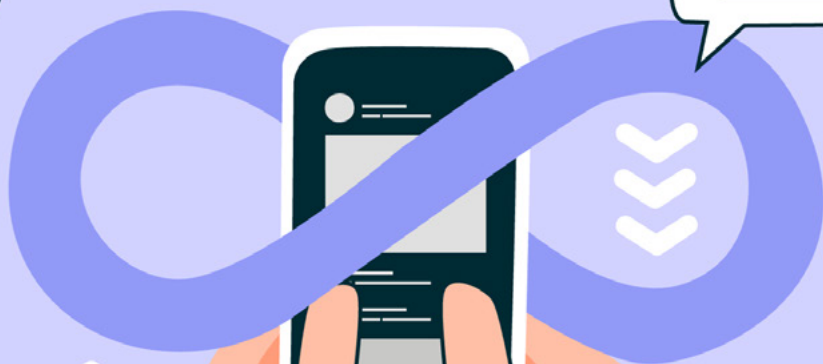




# Virtual Freedom

Towards Ending the Cybercrime Law's  
Repression of Online Freedom  
of Expression in Egypt



# **Virtual Freedom:**

## **Towards Ending the Cybercrime Law's Repression of Online Freedom of Expression in Egypt**

August 2025



All printing and publication rights reserved. This report may be redistributed with attribution for non-profit purposes under Creative Commons license.

[www.creativecommons.org/licenses/by-nc/3.0](http://www.creativecommons.org/licenses/by-nc/3.0)

This study was prepared by Amr Abdel Rahman, director of EIPR's Civil Liberties Unit. The desk research and data collection was carried out by EIPR's researcher Mahmoud Nagy. Lobna Darwish, director of the Women's Rights and Gender Program, provided advice and comments on various drafts of this study. The final review and editing was made by Karim Ennarah, deputy executive director of research at EIPR.

**The Egyptian Initiative for Personal Rights (EIPR) has been working since 2002 to strengthen and protect basic rights and freedoms in Egypt, through research, advocacy and litigation in the fields of civil liberties, economic and social rights, and criminal justice.**

For more information see <https://eipr.org/en>

## **Introduction**

Legislative, judicial, and security restrictions on digital expression have expanded in Egypt over the past dozen years. A range of previously legal acts have been criminalized, special penalties introduced, and existing penalties increased if crimes are committed online. The Anti-Terrorism Law No. 94 of 2015, the Press and Media Regulation Law No. 180 of 2018, and the Cybercrime Law No. 175 of 2018 are full of examples of this clampdown.

The Public Prosecution has introduced a new form of social media censorship by establishing an “electronic monitoring unit” to surveil such crimes in real time. It has also increased the number of charges it levels using crimes based on old, largely unutilized legislative articles, either from the Penal Code (such as articles 80 (d), 102 (bis), and 188 criminalizing various modes of spreading false news, and article 306 (bis a) criminalizing certain forms of defamation and slander) or the Telecommunications Regulation Law No. 10 of 2003 (especially article 76, which criminalizes “deliberately causing a nuisance using social media”).

In parallel with legislative and judicial developments, security practices have reflected a tendency to restrict various forms of expression if they find their way online, by both illegally blocking numerous websites and arresting citizens who have published content deemed by the security services to violate the Constitution and law.

As the scope of criminal acts has widened, the circle of those targeted by the security and judicial authorities has broadened prodigiously to include members of legally recognized political parties, those accused of terrorism or joining illegally established groups, journalists, media professionals, opinion writers, visual content creators, and users of private social media accounts who are not known for any activity in the public domain.

These restrictive trends emerged between 2013 and 2023, a decade that state institutions described as an “exceptional” time of protracted confrontation between the state and armed extremist groups, and widespread political mobilization of oppositional groups using the internet to reach people, in addi-

tion to incidents of sectarian violence. Towards the end of that decade official institutions signalled that the time had come to reconsider these restrictions because the exceptional circumstances had been overcome: the state of emergency was lifted in October 2021, for example, and [national dialogue sessions](#) started in 2023.

We disagree with the term “exceptional” for the circumstances surrounding the endorsement of these laws, and take issue with the idea that exceptionalism justifies legislative and judicial arbitrariness, yet we believe that the state’s acknowledgement that dialogue is needed is a positive development that requires positive engagement.

Our constructive approach is to formulate a democratic normative framework to help legislators and judges define the limits of digital freedom of expression in general and to accurately determine the grounds, mechanisms, and controls for restricting it, without compromising the fundamental objective of the existing constitutional and legal framework: to protect and promote fundamental rights and freedoms, at the core being freedom of expression.

We are well aware that no normative framework, no matter how comprehensive, will resolve the inevitable recurrent disagreement between legislators and judges on the one hand and the public on the other over the limits of freedom of expression. We do not aim to resolve this dispute, but rather to provide a democratic framework for its management that will lift the public debate on the issue out of the spiral of authoritarianism, arbitrariness, fragmentation, and legalization of personal whims.

## **Methodology**

In formulating this democratic normative framework, we rely on the provisions of the 2014 Egyptian Constitution, amended in 2019, and of international human rights law—a component of domestic legislation in accordance with Article 93 of the Constitution—which together constitute a single organic unit. We also rely on best practices as represented in useful jurisprudence from international and regional courts whose contexts are similar to the current Egyptian context.

We chose this starting point as we believe that the texts and interpretations of international human rights conventions, having resulted from negotiations between various countries in a relatively equal framework, are the best-qualified legal corpus for reconciling diverse cultural, political, and security sensitivities without infringing on individuals' rights, freedoms, and wellbeing. Moreover, successive Egyptian governments and various civil society organizations have very actively contributed—each according to its own perspective—and continue to contribute to the development of this complex system, showing varying degrees of keenness to adhere to its provisions and traditions. With its tendency toward practicality and compatibility, it may therefore contribute to developing the positions of the various parties in Egypt and enable the sensitivities of each to be taken into account. As for the current Constitution, our decision to rely on it here despite our critical stance toward many of its articles is self-explanatory, given that it serves as the country's supreme governing law.

The arduous task of using our proposed framework to review this wide range of legislation and judicial applications being outside the scope of this study, we adopt a case-study methodology here and apply the framework to one law, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018. Comprising most of the above-mentioned authoritarian practices—including legalizing the blocking of websites, criminalizing certain acts if committed online, and applying stiffer penalties for existing crimes if committed in that space—this law is a comprehensive expression of the state security institutions' vision of the internet as a space full of threats to the stability of the ruling system of governance and to existing social relations as a whole, with

associated patterns of religiosity and ethics. This vision has been clear since the law was an idea and expressed itself most clearly in the early drafts, which Egyptian human rights organizations described as “[anti-technology](#).”<sup>1</sup>

It is no coincidence that the Public Prosecution and the State Security Prosecution take an expansive approach to this law in order to bring charges against a very wide range of social media users, as its overly broad wording facilitates such an approach and suits these institutions’ broad ideas about “threats to national security” or public order. As a result of their massive expansion, its articles have attracted the attention of various stakeholders, including parts of the public at large, to the extent that discussion of any restriction on freedom of expression online involves their discussion too.

Employing our framework to study this complex law, criticize it, and formulate practical proposals for its amendment may also facilitate the discussion, critique, and amendment of many similar laws with the same philosophy, such as the Anti-Terrorism Law, the Press and Media Regulation Law, and the Telecommunications Law.

To lay out its proposed normative framework, the study begins with a review of the general determinants of the democratic legal regulation of freedom of expression in the virtual sphere as formulated by relevant United Nations mechanisms, namely resolutions, committees’ interpretations, and special rapporteurs’ and working groups’ directives, based on the provisions of international human rights conventions. It also reviews certain judicial interpretations of these texts that are both progressive and practical. In its second part, the study shifts to the application of this proposed framework through a detailed discussion of the context of the issuance of the law in question, the extent of its compliance with the determinants derived from international human rights law, and the impact of non-compliance on its judicial application. In its third and final part, the study offers recommendations for a legislative review of the law guided by the normative framework.

---

<sup>1</sup> EIPR, Association for Freedom of Thought and Expression (AFTE), Daam Center for Information Technology, “Anti-Technology,” Cairo 2016.

## **International human rights law**

UN mechanisms have been aware of the need to develop an approach to democratically regulating the exercise of freedom of expression in virtual space since the beginning of the 2010s. This happened as internet use expanded dramatically and became a reality of contemporary life on which all economic, political, or social activity came to rely. The challenges this posed for governments and other social institutions would include people exploiting cyberspace to plan crimes, not least crimes categorized as terrorist, whether through direct recruitment, incitement, or promotion of ideas, and then individuals spreading racism and hate speech. Before long, activities specific to the medium emerged that violated basic rights, such as stalking, blackmail, defamation, bullying, piracy, and the dissemination of false or fabricated news. Eventually came challenges associated with the use of artificial intelligence (AI).

The vast majority of countries responded by restricting internet access, criminalizing several new activities, and/or increasing penalties for already criminalized activities if they occur online. This was done in the name of protecting the existing social order, especially the interests of vulnerable parties such as children, women, and religious and ethnic minorities. In other words, Egypt is no exception.

This global trend alarmed various parties and generated protest against what they saw as the use of the combat of terrorism and extremism or the protection of women, children, and families as pretexts for attacking freedoms, including those protected by the UN and national constitutions. In short, the sudden widespread use of the internet revived all the major questions that faced the human rights system at its inception, such as around the legality of criminalization, proportionality between crime and punishment, the grounds for restricting public freedoms, and even the content of those freedoms.

Key UN organizations have repeatedly addressed these questions. The General Assembly's resolution [69/166](#) of December 2014 concerns the right to privacy in the digital age, resolution [184/70](#) of December 2015 concerns technology for development, and resolution [125/70](#) of December 2015 contains the

outcome document of the high-level meeting on the overall review of the implementation of the outcomes of the UN's World Summit on the Information Society. The General Assembly reaffirmed the content of these resolutions in resolution [176/75](#) of December 2020 on the right to privacy in the digital age and resolution [202/75](#) of December 2020 on technology for development.

The Human Rights Council issued resolutions 8/20 of July 2012 and 13/26 of June 2014 on the promotion and protection of human rights online. It reaffirmed their content in resolution 16/47 of July 2021. It also issued resolution 7/31 of March 2016 on information and communications technologies and child sexual exploitation, and resolution 15/42 of September 2019 on the right to privacy in the digital age.

These resolutions are very diverse and make different recommendations, but are all based on one cornerstone, expressed in the first article of resolution 16/47 of 2021:

The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.<sup>2</sup>

Even non-human-rights international conventions supporting international cooperation in combating cybercrime stipulate the need to respect the principles of international human rights law, especially those related to guarantees of freedom of expression. The most recent, the [UN Convention against Cybercrime](#) adopted in November 2024,<sup>3</sup> clearly stipulates in its preamble and article 6 signatories' obligation to ensure its implementation conforms with their other obligations under international human rights law. In the second paragraph of article 6, it specifically states:

---

2 United Nations Human Rights Council, Forty-seventh Session, Resolution 16/47 on "Promotion, Protection and Enjoyment of Human Rights on the Internet," 13 July 2012, p. 3.

3 The convention is supposed to be open for official signature in Hanoi in 2025 and then at the UN headquarters in New York until 31 December 2026.

Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.<sup>4</sup>

Although internet privacy is widely recognized, the legal regulation of online expression must be subject to the same guarantees and caveats imposed on the regulation of freedom of expression in other spaces as defined by international human rights conventions. This principle has been repeatedly raised in varying degrees of detail in UN treaty bodies' resolutions and comments, and found its way into the UN resolutions listed above. Human Rights Council resolution 16/47, for example, points out "the need to ensure that measures offline or online for the protection of national security, public order and public health are in full compliance with international law obligations and that the principles of lawfulness, legitimacy, necessity and proportionality are respected."<sup>5</sup>

The aforementioned resolutions all refer to the International Covenant on Civil and Political Rights to identify the content of the right to freedom of expression, which also entails a search within the commentaries of the committee concerned with interpreting the right to freedom of expression in order to derive mechanisms for regulating it without compromising its content. This approach is adopted by several regional and national mechanisms, such as the European Union, the Indian Supreme Court, and the South African Constitutional Court, to which we will refer.

---

4 Report of the Third Committee, Combating the use of information technology for criminal purposes, 27 November 2024, A/79/460, p. 10.

5 Ibid., p. 2.

# 1. Grounds for limiting the right to freedom of expression

Article 5 of [the International Covenant on Civil and Political Rights](#) (ICCPR) addresses the issue of limiting the rights stipulated in it in general, while article 19, and indirectly articles 18 and 20, address the restriction of the right to freedom of expression. The first paragraph of article 5 states:

Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.

This article clearly states that the essence of the detailed provisions of the ICCPR is to provide the broadest possible protection of fundamental rights and freedoms, and to create the appropriate political and social context for their promotion. This is the governing principle of the ICCPR as a whole, which must guide the implementation and interpretation of any of its articles. This approach is consistent with what has become an original principle of interpretation of constitutional and legal texts, i.e., the provisions of a constitution or law are one objective whole, supporting each other to achieve a single goal in the light of which all provisions must be interpreted so as not to contradict each other. The restriction of any right contained in the ICCPR must therefore be aimed at protecting the rights and freedoms of individuals and groups. If the limiting text contradicts this principle, the text must be interpreted in the interest of its application. This is the approach taken by the Human Rights Committee, as well as by other UN mechanisms, on the implementation and interpretation of ICCPR provisions. The interpretation of any restriction on freedom of expression online is no exception.

In light of this governing principle, restrictions on freedom of expression can be read and interpreted either directly in article 19 or indirectly in articles 18 and 20. The third paragraph of article 19 states:

The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

- (a) For respect of the rights or reputations of others;
- (b) For the protection of national security or of public order, or of public health or morals.

The same text is repeated in the third paragraph of article 18 when addressing freedom to practise religion, which is inevitably linked to freedom of expression. Article 20 specifically prohibits “any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.”

Thus the ICCPR identifies five grounds on which the right to freedom of expression can be limited:

- Rights and freedoms of the others
- Public order or public safety
- Public morality
- National security
- Public health

Neither the Human Rights Committee, which is responsible for interpreting the ICCPR, or the Committee on the Elimination of Racial Discrimination, which interprets the Convention on the Elimination of All Forms of Racial Discrimination, consider “propaganda for war or advocacy of hatred” as a separate basis, as its prohibition is part of the protection of others’ rights and freedoms or the maintenance of public order.<sup>6</sup>

These exceptions are an example of the above-mentioned practical/flexible tendency of the human rights system. The constraints of “public order

---

<sup>6</sup> Committee on the Elimination of Racial Discrimination, Recommendation No. 35 Combating speech inciting racial hatred, 26 September 2013.

and morals” are old restrictions carried over, almost unchanged, from eighteenth-century civil/Roman legal traditions. They express the then-prevailing tendency to regard legislation as a tool to strengthen the central national authority of the state vis-à-vis the nationals of other states, local communities, or any other party contesting its sovereign rights.

It is no coincidence that these concepts of public order and moralities emerged in the countries that followed the Roman legal tradition when examining subjects of private international law, specifically the compatibility of foreign traders’ practices—including contracts, mortgages, and loans—with the laws of host states, as well as in the context of bolstering young states’ sovereignty over domestic and foreign nationals. The same concepts resurfaced at the end of the nineteenth century and the start of the twentieth in the context of regulating the practice of religious rites to consolidate the rights of sovereignty vis-à-vis churches contesting the official doctrine of the state. They were likewise repurposed to deal with emerging workers’ movements at the beginning of the twentieth century.<sup>7</sup>

Bringing these old concepts into the UN human rights conventions after World War II was a necessary bargain to ensure that states accepted the principle of voluntary submission to international obligations in their relationship with their nationals. The prohibition of war propaganda and advocacy of racial, national, or religious hatred is understandable given the context of drafting these texts, overshadowed by the horrors of World War II and the threat of a new world war in light of the Soviet-Western conflict.

Given their inherent compatibility and flexibility, as well as the stability of the principle of state sovereignty, states’ integration within an expanded and expanding network of material and cultural exchange, and the associated involvement in public debate of more and more citizens, individuals, and groups of diverse interests, backgrounds, and sensitivities, the UN conventions set foundations for interpreting the exceptions in a manner that does not preju-

---

<sup>7</sup> For more details on the history of the concept of “public order” see M. Ford, The “Order Public” Exception and Adjudicative Jurisdiction Conventions, *International and Comparative Law Quarterly*, 29, 1980.

dice the substantive unity of the ICCPR provisions or bend it away from its governing principle, namely “the protection and promotion of the freedoms of individuals vis-à-vis the authority, or any infringement thereof facilitated or condoned by the public authority.” This is understood from the clear text of ICCPR article 5.

On this basis, the relevant committees and some leading courts have tended to interpret the terms “public order,” “public morals,” and “national security” as referring to a general context in which individuals may exercise their fundamental rights under the ICCPR.

“Public order” and “public safety” shifted, in the comments of the mentioned committees produced in the early nineties of the previous century from being concepts that embody the identity or culture of the state, as in the Roman/civil legal literature, to become determinants of a necessary circumstance of public peace that allows individuals to exercise their freedoms and participate in community life freely, closer to the Anglo-Saxon legal literature.<sup>8</sup> Thus, if a limitation prevents individuals from exercising their freedoms under the pretext of protecting public order, it is a violation of and contrary to ICCPR provisions. The necessary public peace can only be achieved when the public authority takes into account the interests, backgrounds, and sensitivities of the individuals it serves. If it tends toward the exclusion of any of these, it is the exclusion that is a breach of the peace and not the other way around. This is the concept that the Human Rights Committee relied on in its general comment No. 22 interpreting ICCPR article 18, on the regulation of the right to freedom of conscience and belief. In its interpretation of the meaning of public order, the Committee clearly stated that ICCPR application as a whole requires that the cultural and religious diversity of any society be taken as a starting point, and that preserving the general peace of this diverse society requires not deriving the determinants of public order from a single religious or cultural tradition.<sup>9</sup>

---

8 John Finnis, *Natural Law and Natural Rights* (Oxford University Press, 1980) p. 215.

9 Human Rights Committee, forty-eighth session, general comment No. 22, article 18, on freedom of thought, conscience and religion, 27 September 1993, p. 4.

Similarly, the concept of “national security” is intended to protect a state’s sovereignty over its whole territory in order to provide personal security for all residents of that territory, which is a practical necessity for any legitimate exercise of rights and freedoms. While it is inconceivable that people would enjoy full freedom of movement in the event of aggression by another state or civil war, for example, if the imperatives of protecting national security clash with the personal security objective, the restriction becomes void of meaning or counterproductive.

This logic was used by the UN rapporteurs, human rights organizations, and independent experts, who drafted the [Global Principles on National Security and the Right to Information \(The Tshwane Principles\)](#) in 2013. Its preamble states that the purpose of protecting national security is to enable individuals to fully exercise their rights and freedoms. Although the Principles provide no unified definition of national security on account of different contexts and threats, the general determinants of such a definition can be deduced from the document as a whole. National security can be conceived as stable national borders and state sovereignty over its territory against any military or para-military threat, threat to its infrastructure, and threat to the lives and property of its citizens through physical violence and sabotage sponsored from abroad. Principle 9 provides examples of information whose protection or restricted access might be necessary to protect citizens’ personal security.<sup>10</sup>

The pragmatic tendency to consider the diversity of the group governed by state as a reality in designing constitutions and legislation has also inspired new interpretations of “public morality” compared to the ones that were dominant during the times of drafting the UDHR and the related covenants

In general, morality means a set of values and moral convictions that inspire individuals’ actions towards others without legal obligation or coercion. They enable individuals to form autonomous judgments about right, wrong, acceptable, and unacceptable actions, thus facilitating their conscious participation

---

<sup>10</sup> Open Society Foundations, Open Society Initiative, *The Global Principles on National Security and the Right to Information (The Tshwane Principles)*, 12 June 2013, p. 19.

in group life. Any society must therefore create conditions to protect and develop such values and convictions.

Yet there is an inevitable difference between public and private morality. Private morality is a set of values and practices that allow an individual to participate in organic groups (family, extended family, tribe), groups formed around profession, economic status, or activity, or any other closed groups that impose special conditions for membership. Public morality consists of the values and sensitivities that enable an individual to join a broader political group with open membership, such as a nation. Public morality helps manage the common or intersecting affairs of all those sub-groups regulated by private morality. No bundle of private morality, related to religion, region, or tribe, can be elevated to the rank of values governing the life of the nation as a whole, otherwise the concept of the nation as a political unit that includes these sub-units will collapse.

Public morality, the priority, can thus be defined here functionally. It is a set of values and practices for managing relations between members of a diverse political group and enabling them all to participate in its affairs without discrimination or exclusion. The focus being values that support the preservation and survival of the group's political cohesion, such as tolerance, solidarity, social responsibility towards vulnerable parties, mutual respect in public debate, and non-discrimination. The relevant legal text is not then obligated to protect every moral value that is unanimously sanctioned or revered, but only those that contribute functionally to the nation's democratic political life.

In seeing public morality as the common denominator of a society's prevailing values and sensitivities, which helps individuals (whether conservative or progressive, religious or secular) to autonomously exercise their constitutionally

protected rights and freedoms,<sup>11</sup> UN committees and many leading national and regional courts tend to interpret public morality very differently from interpretations predating the late twentieth-century.

Over the past two decades, we have witnessed the creative application of these ideas when dealing with legal problems in complex societies. The most important being the creation of the expression “constitutional morals” or “constitutional ethics,” meaning a set of moral values and sensitivities that can be deduced and distilled from modern democratic constitutional texts—provided that they have been formulated using recognized democratic methods—and from the international human rights conventions resulting from the reconciliation of these various constitutional traditions. National courts that have taken on this task are in the Global South, including the South African Supreme Court and the Indian High Court, whose contexts are similar to that of Egypt.

