REPORT

Egyptian Human Rights Forum

CODING SILENCE

How Law Restricts Digital Rights in Egypt



المنبر المصري لحقوق الإنسان
Egyptian Human Rights Forum
Forum Egyptien pour les Droits de l'Homme

The Egyptian Human Rights Forum (EHRF) is an independent Egyptian human rights organisation founded in March 2018. EHRF aims to promote the implementation and dissemination of international human rights law in Egypt, advocate for a human rights-based approach to democracy and the rule of law, and mainstream human rights in public policy.

EHRF seeks to achieve this mission through dialogue, networking, policy research, advocacy, raising public awareness, capacity building, and the integration of young activists into the work of the human rights movement. The Forum prioritises dialogue with political, civil, and human rights actors both inside Egypt and within the diaspora. Through this dialogue, EHRF aims to build broad consensus around practical measures and alternatives grounded in shared human rights values, which can serve as a foundation for constitutional and legal reforms in Egypt.

In parallel, EHRF coordinates with independent regional and international human rights organisations in order to strengthen international protection mechanisms and expand support for human rights.

Contents

Introduction	4
One: The Constitutional Framework for Digital Rights and Freedoms	7
Two: Website Blocking and Content Control	12
Three: The Licensing Crisis Facing News Websites in Egypt	18
Four: The Expanding Criminalisation of Possessing and Using Telecommunications Equipment	22
Five: Mass Surveillance	26
Six: Weak Personal Data Protection Rules	30
Seven: False News, Insult and Defamation Offences as Tools of Digital Control	33
Eight: Legal Control over Digital Content Creators through "Reclassification" and "Moral Criminalisation"	38
Nine: Counter-Terrorism, the Legislation That Turns the Internet into a Space of Permanent Suspicion	42
Ten: Procedural Justice in Digital Cases	44
Eleven: The Rules Governing Communications Shutdowns	48
Twelve: The Criminalisation of Encryption and Anonymity	50
Thirteen: Criminalising the Possession of Advanced Technologies, the Case of Drones	53
Recommendations	57
Conclusion	60

Introduction

Rights and freedoms are no longer tested in the traditional public sphere alone. A growing share of public life has moved into a digital space governed by telecommunications infrastructure, platform policies, databases, and licensing and oversight mechanisms. In this space, interference with rights and freedoms changes whether a right can be exercised at all: whether one can access information, publish, communicate securely, organise, and carry out journalistic and research work without fear of monitoring or punishment.

Talking about digital rights is therefore not about a separate set of new rights. It is about how existing rights and freedoms are exercised in a technical environment that makes the impact of any restriction faster, broader and harder for society to detect than traditional restrictions.

The Egyptian Constitution provides a general framework within which digital rights can be read as a natural extension of freedom of opinion and expression, freedom of the press and media, the right to access information, the inviolability of private life and the confidentiality of correspondence, and the rule of law and judicial oversight.

This constitutional framework sets protection as the default. Freedom of expression and the media is presented as the rule, the prohibition of censorship as a guarantee, and the confidentiality of communications is surrounded by clear procedural safeguards. The right to information is meant to be a general rule, while exceptions are meant to remain limited and precisely defined.

In practice, however, the problem does not usually begin with an absence of constitutional texts. It begins with how those texts are translated into legislation and procedure, with broad exceptions, weak safeguards and a lack of meaningful transparency. Rather than serving as a tool to give effect to constitutional protection, some laws and regulations become channels that redefine the limits of the right through broad and elastic standards such as national security, public order, public morals and family values.

Digital rights problems in Egypt manifest along several paths. The first is control over content and access to it, where blocking, suspension and removal appear as high-impact tools that can be triggered through criminal, regulatory or structural routes tied to the infrastructure itself.

A second path links digital existence to a prior administrative condition through the website licensing regime. This makes the survival of independent news platforms and digital initiatives dependent on an administrative decision that can be withheld or withdrawn, so that intervention comes first and review comes later.

A third path concerns the expansion of criminal liability in publication cases through elastic provisions that can easily be applied to online expression, turning the space between opinion, information and professional error into a zone of potential prosecution.

A fourth path concerns the construction of permanent surveillance capabilities through technical access built into networks, mandatory data retention and expanded interception powers. Data collection becomes the operating rule and examination a later decision, an arrangement that multiplies the risk of abuse because it turns the whole of society into a ready-to-use data stockpile.

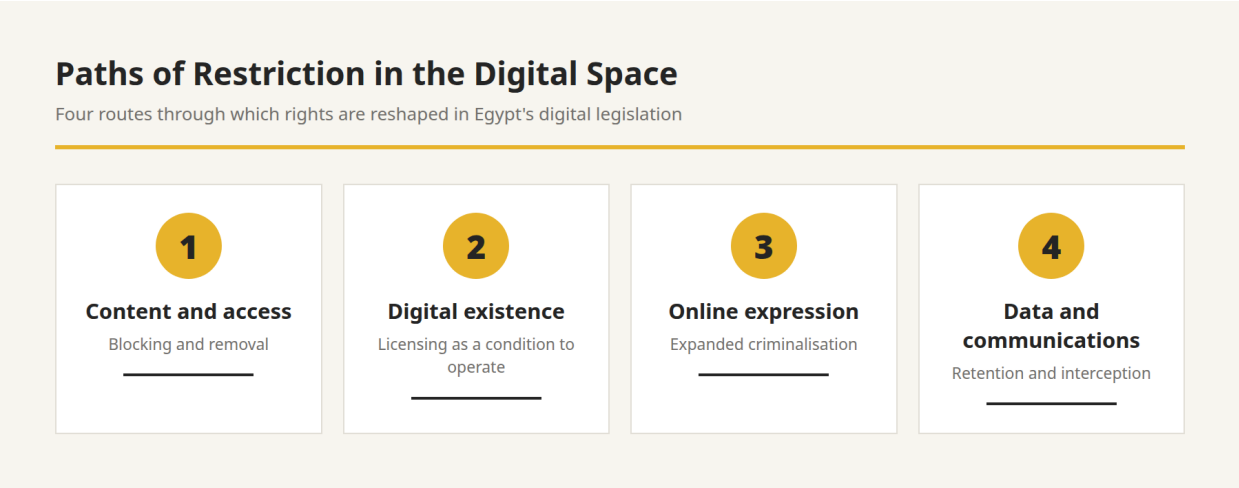


Figure 1: The four paths of restriction in the digital space

Alongside these paths, the question of safeguards emerges as the difference between legitimate regulation and a restriction that destroys the essence of the right. The existence of a procedure such as referral of a decision to a judicial body or a written statement of reasons is not enough if the standards on which the intervention rests are vague, if oversight comes late, if appeal is slow relative to the impact of the decision, or if immediate implementation falls on service providers in a way that pushes them to over-block and over-comply for fear of liability.

Weak transparency also leaves society unable to assess the scale of interference, its criteria and its errors, and makes it difficult to know who is responsible for a decision and how it can be reviewed, which in practice undermines the right to an effective remedy.

From another angle, the regulation of technology itself adds a new layer of risk. When digital protection tools such as encryption, communication tools or advanced technologies are treated as capabilities conditional on prior permission, the protective right itself becomes suspendable. The debate is then no longer about criminalising a specific harmful act, but about pre-emptive criminalisation that reaches possession, use, or research and experimentation, and forces the technical, research and economic sectors to operate under a constant threat of uncertainty.

This makes compliance an arduous task, makes selective enforcement a real possibility and raises the cost of innovation, especially for small actors, researchers and independent initiatives.

On this basis, this report, Coding Silence: How Law Restricts Digital Rights in Egypt, examines the structure of the legal regulation of the digital space in Egypt from a human rights perspective, in order to understand its logic and its effects on the limits of rights and their safeguards. It shows how the relationship between rule and exception is being redistributed in legislation and practice,

how legal predictability is declining, and how this affects freedom of expression, journalistic, research and technical work, and the rights to privacy and to knowledge.

The report also documents the emergence of a legal environment that produces a chilling effect, drives self-censorship and shrinks the space for public participation even before any conviction. Its analysis rests on testing the key elements of any intervention affecting digital rights: the clarity of the legal rule, the narrowness of the standard for intervention, the necessity and proportionality of the measure, the effectiveness of judicial oversight, the availability of fast and comprehensible avenues of appeal, and a degree of transparency that prevents abuse and allows public scrutiny.

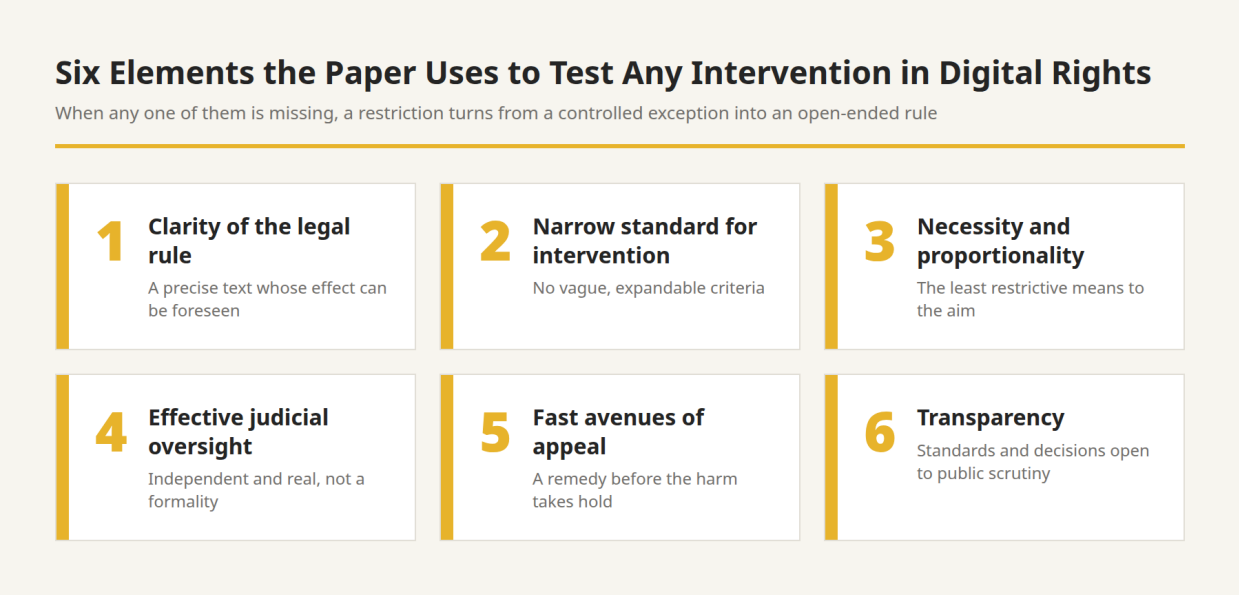


Figure 2: The key elements for testing the legitimacy of any intervention

Accordingly, the report puts forward recommendations to restore the balance between protection requirements and the essence of rights and freedoms and their procedural safeguards. The aim is to rein in the role of the state so that it does not become a general administrator of the digital sphere operating on a logic of permanent suspicion. Real security in the digital space is not achieved by widening the scope of intervention, but by building clear and predictable rules, independent oversight safeguards, policies that encourage secure communications and data protection, and a legal system that prevents the internet from becoming a space that can be suspended whenever interpretation expands or limits disappear.

> **“Real security in the digital space is not achieved by widening the scope of intervention, but by building clear and predictable rules.”**

One: The Constitutional Framework for Digital Rights and Freedoms



The Egyptian Constitution of 2014 (as amended) provides a foundation within which digital rights can be read as an extension of traditional rights and freedoms (freedom of expression, media freedom, the right to privacy, freedom of information and the guarantees of the rule of law) that now operate within a digital and informational space where means of publication and communication and telecommunications infrastructure intersect with the exercise of the rights themselves.

On freedom of expression, Article 65 of the Constitution[1] guarantees freedom of thought and opinion and the right of every person to express their opinion "verbally, in writing, through imagery, or by any other means of expression and publication". This wording naturally encompasses the various forms of digital expression (platform posts, video, podcasts, blogging, public messages and so on) without the need for a specific constitutional provision on the internet.

This framework is completed in the field of media and publication by Articles 70 and 71 of the Constitution. Article 70[2] guarantees freedom of the press, printing and publication in paper, visual, audio and electronic forms, and establishes the right to create media outlets and digital media, while referring certain detailed procedures to the law (such as the procedures for establishing and owning broadcasting stations and electronic newspapers).

Article 71[3] establishes a fundamental guarantee by prohibiting censorship, confiscation, suspension or closure of newspapers and media outlets, permitting an exception only "in time of war or general mobilisation" and within limited censorship. It adds an important restriction on

[1] Article 65: Freedom of thought and opinion is guaranteed. Every person has the right to express their opinion verbally, in writing, through imagery, or by any other means of expression and publication.

[2] Article 70: Freedom of the press and of printing and publication, whether in paper, visual, audio or electronic form, is guaranteed. Egyptians, whether natural or legal persons, public or private, have the right to own and publish newspapers and to establish visual and audio media outlets and digital media. Newspapers may be issued upon notification, as regulated by law. The law regulates the procedures for establishing and owning radio and television broadcasting stations and electronic newspapers.

[3] Article 71: It is prohibited in any way to impose censorship on Egyptian newspapers and media outlets, or to confiscate, suspend or close them. Exceptionally, limited censorship may be imposed on them in time of war or general mobilisation. No custodial penalty shall be imposed for crimes committed by way of publication or publicity. Penalties for crimes relating to incitement to violence, discrimination between citizens or attacks on the honour of individuals are determined by law.

custodial penalties for publication offences, with specific exceptions (such as incitement to violence, discrimination or attacks on personal honour). Within the Constitution itself, this combination produces a balance between the default of protection (prohibition and ban) and expressly stated exceptions.

The Constitution also recognises the right to information as a general rule, which therefore applies to the digital space. Article 68[4] provides that information, data, statistics and official documents belong to the people, and that disclosing them is a right guaranteed by the state to every citizen, with a duty on the state to provide and make them available transparently, while the law regulates the rules for obtaining them, their confidentiality, grievance procedures and penalties for withholding them. The article is significant in the digital context because it explicitly refers to the obligation of state institutions to preserve and digitise official documents "by all modern means and tools", opening a constitutional door to reading digital government, digital archiving and open data as part of the structure of the right to access and circulate information.

On privacy and the confidentiality of communications, Article 57[5] establishes the inviolability of private life and the inviolability and confidentiality of correspondence in all its forms, including electronic correspondence and communications. It prohibits their confiscation, inspection or monitoring except "by a reasoned judicial order, for a specified period, and in the cases defined by law". The Constitution thus sets precise procedural safeguards: a judicial order, reasons, a time limit, and the restriction of interference to specific "cases" that the law must define. Article 57 also contains a constitutional guarantee that goes beyond protecting confidentiality to protecting the "availability of communication" itself: it obliges the state to protect citizens' right to use all forms of public means of communication and prohibits their arbitrary disruption, suspension or denial, referring the regulation of this to the law.

The importance of this is that it establishes a positive obligation on the state that is not limited to refraining from interfering with communications, but imposes a duty to protect access to communication services and their continuity as a precondition for exercising other rights in the digital space (such as expression, receiving information, journalism and organising). At the same time, referring the matter to the law requires, from a constitutional perspective, that any restriction remain governed by necessity, proportionality and predictability, and that regulation not become a channel for cutting off or restricting service without safeguards.

[4] Article 68: Information, data, statistics and official documents belong to the people, and their disclosure from their various sources is a right guaranteed by the state to every citizen. The state shall provide and make them available to citizens transparently. The law regulates the rules for obtaining them, making them available and keeping them confidential, the rules for depositing and preserving them, grievances against refusal to provide them, and the penalty for withholding information or deliberately providing false information. State institutions shall deposit official documents, once no longer in use, with the National Archives, protect and secure them against loss or damage, and restore and digitise them by all modern means and tools, in accordance with the law.

[5] Article 57: Private life is inviolable and may not be infringed. Postal, telegraphic and electronic correspondence, telephone conversations and other means of communication are inviolable and their confidentiality is guaranteed; they may not be confiscated, inspected or monitored except by a reasoned judicial order, for a specified period, and in the cases defined by law. The state shall also protect the right of citizens to use public means of communication in all their forms, and they may not be arbitrarily disrupted, suspended or denied to citizens, as regulated by law.

The Constitution further reinforces procedural protection through its provisions on the "rule of law" and general judicial guarantees. Article 94[6] establishes that the rule of law is the basis of governance and that the state's subjection to the law and the independence of the judiciary are fundamental guarantees for the protection of rights and freedoms. Article 95[7] establishes the principle of criminal legality (no crime and no penalty except by law, and no penalty except by judicial ruling), and Article 97[8] prohibits shielding any administrative act or decision from judicial review. Article 99[9] adds that any assault on personal freedom, the inviolability of private life or other rights and freedoms is a crime not subject to a statute of limitations and affirms the right of the injured party to resort to the courts. Although this system was not written specifically for the digital space, it gives the digital dimension of rights (surveillance, access to data, administrative restrictions on content or communication) a constitutional framework that ties restrictions to legality and judicial oversight.

The Constitution also addresses the concept of information-space security. Article 31[10] considers the security of the information space an essential part of the economy and national security and obliges the state to take the measures necessary to preserve it "as regulated by law". The importance of this article is that it raises cybersecurity to the constitutional level, but at the same time it relies on legislative referral, which makes the definition of risk and the standards and limits of measures decisive for how this obligation is translated into predictable rules.

The Constitution adds an important layer of protection through Article 92,[11] which sets a governing rule that the rights and freedoms inherent to the person of the citizen may not be suspended or diminished, and that no law regulating the exercise of rights and freedoms may restrict them in a way that affects their origin and essence. Article 93[12] grants international human rights agreements, covenants and conventions ratified by Egypt "the force of law" after their publication. Foremost among these instruments is the International Covenant on Civil and Political Rights, which Egypt ratified in 1982. Article 19[13] of the Covenant guarantees freedom of expression,

[6] Article 94: The rule of law is the basis of governance in the state. The state is subject to the law, and the independence, immunity and impartiality of the judiciary are fundamental guarantees for the protection of rights and freedoms.

[7] Article 95: Punishment is personal. There is no crime and no penalty except on the basis of law, no penalty may be imposed except by judicial ruling, and there is no punishment except for acts committed after the law enters into force.

[8] Article 97: Litigation is a protected right guaranteed to all. The state shall bring judicial bodies closer to litigants and work to expedite the resolution of cases. It is prohibited to shield any administrative act or decision from judicial review. No person may be tried except before their natural judge, and exceptional courts are prohibited.

[9] Article 99: Any assault on the personal freedom or the inviolability of the private life of citizens, or on other public rights and freedoms guaranteed by the Constitution and the law, is a crime for which neither criminal nor civil action is subject to a statute of limitations, and the injured party may bring a direct criminal action. The state guarantees fair compensation to the victim of the assault. The National Council for Human Rights may report any violation of these rights to the Public Prosecution and may join the civil action alongside the injured party at their request, all as set out in the law.

[10] Article 31: The security of the information space is an essential part of the economy and national security. The state shall take the measures necessary to preserve it, as regulated by law.

[11] Article 92: The rights and freedoms inherent to the person of the citizen may not be suspended or diminished. No law regulating the exercise of rights and freedoms may restrict them in a way that affects their origin and essence.

