threaten its continuity, and where most young journalists are not members of the Journalists Syndicate. This deprives young male and female journalists from the support and protection provided by the syndicate, making them vulnerable to losing their material and moral rights during contracting or layoffs. Moreover, the sales of Egyptian national and independent print newspapers have deteriorated to the point that they are facing considerable losses.

There are also implications for journalistic content. On the one hand, blocked platforms fear repercussions beyond blocking. On the other hand, non-blocked sites fear crossing "red lines" and risking getting blocked themselves.

Administrators of blocked websites usually try to counter the block using several measures. These include:

1. Alternate links: The website simply uses a different domain instead of the one that was blocked.
2. Proxy links: A blocked website provides links to its content via a proxy service that makes it appear as if your device is connecting from a different geographic location than your actual location.
3. Content Delivery Networks (CDN): A website provides a link to its content via a CDN (for instance, a server belonging to Google), so that sites can only be blocked if the entire CDN used by the blocked website is blocked.

Some websites publish all their content on their Facebook pages, while others may turn to alternative publishing platforms that are not blocked, such as blogging services. However, these measures often require platforms to sacrifice the advertising revenue they gain from people visiting their site. Also, these methods may require the reader to make an additional effort to enter the link of the publication on proxy sites to hide their identity effectively. In both cases, these concessions are not commensurate with the need for quick access to

information by the user, nor with the financial repercussions suffered by these platforms. Moreover, the State is making technical advancements in its blocking policies in an effort to close these remaining modes of access by the public.

AFTE considers that the requirement for websites to obtain licenses from the Supreme Council for Media, and the fact that print newspapers can be established through notification while websites need to go through a license approval process, indicate the Egyptian State's tendency to tighten control over everything related to freedom of access/use of the internet, especially with the expansion of authorities now empowered to block websites and accounts.

Conclusion

In light of this situation, the following recommendations can be made:

1. Renew the public debate on internet censorship practices and their severely negative effects on the status of independent digital journalism in Egypt.
2. Hold a national dialogue wherein the State can disclose its real reasons and concerns regarding the content of blocked websites and review these concerns with the administrators of these blocked platforms.
3. Restore full belief in the right of the public to access information, so that the principle of free circulation of information is protected, while prevention is justified and clear to all. This is in compliance with the articles of the Egyptian Constitution amended in 2014, which protect citizens' freedom of communication and access to information.
4. Reconsider all conflicting laws, especially the Press, Media, and the Supreme Council for Media Regulation Law, which contains many provisions that restrict press freedom, and the Law on Anti-Cyber and Information Technology Crimes, which limits citizens' right to access knowledge.
5. Promulgate a law banning imprisonment for publishing offences.
6. Benefit from the experiences of neighboring countries such as Tunisia and Jordan in cross-cutting issues.
7. Hold roundtables with members of the Egyptian parliament, at which members from civil society organizations opposed to the blocking policy can present their draft proposals for legislation in the presence of officials from the executive, specialized, security, and judicial institutions concerned with blocking.