The South African Supreme Court was the first to develop the concept, and the detailed comments of some of its judges address certain traditional arguments in defining public morality. Judge Albie Sachs, for example, in his opinion in the 1998 case of [“National Coalition for Gay and Lesbian Equality versus the Minister of Justice,”](#) not only echoes classical liberal arguments about the need for the state to remain neutral toward the private lives of its citizens, but seriously discusses legitimate concerns about the potential impact of generalizing an absolute relativity of values on the possibility of moral citizenship. He rejects moral relativity, but calls for deriving the common moral denominator exclusively from the constitution. He writes:

A state that recognises difference [among its citizens] does not mean a state without morality or one without a point of view. It does not

---

11 This approach is derived from previous theoretical jurisprudence dating back to the seventies of the last century 1970s, which began to redefine the content of democratic practices without linking them to a specific ideological content of the prevailing ideologies at that time, whether liberal, socialist, Islamist, or nationalist. But it is a stand-alone content, although an approach does not contradict any of these ideologies, but rather draws inspiration from many of their elements, as they themselves have of those same ideologies that have receded into the background as a result of various developments outside the scope of this study. For a general idea about these theories, see: John Rawls, *Political Liberalism*, Harvard University Press, 1993.

banish concepts of right and wrong, nor envisage a world without good and evil. It is impartial in its dealings with people and groups, but is not neutral in its value system. The Constitution certainly does not debar the state from enforcing morality. Indeed, the Bill of Rights [in the Constitution] is nothing if not a document founded on deep political morality. What is central to the character and functioning of the state, however, is that the dictates of the morality which it enforces, and the limits to which it may go, are to be found in the text and spirit of the Constitution itself.<sup>12</sup>

The [Supreme Court of New Delhi](#) has taken the same approach in recognizing the moral context necessary for the exercise of rights and freedoms, and the need to protect that context. Here, however, its determinants are derived from the unanimously approved Constitution of India, drafted as directives to the nation, regardless of the shifts in the political or cultural views of the majority. In its 2009 decision in the case of “Naz Foundation vs Government of NCT of Delhi and Others,” the court states:

Thus, popular morality or public disapproval of certain acts is not a valid justification for restriction of the fundamental rights under Article 21 [of the contested law]. Popular morality, as distinct from a constitutional morality derived from constitutional values, is based on shifting and subjecting notions of right and wrong. If there is any type of morality that can pass the test of compelling state interest, it must be constitutional morality and not public morality.<sup>13</sup>

Even the older, more traditional and conservative regional courts, such as the European Court of Human Rights, have begun to take this approach to cases of restriction of fundamental rights in the name of preserving public morality. It tended to interpret the articles of the European Convention on Human Rights—in particular article 8 on the restriction of private life on the

---

12 The National Coalition of Gays and Lesbians Equality, v. Minister of Justice, The Constitutional Court of South Africa, Case CCT 11/98, 9 October 1998, (136) p. 132.

13 Naz Found. v. Gov't of NCT of Delhi, (2009) WP(C) No. 7455/2001, 8 (Del. HC) (India).

grounds of preserving public morality—as an objective whole aimed at protecting, promoting and developing individual autonomy, and as a prerequisite for the exercise of the rights and freedoms set forth in the ICCPR. Even when it approved the [prohibition of abortion in the Irish Constitution](#) in 2010, it based its reasoning on that understanding, which led it to what it saw as the rights of the unborn, rather than just finding the ban necessary for preserving public morality in the abstract.<sup>14</sup>

In parallel, seeing that states were restricting freedom of expression on the pretext of combating hate speech, violence, and discrimination, as internet use proliferated and in the context of the so-called war on terror and the wagers of that war attempting to dry up the sources of terrorism in “violent extremism,” international human rights groups have sought to set standards to define hate speech, violence, and discrimination so as to prevent their authoritarian exploitation. They have followed the approach developed by UN mechanisms, which is to consider any restriction on freedom of expression in light of the substantive unity of the ICCPR provisions and its governing principle of ultimately promoting the rights and freedoms of individuals.

Among the most important outcomes of these groups’ consultations are the 2009 [Camden Principles on Freedom of Expression and Equality](#), which provides a precise definition of hatred as “intense and irrational emotions of opprobrium, enmity and detestation towards the target group.” The Principles focus on “incitement” and “advocacy,” terms also used in the ICCPR, explaining that hate speech must include those elements as well as the emotions themselves; these are statements that “create an imminent risk of discrimination, hostility or violence against persons belonging to those [national, racial or religious target] groups.”

Official UN mechanisms responded quickly to the outputs of civil society organizations and began to build on them. The High Commissioner for Human Rights sponsored a round of expert consultations which resulted in the 2012

---

<sup>14</sup> AB and C v. Ireland, [GC], 25579/05, the European Court of Human Rights, 16 December 2010.

[Rabat Plan of Action](#), endorsed by the Commissioner in 2013. The Rabat Plan adopts the definitions set by the Camden Principles and goes a step further by formulating a guiding approach for their application by legislators and judges without prejudice to freedom of opinion and expression. (We address this in detail in the next section.)

The Human Rights Committee and the Committee on the Elimination of All Forms of Racial Discrimination, in its general comments Nos. [34](#) (2011) and [35](#) (2013), then explicitly advocated the adoption of the Rabat Plan of Action as a basis for interpreting ICCPR article 20.

In conclusion, we can say that UN and regional mechanisms, and even some leading national mechanisms, have developed reasonable definitions of the grounds for restricting freedom of expression which are consistent with the reality in which almost all societies now live. While taking into account states' sensitivities and concerns, these definitions do not compromise the essence of international human rights conventions. The definitions are available to legislators and judges, and can be relied on and adapted according to the requirements of local contexts when drafting or applying legislation. More importantly, the definitions form the basis for developing mechanisms and controls of limitations without prejudice to the essence of international conventions. Providing a democratic basis or justification for the restriction of freedom of expression necessarily determines the appropriate mechanism for implementing such limitations on the ground, as we discuss in the next section.

## **2. Mechanisms and controls for limiting freedom of expression**

ICCPR articles 5 and 19 set out the grounds or justifications for limiting freedom of expression but also outline its mechanisms and controls. The first paragraph of article 5 clearly stipulates that no limitation may aim at “the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.”

This double control is known as “proportionality” in some of the literature, while elsewhere it is divided into two controls, namely proportionality and non-prejudice to the content of the right. In this study we follow the approach of the UN Human Rights Committee, which sees one control—proportionality—in the article’s text.

Article 19 specifies two more controls, or conditions, stating that restrictions “shall only be such as are provided by law and are necessary.” These two controls are generally defined as “legality” and “necessity,” or “democratic necessity” in some of the literature.

Any discussion of these controls requires some detail because the wording is general, so disputes and judicial applications have generated various approaches to their interpretation—as happens for all domestic and international legislative texts. Detailed discussion is also needed because it is always easier to develop a democratic definition of a general principle in theory than to implement it on the ground.

We will not follow the order set out in the ICCPR to activate these mechanisms but the more logical order that imposes itself on the discussions of legislators and judges: the process of testing any restriction of rights and freedoms usually begins with the question of legal basis, then the question of necessity, and finally the question of whether the restriction is proportionate to that necessity. This arrangement shows how the elements of such mechanisms relate to each other. Proportionality is organically derived from the assessment of necessity, pursuant to the well-known jurisprudential and legal principle that “necessity shall be assessed,” and both, of course, must have a legal basis.

### **1.2.1 Legality**

This old principle is entrenched in all modern legal traditions and in contemporary constitutions. It emerges from the fact that the origin in civil or public transactions is permissibility or freedom. Such freedom cannot be restricted by any means without a declared, clear, and comprehensive legal text that specifies the mechanisms for appealing against that restriction or its effects.

This achieves what is known in jurisprudence as “legal certainty” or “legal security,” which allows an individual or group to regulate their conduct to comply with the law and avoid violating it.

Thus if a restriction of freedom of expression is stipulated in a law, regulation, or administrative decision, the standards of clarity and certainty must be met, especially if the text is punitive. This is not a purely technical aspect, for the legislators and judges must be aware of all the interests regulated by the law and the balance of power in order that the text reflect the principles of justice.

This has been emphasized by the Human Rights Committee. In paragraph 25 of its general comment No. 34 on article 19, for example, it stated:

A norm, to be characterized as a law, must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.<sup>15</sup>

The legality test therefore requires legislators or judges to ask the following questions:

- Does the legal basis exist in any form in the prevailing legal tradition (law, regulation, precedent, etc.)?
- Does the law clearly define the ground or justification for the restriction (by reference to the five controls mentioned in the previous section)?
- Does the law clearly define the nature of the acts it prohibits or punishes, their intent, and how to prove that they have been committed?
- Does the law clearly define and include the persons subject to its provisions?
- Does the law clearly set out the obligations of those subject to it, and the penalties for breaching such obligations?

---

<sup>15</sup> Human Rights Committee, 102nd session, General Comment No. 34, Article 19 - Freedom of opinion and expression, 12 September 2011, p. 9.

- Does the law clearly define the content, or elements, of the freedom it restricts?
- Is the law comprehensive enough to encompass all conceivable situations?
- Does the law establish mechanisms for grievance or appeal?

In terms of publishing, answering these questions gains increased importance when regulating exercise of freedom of expression online, given that the boundaries between social media administrators and users are not as clear as those between newspaper editors, journalists, and opinion writers. In practice, the definition of platforms, especially in Egypt, is not clear enough in the minds of legislators and judges—exclusively websites, or including, for example, applications for direct personal communication on a telephone? Nor can the obligations of online users be directly deduced by analogy with editors' or journalists' obligations, while mechanisms of investigation and proof may also differ radically between print and electronic publications.

### **1.2.2. Necessity**

After clarifying the legal basis in the aforementioned comprehensive sense, legislators and judges should move on to the necessity question: is this restriction necessary?

The assessment of necessity here must be derived from the definitions mentioned in the previous section. "Public order," "public morality," and "national security" are all defined as conditions allowing individuals to exercise the rights and freedoms set forth in the ICCPR, so any restriction that does not serve this supportive and liberative context is unnecessary. This is consistent with the principle of the substantive unity of ICCPR texts, as detailed above.

Jurisprudence calls this tendency "democratic necessity" or "necessary in a democratic society": in other words, **protection is conditional on the fact that the society is primarily democratic, and any practice, institution, or relationship which does not uphold this condition is not worthy of protection.** Democratic necessity is based on the second paragraph of article

29 of the Universal Declaration of Human Rights: “In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.”

When assessing the necessity condition, legislators and judges must therefore ask the following questions:

**First, does the practice, tradition, institution, or relationship that the legislation seeks to protect provide a context that allows parties’ personalities and moral sense to develop so that they can exercise their rights and freedoms?**

Practices that undermine individuals’ personal security or autonomy may not be subject to legal protection as components of public morality or order, even if they are still part of the common moral sense in some circles—such as circumcision, domestic violence, or customs that discriminate between males and females in inheritance or between citizens on the basis of religion. The protection of such practices runs counter to democratic necessity. Similarly, in contexts described as secular, banning religious rites that do not threaten public tranquility, certain items of clothing, or symbols that do not disdain others cannot be considered components of public morality or conditions necessary for the development of a democratic moral sense. Meanwhile, a very broad spectrum of what might be termed “neutral” practices which may help support individual autonomy and shape public morality, such as state economic policies, governance systems (as long as they are democratic), and electoral systems, all of which must be subject to full public debate without caveats.

**Second, assuming that the conditions for protection are met, is there an immediate threat to the subject of protection that can only be addressed by restricting freedom of expression?**

Approaches proposed to determine the urgency of a threat vary according to its bases. Methods for assessing a potential threat to national security, for example, are different from methods for assessing a potential threat to public

order or morality. Human rights jurisprudence has multiplied accordingly.

