

LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Egypt

Country Report



PARADIGM
INITIATIVE



LONDA 2025

DIGITAL RIGHTS & INCLUSION IN AFRICA REPORT

Report produced and published by Paradigm Initiative
April 2026

This publication may be reproduced for non-commercial use in any form provided due credit is given to the publishers and the work is presented without any distortion.

Copyright ©2026 Paradigm Initiative

374 Borno Way, Yaba, Lagos, Nigeria.
media@paradigmhq.org
www.paradigmhq.org



Creative Commons Attribution-
NonCommercial-NoDerivatives
(CC BY-NC-ND) license

ISBN: 978-978-68-6631-4



Egypt

By Mohamed Farahat

Executive Summary

This report is an evaluation of the state of digital rights in Egypt in 2025 and serves as an update to the Londa Egypt report published in 2024.¹ The year 2025 witnessed five main changes which affect digital rights positively and negatively.

In early 2025, the Egyptian government released the second edition of the National Strategy on AI (2025-2030)². In mid of 2025, Egypt was subjected to a Readiness Assessment Methodology (RAM) by UNESCO in collaboration with

1. Mohamed Farahat, Egypt Digital Rights And Inclusion 2024 Report, Londa, Paradigm Initiative, pp.202-217. <https://paradigmhq.org/wp-content/uploads/2025/04/Londa-2024-2.pdf>
2. .Egypt Artificial Intelligence Strategy ,2025-2023. <https://ai.gov.eg/SynchedFiles/en/Resources/AIstrategy%20English%2016-1-2025-1.pdf>

the Ministry of Communication and Information Technology, which completed Egypt's AI readiness assessment in accordance with UNESCO's Readiness Assessment Methodology (RAM)³ and the final report officially has been published.⁴ In the reporting year, the National Council for Artificial Intelligence (NCAI) approved and released the Open Data Policy⁵. Late 2025 witnessed one of the most significant overdue steps, which is issuing the executive regulation on the personal data protection law five years after the law was passed in 2020. This step has completed the personal data protection legislation and regulation framework and made the law effective. Finally and adversely, in November 2025 the new criminal procedures law was issued, which gives prosecutors the authority to issue surveillance orders for communications, including social media, for an indefinite period. This new development constitutes a clear abuse of digital rights and promotes closing of the civic space.

This report reflects the continuous practices that contribute to the narrowing of the digital civic space in Egypt. The Londa report 2025 highlights the use of different legal tools as justification to abuse digital rights and affirms the inefficiency of adopted safeguards. The focal points of this assessment encompass themes such as internet accessibility and interruptions, freedom of expression in online spaces, privacy and surveillance issues, data protection, cybersecurity, the Universal Service Fund, and advancements in Information and Communication Technologies (ICTs), along with emerging technologies.

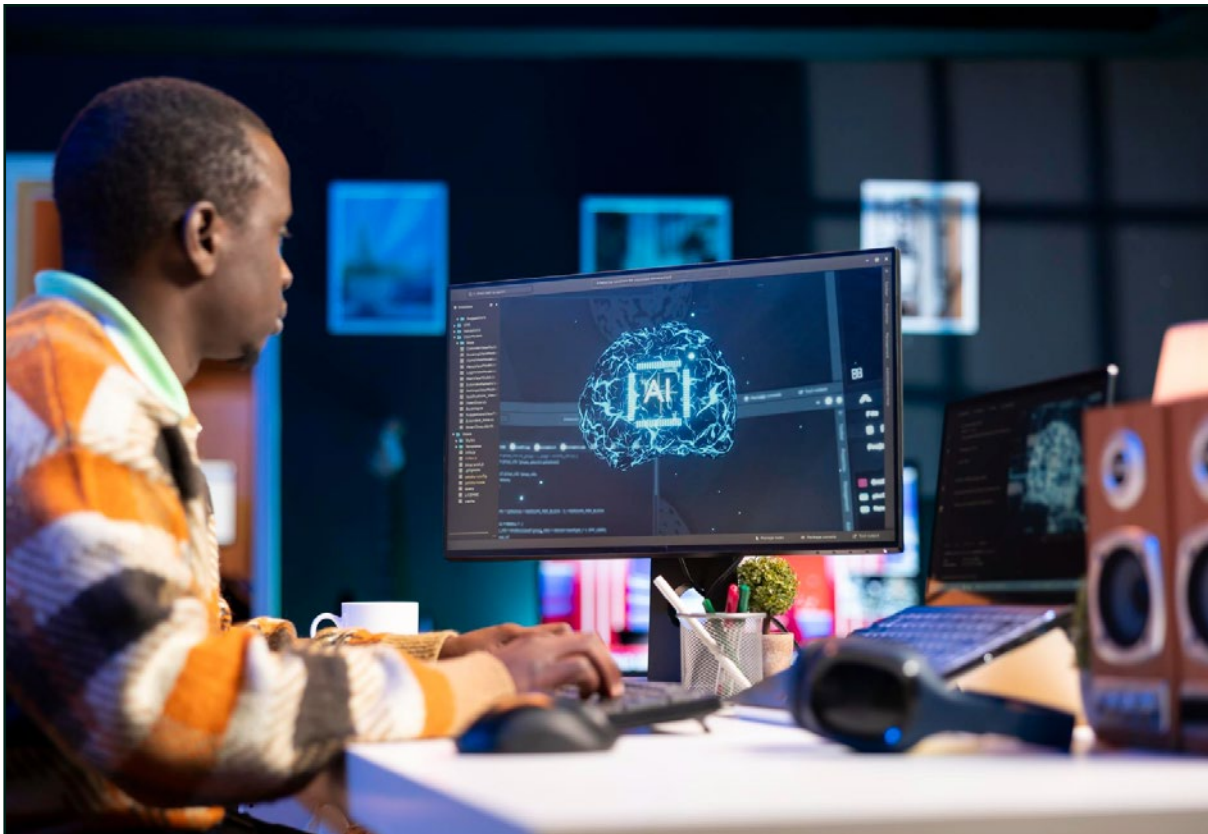
The report findings highlight that while some of the current legal frameworks safeguard the digital rights of internet users, paradoxically, some provisions enable digital rights abuses and are a means to restrict the digital civic space.