[12] Article 93: The state is bound by the international human rights agreements, covenants and conventions ratified by Egypt, which acquire the force of law after publication in accordance with the prescribed procedures.

[13] Article 19: (i). Everyone shall have the right to hold opinions without interference.

including the freedom to seek, receive and impart information through any media, and permits restrictions only where they are provided by law and are necessary for respect of the rights of others or for the protection of national security, public order, public health or morals. Article 17[14] of the same Covenant prohibits any arbitrary or unlawful interference with a person's privacy or correspondence. Accordingly, any legislation or measure that restricts digital rights without meeting the requirements of legality, necessity and proportionality is not merely a constitutional violation; it is also a breach of an international obligation binding on Egypt.

Although the Constitution sets out a vision based on protecting freedom of expression and the media as the default, prohibiting censorship as a rule, and requiring that any interference with the confidentiality of communications or disruption of public means of communication remain an exception bound by procedural safeguards, time limits and effective judicial oversight, part of the subsequent legislation has approached the digital sphere through a logic of authoritarian control rather than the guarantee of rights.

This is evident in the shift of the centre of gravity from clear, predictable rules to elastic standards such as national security, public order, public morals and family values, which allows the scope of a restriction to expand according to interpretation rather than a fixed objective criterion. It is also evident in the transformation of legal regulation into a route for fast, high-impact measures affecting the availability of or access to content (such as blocking, removal or account suspension) that do not always pass through a ladder of safeguards commensurate with the seriousness of their impact, and that amount to "censorship" even when not called by that name.

On privacy, laws have built arrangements that make the collection, retention and on-demand provision of data part of normal operations, which in practice undermines the constitutional philosophy that interference with communications should be specific, reasoned and temporary. In addition, laws have introduced a logic of licensing and prior approval in areas touching digital protection tools themselves (such as encryption technologies or certain communications equipment), recasting the protective right as a conditional capability and increasing deterrence and self-imposed compliance.

These laws therefore represent a shift in function: from law that is supposed to give effect to constitutional guarantees to law that redefines the limits of the right through broad gateways that weaken the essence of constitutional protection. This can be seen in the Law Regulating the Press

(ii). 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.

(iii). 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 (ordre public), or of public health or morals.

[14] Article 17: (i). No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(ii). Everyone has the right to the protection of the law against such interference or attacks.

and Media, the Anti-Terrorism Law, the Anti-Cybercrime Law, the Personal Data Protection Law, and the Telecommunications Regulation Law and its amendments.

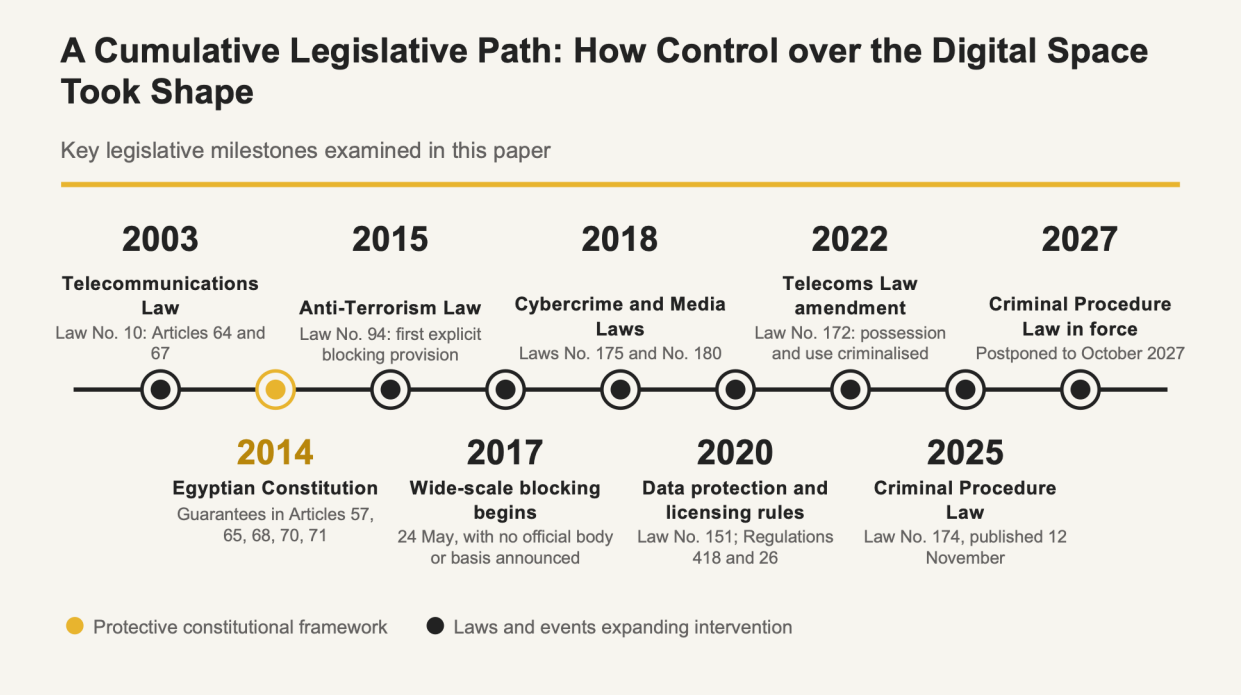


Figure 3: Key legislative milestones, 2003–2027

Two: Website Blocking and Content Control



The space for public participation facing blocking and licensing tools

Since 24 May 2017, blocking has been practised on a wide scale without any official announcement of the body that issued the decision or its precise legal basis. It then gradually expanded to cover political and human rights platforms, technical services and circumvention tools.[15]

In the Egyptian context, blocking is understood as a set of legal, administrative and judicial measures that in practice prevent users from accessing a website, link, content or account, disrupt or stop the broadcast of media material, or place telecommunications networks and services under the authorities' management in a way that enables control over access or continuity. The legal regulation of blocking is fragmented: it is not found exhaustively in a single law, but is distributed across laws dealing with content, laws dealing with telecommunications infrastructure, and laws that expand intervention tools in the name of counter-terrorism.

The Anti-Terrorism Law No. 94 of 2015, the first law to refer explicitly to blocking, presents it as a measure linked to the criminalisation of using networks for terrorist purposes. Article 29[16] of the

[15] Masaar, "Website Blocking in Egypt: Techniques and Laws", May 2024: https://bit.ly/3OEiJmU

[16] Article 29: Anyone who creates or uses a website on telecommunications networks, the international information network or otherwise, for the purpose of promoting ideas or beliefs calling for the commission of terrorist acts, broadcasting material intended to mislead the security authorities or influence the course of justice in relation to any terrorist crime, exchanging messages and issuing instructions between terrorist groups or their members, or conveying information relating to the acts or movements of terrorists or terrorist groups at home or abroad, shall be punished with aggravated imprisonment for no less than five years. Anyone who, without right or by unlawful means, enters a website belonging to any government body with the intent of obtaining, viewing, altering, erasing, destroying or falsifying the data or information on it, for the purpose of committing or preparing to commit any of the crimes referred to in the first paragraph of this article, shall be punished with aggravated imprisonment for no less than ten years.

law criminalises creating or using a website on telecommunications networks or the international information network with the aim of promoting ideas that call for terrorist acts, misleading the security authorities, influencing the course of justice, exchanging messages and instructions between terrorist groups, or conveying information about the movements of terrorists.

Article 49[17] then grants the Public Prosecution or the competent investigating authority (as the case may be) the power to take certain measures against websites, providing that the prosecution or investigating authority may suspend or block the websites referred to in the first paragraph of Article 29, or block any of the forms of use it contains, and seize the devices and equipment used in the crime. Blocking here is presented as a tool to contain the effects of a crime or prevent its continuation.

Under the Anti-Cybercrime Law No. 175 of 2018, blocking follows a more detailed procedural path. Article 7[18] of the law allows the competent investigating authority to order the blocking of a website whenever there is evidence that a site broadcasting from inside or outside the country is posting material that constitutes one of the crimes set out in the law and poses a threat to national security or endangers the security of the country or its national economy.

The article requires the investigating authority to present the blocking order to the competent court, sitting in chambers, within 24 hours, accompanied by a memorandum of its opinion, and the court issues a reasoned decision accepting or rejecting it within no more than 72 hours.

The law also sets out an urgent mechanism that allows investigation and law-enforcement bodies (the police), in cases of urgency due to an imminent danger or harm, to notify the National Telecommunications Regulatory Authority (NTRA), which immediately instructs the service provider to impose a temporary block. The record of the procedure must be presented to the investigating authority within 48 hours, failing which the block is deemed never to have existed.

---

[17] Article 49: In the crimes set out in Articles 12, 15, 19 and 22 of this law, the Public Prosecution or the competent investigating authority, as the case may be, may issue a temporary order to close premises, places, residences and lodgings, provided that the decision is issued by at least a chief prosecutor. Belongings and furniture seized therein are treated as administratively seized property from the moment of seizure until the case is finally decided, and are handed over, after being inventoried and recorded, to a custodian charged with guarding the seals placed on the closed premises; if nothing is seized, the custodian is charged with guarding the seals in the same manner. An acquittal renders the closure order void. The Public Prosecution or the competent investigating authority may suspend or block the websites referred to in the first paragraph of Article 29 of this law, or block any of the forms of use set out in that article, and seize the devices and equipment used in the crime.

[18] Article 7 (Procedures and decisions on blocking websites): Whenever there is evidence that a website broadcasting from inside or outside the country has posted any phrases, figures, images, films or any promotional material or the like that constitutes one of the crimes set out in this law and poses a threat to national security or endangers the security of the country or its national economy, the competent investigating authority may order the blocking of the website or websites concerned, wherever technically possible. The investigating authority must present the blocking order to the competent court, sitting in chambers, within 24 hours, accompanied by a memorandum of its opinion, and the court shall issue a reasoned decision accepting or rejecting it within no more than 72 hours of its submission. In cases of urgency due to an imminent danger or harm from the commission of a crime, the competent investigation and law-enforcement bodies may notify the Authority (the National Telecommunications Regulatory Authority), which shall immediately instruct the service provider to temporarily block the website, websites, links or content referred to in the first paragraph of this article. The service provider must implement the notification immediately upon receipt. The notifying investigation and law-enforcement body must present a record of the measures taken to the competent investigating authority within 48 hours of its notification to the Authority, following the same procedures set out in the second paragraph of this article, and the competent court shall then either uphold or halt the blocking. If the record is not presented within the deadline, the blocking shall be deemed never to have existed. The trial court, while hearing the case or at the request of the investigating authority, the Authority or the parties concerned, may order the lifting of the blocking decision or the modification of its scope. In all cases, the blocking decision lapses upon a decision that there are no grounds for criminal proceedings or upon a final acquittal.

The block may be lifted or its scope modified while the case is being heard, at the request of the investigating authority, the NTRA or the parties concerned.

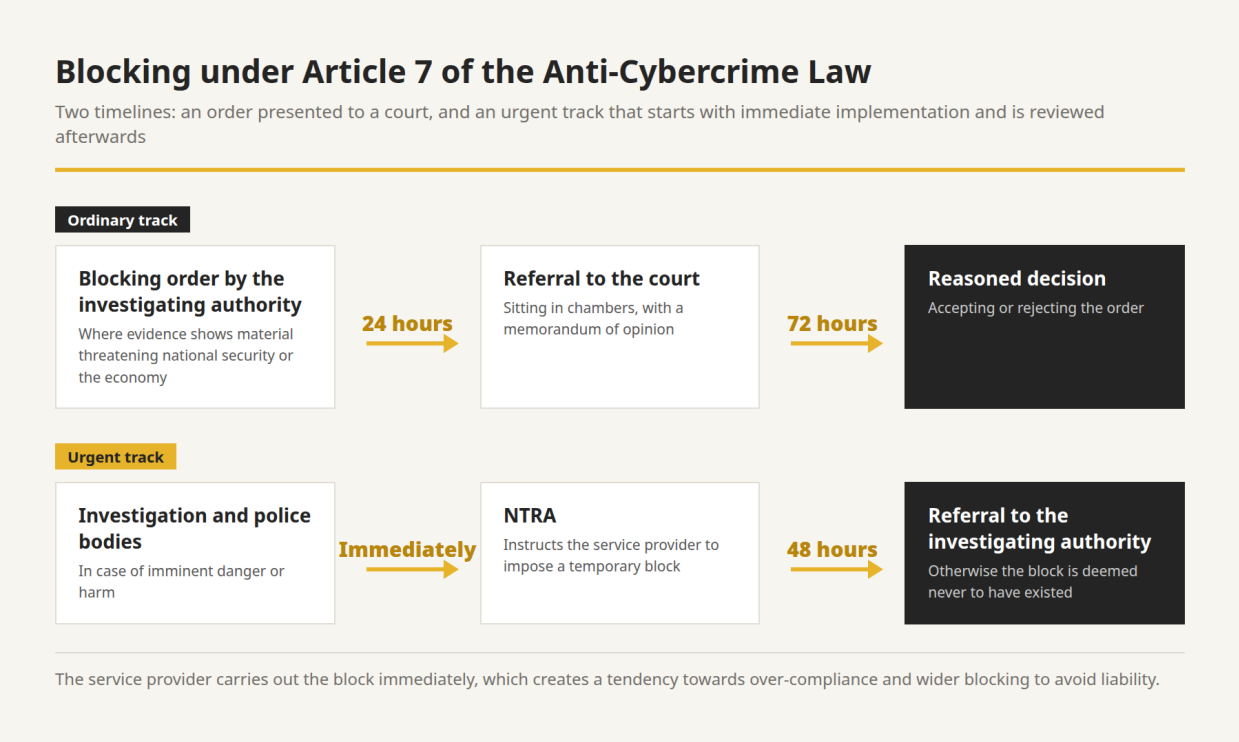


Figure 4: The two blocking timelines under Article 7 of the Anti-Cybercrime Law

Meanwhile, the Law Regulating the Press, Media and the Supreme Council for Media Regulation No. 180 of 2018 frames blocking as a regulatory and supervisory tool over content, press and media outlets, websites, and influential accounts with more than 5,000 followers.

Article 3[19] of the law sets out the principle that censorship, confiscation, suspension or closure of newspapers and media outlets is prohibited, but opens an exception "in time of war or general mobilisation" for limited censorship. In that case, it allows the Supreme Council for Media Regulation (SCMR) to issue a decision to seize copies of a printed newspaper or to "delete or block the offending material" if published in an electronic newspaper or on a website, or to stop its rebroadcast, while providing for the right of those concerned to challenge the blocking decision before the Administrative Court.

Secondly, Article 6[20] of the law ties a website's continued digital activity to obtaining a licence from the SCMR: websites may not be established or managed inside Egypt, nor may offices or branches

[19] Article 3 (Law No. 180 of 2018): It is prohibited in any way to impose censorship on Egyptian newspapers and media outlets, or to confiscate, suspend or close them. Exceptionally, limited censorship may be imposed on them in time of war or general mobilisation. In that case, the Supreme Council may issue a decision to seize copies of a printed newspaper, to delete or block material that violates censorship instructions if published in an electronic newspaper or on a website, or to stop its rebroadcast by a media outlet. Those concerned may challenge the decision before the Administrative Court.

[20] Article 6 (Law No. 180 of 2018): Websites may not be established or managed in the Arab Republic of Egypt, nor may offices or branches of websites operating from outside the Republic be managed, without first obtaining a licence from the Supreme Council in accordance with the rules and conditions it sets in this regard. Without prejudice to the prescribed criminal penalties, in the event of a violation of the preceding paragraph the Supreme Council may take the necessary measures, including revoking the

of websites operating from abroad be managed, without a licence from the Supreme Council, and in case of violation the Council may take measures including revoking the licence, suspending the activity or blocking the website in the absence of a valid licence.

Article 19[21] of the law also expands the scope of intervention in the work of personal websites, blogs and accounts with 5,000 or more followers. It prohibits them from publishing or broadcasting false news or incitement to break the law, violence, hatred, discrimination, attacks on personal honour, insult, defamation or contempt of religions, obliges the Supreme Council to take appropriate action, and empowers it to suspend or block the website, blog or account by its own decision in order to address such violations.

The Telecommunications Regulation Law No. 10 of 2003 does not use blocking as a clear, direct legal term, but its provisions give the state tools to control networks and services that can in practice affect access when activated. Article 64 prohibits telecommunications operators and service providers from using equipment to encrypt telecommunications services without the approval of the NTRA, the Armed Forces and the national security agencies, and requires operators and service providers to provide technical capabilities within the network enabling the Armed Forces and national security agencies to exercise their powers "within the limits of the law", with due regard for the inviolability of private life.

The provision most closely connected to blocking, disruption and denial of access is Article 67, which allows the competent state authorities to place all the telecommunications services and networks of any operator or service provider under their management and to summon the staff responsible for operation and maintenance, in cases of disaster, general mobilisation or any other cases relating to national security.

This is what happened, for example, in 2013, when the Administrative Court ruled to block YouTube for one month and to block all links showing the film in question, relying on a broad interpretation of Articles 64 and 67 of the Telecommunications Regulation Law. Through these provisions the court was able to find a legal justification for obliging the administrative authorities to block content, by broadly interpreting the concept of national security and the need to protect it.[22]

licence or suspending or blocking the website, where there is no valid licence. Those concerned may challenge the decision before the Administrative Court.

[21] Article 19 (Law No. 180 of 2018): Newspapers, media outlets and websites are prohibited from publishing or broadcasting false news or anything that calls for or incites violation of the law, violence or hatred, involves discrimination between citizens, calls for racism, or contains attacks on the honour of individuals, insults or defamation against them, or contempt for the heavenly religions or religious beliefs. Every personal website, personal blog or personal electronic account with five thousand or more followers is bound by the preceding paragraph. Without prejudice to the legal liability arising from violating this article, the Supreme Council must take appropriate action against the violation and may, to that end, suspend or block the website, blog or account by its own decision. Those concerned may challenge the decision before the Administrative Court.

[22] Masaar, "Blocking: An Established Censorship Tool in Egyptian Legislation", December 2021: https://masaar.net/ar/%d8%a7%d9%84%d8%ad%d8%ac%d8%a8-%d8%a3%d8%af%d8%a7%d8%a9-%d8%b1%d9%82%d8%a7%d8%a8%d8%a9-%d9%85%d8%b3%d8%aa%d9%82%d8%b1%d8%a9-%d9%81%d9%8a-%d8%a7%d9%84%d8%aa%d8%b4%d8%b1%d9%8a%d8%b9%d8%a7%d8%aa-%d8%a7/

In light of the above, Egypt's overlapping legislative structure for blocking operates as a multi-track system of restriction, distributed between laws focused on content, laws focused on infrastructure, and laws dealing with exceptional circumstances. A blocking decision can therefore be produced through more than one route: a criminal route that links blocking to preventing the effects of a crime; a regulatory route that presents blocking as a tool for managing the media sphere; and a structural route that gives the state the ability to control the network itself.