In the event that an urgent threat to public or public morality, or propaganda for war and advocacy of violence, discrimination, or hatred, is found, legislators and judges must identify five elements of the speech or action to assess its potential threat to the subject of protection. We derive these elements from the [Rabat Plan of Action](#):

- **Speaker's standing:** It is obvious that the impact of speeches by heads of state, government officials, or popular political and religious leaders will be different from that of the ordinary social media users, but legislators and judges can find it hard to assess social media users' influence, especially due to the phenomenon of "influencers," who may influence the convictions of audiences that might be larger than those of most political and religious leaders.
- **Speech content:** Does it include explicit incitement to certain acts that may breach public peace and morality as defined above, or is it just an opinion, criticism, question, or other speech act?
- **Speech purpose:** Even if the speech contains what can be classified as incitement, was this the speaker's intention? Intention can be determined by assessing the speaker's awareness of the references or metaphors contained in their speech and whether such references occurred in their prior speech acts.
- **Speech context:** If the speech contains explicit incitement and emanates from an influential speaker, is it possible, in light of social and cultural determinants, for that incitement to trigger immediate hateful acts? This can be inferred through precedents in the same or similar contexts.
- **Speech extent and frequency:** Is the speech echoed in a wide-ranging means of communication? Speech posted on a private account, for example, has different reach from speech broadcast on a leading media outlet.

As for assessing the urgency of a threat to national security, the examples set out in principle 9 of Tshwane Principles can be used as a guideline for limiting

a fundamental aspect of freedom of expression, namely accessing and imparting of information by any public means, as provided for in the second paragraph of ICCPR article 19. Principle 9 sets out five categories of information that governments may withhold as its disclosure may in some cases threaten citizens' security and thus their ability to exercise their rights and freedoms:

1. Information about ongoing defense plans, operations, and capabilities for the length of time that the information is of operational utility.
2. Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.
3. Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions against threats or use of force or sabotage, the effectiveness of which depend upon secrecy.
4. Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters.
5. Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.

These categories curb tendencies to over-interpret the concept of national security to include various information types, policies, and practices within its scope (such as the state's financial policies and economic orientations), which ultimately ends up criminalizing criticism of the government in general on the grounds that any criticism of any public policy could pose a threat to national security.

**Third, are restrictive measures in place and how effective are they? Is there a need for new measures?**

This step is of great importance in light of a general tendency to issue special laws to regulate freedom of expression online and special penalties for online

crimes. Freedoms exercised in the physical sphere are subject to the same legal protection in the virtual sphere, so if any of these freedoms are subject to limitations that comply with the preceding conditions in the physical sphere, there is no need to introduce further restrictions on them in the virtual sphere—unless aimed at providing double protection for these freedoms.

More than one UN mechanism has expressed deep concern about the opposite tendency in most countries, that is, to regulate freedom of expression online through separate laws, which usually harshen penalties and not vice versa.

In fact, all laws regulating freedom of expression in general contain forms of limitation that are sufficient to restrict any form of expression that poses a threat in line with democratic necessity. Some of these laws apply to material more widely disseminated than material circulated on social media, such as television broadcasts, religious sermons, and educational curricula. As speech of such wide dissemination is regulated by existing laws, there is no logic in subjecting speech on social media to separate laws under the pretext of its wide dissemination, especially since such speech is not different in either content or form.

### **1.2.3. Proportionality**

If the legal basis for a restriction is confirmed and its democratic necessity is determined in the form of an existing threat to certain rights or to the context supporting the exercise of rights, the final step is to assess whether restriction measures are proportionate to the magnitude of the perceived threat.

There is no single agreed approach to assessing this proportionality, but various approaches have common ground. Some texts define proportionality as following the method of least intervention, but this is highly abstract and requires the identification of concrete indicators of minimal intervention. While the Human Rights Committee does not bind signatory states to a single methodology or test to assess proportionality, the European Court of Human Rights and several regional courts follow approaches that differ according to the right to be restricted, as do other European institutions such as [the Coun-](#)

[cil of Europe](#).<sup>16</sup> Many of these institutions and courts also combine tests of proportionality with tests of necessity or, conversely, devote a special space to an independent test of non-prejudice to the content of the right.

By reading these approaches in comparison, we propose five integrated steps to assess the proportionality of restriction measures to the magnitude of the perceived threat.

**First, is the punishment prescribed proportional to the nature of the crime?**

This is the simplest and clearest form of proportionality, since a crime consists of various acts, each of which must be punished in proportion to its magnitude. Planning, for example, is different from incitement to commit a crime, and both are different from the crime's execution. The law should establish different penalties proportional to the roles of the accused in each stage of a crime, as someone who only participated in its planning cannot be penalized in the same way as those who committed it. The planning is different from the crime itself, while an ancillary or predicate crime (one component of a larger crime) is different in turn—for instance, damaging property when an assassination attempt is made against a state official. Dropping the distinctions between these acts is the clearest violation of the principle of proportionality. An example of this is applying the same penalty to the various parties who instigated, planned, carried out, or financed a particular crime, without regard to the impact of each of act.

**Second, is the scope of the restriction reasonable?**

Restrictive measures are to be designed carefully to ensure that they target parties and acts that pose a threat to the protected subjects and not others. For example, blocking an entire website that circulates discriminatory speech is not proportionate to the perceived threat as it blindly treats all users and employees of the site as the same and punishes the vast majority who pose no

---

<sup>16</sup> Particular mention may be made here of the detailed steps proposed by the Council of Europe's Guide to Action on the interpretation of article 9 of the European Convention on Human Rights on the right to freedom of expression. Dominika Bychawska-Siniarska, *Protecting the Right to Freedom of Expression Under the European Convention on Human Rights*, Council of Europe, July 2017.

threat to the protected subject. Indeed, all the legal mechanisms we reviewed warn against blocking websites as a blind mechanism that violates the rights of most users. [The 2022 report of the High Commissioner for Human Rights](#), a comprehensive review of internet shutdowns, excludes from this warning sites dedicated to fraud, sexual exploitation, and other already criminalized practices.<sup>17</sup> The 2024 UN Convention against Cybercrime does not propose blocking as a preventive mechanism.<sup>18</sup>

The same criterion applies to punitive provisions, especially custodial ones. Legislators and judges should question the feasibility of imposing huge financial or custodial penalties for very common morally unacceptable practices committed daily on a large scale. On social media these include insults, slander, and obscene language, publishing material that the majority considers pornographic, disgusting, or repulsive, republishing rumors or false news, calling for non-respect for traffic rules or public morals, and ridiculing religious values or beliefs revered by the majority or certain minorities. Excessive criminalization of such activities would increase the number of criminals to unimaginable limits. Would excessive financial penalties or depriving those involved of their liberty act as a deterrent or it would it just put perpetrators at risk without much reducing the problem? Would it be better to confront these activities through public dialogue, and for state institutions and civil society to proactively support and promote democratic values?

### **Third, does the restriction take into account vulnerable parties' interests?**

An equally important consideration relates to guarding against the expansion of restrictive practices toward parties more likely to be vulnerable in our society, such as children, women, religious and ethnic minorities, refugees, migrants, people with disabilities, and those with less access to education and general culture. All types of people are now daily users of social media and it is inconceivable that everyone can be aware of all the rules to be followed

---

17 UN High Commissioner for Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, Human Rights Council, fiftieth session, 13 May 2022.

18 Report of the Third Committee, Combating the use of information technology. op. cit., p. 43.

when posting, especially since we are not talking about clear crimes such as theft, fraud, or frequent incitement to violence.

The broad criminalization of certain speech and acts, even strictly defined by law, may target vulnerable users more than those with more privilege. The clarity of a law (assuming it is clear) cannot be invoked here, since the issue is structural disparity in users' knowledge and capabilities. Thus, excessive criminalization of morally reprehensible acts, or acts that contradict the pursuit of democratic values and ethics, means in practice reinforcing discrimination and marginalization of many groups.

In recent years legal texts on cybercrime have sought to deal with a wide range of perpetrators as victims or vulnerable parties, encouraging state institutions and civil society to adopt non-punitive measures to consolidate controls on social media use. Article 53 of the UN Convention against Cybercrime, for example, proposes a long list of preventive measures aimed at raising public awareness of internet use controls and proactively protecting marginalized groups from engaging in online criminal activities through positive, non-punitive interventions by state institutions and civil society.

#### **Fourth, are the resources allocated to the restriction reasonable?**

Linked to the above two conditions is the need for proportionality between the resources allocated for a restriction and the size of the perceived threat. Disproportionate measures include the establishment of special courts and the allocation of specific circuits from existing courts, which creates financial and administrative pressures and consumes judges and prosecutors' time and effort to counter practices that can be countered in less costly and more effective ways. Such measures eat into the financial and human resources available to face the most serious and urgent threats.

It is not necessary, for example, to transfer the crimes of insult, slander, and defamation away from the framework of civil courts, or to consider them crimes of public law, due to the above-mentioned prevalence of these practices and the great pressure they would place on the public prosecution and criminal courts.

### **Fifth, does the restriction prejudice the content of the right?**

This requirement is explicitly stated in ICCPR article 5 and repeated elsewhere in the Covenant in relation to the conditions for restricting rights. The content of the right is, in short, the powers and immunities the legal text grants to the right holder, which are usually expressly mentioned in that text. In the event of disagreement over interpretation, treaty committees are to clarify these elements in their comments and judgments.

Article 19 clearly defines the content of freedom of opinion and expression in its first and second paragraphs:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Thus, no restrictive measure may directly limit individuals' ability to form opinions, seek, receive, or impart information in any form. Blocking websites, for instance, is a clear example of a restrictive measure that violates the content of the right to freedom of expression by depriving the public of one of its essential elements, namely the receipt and circulation of information. Other punitive measures that are not allowed because they prevent those subject to them from exercising basic elements of freedom of expression include prohibiting the use of social media for a period of time, closing online accounts, or blocking content produced by those being punished. The removal of content that incites violence or discrimination or defames a person is not a violation of the content of the right, as such removal is necessary to alleviate the damage caused by the crime, provided that it does not stretch to depriving the content's producer from exercising their right to freedom of expression in future. In the case of a custodial penalty, it should not include depriving the detainee of reading or communicating with newspapers, accessing social media, or other customary rights of detainees.

While following these steps when defining the grounds and justification of a

restriction— assessing its legality and necessity and the extent to which its measures are proportional to this necessity—will not definitively eliminate disagreement between legislators and judges over the grounds and mechanisms for restricting freedom of expression online, failure to follow them invites arbitrary interpretation and the legalization of personal whims and convictions. Here we aim to control the practice; resolving the disputes is beyond the competence of this study. Following the steps above will lead to a disciplined practice with broad societal acceptance and higher legitimacy.

## **2. Case study: The Anti-Cyber and Information Technology Crimes Law**

### **2.1. The context of the promulgation of the law and its effects**

Since 2000 successive legislative and executive authorities in Egypt have adopted legislative frameworks to regulate online expression in conjunction with the expansion of internet use and its permeation into all aspects of civil and political life. The 2003 [Telecommunications Regulation Law No. 10](#) was issued mainly to regulate the technical aspects of internet use, such as licensing rules, permits, and spectrum management, in addition to establishing an internet governance framework, the most important element being the National Telecom Regulatory Authority (NTRA). The law includes punitive provisions in chapter 7, most having to do with crimes related to the destruction of telecommunications infrastructure (article 71), the establishment and operation of a telecommunications network without license (article 72), the interception of radio waves (article 74), and other acts not necessarily related to content published.

However, the penal section of the law criminalizes certain practices that violate users' privacy or one of the grounds mentioned in the ICCPR, specifically national security. Article 73 of the law punishes with imprisonment and a fine anyone who broadcasts the content of messages circulating through means of communication or user data, which is considered a crime for infringing on

the right to privacy. Article 77 also punishes with imprisonment and a fine anyone who imports or manufactures telecommunications equipment without a license, and increases the penalty if the purpose is harming national security.

Article 76 punishes with either imprisonment or a fine of between LE500 and LE20,000, or both, whoever:

1. Uses or assists in using illegitimate means to conduct telecommunication
2. Premeditatedly disturbs or harasses a third party by misusing telecommunication equipment

The law shows that the initial quest to regulate online expression in Egypt was shaped by two contradictory tendencies. The dominant tendency was to provide a regulatory framework that facilitates internet service, codifies its governance, and protects and promotes some users' rights, especially the right to privacy and data protection, in a way that would support investment in the sector and facilitate its use for commercial purposes. The other, more reticent tendency was to fear that the open space of the internet would be exploited to commit acts that harm or prejudice national security; the law does not clarify what is meant by this, but its wording suggests that the intention was primarily to combat espionage or the use of the internet to facilitate terrorism.

The predominance of the regulatory and supportive tendency is evident in the fact that the legislators did not curb individual users' online freedom of expression, with the exception of article 76, almost exactly copied from article 166 (bis) of the Penal Code on the use of the telephone to disturb others. It was the following years that would reveal the internet's broad potential for political mobilization and shaping public opinion; at the time, restricting freedom of expression online was not an urgent concern for lawmakers.

State focus on security increased between 2011 and 2013, and the tendency to support internet users' rights was almost completely set aside. Security concern came to be a governing principle of legislation dealing with online expression. As it became the main medium of political mobilization, those years revealed the internet's enormous potential in shaping and interacting with public opinion. The ruling elite that came to power in July 2013, seeking to

restore “stability” at all costs, had its own approach to regulating social media use and saw the internet as a threat to its goal of stability.

The [Anti-Terrorism Law](#) No. 94 of 2015 was issued in this context, legalizing the blocking of websites and social media pages. Article 29 introduced a new crime known as “creating and managing websites with the aim of promoting ideas and beliefs calling for the commission of terrorist acts” and article 49 allowed the Public Prosecution or the competent investigative authority to block websites as a precautionary measure.

This was followed by the issuance of [Law No. 180 of 2018](#) (the Press and Media Regulation Law), reflecting the general fear of internet users. Article 4 empowered the Supreme Council for Media Regulation (SCMR) to prevent the import, circulation, or display of publications, newspapers, or media or advertising materials issued or broadcast from abroad due to “national security considerations.” It also allowed the SCMR to prohibit “the circulation of pornographic publications or materials, or those addressing religions or religious doctrines that are liable to disturb public peace or incite discrimination, violence, racism or hatred.” Article 10 prohibited restrictions that would impede the provision or availability of information, equal opportunities between print and electronic newspapers and broadcast media, or their right to information, but without prejudice to “the requirements of national security or the defence of the homeland.” Article 19 codified the SCMR’s authority to block websites if a newspaper, media outlet, website, or personal account with more than 5000 followers “publishes or broadcasts false news or what calls for or incites breach of law, violence or hatred, or involves discrimination between citizens, or calls for racism, or includes defamation, insult or defamation of individuals, or disdains the monotheistic religions or religious beliefs.”

Despite its clearly restrictive orientation, the Press and Media Regulation Law did not break away from the constitutional controls that prohibit custodial penalties for crimes committed through publication and publicity, which inevitably includes online publication. Article 29 reaffirms article 71 of the Constitution, which stipulates that “no custodial penalty shall be imposed for publication or publicity crimes, except for crimes related to incitement of vio-

lence, discrimination between citizens, or defamation of individuals.”

Also in 2018, however, came [Law No. 175 on combating information technology crimes](#) (the Cybercrime Law), further controlling online expression and limiting freedom of expression in general as much as possible by using all punitive means and tools, even those in violation of the Constitution. This law crystallized and made explicit the new ruling elite’s vision of the internet as a threat.

That vision was evident in the earliest stages of drafting the legislation. In 2015, the year the Anti-terrorism Law passed, the Cabinet formed a committee to prepare a law on information technology crimes. It discussed a first draft, on which EIPR and other human rights organizations commented,<sup>19</sup> but then discussions stalled. In May 2016, the Parliament’s Defense and National Security Committee submitted a proposal drafted by committee member and MP Tamer Al-Shahawi explaining that the philosophy and objectives of the law were part of “the mission entrusted to the House of Representatives, being the legislative authority, and in connection with the successive threats to Egyptian national security in all local, regional, and international circles, and in view of the changing nature of threats in recent years and their reliance on modern information technologies and cyberspace.” The committee said it was therefore necessary to “develop legal frameworks and legislation to ensure the protection of the state from all threats in this regard.”<sup>20</sup>

After the House of Representatives drafted the final version of the law, its objectives and philosophy were outlined in a 2018 report prepared by a joint committee of members of the committees of Telecommunications and Information Technology, Constitutional and Legislative Affairs, and Defense and

---

19 EIPR, Association for Freedom of Thought and Expression (AFTE), Support for Information Technology Center, “Anti-Technology”, op. cit.

20 Masaan Technology & Law Community, Legislative Contexts for Passing Internet Laws, 18 April 2022; Available at: <https://masaar.net/ar/%D8%A7%D9%84%D8%B3%D9%8A%D8%A7%D9%82%D8%A7%D8%AA-%D8%A7%D9%84%D8%AA%D8%B4%D8%B1%D9%8A%D8%B9%D9%8A%D8%A9-%D9%84%D8%A5%D9%82%D8%B1%D8%A7%D8%B1-%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86-%D8%A7%D9%84%D8%A5/>.

National Security.<sup>21</sup> Objectives included:

- Combating the illegal use of computers, information networks, and information technologies and related crimes, while accurately determining punishable acts.
- Establishing rules, provisions, and measures to be followed by service providers to secure the provision of communication services through information technology, and determining their related obligations.
- Protecting personal data and information from exploitation offensive to its owners, especially as traditional criminal texts on the protection of individuals' privacy and the sanctity of their private lives were insufficient in dealing with threats and risks created by the use of information technology.
- Protecting government data and information, and the information systems and networks of the state and public legal entities from interception, penetration, tampering, destruction, or disruption.

The law clearly reflects the internet-as-threat approach. Starting with its definitions, it broadened the justifications for restricting freedom of expression online so that the restrictions became tighter than in any previous authoritarian context in Egypt. For example, Article 1 of the Law defines “national security” as follows:

Anything related to the independence, stability, security, unity, and safety of the country as well as to the affairs of the Presidency of the Republic, the National Defense Council, the National Security Council, the Ministry of Defense and Military Production, the Ministry of Interior, the General Intelligence Service, the Administrative Control Authority, and the bodies thereof.

The second chapter of the law included the first procedural regulation of blocking websites and pages. Article 7 allows the investigating authority to block websites not only due to ongoing investigations, as in the case of the Terrorism Law, but “if there is evidence that a website, broadcast from inside

---

<sup>21</sup> Ibid.

or outside the country is displaying words, numbers, images, films, any publicity or other materials that would be an offence of those stipulated in this law, jeopardize the national security or economy.”

Alongside article 8, article 7 elaborates on the procedures for blocking websites and the mechanism for appealing against such decisions.

The law's third chapter deals with crimes committed using information devices, networks, or systems, such as those related to bank cards or private life or that occur on an information system owned by an individual or the state, such as hacking emails or websites, and relevant penalties.

The same chapter includes a special part on crimes violating the sanctity of private life, which tried to keep pace with the emerging violations of the right to privacy, such as surveillance, electronic extortion, and defamation. Article 25 states:

Anyone who infringes a family principle or value of the Egyptian society, encroaches on privacy, sends many emails to a certain person without obtaining his/her consent, provides personal data to an e-system or website for promoting commodities or services without getting approval, or publishes, via the information network or by any means of information technology, information, news, images, or the like that infringes on the privacy of any person involuntarily, whether the published information is true or false, shall be punished by imprisonment for no less than six months and a fine of no less than LE50,000 and no more than LE100,000 Egyptian, or by one of these two penalties.

Article 26 also punishes with between two and five years' imprisonment and a fine of between LE100,000 and LE300,000, or one of the two penalties, anyone who deliberately uses an information program or technology in processing a third party's personal data to connect it with abusive content or display it to the detriment of that party's reputation.

Article 34 stipulates imprisonment if an offence is committed with the aim of disturbing the public order, jeopardizing the safety and security of soci-

ety, harming national security or the economic position of the country, obstructing or hindering the work of public authorities, suspending the provisions of the Constitution, laws, or regulations, or compromising national unity or social harmony.

The law's penal articles expanded the scope of criminal responsibility, stipulating that

in cases other those stipulated herein, anyone who creates, manages, or uses a website or a private account on an information network for the purpose of committing or facilitating a punishable crime shall be punishable by imprisonment for no less than two years and a fine of no less than LE100,000 and no more than LE300,000, or by one of these two penalties.

## **2.2 Grounds and mechanisms for restricting freedom of expression in the law**

In this part of the study, we apply the framework proposed in section 1 to the texts and applications of the Cybercrime Law with the aim of generating proposed amendments that reduce the authoritarian nature of its articles as much as possible and bring them closer to the normative democratic framework. Many local and international human rights organizations have already commented on the law, during its preparation, discussion, and/or after its issuance; several of them also filed cases before the Supreme Constitutional Court disputing the constitutionality of some of its articles. Together these cases amount to a detailed explanation of how the articles contradict the current Egyptian Constitution. Here we point to those criticisms we agree with and rely in particular on the appeals against articles [25](#) and [27](#) published on the website of Masaar, a group of lawyers and technologists promoting digital rights and related freedoms in Egypt. We try to accommodate these organizations' criticisms within our proposed framework in such a way that pinpoints the logical links between them and that will facilitate their use in proposals to repeal or amend other laws in a systematic manner.

### 2.2.1 Legality

**First, does the law clearly define the basis or justification for the restriction (by reference to the five grounds mentioned in section 1)?**

Some articles of the law are based on the traditionally common legal practice in Egypt, influenced by Roman/civil traditions, of considering the preservation of “public order,” public morality,” and “national security” legitimate grounds for restricting freedom of expression online. The law refers to these grounds in articles 7, 26, and 34. In this regard it does not violate the Constitution or the ICCPR, provided that these grounds are interpreted in the light of the substantive unity of ICCPR provisions and the Constitution, as well as the general principle governing them, which is the protection and promotion of the rights and freedoms of individuals and civil and political groups. The jurisprudence of Egyptian supreme courts contain several precedents that interpreted such grounds without prejudice to this principle.

However, unlike other relevant laws promulgated around the same time, as listed section 2.1, the Cybercrime Law foreclosed democratic interpretation of some of the grounds and added further grounds for restriction that are contained in neither the Constitution or the ICCPR and have no precedent in the Egyptian legal tradition, including laws overturned by the Supreme Constitutional Court.