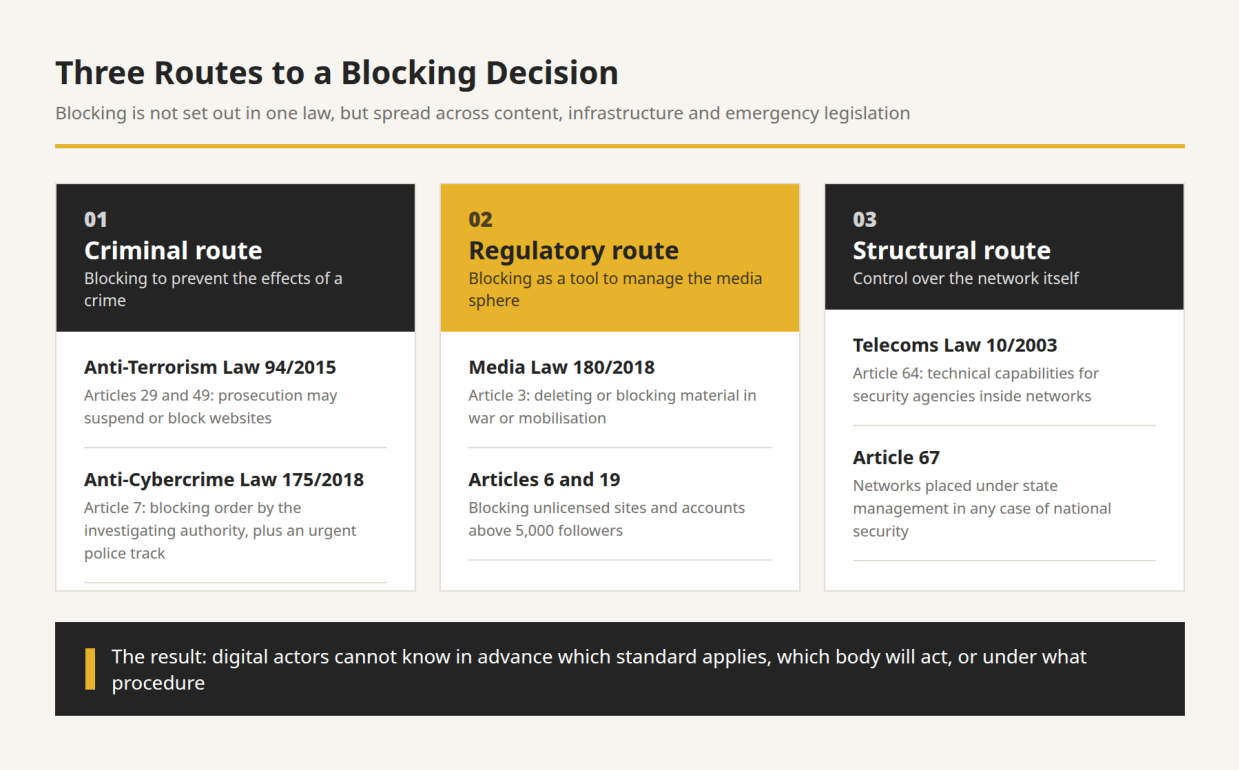


Figure 5: The three legal routes to blocking

This fragmentation undermines predictability. Digital actors cannot know in advance which standard will be applied, which body will act, or under which procedures. This turns the right of access to information from a rule into a suspendable condition, and keeps the logic of exception present even in contexts that do not call for it by their nature.

> **“The right of access to information turns from a rule into a suspendable condition.”**

From the perspective of safeguards, turning blocking into a procedural act does not in itself settle the question of constitutional legitimacy. The essence of protection depends less on the existence of formal steps (referral, validation, reasons) than on the narrowness of the standard, the effectiveness and independence of oversight, and the limits of the impact.

Where broad concepts such as national security or imminent danger exist without precise definitions, judicial oversight, even when invoked, is constrained by the nature of a standard open to expansive interpretation. Placing the burden of immediate implementation on service providers also creates a tendency towards over-compliance and over-blocking to avoid liability, increasing the risk of excessive blocking, undermining the public's right to know and producing a self-censoring effect.

Three: The Licensing Crisis Facing News Websites in Egypt

The licensing crisis lies in the fact that a large segment of independent news websites and digital initiatives operate inside Egypt in a fragile legal position, because "digital existence" itself has been tied to a prior administrative condition: obtaining a licence. The licence is thus closer to a condition of existence than to limited professional regulation. An operating website can be treated as an "illegal" activity simply because it lacks a permit, which opens the door to measures that threaten its continuity even before any specific professional violation is discussed.

> **"The licence is closer to a condition of existence than to limited professional regulation."**

The legal regulation of website licensing in Egypt rests on three instruments:

- The Law Regulating the Press, Media and the Supreme Council for Media Regulation No. 180 of 2018, which contains the general rules governing the licensing of websites, particularly those operating in journalism, media and advertising;
- The law's Executive Regulations, issued by Prime Ministerial Decree No. 418 of 2020, to which the law refers procedural rules;
- The Licensing Regulations of the Supreme Council for Media Regulation, issued by SCMR Decree No. 26 of 2020, to which the law refers the practical details on fees and licence templates.

At the level of the Media Law, the legislator first extends its provisions to press and media entities, institutions and outlets and to websites, with specific exceptions for personal accounts or websites, and obliges existing entities to regularise their status within six months of the entry into force of the Executive Regulations, under Article 2 of the promulgation articles.

It then sets the general rule on website licensing in Article 6,[23] which provides that websites may not be established or managed in the Arab Republic of Egypt, nor may offices or branches of websites operating from outside the country be managed, without a licence from the Supreme Council in accordance with the rules and conditions it sets.

[23] Article 6 (Law No. 180 of 2018): Websites may not be established or managed in the Arab Republic of Egypt, nor may offices or branches of websites operating from outside the Republic be managed, without first obtaining a licence from the Supreme Council in accordance with the rules and conditions it sets in this regard. Without prejudice to the prescribed criminal penalties, in the event of a violation the Supreme Council may take the necessary measures, including revoking the licence or suspending or blocking the website, where there is no valid licence. Those concerned may challenge the decision before the Administrative Court.

The provision links the licence to a subsequent administrative consequence in case of violation, allowing the Council, without prejudice to criminal penalties, to take the necessary measures where licence terms are breached or no licence has been obtained, including revoking the licence or suspending or blocking the website. The licence under the Press and Media Law is therefore a mechanism for regulating digital content and tying continued operation to administrative compliance.

The Executive Regulations of the Media Law break this general framework down into timelines, forms, fees and jurisdictional limits. Within the provisions on the establishment and operation of media outlets and websites, the Regulations provide that the Council shall prepare the forms for applications to establish or operate media outlets, and that these forms shall include detailed information on the owner and legal representative, language, nature of activity, sources of funding, administrative and editorial structure, the person responsible for broadcasting, the programme director and the place of broadcast.

Including elements such as sources of funding and editorial structure places the institutional independence of digital initiatives within the scope of administrative assessment, and makes it possible to use "disclosure requirements" as a means of pressure or obstruction, particularly in an environment where the media sphere is highly politically sensitive.

The Regulations then turn to financial and time-related rules. Article 11[24] of the Executive Regulations provides that an application to establish or operate a media outlet or website is submitted to the Council's General Secretariat on the designated form, accompanied by a receipt for payment of a set fee, which is stated expressly as EGP 50,000 for a website. Applications are referred to the competent licensing committee within one week of receipt, and the committee must prepare a report with its opinion within thirty days of referral, after which the report is presented to the Council to decide whether to grant or refuse the licence.

Article 12[25] provides that the Council's decision to grant or refuse the licence shall be issued within ninety days of receipt of a complete application, and that the applicant is notified by registered letter with acknowledgement of receipt. This deadline is, however, merely directory: missing it has

[24] Article 11 of Prime Ministerial Decree No. 418 of 2020 issuing the Executive Regulations of the Law Regulating the Press, Media and the Supreme Council for Media Regulation: "An application to establish or operate a media outlet or website shall be submitted to the General Secretariat of the Supreme Council on the form prepared for this purpose, accompanied by a receipt for payment of a fee of two hundred and fifty thousand pounds for a media outlet and fifty thousand pounds for a website. The General Secretariat shall enter applications in a special register kept for this purpose, recording the action taken on each. The General Secretariat shall refer applications to the competent licensing committee of the Supreme Council within one week of receipt, and the committee shall prepare a report with its opinion after examining the application, to be presented to the Supreme Council within thirty days of referral, in order to decide whether to grant the licence. The licence shall be valid for five years and may be renewed upon an application submitted by the licensee to the Supreme Council six months before its expiry; renewal requires payment of a fee of the same amount as set out in the first paragraph of this article, after review of the renewal conditions."

[25] Article 12 of Prime Ministerial Decree No. 418 of 2020: "If the licence application is incomplete, the Supreme Council must notify the applicant to complete it within thirty days of the licensing committee's report being presented to it, by registered letter with acknowledgement of receipt. The Supreme Council shall decide to grant or refuse the licence by a majority of members present within thirty days of the licensing committee's report being presented to it, with notification by registered letter with acknowledgement of receipt. The Supreme Council shall decide to grant or refuse the licence by a majority of members present within ninety days of receiving the application complete with all information and documents, and shall notify the applicant of its decision by registered letter with acknowledgement of receipt. Those concerned may challenge the Supreme Council's decision before the Administrative Court."

no legal consequence. This contrasts with the rules governing print newspapers, under which the Council's failure to respond within the set period is deemed tacit approval of the licence.

Problems arise with the financial and time conditions. High application fees for operating websites create a real barrier to entry for small initiatives and independent projects, and turn the licence into a start-up cost that is out of proportion to the inherently low-cost nature of digital publishing.

Moreover, the deadlines for reviewing applications and issuing decisions, even though they are set out in the Regulations, are not coupled with an effective mechanism that prevents applications from being stalled through silence: a failure to respond within the deadline does not produce "tacit approval", as is the case in some systems more protective of pluralism.

The Executive Regulations also provide that the licence lasts five years and is renewable upon an application submitted six months before expiry, with renewal requiring payment of the same fee after the conditions are reviewed. Under Article 16,[26] the Regulations require licensed media outlets and websites to retain all material broadcast for at least one year and to deposit a copy with the Council, and to keep a copy of the servers hosting the electronic version inside the Arab Republic of Egypt in a location that is "secure and known to the Council", which may not be changed without the Council's approval.

These requirements may appear reasonable from a regulatory perspective, but they go beyond the idea of a "licence" to impose ongoing operational obligations such as archiving content, depositing a copy with the Council and localising servers inside Egypt in a place known to it. This may make it easier to consult archives and to implement any subsequent regulatory measures, without necessarily implying direct censorship. On the other hand, it heightens the sensitivity of archive and operational data security, which calls for clearer safeguards on the limits of requests, their procedures and the right to appeal, in order to reduce the risk of abuse or leaks.

[26] Article 16 of Prime Ministerial Decree No. 418 of 2020: Licensed media outlets and websites must retain all material broadcast for no less than one year from the date of broadcast and deposit a copy of it with the Supreme Council monthly. A copy of the servers hosting the electronic version must be kept in a location determined by the media outlet or website inside the Arab Republic of Egypt, provided that it is secure and known to the Supreme Council, and it may not be changed without the Supreme Council's approval.

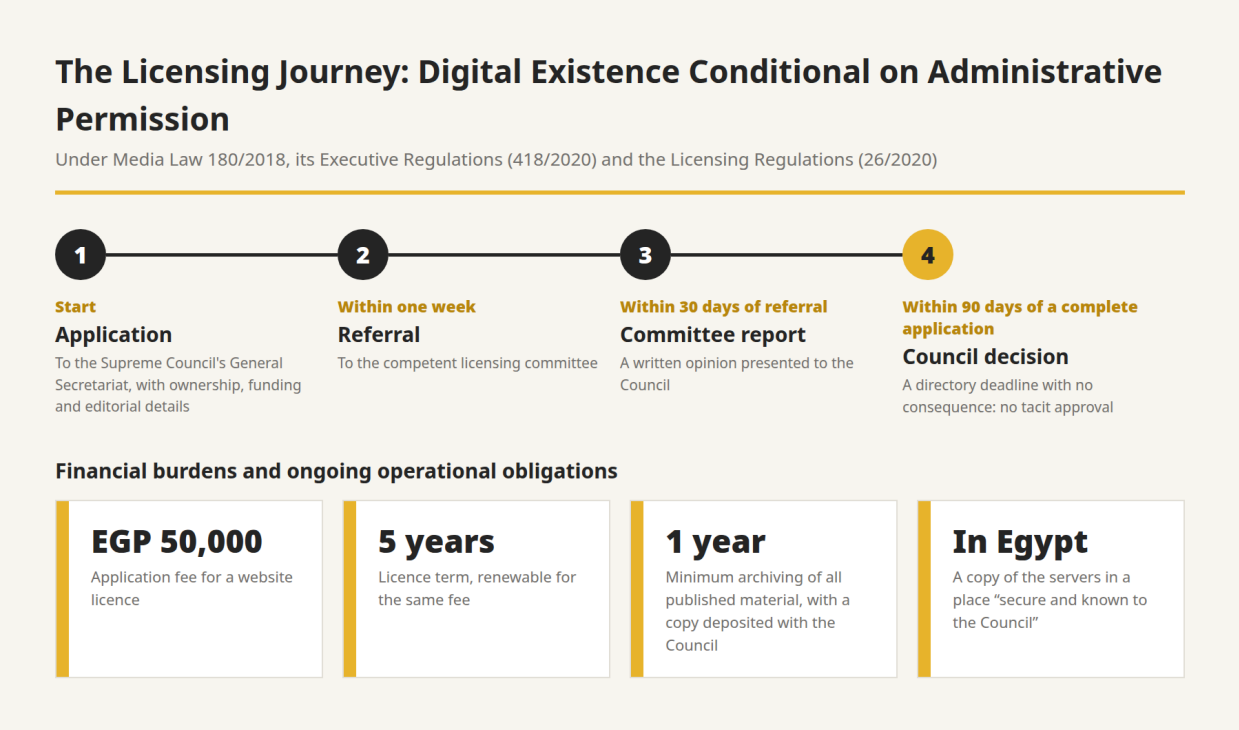


Figure 6: The stages and burdens of website licensing

The Licensing Regulations, under Article 5,[27] provide that licence templates issued by the Supreme Council set out rights, obligations and conditions that may not be violated, all of which are considered essential terms of the licence. They grant broad discretionary latitude in setting the rules for granting licences and the templates for accepting licence applications.

In light of the above, the licensing system works as a mechanism that turns digital journalistic existence into existence conditional on revocable administrative permission. Once legality is tied to a licence, failure to obtain one, or any dispute over its renewal, becomes a ready-made entry point for triggering suspension and blocking tools outside the logic of after-the-fact accountability for specific content. The licence thus changes from a founding procedure into an ongoing disciplinary tool that enables the regulator to control the continuity of independent platforms, and in practice expands the use of blocking as a tool for managing the digital public sphere rather than as a limited, exceptional measure.

[27] Article 5 of Decree No. 26 of 2020 issuing the Licensing Regulations of the Supreme Council for Media Regulation: "The licence templates issued by the Supreme Council set out all rights, obligations and conditions that may not be violated, all of which are considered essential terms of the licence."

Four: The Expanding Criminalisation of Possessing and Using Telecommunications Equipment

The 2022 amendments to Egypt's Telecommunications Regulation Law marked a qualitative shift in the law, when the Cabinet approved a draft amendment[28] aimed at increasing penalties for possessing and using illegal mobile signal boosters as part of a plan to "regulate the telecommunications system".

This framing puts a specific phenomenon up front, but produces a general legislative solution that goes beyond the phenomenon and establishes an expandable rule. The draft then went to the House of Representatives, the final text was approved, and at the end of December the amendment to the Telecommunications Regulation Law was issued as Law No. 172 of 2022.[29]

The amendment centred on replacing two provisions: the first paragraph of Article 44 and Article 77 of the law.[30] Under the new wording, the prohibition is no longer confined to the stages of bringing equipment to market (such as import, manufacture or assembly), but extends to acts at the heart of everyday practice, such as possession, use, operation, installation and marketing.

[28] Al-Shorouk, "Government approves amending provisions of the Telecommunications Regulation Law and increasing penalties for possessing mobile signal boosters", July 2022: https://www.shorouknews.com/news/view.aspx?cdate=28072022&id=e654a0cf-d8e4-4639-b3fa-b69e8b2ebbfc

[29] The amendment to the Telecommunications Regulation Law was issued as Law No. 172 of 2022 and published in the Official Gazette (Issue 51 bis (e), 26 December 2022): https://mediadr.sis.gov.eg/handle/123456789/49930

[30] Text of the amendments as published in the Official Gazette, Issue 51 bis (e), 26 December 2022. The first paragraph of Article 44 and Article 77 of the Telecommunications Regulation Law issued by Law No. 10 of 2003 are replaced by the following. Article 44, first paragraph: It is prohibited to import, manufacture, assemble, possess, use, operate, install or market any telecommunications equipment without first obtaining a permit from the Authority, in accordance with the standards, specifications and types of equipment it approves. Article 77: Subject to the last paragraph of Article 48 of this law, anyone who imports, manufactures, assembles or markets any telecommunications equipment without a permit from the Authority, in violation of the first paragraph of Article 44, shall be punished with imprisonment of no less than one year and no more than five years and a fine of no less than two million pounds and no more than five million pounds, or either penalty. Anyone who possesses, uses, installs or operates any telecommunications equipment without a permit from the Authority, in violation of the first paragraph of Article 44, shall be punished with imprisonment and a fine of no less than one hundred thousand pounds and no more than three hundred thousand pounds, or either penalty; this penalty does not apply to wireless devices for which the Authority issues a general licence for possession, use, installation or operation, without prejudice to Article 44. The penalty shall be aggravated imprisonment if the import, manufacture, assembly, possession, installation, operation, use or marketing of the unlawful equipment is for the purpose of harming national security. The penalties in the first, second and third paragraphs are doubled in their minimum and maximum in case of recidivism. In all cases, the court shall order the confiscation of the equipment involved and its components.