Its first article on definitions provides a very broad definition of “national security,” with no concrete objective criterion, effectively allowing the Public Prosecution and the judiciary to criminalize various forms of expression. It defines national security as everything related to “the independence, stability, security of the homeland and the unity and territorial integrity of its territory.” It also states that discussion of the affairs of certain executive bodies may prejudice national security, without specifying which type of “affairs.” In practice this means criminalizing criticism of these bodies. The article further states that national security includes “everything related to the affairs of the Presidency of the Republic, the National Defense Council, the National Security Council, the Ministry of Defense and Military Production, the Ministry

of Interior, the General Intelligence Service, the Administrative Control Authority, and the bodies thereof.” Unlike the examples proposed in the Tshwane Principles, it does not refer to specific information held by these bodies or to specific decisions they make.

The grounds created by the law include the “family principles and values of Egyptian society” (article 25), “safety and security of society,” “national unity,” “social peace,” and “the economic position of the country” (article 34).

Examples of such grounds of restriction cannot be found in either the ICCPR, which lists only five grounds, or in the current Constitution, which does not depart from the ICCPR limitations—as in its restriction of freedom of expression in cases of incitement to hatred, violence, discrimination, or defamation (article 71).

In seeking to increase the justifications for restriction, the legislators ignored the Egyptian Supreme Constitutional Court’s invalidation of similar phrases in other laws, such as in Law No. 33 of 1978 on “the protection of the home front and social peace,”<sup>22</sup> and the Egyptian Parliament’s deletion of almost the same phrases from the Penal Code under [Law No. 147 of 2006](#).

In general, the judgements of the Supreme Constitutional Court do not depart from the standards established by international human rights law when testing a law’s legality. In 1997, in its judgment in lawsuit No. 84 of judicial year 17, the court put it clearly:

Since the real scope of the principle of legality of crimes and penalties is determined in the light of two guarantees that ensure its purposes, first: the penal texts shall be worded in a clear and specific manner that is not vague or ambiguous, so that these texts do not become like nets or traps that the legislator set to hunt—through their breadth or concealment—those who fall in them or misposition them. It is a guarantee that those who are addressed by punitive texts shall be aware of them, so that their

---

22 Supreme Constitutional Court’s Ruling No. 56 of judicial year 6 on the constitutionality of Article 44 of Law No. 33 of 1978 on the protection of the home front and social peace, 21 June 1986

behavior is not contrary but in harmony and in compliance with them.<sup>23</sup>

As explained in section 1, longstanding jurisprudential and judicial traditions hold that the terms “public order,” “public morality,” and “national security” can be interpreted as referring to the contexts necessary for individuals to exercise their fundamental freedoms and rights. Despite their ambiguity they are general and flexible enough to be interpreted accordingly, as we saw above in Indian and South African supreme court rulings. The new grounds in the Cybercrime Law are so abstract that it is impossible to subject them to such an interpretation, which would be consistent with the Constitution and international laws.

How can the phrase “the economic position of the country,” for example, be interpreted? What is the objective criterion for identifying an “economic position of the country” so that it can be decided whether it is threatened or not when assessing the necessity of a restriction? Does the phrase refer to the country’s position on the global economic indexes that determine its ability to attract investment and grants? Or to a particular economic system, as stated in the second chapter of the Constitution, titled “Economic Components”? It is unclear, and clarity is essential for moving on to test necessity and proportionality.

As for “the family principles and values of Egyptian society,” does this mean a specific set of values that a majority of Egyptians revere regarding family relations? If so, how does it differ from the broader concept of “public morality,” which necessarily encompasses such family values? Or does it mean a particular form of family, a nuclear family based on heterosexual marriage? If this is what is meant, deviation from it is already criminalized in the Penal Code and other laws under more disciplined terms (our own position on criminalizing such deviance is not within the scope of this discussion). Confusion around this ambiguous concept is reflected in the citations of the courts that have applied the law: as they did not find anything to help them determine the meaning in the preparatory works or previous higher court rulings, they

---

23 Supreme Constitutional Court’s Judgment No. 84 of judicial year 17, 15 March 1997.

resorted to the weakest source, namely jurists' writings. The rulings of the economic courts cite a single paragraph from a single, modern jurisprudential source, written to explain the law and comment on its provisions: Counselor Bahaa al-Marri's 2019 book, the title of which translates as *Explanation of the Anti-Information Technology Law and the Authenticity of Digital Evidence in Proof*. For example, the Cairo Economic Court says in its judgment in Misdemeanor No. 633 of 2022 (Cairo Economic Misdemeanors):

The material element of the crime of infringing on any of the family principles and values of Egyptian society lies in the use of information technology, information networks, or the internet to broadcast, send, or address individuals in a way that destroys family bonds, belittles positive action for the family, induces disharmony among its members, or undermines the controls and principles that govern it. Material behavior in this form also occurs by publishing via the internet, social media, email, or any electronic method anything that favors or calls for insincerity, dishonesty, disrespect for parents or chastity, or calls for destroying the value of science and religiosity, whether directly or indirectly, and whether by an article, electronic message, visual or audio material, drawing, caricature, series, or film, as long as the publication is through information technology... the matter of whether or not the perpetrator's behavior infringes on the family principles and values is subject to the discretion of the trial judge, who concludes it in light of the values and principles of the Egyptian family that have settled in people's minds and that people have become familiar with.<sup>24</sup>

This increased the ambiguity by adding new general concepts also requiring interpretation that are perhaps more haphazard and arbitrary than the concept of "family values and principles" itself, such as "positive action for the family" and chastity. In order to get out of this interpretive dilemma, the paragraph gives unprecedented power to the trial judge to interpret a punitive legal text in light of "what has settled in the minds of the people." This violates

---

<sup>24</sup> Cairo Economic Court's Judgment (Third Circuit - Economic Misdemeanors) in Misdemeanor Case No. 633 of 2022, 31 May 2022.

the standards established by Egypt's Supreme Constitutional Court and all international human rights standards as detailed in section 1.

**Second, does the law clearly define the nature of the acts it prohibits or criminalizes, their intent, and how to prove it?**

The ambiguity in defining the grounds for restricting freedom of expression in the Cybercrime Law led to similar ambiguity in determining the acts to be criminalized and their intent. This ambiguity is multifaceted.

First, it is unclear whether the act criminalized in article 25 (“infringing a family principle or value of the Egyptian society”) is infringement on family values and principles in general or on the privacy of individuals in particular, as one family value or principle. The title of this chapter of the law (III) cites “crimes related to the sanctity of private life,” and the rest of the crimes it lists are in fact related to acts of infringement on individuals’ private life, such as “sending many emails to a person without his consent,” “giving data to a system or website to promote goods or services without the consent of the person,” “publishing information, news, images and the like, that violate the privacy of any person without his consent, whether the published information is true or untrue,” and “using an information program or technology to process the personal data of others to link it to content contrary to public morals or to show it in a way that would prejudice the person’s status or honor.” These examples suggest that the criminal act is an infringement on individuals’ privacy. The legislators may have been thinking of common practices on social media, such as sending someone unsolicited sexual content, but if so that could have been stated clearly.

This ambiguity has produced contradictory judicial applications. The conduct of the Public Prosecution has often contradicted that of the courts. In some of its rulings the Economic Court has taken a strict approach to interpreting the article which has resulted in acquittal due to lack of clear criminal intent, as in the ruling of the Cairo Economic Court in misdemeanor No. 246 of 2020,

known as the first “TikTok girls” case.<sup>25</sup> At other times the court has interpreted the text as criminalizing all acts that “outrage public decency” or public morality, and thus as an interpretation of the relevant provisions of the Penal Code, as is in its judgment in misdemeanor No. 633 of 2022.

The Public Prosecution has consistently considered all acts classified as outrageous “public decency or public morality” and even insult and slander as “infringement on family principles and values of Egyptian society.” In practice, this increases penalties without a clear textual basis; the crime of insult and slander, for example, is not punishable by imprisonment in the Penal Code except in specific cases. This is a flagrant violation of the principle of criminal legality, which is constitutionally protected in article 95: “there shall be no crime or punishment except pursuant to a law.”

Second, it is difficult to determine the nature of the criminal acts that pose a threat to national security, which are punishable by imprisonment under article 34, taking into account the breadth of the concept. For example, is the eligibility and competence of those who assume posts in the executive bodies listed, and the rules for their selection, among the “affairs” prohibited from discussion? How can such discussion be considered a breach of national security? How can legal security or certainty be ensured in light of this law’s unprecedented scope?

Third, article 27 does not distinguish between planning and committing crimes through an electronic account, thus requiring interpretation by prosecutors and judges. Masaar has drawn attention to this ambiguity, explaining that the crime of “managing, creating, or using an account” is a preparatory act that should not be criminalized unless it is intentional or dangerous.<sup>26</sup> “Danger crimes” pose a general threat to individuals’ security—such as possessing weapons without license or putting children in conditions that threaten their safety or expose them to a possible crime—even if they do not result in direct harm to life and property, and they may be punished whether or

---

25 Cairo Economic Court (Third Circuit - Misdemeanor Appeals), Misdemeanors No. 246 of 2020 and No. 479, 12 January 2021.

26 Masaar Technology & Law Community, Legislative Contexts, *Ibid.*

not damage occurred.<sup>27</sup> For example, the founders of a site dedicated to an unlicensed arms trade, or the founders and users of a site dedicated to posting child pornography, regardless of the direct harm inflicted, could be punished.

This distinction is pivotal because if a crime is unintentional it does not exist unless harm is achieved; therefore there is no attempt or preparation for it that requires punishment. If it is a “crime of damage” that directly affects certain individuals, the penalty for attempting and preparing for it must be strictly proportional to the nature of the harm caused and not defined in absolute terms regardless of that nature.

The danger of the general and stretchy wording of article 27 becomes clear here because it does not distinguish between crimes. It applies itself to any “crime punishable by law,” whether the crime is intentional or not, harmful or dangerous, or mentioned in this law or not, including crimes that are not punishable by confinement. It is neither reasonable nor logical to have a legal text that stipulates confinement for a period of not less than two years for a crime normally punishable by a fine—such as insult and slander. Again, this is the creation of a criminal punishment without a clear and specific legal text, in clear violation of article 95 of the Constitution.

This lack of reasonableness has not prevented the Public Prosecution from referring people to trial on charges of “using an electronic account” to commit a very wide range of crimes, in what appears to be an attempt to intimidate social media users, especially those who have accounts with many followers.

**Third, does the law clearly and comprehensively define the persons addressed by its provisions and their obligations?**

Confusion and ambiguity extend to this point as well, especially in article 27 of the law. As with article 25, the text contradicts the title of the chapter that contains it. Article 27 is in chapter 4, on crimes “committed by a site administrator,” but it includes punishment for “users” of sites and accounts.

---

<sup>27</sup> Mahmoud Naguib Hosni, *Explanation of the Penal Code “General Section: The General Theory of Crime and the General Theory of Punishment and Precautionary Measure”*, University Press, 2017, p. 317.

The limitation of those subject to the article to site administrators can also be inferred from the other articles in the chapter (articles 28 and 29), which define their subjects as “any person in charge of managing a site, a private account, an email, or an information system” in the context of the crimes of tampering with evidence or exposing the site or account to one of the crimes stipulated in the law. Article 11 of the law’s executive regulations also speaks exclusively of the obligations of site administrators.

This contradiction is likewise reflected in the contradictory conduct of the Public Prosecution and the courts. The Public Prosecution has generalized the accusation and referred those accused of a very wide range of crimes to the Economic Court on the charge of “using an electronic account.” In the vast majority of cases the court has then acquitted defendants of this accusation, since the article provisions apply to site administrators rather than users; it deduces this from two facts: the article is in the chapter on the crimes of site administrators and the executive regulations mention site administrators, suggesting that the legislators did not intend to criminalize users.

The Cairo Economic Court followed this deductive approach in Case No. 1592 of 2021, for example, in which Hossam Bahgat, executive director of the EIPR, was accused of using an electronic account to commit the crime of “insulting the National Election Authority.” The court’s reasoning was as follows:

The defendant, as evident by lawsuit documents, is a user of a private account on social-media sites Facebook and YouTube, whose status as per the terminology specified by the mentioned law is a user of a private account within social media sites Facebook and YouTube, his crimes are not categorized under those of a website administrator which were specified by article 27 of the mentioned law, as this article has addressed website administrator with his identifying description pre-specified and whose competencies and obligatory procedures that he must follow and implement were confirmed by the executive regulations of the law in articles 2, 3, and 11. Especially as the defendant in this lawsuit as a user of an account on social-media site Facebook or any natural person who has a private account on social-media sites doesn’t have the competency

to implement what articles 2 and 3 of the above-mentioned executive regulations require, and by which the court concludes as per the preset rules that those concerned with applying the provision of article 27 of the mentioned law are website administrators, and managers of CIT service providers which own, manage, or operate critical information infrastructure, as for the crimes they commit in person or by their supervisory status specified by the aforementioned article.<sup>28</sup>

In a few other cases, however, the court has considered the user of a private account to be a “manager or creator” of a website if it is proven that the account was created specifically to assist in a crime. The Cairo Economic Court followed this approach in its judgment in Case No. 256 of 2020, finding that the defendant’s personal Facebook account was created specifically to facilitate human organ trafficking, and the defendant was therefore subject to the article.<sup>29</sup>

This contradiction between the Public Prosecution’s and the courts’ approaches is caused by the ambiguity of the article and its failure to identify the subjects of its provisions, robbing it of one of the most important conditions for its legitimacy.

### 2.2.2. Necessity

**First, does the practice, tradition, institution, or relationship that the legislation seeks to protect provide its parties with a context that allows their personalities and moral sense to develop so that they can exercise their rights and freedoms?**

The extreme ambiguity in defining the grounds of restriction and the subjects of criminal protection in this law leads to the impossibility of determining

---

28 Cairo Economic Court (Third Circuit - Economic Misdemeanors), Misdemeanor No. 1592 of 2021, 29 November 2021.

29 Cairo Economic Court (Third Circuit - Economic Misdemeanors), Misdemeanor No. 256 of 2020, 31 January 2021.

whether the protection of these subjects is a legislative necessity in the first place. If neither legislators or judges are able to define what is meant by “family values and principles” or “the economic position of the country,” how can it be decided whether a particular act represents a threat to them? This ambiguity invites arbitrariness, partiality, and capricious judgments. More seriously, it may function as a back door for using “social peace,” “national unity,” or “family principles and values” to protect practices criminalized in other laws. These include domestic violence and discrimination between citizens based on local customs, especially in terms of religious freedoms. Thus, the standard of “democratic necessity,” which holds that protected values, practices, and relationships must be necessary to form a context that allows everyone to exercise their rights and freedoms, may collapse and the opposite context be achieved.

**Second, do criminalized acts pose an immediate threat to the subject of protection that can only be addressed by restricting freedom of expression?**

Neither the law, its executive regulations, the prosecution’s referrals, nor the judicial applications provide any standard to assess the threat that the acts criminalized in the law pose to any subject of protection. We can only refer to the report of the joint parliamentary committee that drafted the law, although it has no serious discussion of the need to include such restrictions in legislation aimed at “protecting internet users” but instead general and abstract phrases about the need to “combat the illegal use of computers” and “protect government and personal data and information” without specifying the threat(s).

Neither the referral orders nor the Public Prosecution statements that often accompany them when bringing the charge of infringement of “the principles and values of Egyptian family” have assessed the status of the defendants, the content and intent of their speech and practices, or the context, extent, and frequency of these practices. The law also lacks any criterion to assess the urgency of the threat posed by an act that the Public Prosecution deems a violation of national security. It gives no examples of information whose disclosure would constitute a violation or of decisions whose discussion is prohibited.

The Cybercrime Law's criminalization is in fact absolute, in contrast to related laws. Law No. 180 of 2018 regulating the press and media, for example, stipulates an arbitrary consideration in assessing the status of a content creator: an account must have 5000 followers (article 19) in order to impose penalties for the crimes it lists. The Anti-Terrorism Law No. 94 of 2015 punishes with a fine (article 35) "whoever intentionally, by any means, publishes, broadcasts, displays, or promotes false news or statements on terrorist acts inside the country or anti-terrorism operations contrary to the official statements released by the Ministry of Defense." The Cybercrime Law is devoid of any standard, even if arbitrary, and its articles 25, 27, and 34 criminalize the acts of any user if the judge sees them as a threat to any of the grounds given.

This inability to determine necessity has resulted in a tendency to apply the law arbitrarily. While the Public Prosecution refers a large number of defendants to trial based on what it deems a threat to the subjects of protection contained in the law, without considering the previously explained differences, court rulings are selective or contradictory in determining the extent of the threat, and no specific standard can be derived from them. The Cairo Economic Court for example, in its judgment in Case No. 633 of 2022, considered a Facebook user's offer to present himself as muhallil (a man who marries a divorced Muslim woman and divorces her so that she can return to her ex-husband) as an immediate threat to the family values and principles of Egyptian society, but its ruling in Case No. 246 of 2020 did not consider a TikTok user's call for girls to have direct private conversations with young men through a specific application as a threat to the same values. In neither case was a standard present, and the rulings were devoid of any assessment of the extent of the threat.

**Third, are restrictive measures in place? If so, how effective are they? Is there a need for new measures?**

As mentioned above, all acts criminalized by the Cybercrime Law have already been criminalized by other laws with proportional penalties. There is no clear evidence that previous laws failed to provide adequate deterrence against those acts. The previous laws sometimes even impose harsher penalties. In-

fringement of “the values and principles of the Egyptian family” is already criminalized in article 308 of the Penal Code, which stipulates a prison sentence of six months to two years for insulting, slandering, cursing, or attacking the dignity and reputation of others, while article 25 of the Code sets a maximum penalty of no more than six months in prison. This shows the extent of the randomness in determining this crime and its penalty. Broadcasting false news with the aim of disturbing the public peace or the financial position of the state, causing panic or harming the public interest is criminalized under articles 80 (d), 102 (bis), and 188, with a penalty of up to one year’s confinement and a fine, which increases in wartime. It is thus unclear what deterrence is added by the re-criminalization in the Cybercrime Law.

### 2.2.3. Proportionality

**First, is the punishment prescribed proportional to the nature of the crime?**

Articles 27 and 34 breach this principle because they introduce new penalties for acts that are not criminalized or increase penalties for acts that do not require it. Article 27, for example, stipulates confinement for a period of not less than two years for “creating, managing and using an account,” which can at best be a preparatory act or offence related to the primary offence, without regard to the penalty for the primary offence itself, which may have no imprisonment penalty or a shorter prison term.

Crimes such as insult and slander, typically committed using social media, are a telling example. Imprisonment for this crime was dropped under the amendments introduced to the Penal Code in 2006; articles 306 and 307 maintain a fine only unless the crime includes “defamation of the honor of individuals or harm to the reputation of families.” If insult and slander are the primary offence, then, and the use of an electronic account is ancillary or preparatory, the judge is in the strange position of having to impose a fine for the primary offence and imprisonment of at least two years for the ancillary offence.

Article 34 of the Cybercrime Law considers the violation of national security a serious crime that requires “imprisonment.” Taking into account the law’s broad definition of national security, which includes discussion of the “affairs” of the Interior Ministry, insulting a large number of public officials becomes an offense punishable by aggravated imprisonment, while the Penal Code (article 308) stipulates a two-year prison sentence as the maximum penalty for journalism that attacks individuals’ honor or a family’s reputation. Article 34 also puts the judge in a paradoxical position when considering the crime of insulting a public official, obliged to issue a more serious prison sentence for the ancillary crime (the use of an account) than the primary offense.

This disproportionality not only violates the established Penal Code principle on the necessity of “proportionality of penalties to crimes,” but also article 95 of the Constitution: “there shall be no crime or punishment except pursuant to a law.” The law here allows judges to devise crimes and punishments that are not clearly stipulated.

### **Second, is the scope of the restriction reasonable?**

The law represents an unprecedented expansion of the scope of those to whom precautionary or punitive measures apply. Articles 7 and 8, which regulate the blocking of websites endangering “the country’s national security and economy,” effectively punish the vast majority of users and employees who are not involved in these crimes, even though no clear evidence exists that blocking is a deterrent. The law also subjects a far wider range of people to punitive provisions than ever before, as explained above in the case of article 27, which criminalizes preparatory acts for crimes, and article 25, which may criminalize any act that does not conform to the judge’s whims or moral convictions.

### **Third, does the restriction take into account the interests of vulnerable parties?**

The law’s conceptual ambiguity, the broad applicability of its penalties, and their unjustified harshness makes it a trap for a range of internet users establishing fragile and new employment relationships with social-media platforms that challenge prevailing convictions about social positions and roles, and

where they lack legal knowledge and protection. One example is of the 2020 case of young women creating content on TikTok, Likee, and Instagram, in which the law's broad provisions led to the abuse of a group in need of protection rather than punishment. These new elastic employment relationships require that the legal responsibility for a crime, when a crime is actually committed, be placed on the stronger party in the relationship, namely the site administrators and not the users. This was not the case. In its report on two of these cases, [EIPR explained](#) that neither the Public Prosecution nor the Economic Court seriously sought to impose any criminal penalty on the administrators of the main website through which the alleged crimes were committed, but rather allowed the administrators to travel freely during the hearings, in contravention of the logic of the accusations brought against the users.

These young women also needed protection from harassment by groups on social media who committed crimes such as stalking, extortion, defamation, infringement on the sanctity of private life, insult, and slander, and then, using their distinguished social position as men (some of whom are lawyers), pushed the Public Prosecution to persecute the women and girls who were their targets rather than assisting them.

The law's absolute approach to crime and punishment will lead to further prosecution against vulnerable parties, especially as various demographic groups seek to earn a living through online content sharing. Like any economic activity, content sharing needs to be regulated to protect those employed, not criminalized in an absolute yet ambiguous manner. Regulation should be guided by labor laws to protect the most vulnerable parties, namely social media users. Such protection does not involve exemption from punishment for such parties if they do participate in a crime, provided that the crime is precisely defined as per the criteria listed in section 1 above.

#### **Fourth, are the resources allocated to the restriction reasonable?**

The law burdens the Economic Court with a very wide range of cases that do not fall within its jurisdiction and are not provided for by the law establishing it. The Cybercrime Law designates that court to exclusively look into

the crimes it contains, but practice has shown that this transfer of jurisdiction led to the court's departure from its primary function of hearing economic disputes to improve the investment environment.