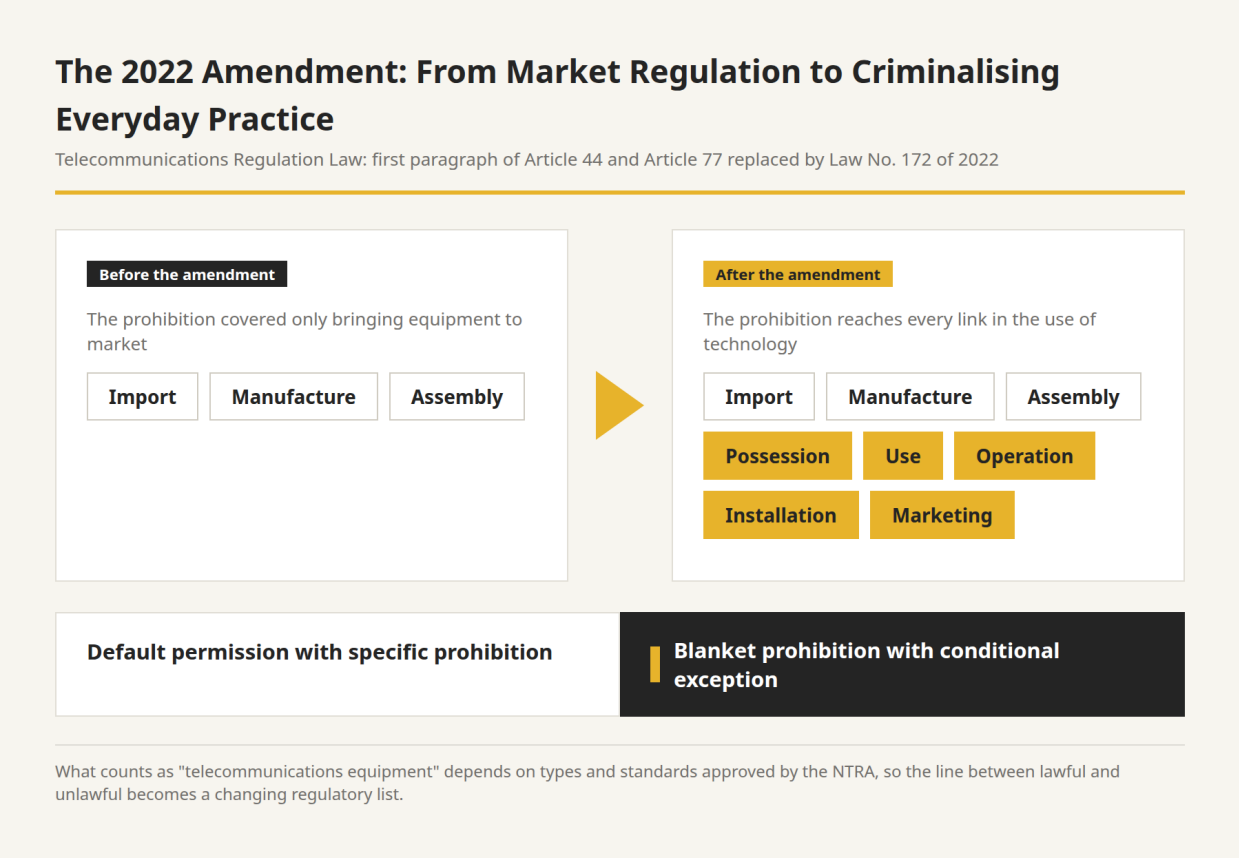


Figure 7: The scope of the prohibition before and after the 2022 telecommunications amendment

Regulation is therefore no longer limited to the links in the chain that bring equipment to market, but extends, by the text itself, to the level of everyday practice, because the prohibition covers possession, use, operation, installation and marketing.

As a result of this breadth, permit requirements may extend to routine technical activities that are legitimate in themselves, such as maintenance, repairs and field testing, whenever the tools used are considered "telecommunications equipment". The scope of what counts as "telecommunications equipment" is also tied in practice to the types and standards approved by the NTRA, making compliance dependent on a regulatory classification that may widen or narrow.

The current rule therefore does not only target high-risk equipment or directly harmful uses, but opens the way for common technical practices to be treated as presumptively suspect unless permit requirements are met.

Another problem is that the text treats "telecommunications equipment" as a single block, whereas technologies are not equal in their risks or functions. Some equipment may be used to jam frequencies, disrupt networks or undermine the integrity of communications, but most equipment consists of ordinary operating tools, testing and maintenance tools, components of wired and wireless networks, or measuring devices and accessories needed by technicians and researchers. When the same criminal logic is applied to this entire spectrum, the law becomes a generator of arbitrariness, and control over technology shifts from targeting specific risks to general, pre-emptive control that criminalises possession, use, operation, installation and marketing.

The restrictive effect is compounded by the way the law refers to the NTRA. The provision ties the legality of an act to standards, specifications and types "approved by the Authority". The line between lawful and unlawful thus depends in practice on changing regulatory lists and standards rather than on a precise, stable legislative definition that can be easily applied. To the extent that these lists and standards lack transparency or are not easily accessible, compliance becomes an arduous process based on constantly checking the Authority's decisions, rather than on a clear legal rule that a citizen, technician, trader or researcher can understand on its own terms.

This point matters because we are dealing with a rule with criminal consequences, in which the administrative classification of equipment becomes a condition for avoiding punishment. The relationship between the individual and the law shifts from "default permission with specific prohibition" to "blanket prohibition with conditional exception", weakening the ability to comply and making technology itself an object of restriction before it can be a means of exercising rights or of legitimate economic or research activity.

The breadth of the text also reverses the burden of compliance. Instead of the authorities having to prove that specific equipment was used harmfully, caused interference or threatened networks, individuals and technical actors must prove in advance that what they have is "permitted and approved". This shift produces a broad chilling effect even without intensive criminal enforcement, because mere uncertainty about the scope of "telecommunications equipment" and what counts as "approved" is enough to create self-censorship among users and technicians, and to deter them from acquiring, testing or trading equipment that may be necessary for work, research or maintenance.

The effect also extends to the economic and technical sphere. Maintenance markets, spare parts, second-hand sales, small workshops and local service providers depend on trading in equipment, parts and accessories that could, under a broad interpretation, be classified as telecommunications equipment. When this market becomes subject to criminal risk linked to permits, compliance costs such as fees, permits, procedures and potential business interruption rise sharply, which small actors certainly cannot bear. This can create an indirect monopolistic effect: those with the administrative and financial capacity to manage permits and standards will survive, and those without it will retreat or operate under permanent threat.

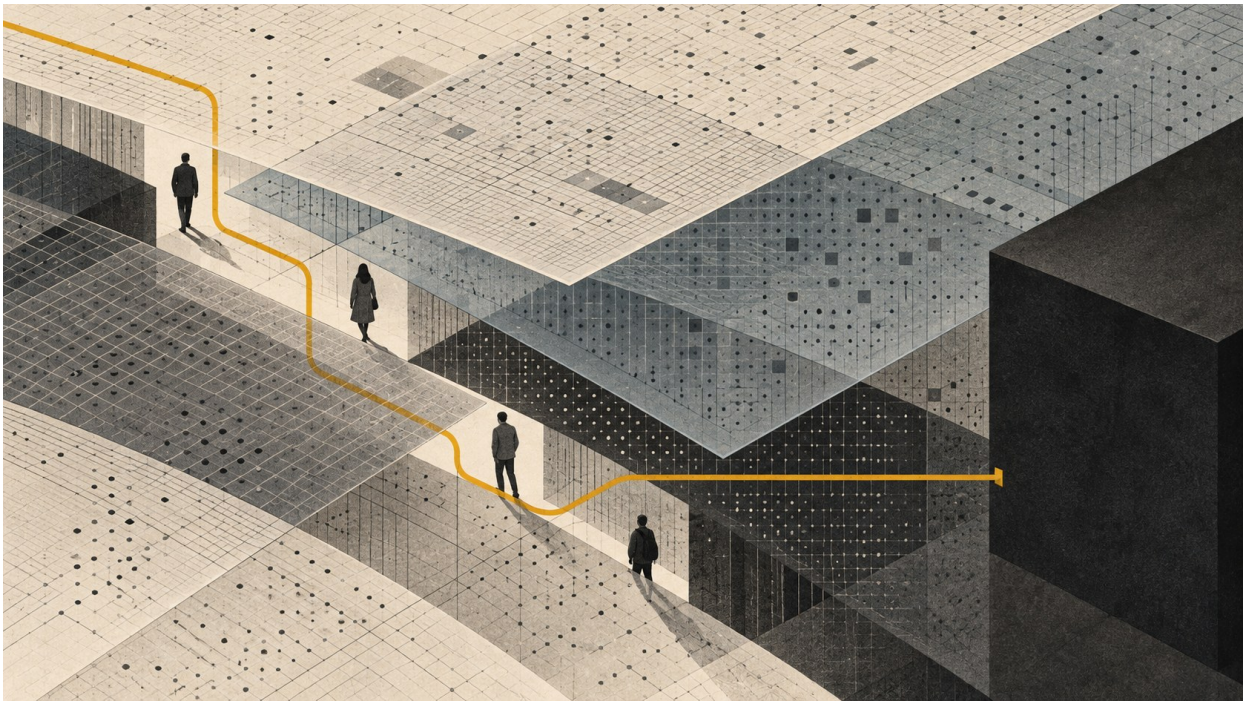
Similar consequences emerge for the research and educational community. Research in networking, information security and wireless communications often requires tools for measuring, testing, assembling, modifying and operating a range of equipment. When this activity is placed within the scope of prior criminal suspicion, technical innovation becomes conditional on approvals that may be unclear or slow, and there is a growing tendency to avoid certain research projects, move them abroad, or confine them to large institutions.

In terms of enforcement, this legislative structure increases the risk of selective targeting. Because the text is broad and much of the equipment is dual-use, determining a violation in practice may depend more on the context of seizure, inspection and administrative assessment than on tangible

harm. This kind of breadth creates a high likelihood of detention, confiscation and criminalisation based on discretion, and makes the protection of legitimate technical work that carries no exceptional risk even more fragile.

The rationale usually advanced by the state for such amendments rests on the vocabulary of national security, protecting networks from interference, and preventing the illegitimate use of signal boosters and similar devices. In principle, this rationale is not objectionable in itself. From a digital rights perspective, however, its assessment depends not only on the stated aim but on the nature of the restriction, its tools and its safeguards: how clear the rule is and how well its scope is defined; whether it can distinguish between high-risk and ordinary equipment; whether there are practical exceptions for maintenance, research and experimentation; whether standards are transparent, easily accessible and open to effective challenge; and whether sanctions are graduated so that criminal punishment remains a last resort.

Five: Mass Surveillance



The accumulating layers of data collection and interception

Egypt's legislative structure treats mass surveillance as a permanent operational capability managed through cumulative, ongoing rules, rather than as intervention when necessary. Networks are legally designed to remain accessible to institutions, data is stored in advance, and interception procedures are simplified. This kind of arrangement increases the risk of broad interference, because a capability built as an operating rule tends to expand and recur even beyond the most serious cases.

To understand how this system works, it helps to view surveillance as layers that integrate rather than merely sit side by side. The state does not rely on a single tool (such as content interception), but on a chain of tools covering infrastructure (the network), data (retention), procedures (authorisations) and classifications (terrorism cases), supplemented by less visible links relating to sharing, storage and information security.

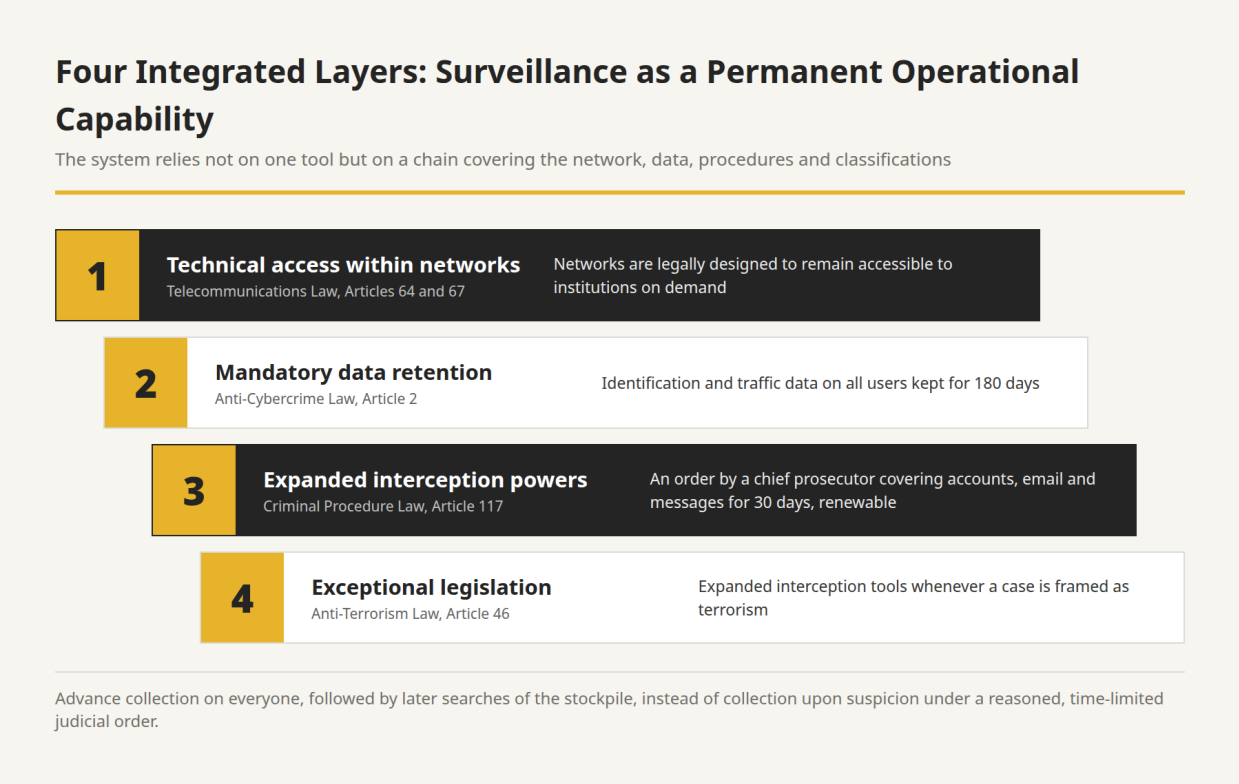


Figure 8: The four layers of surveillance and their legal basis

Layer One: Technical Access Built into Networks

The first layer sits within the networks and infrastructure themselves, established by the Telecommunications Regulation Law No. 10 of 2003 in Article 67, which places the national security agencies at the core of the legal design of the relationship between the state and telecommunications operators.

Under this framing, the network becomes a domain that must remain accessible to institutions on demand. This moves the debate from whether surveillance exists to how the capacity for surveillance has been built into the infrastructure itself. It follows that the value of safeguards depends not on declarations of general principle, but on the limits placed on requests, their documentation and independent oversight of their use, none of which exist in Egypt.

Layer Two: Mandatory Data Retention as the Rule

The Anti-Cybercrime Law (Article 2)[31] obliges service providers to retain usage data for 180 days, including identification data, traffic data and related information that makes it possible to trace

[31] Article 2 of the Anti-Cybercrime Law (Obligations and duties of the service provider). First: Without prejudice to this law and the Telecommunications Regulation Law No. 10 of 2003, service providers shall: (1) keep and store the log of the information system or of any means of information technology for 180 consecutive days, the data to be kept and stored being: (a) data enabling identification of the service user; (b) data relating to the content of the information system handled, where under the provider's control; (c) data relating to communications traffic; (d) data relating to terminal devices; (e) any other data specified by decision of the Authority's board of directors; (2) maintain the confidentiality of the data kept and stored and not disclose it without a reasoned order from a competent judicial body, including the personal data of any users of their service or any data or information relating to the websites and private accounts those users access, or the persons and bodies with whom they communicate; (3) secure data and information so as to preserve their confidentiality and prevent their interception, penetration or damage. Second: Without prejudice to the Consumer Protection Law No. 67 of 2006, the service provider must make the following information available to its

patterns and relationships. What deserves emphasis here is that this data, even when it does not include content, is not low-sensitivity: metadata (source, destination, time, duration, type of service and so on) can draw a precise map of digital life, such as circles of communication, patterns of movement, recurring points of contact and associations of interest.

> **"Surveillance shifts from collection upon suspicion to advance collection on everyone, followed by later searches of the stockpile."**

Surveillance thus shifts from collection upon suspicion, under a reasoned judicial order for a specified period, to advance collection on everyone followed by later searches of the stockpile. This pattern increases the risk of abuse because it makes wide-scale interference the default, and leaves the question of who is examined and why to later decisions that are neither transparent nor open to challenge. The legislative effect of this provision is that data retention is not merely a matter of commercial or privacy policy, but an obligation that exposes a company to liability if it fails to comply, because the law itself ensures the data exists and is ready for use.

Layer Three: Expanded Interception Powers in Criminal Procedure

Expanding interception powers within the criminal procedure system is not only about expanding investigative tools. It shifts the centre of gravity towards pathways that normalise interception in investigations, particularly when the power to issue orders lies with a body closer to the day-to-day investigative system and operates under broader discretionary standards.

The amendments in the new Criminal Procedure Law include provisions granting the prosecution broad discretionary powers over pre-trial detention, interception of communications and travel bans, shifting the centre of gravity from strict judicial oversight to the authority of the Public Prosecution, a lower judicial tier. This means widening the scope of communications surveillance and transforming it from a measure limited in time and cause into a practice that can be normalised in investigations.[32]

Layer Four: Exceptional Legislation under the Umbrella of Counter-Terrorism

The fourth layer consists of legislation of an exceptional nature that raises the ceiling of intervention under the umbrella of counter-terrorism. The Anti-Terrorism Law No. 94 of 2015, in

users and to any competent government body, in a form and manner that is easily, directly and continuously accessible: (1) its name and address; (2) its contact information, including electronic contact address; (3) its licence details identifying it and the competent supervisory body; (4) any other information the Authority considers important for protecting service users, as specified by decision of the competent minister. Third: With due regard for the inviolability of private life guaranteed by the Constitution, service providers and their affiliates shall, upon the request of national security bodies and according to their needs, provide all technical capabilities enabling those bodies to exercise their powers in accordance with the law. Fourth: Information technology service providers and their agents and distributors responsible for marketing these services shall obtain users' data, and others are prohibited from doing so.

[32] Articles 114, 117 and 531 of Law No. 174 of 2025 issuing the Criminal Procedure Law.

Article 46,[33] grants expanded tools for intercepting communications and surveillance, and lends these measures broader legitimacy when cases are framed as terrorism offences.

As definitions of terrorism and its promotion expand, so does the room to bring digital activity or political or journalistic communication within this framework. Interception tools are then invoked in a form that appears lawful, while in reality the circle of suspicion and intervention widens.

These layers are compounded by a gap in safeguards, accountability and data security. Mandatory retention creates a huge stockpile of sensitive data, raising the risk of misuse or expanded access, as well as the risk of leaks or breaches, risks that cannot be separated from the protection of privacy itself. The accumulation of powers among multiple bodies and the multiplicity of possible legal routes to access also blur the practical limits of intervention and weaken traceability and effective public scrutiny.

In this context, any discussion of privacy that does not analyse data retention rules, access pathways and oversight of use is incomplete, because the ceiling of digital rights is determined in practice by how disciplined this structure is, not by the mere existence of the right in legal texts.

[33] Article 46 of the Anti-Terrorism Law No. 94 of 2015: "In a terrorist crime, the Public Prosecution or the competent investigating authority, as the case may be, may authorise by reasoned order, for a period not exceeding thirty days, the monitoring and recording of conversations and messages received through wired and wireless and other modern means of communication, the recording and filming of what takes place in private places or through communications or information networks or websites and what is posted on them, and the seizure of ordinary or electronic correspondence and messages, printed matter, parcels and telegrams of all kinds. The order referred to in the first paragraph of this article may be renewed for one or more further periods."

Six: Weak Personal Data Protection Rules

The Personal Data Protection Law No. 151 of 2020 was issued as the first relatively comprehensive framework for regulating the handling of personal data in Egypt. In its theoretical design, the law presents itself as a system that sets principles for lawful processing, grants rights to data subjects and imposes security and procedural duties on controllers and processors.

Assessing the strength of protection, however, depends not only on the existence of these principles, but on their enforceability, the limits of the exceptions that restrict them, the nature of the body responsible for applying them, and its independence and transparency. The law creates a strong new backing for privacy, but at the same time builds enforcement exceptions that make privacy a right easily suspended when security considerations are invoked and when independent oversight and transparency, as preconditions for protection, are absent.

This is evident in the scope of the exceptions in Article 3[34] of the law's promulgation articles. Among other things, the article excludes from its application data processed for personal use, data processed for official statistical purposes or in application of a legal provision, data processed exclusively for media purposes subject to conditions, and data relating to law-enforcement records, investigations and court cases. It then sets out a broad exception for data held by national security bodies and whatever they deem necessary for other considerations.

The law establishes a mechanism giving national security bodies direct influence over the circulation of data held by other entities: at the request of the national security bodies, the Data Protection Centre must notify the controller or processor to modify, erase, withhold, or cease making available or circulating data within a specified period, and the controller or processor is bound to implement the notification.

"Privacy is named as a right, and then gateways of exception are opened that tie the ceiling of protection to the structure of power and its channels."

[34] Article 3 (promulgation articles of Law No. 151 of 2020): The provisions of the attached law do not apply to: (1) personal data held by natural persons about others and processed for personal use; (2) personal data processed for the purpose of obtaining official statistical data or in application of a legal provision; (3) personal data processed exclusively for media purposes, provided that it is correct and accurate and is not used for any other purpose, without prejudice to the legislation regulating the press and media; (4) personal data relating to judicial police records, investigations and court cases; (5) personal data held by national security bodies and whatever they deem necessary for other considerations; at the request of the national security bodies, the Centre must notify the controller or processor to modify, erase, withhold, or cease making available or circulating personal data within a specified period in accordance with national security considerations, and the controller or processor must implement the notification within that period; (6) personal data held by the Central Bank of Egypt and the entities subject to its supervision and oversight, except money transfer companies and exchange companies, which shall observe the Central Bank's rules on handling personal data.

Another exception concerns data held by the Central Bank or entities licensed by the Central Bank to operate in Egypt (the banking sector and the non-banking financial sector). This means an entire sector is removed from the general data protection system, producing unequal levels of protection and enforcement depending on who holds the data, and in practice limiting individuals' ability to use general protection mechanisms against an exempt entity.



Figure 9: Exceptions to the scope of the Personal Data Protection Law

As for the law's Executive Regulations, instead of focusing on transparent and specific safeguards that restrict the circulation of data and give data subjects clear complaint mechanisms, they introduce a wide network of prior regulatory requirements, such as requiring a licence or permit to act as a controller or processor, and tying data collection to approvals and mechanisms endorsed by the Centre.[35]

This legal design may be understood from a regulatory perspective as an attempt to organise the market, but at the same time it ties protection to heavy administrative compliance and gives the regulator a broad role in approving mechanisms and standards, raising questions about its independence, the publicity of its decisions, the consistency of its standards and the possibility of effectively challenging approval and licensing decisions.

There are also concerns about how data breaches are managed under the Executive Regulations. The Regulations require the reporting of data breaches and add a special track where an incident is "related to national security protection considerations", requiring immediate reporting. They

[35] Masaar and the Egyptian Initiative for Personal Rights (EIPR), "The Executive Regulations of the Personal Data Protection Law: Testing the Conversion of General Rules into Accountable Obligations", February 2026: https://masaar.net/ar/testing-the-executive-regulations-data-protection-law/

then require the Centre to provide a special communication channel for receiving reports related to national security and to coordinate with the national security bodies on mechanisms for notifying them upon receipt of such reports.

These rules do not negate the obligation to notify data subjects, but they show that breach management is not understood only as a protection pathway for individuals: it includes a parallel institutional channel of a security nature in certain cases, which may alter the balance of transparency and the nature of the information circulated about the incident and its scope.[36]

Another equally serious effect appears in the exceptions for journalistic and media work. The law exempts data processing for journalistic or media purposes on condition of accuracy and non-use for other purposes, while affirming that this is without prejudice to the laws regulating the press and media.

This exception does not appear to function as independent protection for the journalistic environment and its sources so much as remaining governed by another regulatory framework that can impose broad administrative restrictions on publication and platforms, limiting the protective value of the exception whenever the demands of media regulation conflict with those of data protection.

In short, Egypt has a data protection law with a modern appearance, but the protection equation remains unstable as long as security exceptions remain broad and expandable, and as long as the enforcement model rests on licences, approvals and standards drafted and adopted by a Centre that is supposed to guarantee the right. Privacy is named as a right, and then gateways of exception are opened that tie the ultimate ceiling of protection to the structure of power and its channels rather than to human rights and legal principles alone.

[36] Ibid.

Seven: False News, Insult and Defamation Offences as Tools of Digital Control

Egypt's Penal Code No. 58 of 1937 functions today as one of the most effective tools for restricting digital rights. Its effectiveness stems from its being a vast repository of elastic offences that can easily be applied to speech published online.

What most clearly opens the door to applying these provisions to online expression is that the Penal Code itself sets a broad definition of publicity and incitement, which explicitly includes publication by any other means of publicity, and brings attribution, insult, defamation or incitement within the scope of criminalisation if committed by one of the means set out in Article 171.

Article 171[37] addresses public incitement by speech, shouting, act or gesture, or by writing, drawings, images or symbols, or by any other means of publicity. This expanded concept of publicity is what allows a social media post, blog entry, comment or video to be treated as public publication whenever it is deemed to have reached others or been made available to them, even if it was restricted (of limited publicity, such as posts visible to friends only or to specific contacts). This is where the Penal Code's arsenal of offences affecting digital expression begins, the best known being false news, insult and defamation, and insulting or disparaging state bodies or officials, alongside offences related to belief, religion, or incitement to hatred and discrimination, and "indecent publication".

[37] Article 171 of the Egyptian Penal Code No. 58 of 1937: "Anyone who incites one or more persons to commit a felony or misdemeanour by speech or shouting uttered publicly, by an act or gesture made publicly, or by writing, drawings, pictures, photographs, symbols or any other method of representation made public, or by any other means of publicity, shall be deemed an accomplice in the act and punished with the penalty prescribed for it if the incitement results in the felony or misdemeanour actually being committed. If the incitement results merely in an attempt, the judge shall apply the legal provisions on punishing attempts. Speech or shouting is deemed public if uttered or repeated by mechanical means in a public gathering, public road or any other frequented place, or if uttered or repeated so that it can be heard by anyone in such a road or place, or if broadcast by wireless or any other means. An act or gesture is deemed public if it takes place in a public gathering, public road or other frequented place, or so that it can be seen by anyone in such a road or place. Writing, drawings, pictures, photographs, symbols and other methods of representation are deemed public if distributed indiscriminately to a number of people, displayed so that they can be seen by anyone on a public road or in a frequented place, or sold or offered for sale in any place."

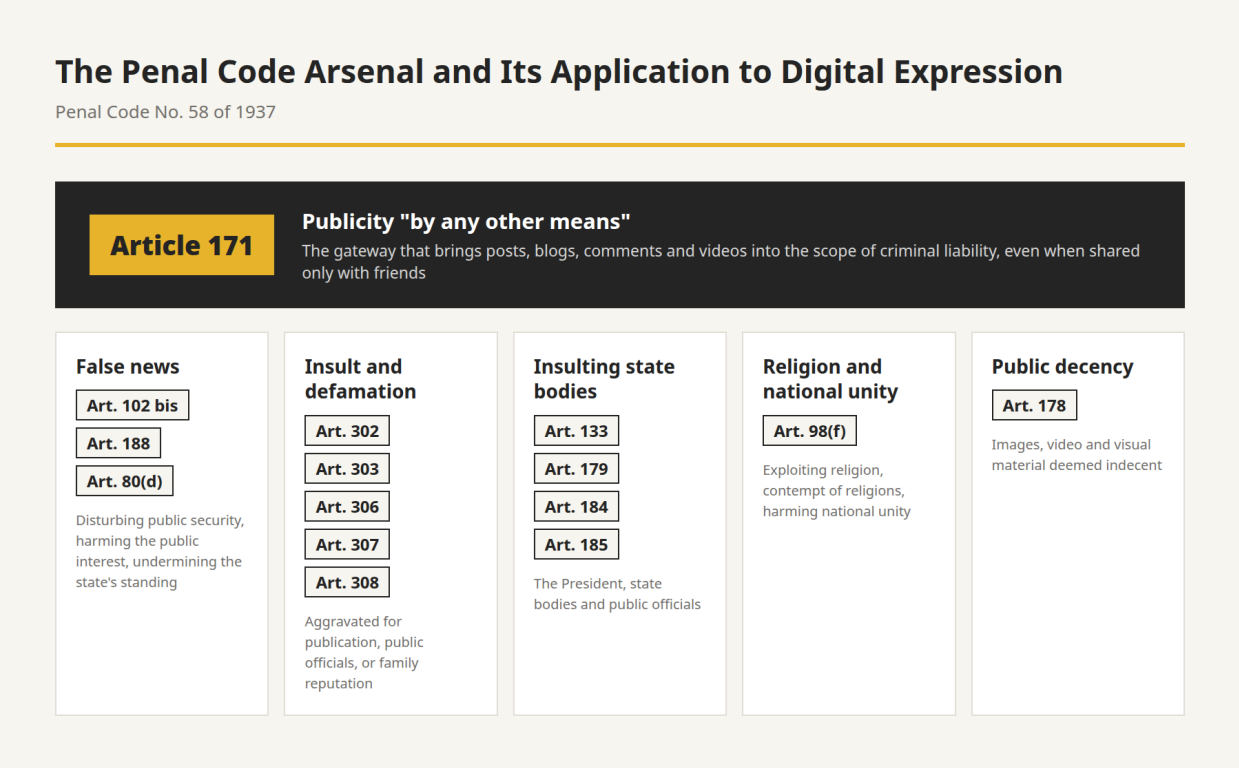


Figure 10: Penal Code articles used to prosecute digital expression

On publishing false news, criminalisation is spread across several articles with different limits and circumstances. Article 102 bis[38] punishes anyone who deliberately broadcasts false news, statements or rumours if this is liable to disturb public security, spread terror among people or harm the public interest, with a harsher penalty in time of war.

The scope of the false news offence extends to possessing writings or publications containing such false news if they are intended for distribution or for others to see, as well as possessing printing, recording or other means of publicity designated for printing, recording or broadcasting such content.

At another level, Article 188[39] focuses on the act of publishing, with bad intent, false news, statements or rumours, or fabricated or forged papers, or papers falsely attributed to others, if this is liable to disturb public peace, cause panic among people or harm the public interest, and sets a penalty of imprisonment and a fine, or either.

[38] Article 102 bis of the Egyptian Penal Code No. 58 of 1937: "Anyone who deliberately broadcasts false news, statements or rumours, if this is liable to disturb public security, spread terror among people or harm the public interest, shall be punished with imprisonment and a fine of no less than fifty pounds and no more than two hundred pounds. The penalty shall be rigorous imprisonment and a fine of no less than one hundred pounds and no more than five hundred pounds if the crime is committed in time of war. The penalties in the first paragraph apply to anyone who, personally or through an intermediary, possesses or holds writings or publications containing any of the matters set out in that paragraph if intended for distribution or for others to see, and to anyone who possesses or holds any means of printing, recording or publicity designated, even temporarily, for printing, recording or broadcasting any of the foregoing."

[39] Article 188 of the Egyptian Penal Code No. 58 of 1937: "Anyone who publishes with bad intent, by any of the aforementioned means, false news, statements or rumours, or fabricated or forged papers or papers falsely attributed to others, if this is liable to disturb public peace, cause panic among people or harm the public interest, shall be punished with imprisonment for no more than one year and a fine of no less than five thousand pounds and no more than twenty thousand pounds, or either penalty."

This highlights a logic that recurs frequently in practice. Falsity does not always have to be established by an explicit evidentiary standard or specific verification procedures; according to the text, it is enough that bad intent is present and that the publication is liable to produce one of the general effects listed in the law (such as disturbing public peace or harming the public interest). The article sets criteria that cannot be disproved or rebutted, such as whether the news or statement was published with bad intent, a discretionary matter that is difficult to prove.

Along a line more closely tied to the state's image abroad, Article 80(d)[40] criminalises broadcasting false news, statements or rumours abroad about the country's internal conditions if this is liable to weaken the financial confidence in the state or its prestige and standing, or to harm national interests, with a harsher penalty in time of war.

Since the internet is inherently transnational, the global circulation of content can in principle bring posts accessible outside the country into the scope of debate about applying this provision, depending on whether the investigating authorities consider its elements to apply to a particular case.

On insult and defamation as offences affecting online freedom of expression, particularly where the expression is political, journalistic or public criticism, the Penal Code defines defamation in Article 302[41] as attributing to another person, by one of the means set out in Article 171, matters which, if true, would require that person's legal punishment or expose them to contempt among their fellow citizens. This provision can therefore be used against online publication as a form of publicity.

Article 303[42] then sets the penalty for defamation as a fine within certain limits, increased if the defamation targets a public official, a person holding a public representative office or a person entrusted with a public service, in connection with the performance of their duties. In parallel, Article 306[43] defines insult as any insult that does not include the attribution of a specific fact but

[40] Article 80(d) of the Egyptian Penal Code No. 58 of 1937: "Any Egyptian who deliberately broadcasts abroad false news, statements or rumours about the internal conditions of the country, if this is liable to weaken the financial confidence in the state or its prestige and standing, or who engages in any way in an activity liable to harm the national interests of the country, shall be punished with imprisonment for no less than six months and no more than five years and a fine of no less than 100 pounds and no more than 500 pounds, or either penalty. The penalty shall be rigorous imprisonment if the crime is committed in time of war."

[41] Article 302 of the Egyptian Penal Code No. 58 of 1937: "A person is guilty of defamation who, by one of the means set out in Article 171 of this law, attributes to another matters which, if true, would require that person's punishment under the law or expose them to contempt among their fellow citizens. However, criticism of the acts of a public official, a person holding a public representative office or a person entrusted with a public service does not fall under the preceding paragraph if made in good faith and not exceeding the acts of the office, representation or public service, provided that the accused proves the truth of every act attributed to the victim; the investigating authority or the court, as the case may be, may order administrative bodies to produce papers or documents in their possession supporting the evidence presented by the accused to prove those acts. The defamer may not offer evidence to prove the defamatory matters except in the case set out in the preceding paragraph."

[42] Article 303 of the Egyptian Penal Code No. 58 of 1937: "Defamation shall be punished with a fine of no less than five thousand pounds and no more than fifteen thousand pounds. If the defamation targets a public official, a person holding a public representative office or a person entrusted with a public service, in connection with the performance of the office, representation or public service, the penalty shall be a fine of no less than ten thousand pounds and no more than twenty thousand pounds."

[43] Article 306 of the Egyptian Penal Code No. 58 of 1937: "Any insult that does not include the attribution of a specific fact but in any way offends honour or reputation shall be punished, in the cases set out in Article 171, with a fine of no less than two thousand pounds and no more than ten thousand pounds."

that in any way offends honour or reputation, and punishes it, where publicity under Article 171 is present, with a fine within its limits.

Nor does the matter stop at publication by individuals (as opposed to a news organisation), because the law sets aggravating mechanisms tied to the means of publication. Article 307 provides that if certain offences (including Articles 182 to 185, 303 and 306) are committed through publication in a newspaper or printed matter, the minimum and maximum fines are doubled, a logic that makes "public publication" an aggravating factor in itself. Article 308 then goes further where disparagement, insult, defamation or abuse involves attacks on the honour of individuals or damage to the reputation of families, making the penalty both imprisonment and a fine within the limits it sets, and setting a minimum term of imprisonment and a minimum fine in cases of publication in newspapers or printed matter.

In cases involving insult or disparagement of the state, its institutions or officials, an area that frequently intersects with political expression online, a group of articles criminalises forms of insult or abuse directed at a public official, a public body or the head of state. This can lead to custodial penalties for publication, as well as the possibility of expanded charges where political criticism is involved. Article 133[44] punishes anyone who insults, by gesture, word or threat, a public official, a member of the police or any person entrusted with a public service during or because of the performance of their duties, with a harsher penalty if the insult is directed at a court or council during a session. Article 185[45] sets a specific penalty for insulting a public official, a person holding a public representative office or a person entrusted with a public service in connection with the performance of their duties.

At another level, Article 179[46] punishes insulting the President of the Republic by any of the aforementioned means, that is, through means of publicity, which brings digital posts and comments within the scope of potential application whenever they are characterised as an insult. Article 184[47] punishes anyone who insults or abuses the House of Representatives or other state bodies, the army, the courts, or public authorities or agencies by any of the aforementioned means, which means that sharply critical expression towards state institutions may be recast in criminal terms as insult or abuse at the discretion of the prosecution or the court.

[44] Article 133 of the Egyptian Penal Code No. 58 of 1937: Anyone who insults, by gesture, word or threat, a public official, a member of the police or any person entrusted with a public service during or because of the performance of their duties shall be punished with imprisonment for no more than six months or a fine not exceeding two hundred Egyptian pounds. If the insult is directed at a judicial or administrative court or council, or one of its members, during a session, the penalty shall be imprisonment for no more than one year or a fine not exceeding five hundred Egyptian pounds.

[45] Article 185 of the Egyptian Penal Code No. 58 of 1937: "Anyone who insults a public official, a person holding a public representative office or a person entrusted with a public service, in connection with the performance of the office, representation or public service, shall be punished with a fine of no less than ten thousand pounds and no more than twenty thousand pounds, without prejudice to the application of the second paragraph of Article 302 where the insult is linked to a crime of defamation committed by the same accused against the same victim."

[46] Article 179 of the Egyptian Penal Code No. 58 of 1937: Anyone who insults the President of the Republic by any of the aforementioned means shall be punished with a fine of no less than ten thousand pounds and no more than thirty thousand pounds.

[47] Article 184 of the Egyptian Penal Code No. 58 of 1937: "Anyone who insults or abuses, by any of the aforementioned means, the House of Representatives or other state bodies, the army, the courts, or public authorities or agencies shall be punished with imprisonment and a fine of no less than five thousand pounds and no more than ten thousand pounds, or either penalty."

In the area of expression relating to religion, belief or communities, the Penal Code contains provisions used to criminalise forms of speech. Article 98(f)[48] punishes anyone who exploits religion to promote extremist ideas, by speech, writing or any other means, with the intent of inciting sectarian strife, disparaging or showing contempt for one of the heavenly religions or its denominations, or harming national unity. This wording combines the element of intent with the element of means, making online publication open to prosecution whenever the elements of an offence against national unity are deemed present; under this wording, the medium itself (the digital space) becomes exposed to the penalties for offences of exploiting religion.

In cases of indecent publication affecting images, video and visual material circulated digitally, Article 178[49] criminalises publishing, making or possessing, with intent to trade, distribute or display, printed matter, manuscripts, drawings, images, symbolic signs or other objects or images in general if they offend public decency, punishable by imprisonment and a fine, or either.

[48] Article 98(f) of the Egyptian Penal Code No. 58 of 1937: "Anyone who exploits religion to promote, by speech, writing or any other means, extremist ideas with the intent of inciting sectarian strife, disparaging or showing contempt for one of the heavenly religions or the denominations belonging to it, or harming national unity, shall be punished with imprisonment for no less than six months and no more than five years or a fine of no less than five hundred pounds and no more than one thousand pounds."

[49] Article 178 of the Egyptian Penal Code No. 58 of 1937: "Anyone who publishes, makes or possesses, with intent to trade, distribute, rent, post or display, printed matter, manuscripts, drawings, advertisements, engraved or carved images, hand-drawn or photographic images, symbolic signs or other objects or images in general, if they offend public decency, shall be punished with imprisonment for no more than two years and a fine of no less than five thousand pounds and no more than ten thousand pounds, or either penalty."

Eight: Legal Control over Digital Content Creators through "Reclassification" and "Moral Criminalisation"

Legal control over digital content creators in Egypt operates through two parallel tracks that converge in their result, although they differ in their tools. The first is a regulatory and administrative track that reclassifies influential accounts as publication outlets subject to a regulatory jurisdiction similar to that governing traditional media. The second is a criminal track that expands criminalisation to reach forms of digital expression under vague moral and social headings. Together, the two tracks place content creators between a logic of regulatory compliance that threatens suspension or blocking, and a logic of criminal suspicion that opens the door to imprisonment and fines.