### **Fifth, does the restriction prejudice the content of the right?**

The penalties and precautionary measures contained in the Cybercrime Law constitute a clear violation of the right to freedom of expression as defined in the ICCPR and the relevant articles of the Constitution. The clearest form of this violation is the power to block websites, in articles 7 and 8 of the law. As mentioned, this collective punishment of employees not involved in any crime violates a key component of the right enshrined in the second paragraph of ICCPR article 19, namely the freedom of everyone "to seek, receive and impart information and ideas of all kinds." This component is also protected by article 68 of the Egyptian Constitution, guaranteeing the right to access information.

The penal provisions that impose custodial penalties in this law also indirectly violate the components of the right to freedom of expression contained in the second paragraph of article 19 of the Covenant, or those contained in articles 65, 68 and 71 of the Egyptian constitution, especially those prohibiting the imposition of a custodial penalty for crimes committed through publication and publicity. Considering that these penal articles do not have a legitimate, precisely defined, and comprehensive basis, it is clear how serious the violation of the components of the right is.

## **3. Suggested options for legislators, the prosecution, and the judiciary**

In light of the democratic normative framework we have outlined, and the contradictions and violations of the Constitution that become clear by applying it to the Cybercrime Law, we propose to legislators, the Public Prosecution, and judges some options for bringing the law closer to such a framework. We propose these options in order of preference. The options do not

contradict each other, and executing one does not prevent the activation of the others at a later stage.

### **Option 1: A comprehensive review of the articles of the Cybercrime Law**

This is the ideal scenario, but it requires political will and a broad, transparent, and open dialogue between the various stakeholders so that all their concerns can be taken into account. Assuming the will is present and the time for dialogue ripe, we suggest that the review include:

- Amending the definition of “national security” in article 1 to regulate its use and achieve the conditions of legality in terms of defining the nature of crimes and the persons addressed by the law and their obligations. We propose that the definition refers to a specific objective criterion, namely the stability of state borders and its sovereignty over its territory, against any external military threat or a threat to its infrastructure, and to the lives and property of its citizens, through acts of physical violence and sabotage sponsored from abroad. This would limit the tendency for excessive interpretation that broadens the concept of a threat to national security to include any act that may threaten the stability of the existing political system or the interests of the ruling elite. The reference to “the affairs of the Presidency of the Republic, the Ministry of Defence, the National Defense Council, the National Security Council, the Ministry of the Interior, and the Administrative Control Authority” must accordingly be deleted, as they are all public institutions that should not be exempted from public scrutiny. In any case, these institutions may withhold certain information or disallow public comment on it provided that they demonstrate its impact on national security within the specific definition mentioned above.
- Specific definitions of “public order” and “public morality” should be included in article 1. Their absence is incomprehensible considering that the law includes crimes and punitive provisions related to violating both. The numerous legal texts we mention above can guide the definition of these terms, transforming them into the context necessary to reassure cit-

izens of their physical security and property, and facilitate a moral sense that enables them to exercise their rights and freedoms and participate in public life.

- Website blocking, mentioned in article 7, should be reframed as a precautionary measure allowed only when requested by investigative authorities during an investigation, and not a measure activated by merely establishing evidence that a website broadcast material that would be an offense or jeopardize national security or the economy. This amendment would refine the wording of the article by linking it to an objective criterion, namely the criminal investigation of a crime. It would also balance the interests and requests of the various stakeholders, as it would still allow blocking under specific conditions and with procedures for appealing the decision, as stated in article 8.
- Article 25 should be amended by deleting the reference to “family values and principles in Egyptian society,” as this criminalization does not add anything and encourages arbitrary and excessive criminalization and punishment. The forms of criminalization mentioned in articles 25 and 26 should be sufficient to protect individuals’ private life and ensure that personal data is not used to produce content that violates public morality, redefined in article 1 as mentioned.
- Article 27 should be deleted due to the clear unconstitutionality of criminalization without a legal basis, and due to the lack of proportionality it creates between crime and punishment. The article creates no new deterrent to serious crimes that pose a significant threat to public order or national security, as they are criminalized in other laws and subject to various severe penalties, which exceed the prison term and fine stipulated in said article.
- In Article 34, the phrase “harming the economic position of the country, hindering or obstructing the work of public authorities, disrupting the provisions of the constitution, laws or regulations, or harming the national unity and social peace” should be deleted. The article should also identify

the acts that pose a threat to national security in the sense described above. It should clarify that the intention must be to disclose or comment on information that constitutes a breach of any of the five aspects mentioned in the Tshwane Principles, namely ongoing defense plans, detailed plans for the protection of critical infrastructure and institutions against sabotage, and information on military systems, military communication, intelligence sources, and information received from other countries or through diplomatic channels. Criminalization in this article will not be fully regulated unless a law is issued that regulates the right to access information and specifies the rules of disclosure, confidentiality, and the powers vested in those who manage information related to national security.

Option 2: The executive regulations should be amended to determine the legislator's purposes in certain articles of the law

If comprehensive legislative review of the law cannot be immediately achieved, the prime minister may use the powers granted to that role under article 170 of the Constitution to add certain articles to the law's executive regulations to clarify ambiguities, and contradictions revealed by court rulings, without suspending, amending, or introducing an exception to any of its provisions, and without waiting for a legislative amendment by the Parliament or a ruling on the constitutionality of any of these articles by the Supreme Constitutional Court. Amendments to the executive regulations can clarify ambiguities as follows:

- A text can be added that demystifies what is meant by the family values and principles of Egyptian society, by clearly linking the text to its context, which is the chapter on crimes of infringing on the private life of individuals; accordingly, what the crime is here is encroachment upon individuals' private life with any material that violates the family values and principles of Egyptian society.
- A specific definition can be added for the grounds of restriction not defined in article 1 of the law, namely "national unity, social peace, and the economic position of the country," by linking them all to the established

traditions that define these concepts in light of the objective unity of the principles of the Egyptian Constitution, which all refer to the context necessary for citizens to exercise their rights and freedoms. Explanatory examples of acts that constitute a crime in accordance with the law can be added.

### **Option 3: The Public Prosecutor should issue a circular explaining the steps of investigation and referral**

The Public Prosecutor cannot take on the task of interpreting the vague provisions of the Cybercrime Law, but can assist members of the Public Prosecution in conducting disciplined investigations and bringing charges in accordance with the correct interpretation of the law's provisions as contained in its executive regulations. This is especially necessary because the law includes many technical aspects. (In 2004, the Public Prosecutor issued a circular explaining how to implement certain articles of the Telecommunications Regulation Law No. 10 of 2003.<sup>30</sup>) The circular could:

- Emphasize a commitment to the context of article 27 of the law and article 11 of the executive regulations, which attribute the crime of “using an electronic account” to the administrators and creators of a website, and not to its users.
- Determine what an investigation should address in the crimes of violating “the values and principles of Egyptian family” as encroaching upon the private life of individuals, as well as in the crimes of harming the “economic position of the country,” “national unity,” and “social peace.” The circular should also determine what should not be addressed in such an investigation, so that the interrogation of the accused does not become a search for intentions or an inquiry into another content that is not related to the subject of the crime and should not be used against the accused when charged.

---

30 Circular No. 7 of 2004 regarding the Telecommunications Regulation Law No. 10 of 2003 and what to take into account.

## **Conclusion**

In this study, we have outlined a normative democratic framework to regulate the debate on the limits of freedom of expression online, and the mechanisms and grounds for restricting it. In developing this framework, we built on a sizeable legacy of legal rules and interpretations developed by UN human rights mechanisms, regional mechanisms, and national courts, especially in contexts similar to Egypt.

The proposed framework includes definitions for the five grounds recognized as justifications for restricting freedom of expression in general: the rights and freedoms of others, public order, public morality, national security, and public health. These definitions combine the appropriate openness for increasingly complex and intertwined social contexts and a pragmatism that aims for the approval of states, which are so far the only political units entrusted with applying international human rights laws.

The proposed framework also includes three controls or tests to help legislators and judges in the task of restricting the right to freedom of expression in specific cases, or assessing existing restrictions, without jettisoning the content of the right—which is central for the human rights system as a whole—and without overturning the relationship between restrictions as exceptions and permissibility or freedom as the origin. These controls are: legality, necessity, and proportionality. Here we were guided by the same progressive and compatible tendencies characteristic of the international human rights system. As much as possible, we made these steps detailed, divided into sub-steps, and supported by examples.

In the second section, we applied this framework to the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 (the Cybercrime Law) as a case study revealing of the legislative philosophy governing the approach of the current ruling elite in Egypt to freedom of expression online. This approach sees the internet as a threat to the stability of the social system and thus seeks to restrict freedom of expression through it, even in violation of the Constitution. In examining the provisions of the law in light of the pro-

posed controls, as well as citing some of its judicial applications, we concluded that the law in its current form does not comply with any of the controls on restricting freedom of expression—not in terms of legality, necessity, or proportionality.

- The law does not specify precisely or clearly the acts it criminalizes or the manner in which they can be proven or the criminal intent thereof, nor does it specify precisely, clearly, or comprehensively the persons subject to its provisions or their obligations.
- The law does not specify the subjects of legal protection, whether protection is necessary in a democratic society, the nature of the threats involved, or whether confronting them requires restricting users' freedom of expression. It also criminalizes acts already criminalized in other laws without providing evidence of the need for further criminalization or harsher punishment.
- The law provides precautionary and punitive measures disproportionate to the nature of the threat facing the subjects of protection. It expands the scope of restriction to unreasonable limits, violates the content of freedom of expression, does not take into account the interests of vulnerable parties, and allocates unnecessary resources to restriction.

The results in practice of this has been:

- The explicit constitutional violations of criminalization without a clear legal text, and the imposition of custodial penalties for crimes elsewhere excluded from such penalties.
- An unprecedented expansion of the powers granted to trial judges to identify criminal acts and sources of threat, which were marred by ambiguity in the law.
- Significant contradictions between the conduct of the prosecution and that of courts, and even between the rulings of the same court.
- A lack of security or legal certainty that enables internet users to under-

stand the legislator's intention and behave accordingly so as not to violate the law has made the law a "trap" for internet users.

To transform this trap into a safety net, we have proposed on the basis of the normative framework three options, which are not mutually exclusive, for legislators and judges:

1. Review the provisions of the law comprehensively to ensure their consistency with the Constitution and international human rights law.
2. Amend the law's executive regulations to clarify some of its ambiguities, without addition, deletion, or exclusion of any of its provisions.
3. Issue a circular from the Public Prosecutor to Public Prosecution investigators specifying the controls and procedures for investigating and leveling charges based on the law.

Reviewing the provisions of the Cybercrime Law, or at least reducing their ambiguity, will remove a major obstacle to a comprehensive legislative review of the system governing expression online. This review will not be complete without applying the same standards to related and interacting laws, foremost the Anti-Terrorism Law No. 94 of 2015, the Press and Media Regulation Law No. 180 of 2018, and the Telecommunications Regulation Law No. 10 of 2003, in addition to several relevant Penal Code provisions. We have briefly addressed some of the problems in the texts of these laws, which share the philosophy of the Cybercrime Law.

The desired legislative review requires special legislation to regulate freedom of information as an integral component of freedom of expression, which gains importance when practiced online. This would precisely determine what data and information may be withheld and protected and whose disclosure constitutes a punishable crime, and would thus create security or legal certainty for Egypt's internet users.