First: Reclassification and Subjecting Content Creators to a Regulatory Jurisdiction Similar to Traditional Media

The Press and Media Law does not stop at regulating press and media institutions as professional entities, but extends its reach to the personal digital sphere through the criterion of audience size. Article 19[50] does not impose prohibitions only on newspapers, outlets and websites, but binds personal websites, blogs and accounts to the same prohibitions once they reach five thousand followers or more.

The content of a personal account is therefore no longer mere individual expression, but is legally treated as a public publication medium expected to comply with regulatory standards originally designed for the press and media sector. The shift is all the sharper because the text does not merely state the obligation, but requires the Supreme Council to take appropriate action and empowers it to suspend or block the website, blog or account by its own decision, with the possibility of appeal before the administrative courts.

In practice, this means that content creators enter into a regulatory relationship with an administrative body, not because their activity has taken an institutional or professional form, but because their audience has grown. In this model, practices such as satire, experimentation, informal language and quick commentary become more sensitive, because the standard of

[50] Article 19 (Law No. 180 of 2018): Newspapers, media outlets and websites are prohibited from publishing or broadcasting false news or anything that calls for or incites violation of the law, violence or hatred, involves discrimination between citizens, calls for racism, or contains attacks on the honour of individuals, insults or defamation against them, or contempt for the heavenly religions or religious beliefs. Every personal website, personal blog or personal electronic account with five thousand or more followers is bound by the preceding paragraph. Without prejudice to the legal liability arising from violating this article, the Supreme Council must take appropriate action against the violation and may, to that end, suspend or block the website, blog or account by its own decision. Those concerned may challenge the decision before the Administrative Court.

violation in Article 19 is broad (false news, incitement, hatred, discrimination and so on) and is enforced through a fast-acting administrative decision.

This does not mean that appeal is unavailable; it is available. But it means that intervention comes first and review later, an arrangement that increases the tendency towards pre-emptive compliance among creators and influencers, who prioritise the safety of their accounts and continued access to their audience over the space for free expression.

Second: Moral and Social Criminalisation as a Criminal Track Pursuing Personal Expression

On a parallel track, the Anti-Cybercrime Law introduces a different layer of control. It is not based on reclassifying content creators as regulated actors, but on turning them into criminal suspects through provisions that intervene in digital identity, patterns of behaviour and expression. Articles 24 and 25 emerge here as the two key pillars.[51]

Article 24 criminalises creating an email address, website or account and falsely attributing it to another person, with graduated and harsher penalties if the use of the account harms the person to whom it was attributed or if the offence targets a public body.[52]

In principle, this criminalisation provides protection against impersonation and blackmail. The problem arises, however, when the limits of "fabrication" in practice come to affect widespread digital practices such as parody accounts, pseudonyms and satirical impersonation, particularly in an environment where political criticism overlaps with public-order sensitivities.

The risk is therefore not understood only as a risk to individual reputation, but as pressure on the right to appear in multiple forms in the digital space, narrowing the room for modes of expression based on anonymity, satire or digital personas that do not match one's official name.

Article 25 produces a more complex model, because it combines in a single article disparate headings: attacks on family values on the one hand, and multiple forms of privacy violation, digital

[51] Article 24 of the Anti-Cybercrime Law (Crimes relating to the fabrication of websites, private accounts and email): Anyone who creates an email address, website or private account and falsely attributes it to a natural or legal person shall be punished with imprisonment for no less than three months and a fine of no less than EGP 10,000 and no more than EGP 30,000, or either penalty. If the offender uses the fabricated email, website or account in a way that harms the person to whom it is attributed, the penalty shall be imprisonment for no less than one year and a fine of no less than EGP 50,000 and no more than EGP 200,000, or either penalty. If the crime targets a public legal person, the penalty shall be imprisonment and a fine of no less than EGP 100,000 and no more than EGP 300,000. Article 25 (Crimes relating to violations of the inviolability of private life and unlawful information content): Anyone who attacks any of the family principles or values of Egyptian society, violates the inviolability of private life, sends numerous electronic messages in bulk to a specific person without their consent, provides data to an electronic system or website to promote goods or services without consent, or publishes, through the information network or any means of information technology, information, news, images or the like that violate the privacy of any person without their consent, whether or not the published information is true, shall be punished with imprisonment for no less than six months and a fine of no less than fifty thousand pounds and no more than one hundred thousand pounds, or either penalty.

[52] Masaar, "The Crime of Fabricating Accounts and Its Relationship to Parody and Fake Accounts", May 2021: https://masaar.net/ar/%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9-%D8%A7%D9%84%D8%AD%D8%B3%D8%A7%D8%A8%D8%A7%D8%AA-%D9%88%D8%B9%D9%84%D8%A7%D9%82%D8%AA%D9%87%D8%A7-%D8%A8%D8%A7%D9%84%D8%AD%D8%B3/

harassment and promotion without consent on the other, with a penalty of imprisonment and a fine.

This combination creates two overlapping effects:

- First, the concept of family values remains an inherently broad standard, open to expansive interpretation, which allows moral criminalisation to shift from protecting people from specific harm to policing forms of expression and personal choice.
- Second, the article does not clearly distinguish between specific harm (violating a particular person's privacy or direct harassment) and a value judgement about content, so heterogeneous acts sit side by side within a single penal template.

Masaar's analyses of this article support the view that its ambiguous wording, especially the phrase "attacking family values", opens wide room for expanding charges, weakening predictability and undermining the principle of criminal legality. Egyptian civil society organisations have documented the use of Article 25 as the heading for a pattern of prosecutions that criminalise acts which, for the most part, were not crimes offline, and read it as a tool of social control with class and gender effects.[53]

The combination of these two tracks (reclassification and moral criminalisation) produces a double squeeze on content creators. On the one hand, they are pushed towards regulatory compliance because their accounts may be treated as publication outlets that can be administratively suspended or blocked under broad prohibitions. On the other hand, they face a criminal track that can reach their modes of appearance and expression through vague moral and social headings or through the criminalisation of certain forms of digital identity construction.

[53] Egyptian Initiative for Personal Rights (EIPR), "Disciplining Society: Legal Prosecution under the Banner of 'Egyptian Family Values'", December 2025: https://eipr.org/publications/%D8%AA%D8%A3%D8%AF%D9%8A%D8%A8-%D8%A7%D9%84%D9%85%D8%AC%D8%AA%D9%85%D8%B9-%D8%A7%D9%84%D9%85%D9%84%D8%A7%D8%AD%D9%82%D8%A9-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A%D8%A9-%D8%A8%D8%B1%D8%B9%D8%A7%D9%8A%D8%A9-%D9%82%D9%8A%D9%85-%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A%D8%A9

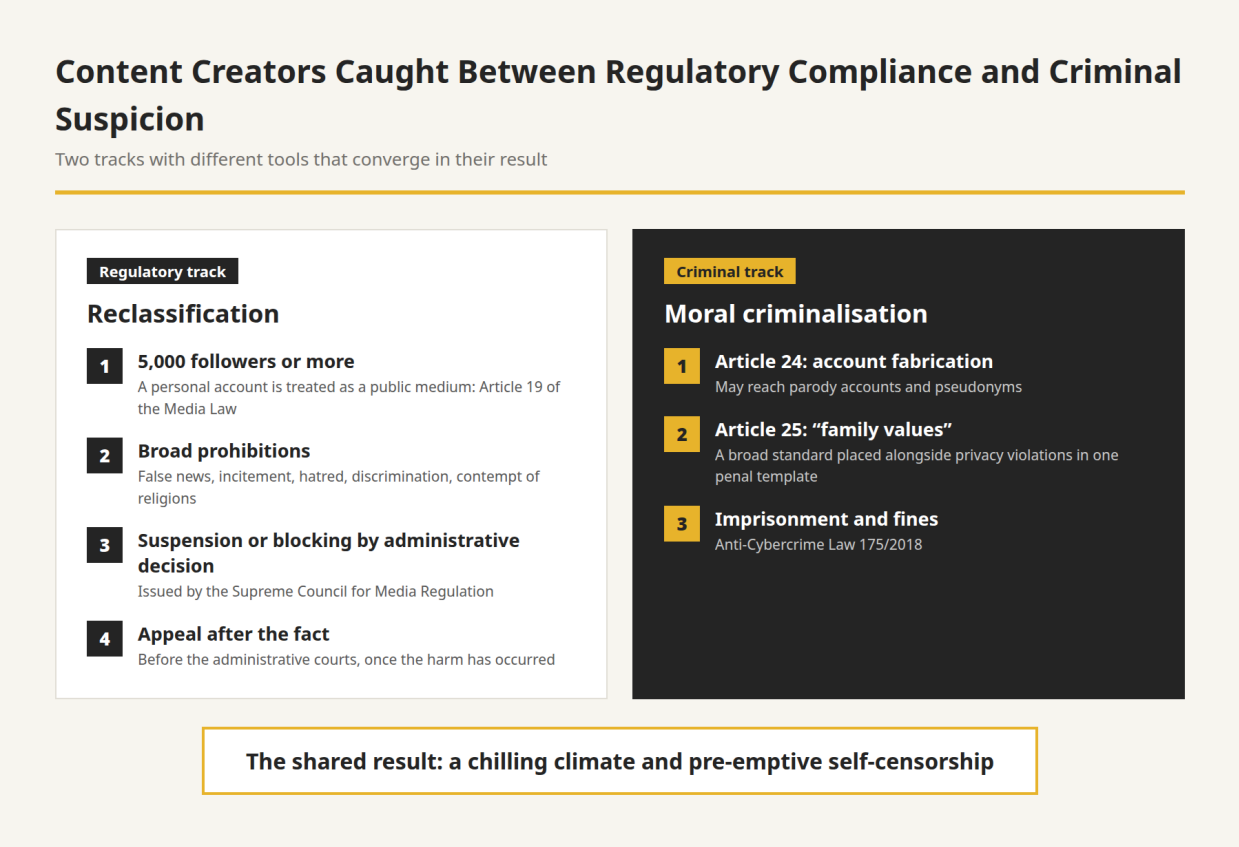


Figure 11: The regulatory and criminal tracks facing content creators

This leads not only to prosecutions and penalties, but to a chilling climate that drives self-censorship and reshapes the digital public sphere, so that those with the widest reach or the greatest social difference are the most exposed to administrative regulation and moral criminalisation.

Nine: Counter-Terrorism, the Legislation That Turns the Internet into a Space of Permanent Suspicion

The state of digital rights in Egypt cannot be accurately described without placing the Anti-Terrorism Law No. 94 of 2015 at the centre of the picture. This law does not function merely as a punitive framework for confronting armed violence, but as a legislative reading that redefines the entire digital space as a security domain, in which freedom of expression, the flow of information and privacy are managed as elements that can be suspended the moment the terms "national security" and "terrorism" are invoked.

> **"Truth becomes a matter of administrative decision rather than the fruit of independent investigation."**

This effect begins with the broad definition of terrorism and terrorist acts, which allows it to stretch beyond direct violence, as set out in Article 2[54] of the law. The article is not limited to the traditional definition of terrorism relating to armed violence but includes any use of threats or intimidation aimed at disrupting public order, endangering the safety and security of society, harming people or spreading terror among them, or infringing rights and freedoms. As worded, the definition includes general terms that are legally impossible to pin down, whose scope and the conduct that would trigger them cannot be known. In the digital sphere, this breadth takes shape along two interlinked tracks:

- The first track is the criminalisation of promotion and propaganda as a direct gateway to prosecuting content. Article 28[55] criminalises the direct and indirect promotion of terrorist

[54] Article 2 of the Anti-Terrorism Law No. 94 of 2015. In applying this law, the following terms have the meanings set out beside them: (a) Terrorist group: any group, association, body, organisation or gang of at least three persons, or other entity established as such, whatever its legal or de facto form, inside or outside the country, and whatever its nationality or the nationality of its members, that aims to commit one or more terrorist crimes or uses terrorism as one of its means to achieve or carry out its criminal purposes. (b) Terrorist: any natural person who commits, attempts, incites, threatens or plans a terrorist crime, at home or abroad, by any means, even individually, or contributes to such a crime within a joint criminal enterprise, or leads, heads, manages, creates, founds or is a member of any of the terrorist entities set out in Article 1 of Presidential Decree-Law No. 8 of 2015 on regulating the lists of terrorist entities and terrorists, or finances them, or knowingly contributes to their activity. (c) Terrorist crime: any crime set out in this law, and any felony or misdemeanour committed using a means of terrorism or with the intent of achieving or carrying out a terrorist purpose, or calling for or threatening to commit any of the foregoing, without prejudice to the Penal Code. (d) Conventional weapons: weapons, ammunition, explosives and gelatinous materials as defined by law. (e) Non-conventional weapons: nuclear, chemical, biological, radiological and bacteriological weapons and materials, or any other natural or artificial substances, solid, liquid, gaseous or vapour, whatever their source or method of production, capable of taking lives or causing serious physical or psychological injury, or damaging the environment, buildings or installations. (f) Funds or assets: all physical and virtual assets and their proceeds and economic resources, including oil and other natural resources, and property of any kind, tangible or intangible, movable or immovable, including documents, national or foreign currencies, securities or commercial papers, instruments and documents evidencing any of the foregoing in any form, including digital or electronic form, bank credit, bank cheques and letters of credit, and any interest, profits or sources of income arising from or generated by such funds or assets, or any other assets prepared for use in obtaining funding, products or services, and all rights relating to any of them, including virtual assets that have a digital value that can be traded, transferred or converted to digital form and used as a means of payment or investment.

[55] Article 28 of the Anti-Terrorism Law No. 94 of 2015: "Anyone who promotes or prepares to promote, directly or indirectly, the commission of any terrorist crime, whether by speech, writing or any other means, shall be punished with imprisonment for no

ideas or activities through writing, speech, publication or broadcasting. These formulations bring expression into a system of suspicion, particularly in an Egyptian context where the charge of "promotion" has expanded to include conveying information, analysing policies or even publishing testimonies that contradict the official narrative. This kind of criminalisation does not require proof that any violent act occurred; it is enough to claim that the content creates a climate, sympathy or justification for an act, a grey zone in which the power of interpretation swells at the expense of free expression.

- The second track is the restriction of journalistic publication and the entrenchment of the official narrative through punitive tools. The Anti-Terrorism Law, particularly Article 35,[56] contains provisions penalising the publication of information about terrorist operations that contradicts official statements issued by the state. This is an extremely sensitive point, because it makes truth a matter of administrative decision rather than the fruit of independent investigation. The practical result is the narrowing of investigative journalism, the criminalisation of coverage that relies on witnesses or unofficial sources, and a deterrent effect that leads newsrooms to avoid security files altogether, with direct consequences for the public's right to know and for civil society's ability to monitor and verify.

The angle most directly connected to digital rights is that counter-terrorism laws open wide space for restrictive measures of an administrative nature with limited oversight, such as travel bans, surveillance, restrictions on communications and prosecution before specialised prosecution offices. These measures have a greater capacity to affect the digital sphere because they operate quickly and with a low threshold of procedural safeguards.

less than five years. Promoting ideas and beliefs calling for the use of violence by any of the means set out in the preceding paragraph is considered indirect promotion. The penalty shall be imprisonment for no less than seven years if the promotion takes place inside places of worship, among members of the armed forces or police, or in places belonging to these forces. The same penalty as in the first paragraph applies to anyone who possesses or holds any means of printing, recording or publicity used or prepared for use, even temporarily, for printing, recording or broadcasting any of the foregoing."

[56] Article 35 of the Anti-Terrorism Law No. 94 of 2015: "Anyone who deliberately, by any means, publishes, broadcasts, displays or promotes untrue news or statements about terrorist acts committed inside the country, or about operations to combat them, contrary to the official statements issued by the Ministry of Defence, shall be punished with a fine of no less than two hundred thousand pounds and no more than five hundred thousand pounds, without prejudice to the prescribed disciplinary penalties. Where the crime is committed by a legal person, the person responsible for its actual management shall be punished with the same penalty as in the first paragraph, as long as the crime was committed on its behalf or for its benefit, and the legal person shall be jointly liable for any fines and compensation awarded. In all cases, the court may bar the convicted person from practising their profession for no more than one year if the crime was committed in breach of the principles of their profession."

Ten: Procedural Justice in Digital Cases

The amendments in Egypt's new Criminal Procedure Law were adopted under Law No. 174 of 2025, with substantive changes to articles that had been the subject of a presidential objection. The law was published in the Official Gazette on 12 November 2025, and its entry into force was originally set for 1 October 2026, before the House of Representatives approved, on 30 September 2026, a one-year postponement, moving its entry into force to October 2027.

The amendments include substantive changes that alter established procedural concepts in one way or another. In reality, they codify new practices to which the authorities and law-enforcement bodies in Egypt have grown accustomed in recent years. The most significant amendments relevant to digital rights can be highlighted as follows:

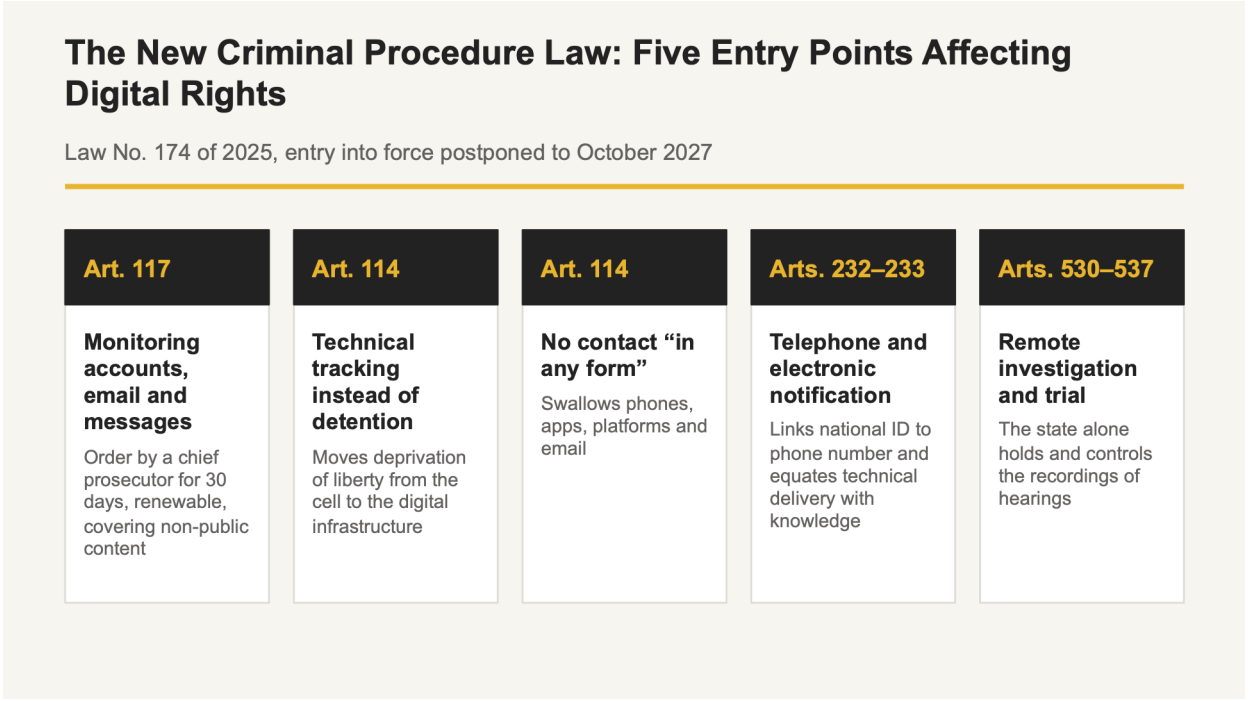


Figure 12: Provisions of the new Criminal Procedure Law relevant to digital rights

First: Surveillance of Communications and Digital Content

Article 117[57] of the Criminal Procedure Law moves surveillance from the narrow field of wiretapping, meaning listening to voice calls, to a broad and detailed digital field covering social

[57] Article 117 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "Members of the Public Prosecution of at least the rank of chief prosecutor, in investigating the felonies set out in Parts One, Two, Two bis, Three and Four of Book Two of the Penal Code, shall have, in addition to the powers of the Public Prosecution, the power to issue a reasoned order, for a period not exceeding thirty days, to seize letters, messages, telegrams, newspapers, printed matter and parcels, and to monitor wired and wireless communications, social media accounts and their various non-public contents, email, and text, audio or visual messages on phones and devices and any other technical means, and to seize the media containing them, or to record conversations held in a private place, whenever this is useful in revealing the truth. The order referred to in the first paragraph may be renewed for one or more similar periods. In investigating the felonies referred to in the first paragraph, other than those set out in Part Three of Book Two of the Penal Code, these members shall also have the powers of the summary judge with respect to the period of pre-trial detention. They shall furthermore have the powers of the misdemeanour appeals court sitting in chambers, provided for in Article 123 of this

media, email, and text and voice messages stored on devices. It grants members of the prosecution of at least the rank of chief prosecutor the power to issue a reasoned order for up to thirty days that is not limited to monitoring wired and wireless communications, but extends explicitly to social media accounts and their various non-public contents, email, and text, audio or visual messages on phones and devices and any other technical means, with the order renewable for similar periods.

The problem is not the existence of an investigative tool, but the breadth of what can be intercepted and monitored, including data and communications whose impact by nature extends beyond the person under investigation to their circles of communication. Every expansion of digital surveillance raises the cost of public participation and of human rights, journalistic and trade union work, because its chilling effect requires no conviction; the sense of possibly being monitored is enough.

Second: Turning Alternatives to Detention into a Digital Tracking System

Article 114[58] of the Criminal Procedure Law adds to the measures that may replace pre-trial detention "the use of technical means to track the accused", referring its regulation to a decree by the Minister of Justice in coordination with the Ministers of Interior and Communications.

This provision creates a specific risk to digital freedoms, because technical tracking reproduces restriction before conviction in the form of close surveillance of movement and possibly of daily behaviour, and turns the private sphere into a space of coerced compliance. Tracking is not automatically a lighter alternative; it transfers the deprivation of liberty from the place of detention to the digital infrastructure: location data, movement logs and perhaps compliance records that can be mismanaged or undergo function creep beyond their purpose.

Third: Restrictions on Communication

Article 114 of the Criminal Procedure Law includes a measure requiring the accused to refrain from receiving, meeting or contacting specified persons "in any form whatsoever". In the digital environment, the phrase "in any form" swallows up phones, apps, platforms, email and media messages, and creates a compounded risk, such as the ban expanding to cut off support and work networks.

law, when investigating the crimes set out in Part One and Section One of Part Two of Book Two of the Penal Code, provided that each period of detention does not exceed fifteen days."

[58] Article 114 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "In the cases set out in Article 113 of this law, and in other misdemeanours punishable by imprisonment, a member of the Public Prosecution may, instead of pre-trial detention, issue a reasoned order imposing one of the following measures: (1) requiring the accused not to leave their residence or domicile; (2) requiring the accused to report to a police station at specified times; (3) prohibiting the accused from frequenting specified places; (4) requiring the accused not to leave a specified geographic area without the permission of the Public Prosecution; (5) requiring the accused to refrain from receiving, meeting or contacting specified persons in any form whatsoever; (6) temporarily prohibiting the accused from possessing or holding firearms and ammunition and requiring them to hand these over to the police station in whose jurisdiction they reside; (7) using technical means to track the accused where the conditions for their use are met, as regulated by a decree of the Minister of Justice in coordination with the Ministers of Interior and Communications."

Fourth: Telephone Notification Centres and Linking Procedures to a Phone Database

Article 232[59] of the Criminal Procedure Law establishes a centre under the Ministry of Justice to look up the national ID number of the accused and the mobile number registered to it, send judicial notifications of trial sessions or telephone and electronic judicial warnings, and prepare a report confirming receipt of these messages. Article 233[60] provides for a regulatory decree to set out the mechanism for proving the sequence of telephone and electronic notifications and how their delivery is verified.

This structure raises direct digital concerns, because operating it means creating a permanent government pathway for compiling communications data and linking it to the national ID number within criminal proceedings. The risk is not limited to leaks, but includes function creep and the transformation of receipt reports into procedural presumptions that could seriously affect the right of defence if practice settles on equating technical delivery of a message with actual knowledge on the part of the person, particularly given unequal control over phones within families or workplaces and unequal access to devices and services.

The problem lies in the fact that the purpose of notification is to ensure that the accused actually knows about sessions, warnings or even summonses to appear before the prosecution. If a person is presumed to have known simply because the notification reached their phone, numerous problems follow, because this ignores questions about ownership of the phone line, proof of possession, presence inside the country, and the possibility that the line has been changed or the phone has broken down. These are procedural problems the law ignores.

Fifth: Remote Investigation and Trial Procedures

Articles 530 to 537 of the Criminal Procedure Law set out what can be described as a framework for remote investigation and trial using modern audio and visual means of communication. Article 531[61] opens the door to using this track in sensitive proceedings such as reviewing pre-trial

[59] Article 232 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "A telephone notification centre under the Ministry of Justice shall be established within the jurisdiction of each summary court, responsible for obtaining from the Civil Status Sector the national ID number of the accused and the mobile phone number registered to it, in accordance with the systems and rules applied in the Civil Status Sector and without conflicting with the requirements of national security and the confidentiality of national databases, and for sending telephone and electronic notifications and preparing a report confirming receipt of these messages. The competent judge shall assess the fee due for telephone notification in accordance with Article 16 of Law No. 90 of 1944 on judicial and notarisation fees in civil matters, to be paid by whoever is ordered to bear the criminal costs. The fee referred to in the second paragraph shall be allocated to developing notification centres and preparing the necessary databases."

[60] Article 233 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "Papers served by bailiffs must include the following: the day, month, year and hour of service; the case concerned, its subject and the capacity of the person served; the name of the bailiff and the court where they work; the name, surname, profession or occupation and domicile of the person served, or, if unknown at the time of service, their last known domicile; the date and place of the procedure concerned; the name and capacity of the person to whom the copy was handed and their signature on the original acknowledging receipt; and the bailiff's legible signature with their full name on both the original and the copy. The Minister of Justice, in coordination with the competent minister, shall issue a decree setting out the mechanism for proving the sequence of telephone and electronic notifications and how their delivery is verified."

[61] Article 531 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "The competent investigating or trial authority, as the case may be, may conduct all or some of the investigation or trial procedures provided for in this law remotely with the accused, witnesses, victims, experts, civil claimants and those civilly liable. It may take such procedures with respect to reviewing pre-trial detention and measures and their extension, provisional release and appeals against their orders. It may, as the case may be, decide

detention orders and measures and their extension, provisional release, and appeals against these orders.

Article 534[62] grants investigating and trial authorities the power to record and store all proceedings conducted remotely and transcribe them into minutes, with official signatures but without the signatures of the accused, witnesses or others on each page. Article 537[63] then ties the equipping of courtrooms and devices to coordination between the Ministries of Justice and Interior and other bodies.

The risk here is that once a hearing becomes a digital event, confidentiality, publicity and the rights of the defence become a matter of operating infrastructure, raising questions such as who controls recording and storage, what the limits on access are, how long recordings are retained, and how technical failures and outages are managed. The existence of these provisions does not resolve the risk unless technical and procedural safeguards are built to prevent recording and storage from becoming an additional source of surveillance or a tool of unequal dispute over what actually happened in the hearing. The state alone holds and controls the record of what happened in hearings; if a violation is committed during a hearing by the state or the court, the defence will have to ask the state, which is its adversary, to agree to provide a copy of the recording showing the errors that occurred.

to prevent disclosure of the true identity of witnesses using all appropriate modern means and technologies of communication while they give their statements, all with due regard for Article 525 of this law."

[62] Article 534 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "The competent investigating and trial authorities may take whatever measures they consider appropriate to record and store all procedures conducted remotely through modern means and technologies of communication, transcribe them into minutes, with the assistance of an expert if needed, and deposit them in the case file. The member of the Public Prosecution, the investigating judge or the presiding judge, and the clerk, shall sign each page without the need for the signature of any of the accused, witnesses, experts, translators or any other signature."

[63] Article 537 of Law No. 174 of 2025 issuing the Criminal Procedure Law: "The Ministry of Justice, in cooperation and coordination with the Ministry of Interior and the relevant bodies and ministries, shall prepare the rooms and communication equipment required to carry out remote investigation and trial procedures using modern means and technologies of communication in the competent bodies, in penal institutions and reform and rehabilitation centres, and in other relevant departments, and shall provide the necessary technical assistance."

Eleven: The Rules Governing Communications Shutdowns

The oldest legal framework that opens the possibility of directly disrupting communications is the Telecommunications Regulation Law No. 10 of 2003. What matters most is not shutdowns as a term or political decision, but the power that Article 67[64] of the law grants to the competent authorities to place under their management all the telecommunications services and networks of any operator or service provider and to summon the staff responsible for operation and maintenance, in cases of disaster or general mobilisation, followed by broader wording that allows intervention in "any other cases relating to national security".

In practice, this wording creates a power at the level of infrastructure, not content. It does not speak only of stopping a particular service, but of transferring the management of the network and its services to the state whenever the specified cases arise.

The danger of Article 67 stems from two interlinked elements. The first is the vagueness of its governing terms, particularly "the competent authorities" and the standard of "any other cases relating to national security", for which the law sets no threshold of proof or operational definition that would limit their expansion.

The second is that the text does not in itself set detailed conditions on the duration of intervention, its geographic scope, the proportionality between the threat and the measure, or subsequent transparency requirements. The article thus becomes in practice a gateway that can be invoked across a wide range of situations, from partial management of the network to a total shutdown.

This reading is reinforced when Article 67 is read within the system of the Telecommunications Law itself. The law in principle treats service continuity as an obligation on licensees: Article 25[65] provides that the licence sets out the licensee's obligations, including "the obligation to continue

[64] Article 67 (Law No. 10 of 2003): The competent state authorities may place under their management all the telecommunications services and networks of any operator or service provider and summon its staff responsible for operating and maintaining those services and networks, in the event of a natural or environmental disaster, in cases where general mobilisation is declared under Law No. 87 of 1960, and in any other cases relating to national security.

[65] Article 25 (Law No. 10 of 2003): The licence issued sets out the obligations of the licensee, which include in particular: (1) the type of service and technology used; (2) the licence term; (3) the geographic limits of service provision and the wired and wireless coverage plan and its implementation stages; (4) service quality and efficiency standards; (5) the obligation to continue providing the service and the procedures to be followed in the event of service interruption or suspension; (6) setting the service price and collection methods and announcing them; (7) making the service available to users without discrimination; (8) complying with the national numbering plan set by the Authority; (9) observing universal service requirements; (10) providing relief and emergency communication services free of charge and providing directory services, according to the type of licensed service; (11) obligations relating to not harming national security; (12) obligations relating to technical rules on health, environmental, planning and construction safety in accordance with standards set in agreement with the relevant ministries and state bodies; (13) contributing to scientific research and training; (14) paying what the Authority determines in return for the burdens it bears in verifying the licensee's compliance, as well as financial guarantees and all periodic dues; (15) providing the information and data the Authority requests relating to the subject of the licence; (16) paying financial penalties and compensation; (17) providing services under free-competition rules; (18) establishing a system for receiving and investigating complaints and repairing faults efficiently; (19) guaranteeing the confidentiality of the licensee's customers' communications and calls and setting the rules necessary to ensure this.

providing the service and the procedures to be followed in the event of service interruption or suspension".

This provision reflects a regulatory logic that sees a shutdown as an exceptional event requiring procedures. Article 67, however, operates as an overriding exception that allows management to be transferred to the state in broad circumstances, making "service continuity" conditional on a sovereign or security decision whenever the exception is activated.

The Telecommunications Regulation Law sets out a clear mechanism for compelling service providers to comply with the requests and decisions of national security bodies: Article 82[66] punishes with imprisonment anyone who disobeys the summons orders provided for in Article 67, with a harsher penalty in time of war or general mobilisation, and the possibility of a court decision to suspend the licence temporarily until the summons is complied with.

The significance here is that the state's power does not operate only through requests for cooperation from companies, but through a legal capacity to enforce implementation and punish refusal, which places service providers in a relationship of quasi-coerced compliance whenever Article 67 is invoked.

In terms of application, the events of 28 January 2011 stand out as the most telling example of the state's ability to move from partial control to a total shutdown. Masaar's timeline of internet censorship documents that the most significant event of 2011 was the nationwide shutdown of internet and communications services on 28 January.[67]

The impact of communications shutdowns is not confined to freedom of expression: a shutdown acts as a comprehensive disruption of society's ability to organise, document and access information and essential services, because the internet is not merely a publishing medium but a network of coordination and daily dependence. Since the Telecommunications Law gives the state, through Article 67, broad power to control the network itself, and reinforces enforcement with provisions criminalising failure to respond to summons orders, shutdowns become part of the toolkit for managing the digital public sphere by controlling the very possibility of communication, and not merely by dealing with content.

[66] Article 82 (Law No. 10 of 2003): Anyone who disobeys the summons orders provided for in Article 67 of this law shall be punished with imprisonment. The penalty shall be rigorous imprisonment if the crime is committed in time of war or in cases where general mobilisation is declared under Law No. 87 of 1960 on general mobilisation.

[67] Association for Freedom of Thought and Expression (AFTE), "Isolation: On the Communications Shutdown during the January 2011 Revolution", March 2018: https://afteegypt.org/research/monitoring-reports/2018/03/29/14918-afteegypt.html

Twelve: The Criminalisation of Encryption and Anonymity



Protecting communications and privacy in the digital sphere

Egyptian legislation shows that encryption is not treated as a protective safeguard inherent to privacy and the security of communications, but as a capability managed through a logic of prior permission. This legal positioning redefines the relationship between users and technology: instead of encryption being a default means of protecting communications from unlawful interception, its use becomes conditional on approvals, making protection suspendable by design and not only in cases of misuse.

This is embodied directly in the Telecommunications Regulation Law No. 10 of 2003, where Article 64[68] obliges telecommunications operators and service providers, their affiliates and the users of these services not to use any equipment to encrypt telecommunications services without the approval of the NTRA, the Armed Forces and the national security agencies, with the exception of encryption devices for radio and television broadcasting. Including users among those addressed by the prohibition means the rule concerns not only infrastructure or operators but extends to the

[68] Article 64 (Law No. 10 of 2003): Telecommunications operators and service providers, their affiliates, and users of these services may not use any equipment to encrypt telecommunications services without first obtaining the approval of the Authority, the Armed Forces and the national security agencies; this does not apply to encryption devices for radio and television broadcasting. With due regard for the inviolability of citizens' private life protected by law, every operator or service provider shall provide, at its own expense and within the telecommunications network it is licensed to operate, all technical capabilities, including equipment, systems, software and communications within the network, that enable the Armed Forces and national security agencies to exercise their powers within the limits of the law, provided that service provision coincides with the provision of the required technical capabilities. Telecommunications service providers and operators and their agents responsible for marketing these services shall also obtain accurate information and data on their users, whether citizens or various state bodies.

individual level, moving encryption from the realm of personal protection to that of an administratively restricted capability.

The effect of this regulation is amplified because breaching it is not merely a regulatory violation: Article 81[69] sets a penalty of imprisonment and a fine for anyone who violates Article 64 and adds, beyond that, a consequence for licences, which are suspended temporarily until the equipment, systems and communications software referred to are provided.

The presence of a custodial penalty gives the rule a strong deterrent effect even without any broad announcement of how it applies to modern technologies, because the question of "what counts as an encryption device" remains a matter of interpretation. This produces uncertainty that pushes people to avoid protective tools or hesitate to use them, especially among those most at risk, such as journalists, researchers and activists.

At the same time, restrictions on encryption do not operate separately from the rest of the Egyptian system. As noted above, the Anti-Cybercrime Law requires service providers to retain logs and customer usage data for 180 days, including identification data, traffic data and other data that make it possible to trace patterns. This means that much of the capacity for monitoring and analysis does not depend on decrypting message content, because the retention structure itself keeps traffic and network-linkage data available under an existing legal obligation.

A further paradox appears in the Executive Regulations of the Anti-Cybercrime Law, which require information technology service providers to take technical measures including encrypting data and information to preserve their confidentiality using a specified encryption standard (AES-128), while making the service provider responsible for maintaining the confidentiality and security of the encryption key.[70] This shows that the legal system leans towards a model of managed encryption controlled by the service provider, whose keys are held within compliance arrangements, while narrowing the space for encryption controlled by users or falling outside the system of prior approvals.

The result is a dual policy: one track subjects the use of encryption in communications to a logic of permission and punishment, while a parallel track builds broad analytical capacity through data retention and technical compliance by service providers. Encryption thus shifts from a protective right that strengthens the confidentiality of communications into an information security tool

[69] Article 81 (Law No. 10 of 2003): Anyone who violates any of the provisions of Article 64 of this law shall be punished with imprisonment and a fine of no less than ten thousand pounds and no more than one hundred thousand pounds. The court shall also order the temporary suspension of the licence until the violator provides the equipment, systems and communications software referred to in that article.

[70] Article 2 of the Executive Regulations of the Anti-Cybercrime Law: Information technology service providers shall take the following technical and organisational measures in implementation of items (2) and (3) of paragraph One of Article 2 of the law: (1) encrypting data and information so as to preserve their confidentiality and prevent their penetration, using a standard symmetric or asymmetric encryption system no less secure than the Advanced Encryption Standard (AES-128) with an encryption key of no less than 128 bits, while being responsible for maintaining the confidentiality and security of the encryption key … (3) using secure protocols such as the Hypertext Transfer Protocol Secure (HTTPS) … (11) using firewall equipment, devices, systems and software (NGFW, UTM, firewalls) to protect networks and systems.

within a monitored system, while users' protection remains hostage to a framework of approvals and expandable practices.

Thirteen: Criminalising the Possession of Advanced Technologies, the Case of Drones

The regulation of drones in Egypt reflects a broader legislative pattern that treats technical capability as a subject of suspicion before any act, rather than as a tool whose risks can be regulated. The law does not begin by identifying specific harmful uses and then criminalising them. Instead, it imposes a general prohibition covering import, manufacture, assembly, circulation, possession, trade and use, and makes permission possible only through a permit issued by a sovereign body.

The regulation of drones begins with an extremely broad definition in Article 1 of Law No. 216 of 2017.[71] It does not distinguish between technical categories or levels of risk, but adopts a definition covering any object capable of flying without a pilot, whatever its shape or size, that can be loaded with additional payloads posing a threat to national security, and is operated or controlled remotely. Including the phrase "posing a threat to national security" in the definition itself embeds a security presumption in the structure of the legal concept, leaves the scope of application inherently open, and makes it difficult for individuals to foresee what falls under criminal liability without recourse to later assessments.

The law then defines "the competent authority" and "the competent minister" as the Ministry of Defence and the Minister of Defence. This means moving the licensing mechanism from a civilian model (safety, navigation, operating rules) to a sovereign model in which permission is managed through a centralised decision that overrides the logic of the market, civilian applications, scientific research and personal use.

This centralisation translates into a blanket prohibition in Article 2,[72] which extends the ban to public and private legal persons and natural persons, and lifts it only by permit "in accordance with the circumstances, conditions and procedures" set by the Executive Regulations. Possession itself is therefore treated as a criminal act in the absence of a permit, moving the law from criminalising harmful use to criminalisation that precedes use.

[71] Article 1 of Law No. 216 of 2017 regulating the use of mechanically or wirelessly powered aircraft: "In applying this law, the following terms have the meanings set out beside them: (1) Mechanically or wirelessly powered aircraft: any object capable of flying without a pilot and without others being on board, using any type of technology, whatever its shape or size, that can be loaded with additional payloads, whether devices, equipment, weapon systems, ammunition, explosives or other items posing a threat to the national security of the country, and is operated or controlled remotely. (2) Competent authority: the Ministry of Defence. (3) Competent minister: the Minister of Defence."

[72] Article 2 of Law No. 216 of 2017: "Units of the state administrative apparatus, including ministries, departments, agencies and local administration units, public bodies, companies and other public or private legal persons, and natural persons, are prohibited from importing, manufacturing, assembling, circulating, possessing, trading in or using mechanically or wirelessly powered aircraft without first obtaining a permit from the competent authority, in accordance with the circumstances, conditions and procedures set by the Executive Regulations of this law and with due regard for the Civil Aviation Law issued by Law No. 28 of 1981."



Figure 13: The permit and penalty regime under the drone law

The Executive Regulations (Prime Ministerial Decree No. 931 of 2018) reveal that the permit is a detailed control framework, defined as the document issued to carry out the import, manufacture, assembly, circulation, possession, trade or use of drones,[73] and specify that permit applications are submitted to the Armed Forces Operations Authority. They also set a telling procedural rule: a decision within 30 days, with the lapse of that period without a response deemed a refusal, and permits valid for no more than three years and entered in a dedicated register.

The Regulations add a layer of ongoing compliance by requiring permit holders to keep two registers (one for the drones, their specifications and where they were obtained, and the other for dates of circulation and use), subject to review by specialists designated by the competent authority. They set special procedures where the activity ends or the permit is not renewed, including not disposing of the drones and notifying the competent authority within three days pending "regularisation of the situation" or a decision. They also establish a grievance procedure before a committee whose composition and procedures are set by a decree of the Minister of Defence, keeping review within the same framework that issued the decision.

The Regulations do not stop at general procedures, but divide permits by purpose (economic or commercial, sporting, scientific or research) and add conditions that go beyond technical aspects

[73] Article 2 of Prime Ministerial Decree No. 931 of 2018 issuing the Executive Regulations of Law No. 216 of 2017: The import, manufacture, assembly, circulation, possession, trade and use of mechanically or wirelessly powered aircraft shall be carried out according to the following rules and procedures: (1) the permit application is submitted to the Armed Forces Operations Authority, complete with the documents specified by decision of the competent minister; (2) the application states the number of aircraft for which a permit is sought, their specifications and where they will be obtained; (3) the application is decided, by acceptance or refusal, within thirty days of submission, and the lapse of this period without a response is deemed a refusal; (4) the competent authority issues the permit for no more than three years and notifies the permit holder by registered letter with acknowledgement of receipt, sending a copy to the relevant body; (5) the permit is renewed at the request of the permit holder to the competent authority three months before its expiry; (6) the competent authority keeps a register recording the permits issued, their dates and their holders; (7) the permit holder must keep two registers, one recording the aircraft held, their specifications and where they were obtained, and the other recording the dates of circulation and use of the aircraft, both subject to the rules on commercial registers and reviewed by specialists designated by the competent authority; (8) if renewal of the permit is refused or the permitted activity ends, the permit holder must not dispose of the aircraft held and must notify the competent authority, within no more than three days, of all data on these aircraft, pending regularisation of their status or a decision in this regard.

to a system of security and civilian approvals: for economic, sporting and research activities, they require security approvals from specified bodies and the approval of the Ministry of Civil Aviation and the competent state bodies, together with a specification of the purpose and the spatial and temporal scope of use. In the research field, they require an undertaking not to use the drone beyond the scientific purpose, with a limited exception for universities and institutes whose academic structure includes an aviation department, subject to spatial conditions tied to the institution's premises.

A reading of the Regulations also shows that exemptions do not operate automatically even in the "lighter" cases. Masaar's analytical article shows that the Regulations refer to exempting certain types with highly restricted technical specifications (such as very light weight, no GPS or autonomous flight, limits on distance and altitude, and no capacity to carry any payload), but still tie verification of the exemption to an inspection process that includes a report from the Customs Authority and review by Ministry of Defence specialists within 30 days. Even "toy exemptions" thus become a zone of procedural compliance rather than a clear space on which ordinary users can rely without risk.

The penalties confirm that the aim is not "regulating use" so much as "blanket criminalisation" of the absence of a permit. Article 3 provides for imprisonment of one to seven years and a fine, with aggravation up to life imprisonment if the act was for a terrorist purpose, and the death penalty if it resulted in death. It adds confiscation in all cases in favour of the Armed Forces, making the punitive effect twofold: deprivation of liberty and deprivation of property.

The framework gains an additional dimension through Article 4, which grants members of the military judicial police the status of judicial officers with respect to applying the law, its Regulations and the decisions issued to implement it. This confirms that enforcement is not purely civilian, but relies on control tools of a military nature for monitoring, inspection and verification of compliance with registers and permit conditions.

Overall, drone regulation offers a complete model of "criminalising technology": a broad definition that places a security presumption at the heart of the concept; a blanket prohibition of acts including possession; sovereign licensing through the Ministry of Defence with ongoing compliance procedures; custodial penalties and mandatory confiscation; and an enforcement track that includes military judicial police. The weight of this model is all the greater given the wide range of possible civilian uses of drones (in agriculture, infrastructure monitoring, humanitarian response and delivering supplies), which means that a general prohibition with an exception by permit does not merely regulate "risks", but in practice sets the limits within which civilian uses themselves can develop, according to a security logic that precedes the market and innovation.

The regulation of drones in Egypt reflects a broader legislative pattern of turning advanced technologies from tools whose risks can be regulated into a "criminal matter" whose possession is criminalised in itself. This choice does not target specific harmful conduct, but widens the circle of suspicion to include ownership, possession, circulation and use, and then ties decriminalisation to

a permit issued by a sovereign body outside the civilian sphere. The result is broad criminalisation that precedes any act, turns technology into a presumption of danger, and grants the state punitive and exclusionary power.

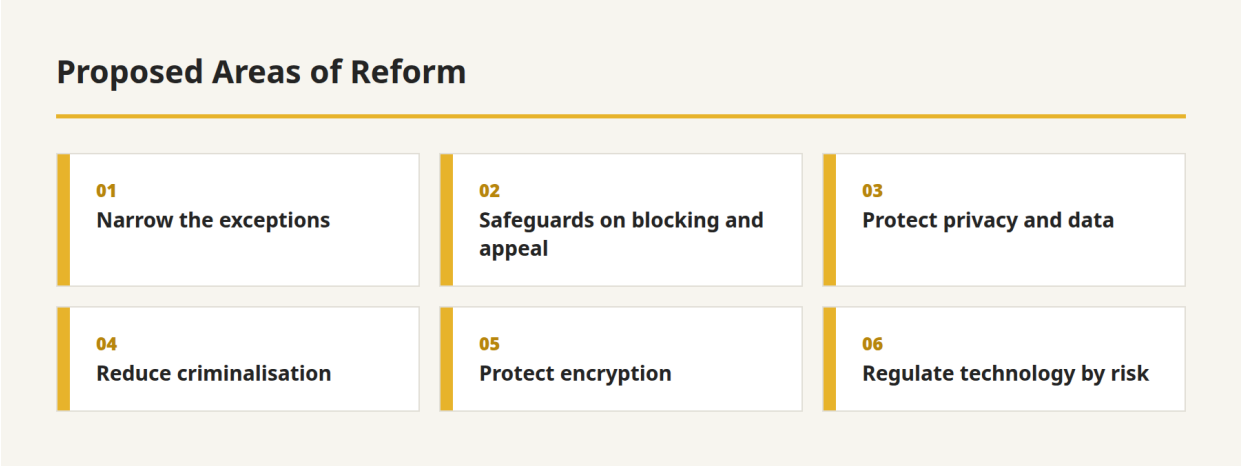
The clearest framework is Law No. 216 of 2017 regulating the use, circulation and trade of mechanically or wirelessly powered aircraft. The law defines these aircraft extremely broadly: "any object capable of flying without a pilot … using any type of technology … whatever its shape or size … and that can be loaded with additional payloads … posing a threat to national security … and is operated or controlled remotely". This definition is not limited to a specific technical category and does not set a verifiable technical criterion, but merges a technical description with a security claim ("posing a threat to national security") within the definition itself, leaving the scope of application inherently open and making it difficult for individuals to foresee what falls under criminal liability.

More importantly, the law determines that "the competent authority" is the Ministry of Defence and "the competent minister" is the Minister of Defence. This is not an administrative detail; it is a decision about legal positioning that makes licensing a sovereign matter rather than civilian regulation of safety, privacy or airspace. In the following article, the law explicitly widens the scope of the prohibition to include possession, circulation, trade, import and more, and confines permission to obtaining a "permit" from the competent authority under its conditions and procedures. Ordinary possession of a technology thus becomes a criminal act unless accompanied by prior permission, instead of criminalisation being tied to harmful or abusive use.

The penalties confirm that this is not "regulatory licensing" but full criminalisation. The law provides for imprisonment of no less than one year and no more than seven years, and a fine of no less than EGP 5,000 and no more than EGP 50,000, or either penalty, for anyone who imports, manufactures, assembles, circulates, possesses, holds or uses these aircraft in violation of the permit system. It then sets qualitative aggravation up to life imprisonment if the acts are committed "for a terrorist purpose", and up to the death penalty if the act results in a person's death. It adds confiscation as a rule, making the punitive effect twofold: deprivation of liberty and deprivation of property. Most telling is the assignment of jurisdiction over cases relating to the application of the law and its Regulations to the military judiciary with respect to application and judicial policing. This entrenches the transfer of a technical and civilian dispute to an inherently exceptional form of trial, puts pressure on fair trial guarantees and weakens effective civilian judicial oversight.

Drone regulation in Egypt therefore offers a complete model for criminalising advanced technologies: a broad definition, a blanket prohibition including possession, non-civilian sovereign licensing, harsh custodial penalties, and military judicial jurisdiction. This model can be extended to other technologies whenever the state wishes to turn "technical capability" into "legal suspicion" instead of regulating harmful uses with clear safeguards.

Recommendations



1. Legislative reform that redefines exceptions and narrows standards

The provisions that permit blocking, suspension, disruption or restriction of content should be reviewed and amended so that they are tied to specific rather than vague standards, with precise definitions of terms such as national security, imminent danger and family values, so that they do not become open gateways for expanding restrictions.

The relationship between law and administrative decision must be reordered so that no administrative decision produces a serious effect on rights without a clear and specific legal basis and without fast and effective judicial oversight.

2. Clear procedural safeguards for blocking and content restriction

Any measure affecting access to websites or accounts must be built on the principle of notification and a written statement of reasons, and on the right to an immediate appeal before an independent judge within short time limits. A rule should preferably be adopted whereby the measure is suspended by default upon appeal if it would cause serious harm that is difficult to remedy, and the competent authorities should be required to publish periodic aggregate data on the number of blocking orders, their scope and their legal basis, without prejudice to specific investigations.

3. End the use of licensing as a condition of existence for digital outlets

The regulation of professional media work should be separated from the idea of permission for digital existence. A simple notification system should replace costly prior licensing for independent news websites, with fees proportionate to the nature of digital publishing, and a rule that prevents applications from being stalled through silence by treating a failure to respond within a set period as approval, or at least requiring the administrative body to issue a reasoned decision open to rapid appeal.

Operational requirements that turn regulation into extended control should also be reduced, and precise safeguards placed on any obligation to archive content or localise servers, in order to protect data security and prevent abuse.

4. Protect privacy by reducing mandatory data retention and controlling access

Mandatory data retention rules must be reviewed to reduce retention periods and scope, and any access to data must be tied to necessity and proportionality and to a reasoned judicial order, with requests documented and open to subsequent review by an independent body.

Strict information security rules should also be imposed on entities that hold data, because the risks of leaks and misuse go to the core of the right to privacy.

5. Strengthen personal data protection and the independence of the enforcement body

The broad exceptions that make protection easy to suspend must be narrowed, and objective criteria set for requests from security bodies so that they do not become binding administrative orders without oversight.

The independence of the enforcement body and the publicity of its standards and decisions should also be strengthened, complaint procedures for individuals simplified, and their rights of access, rectification, erasure and objection guaranteed through practical and fast mechanisms.

6. Reduce reliance on criminal law to police digital expression

False news offences in their vague forms, which tie criminalisation to a general effect open to interpretation, should be reconsidered, and more precise standards set that protect public debate and journalistic verification.

The use of imprisonment in publication and expression cases should also be reduced, and balanced civil alternatives developed for insult and defamation that respect the right to reputation without turning the public sphere into an arena of permanent criminal threat.

7. Protect encryption and anonymity as security tools, not grounds for suspicion

Encryption should be treated as a legitimate means of protecting communications, privacy, and journalistic and human rights work, not as a capability conditional on prior permission extending to users.

Criminalisation should remain focused on specific harmful acts rather than on protective tools themselves, with a clear policy that encourages secure communications instead of pushing users into technical weakness and danger.

8. Regulate dual-use technologies on the basis of risk, not blanket prohibition

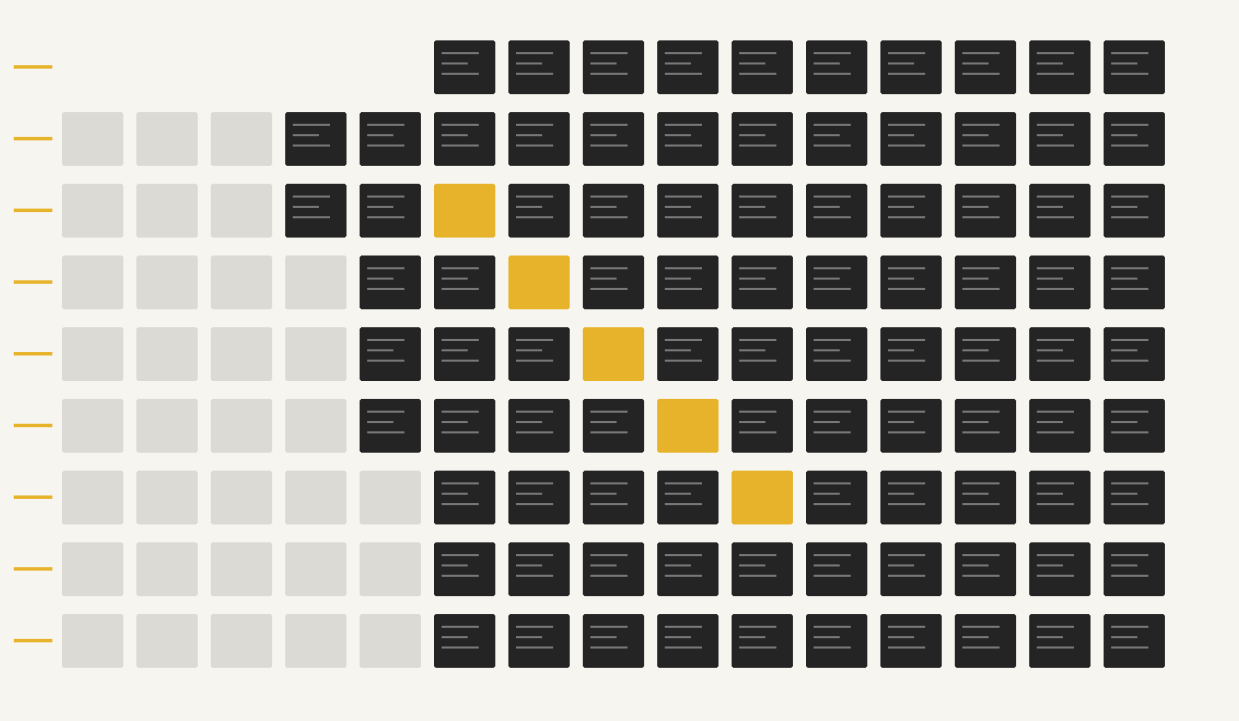
For telecommunications equipment, drones and other technologies, there must be a shift from blanket prohibition with exceptions by permit to regulation that distinguishes between levels of risk and between civilian and research uses. This includes publishing clear and accessible lists and standards, creating practical exceptions for maintenance, research and experimentation, and graduating sanctions so that criminal punishment is a last resort, while guaranteeing an effective right to appeal classification or refusal decisions.

9. Digital rights safeguards in the Criminal Procedure Law before it enters into force

With the entry into force of the new Criminal Procedure Law postponed to October 2027, it is essential to adopt implementing rules that protect against the expansion of digital surveillance and the tracking of individuals under the heading of alternatives to detention, and to ensure that these measures are kept to the minimum necessary, for a specified period, and under genuine judicial supervision.

Arrangements for remote investigation and trial must also include clear guarantees of confidentiality, publicity, the right of defence, and the integrity of recording and retention, so that digital procedures do not become an additional layer of surveillance or a permanent imbalance between the parties.

Conclusion



A rights-based reading of the digital space in Egypt shows that the problem lies less in the absence of legal texts than in the absence of clear operational limits that prevent exceptional intervention from becoming daily practice. When standards widen and the space for discretion grows, predictability declines, pre-emptive compliance increases and self-censorship emerges as the most common outcome. At that point, the right becomes less present in reality even if it remains written in the texts.

This effect does not reach individuals alone, but the entire public sphere, because legal ambiguity undermines trust, reduces society's capacity for debate, verification and accountability, and makes the cost of participation too high for many to bear.

Restoring rights requires resetting the logic that governs regulation: recognising that the default is availability and freedom of expression and communication; that any restriction must rest on a clear law and be necessary, proportionate and the least restrictive means; that it must be subject to effective independent oversight and fast, comprehensible avenues of appeal; and that it must be surrounded by a minimum of transparency that allows public scrutiny and reduces the risk of abuse. These demands are established standards in the international framework for freedom of expression and privacy in the digital age, where legitimate restrictions are a controlled exception, not an open-ended rule.

Once the internet and communications services are recognised as part of the conditions for exercising rights and for daily life and the economy, protecting the digital sphere becomes as much a question of the rule of law as of security. The state's presence is then measured not by the breadth

of its capacity to intervene, but by its ability to manage risks without eroding public trust, without turning society into a circle of permanent suspicion, and without weakening the very rights that regulation is supposed to protect.