The report employed both analytical and qualitative research methodologies.

3. RAM is a key tool to support Member States in their implementation of the UNESCO Recommendation on the Ethics of AI
4. Egypt: artificial intelligence readiness assessment report <https://unesdoc.unesco.org/ark:/48223/pf0000395173?posInSet=1&queryId=39fff3b8-75bb-433c-a655-aef57bffb73d>
5. The National Council for Artificial Intelligence - Egypt. Open Data Policy Arab Republic of Egypt 2025 <https://ai.gov.eg/>

Secondary data was gathered through an extensive literature review. The proposed recommendations call for the implementation of dedicated legislation governing the creation and utilisation of artificial intelligence (AI) systems, focusing on adopting approaches that prioritise human rights in the digital age. It is also imperative to formulate executive regulations (by laws) to streamline the enforcement of data protection laws.

Additionally, introducing access to information law is essential to foster governance that is both transparent and accountable. The report uses Paradigm Initiative's TheScore Index, a digital rights index to evaluate compliance of Egypt with regard to key human rights elements and is inspired by the African Commission on Human and Peoples' Rights' Declaration of Principles on Freedom of Expression and Access to Information.⁶



6. <https://achpr.au.int/en/node/902>

Introduction

Egypt is a North African country with an estimated population of 119,134,103 by end of November 2025⁷ in comparison with 117,406,765 by December 2024⁸. In 2025, 41.91% of the total population lived in urban areas⁹ compared with 41% in 2024, while 58.9% of the total population reside in rural areas, in 2025¹⁰. The country is party to several international human rights treaties that emphasise and guarantee internet freedoms and digital rights, such as the International Covenant on Civil and Political Rights (ICCPR), the African Charter on Human and Peoples' Rights, and the Arab Convention of Anti-Information Technology Crimes (Cybercrimes). Egypt is yet to ratify the 2014 African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). It is therefore

envisaged that Egyptian domestic laws need to be aligned with existing international human rights laws and standards.

Since 2018, Egypt has been enacting legislation that significantly shapes the landscape of digital rights. Laws that govern internet freedoms include the Personal Data Protection Law No. 151 of 2020 and the Law no. 175 of 2018 combating information technology crimes.¹¹ Egypt also enacted national security and anti-terrorism laws. Recently, Egypt enacted the criminal procedures law no.174 of 2025. These recent legislative frameworks have often been utilised to restrict the civic space. Regrettably, the implementation of these measures has also had adverse consequences on media freedoms.¹²

7. Worldometers, Egypt ,<https://www.worldometers.info/world-population/egypt-population/>

8. Worldometers, Egypt , <https://www.worldometers.info/world-population/egypt-population/>

9. Worldometers, Egypt ,<https://www.worldometers.info/world-population/egypt-population/>

10. Worldometers, Egypt, <https://www.worldometers.info/demographics/egypt-demographics/#urb>

11. Mohamed Farahat, (2021). Egypt Digital Rights And Inclusion, LONDA, Paradigm Initiative,. <https://paradigm-hq.org/wp-content/uploads/2021/05/lr-Egypt-Digital-Rights-Inclusion-2020-Report.pdf>, Mohamed Farahat (2021) , Egypt Digital Rights Landscape Report, in T. Roberts (ed.), Digital Rights in Closing Civic Space: Lessons from Ten African Countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.014. AND, Miral Sabry AlAshry, op,cit.,

12. Miral Sabry AlAshry (2022) A critical assessment of the impact of Egyptian laws on information access and

Moreover, in the aftermath of the COVID-19 pandemic, Egypt continues to grapple with the dissemination of false information in its various manifestations, such as misinformation and disinformation.¹³ It is, therefore, evidently imperative to adopt access to information legislation to guarantee the proactive dissemination of credible information to the public by relevant stakeholders and to prevent spreading false information. Generally, there was no significant improvement in the digital rights situation in Egypt in 2024, juxtaposed with the developments observed over the preceding five years. According to Freedom House, Egypt's score for internet freedom was 26 out of 100 in 2019, 27 out of 100 in 2020, and 28 out of 100 in 2023 and 2024.¹⁴ Throughout the five-year period, Egypt was classified as "not free" in the category of internet freedom. The subsequent sections of this report explore the reasons behind the low rate of internet freedoms, examining

whether the root cause lies in legislation or its execution.

Internet Access

As reported by the Egyptian Ministry of Communication and Information Technology (MCIT), in the period from July through September 2025, mobile subscriptions stood at 120.85 million - which constitutes 100% of the total population - compared to 111.12 million in the same period in 2024, with a 8.75% rate of annual growth.¹⁵ From July through September 2025, the fixed line subscriptions stood at 13.86 million, growing 7.12% from 12.94 million in the same period in 2024.

At the beginning of 2025, there were 96.3 million internet users in Egypt¹⁶, while it was 82.01 million in the beginning of 2024¹⁷. Internet penetration was 81.9%¹⁸

dissemination by journalists, *Cogent Arts & Humanities*. P. 1. DOI: 10.1080/23311983.2022.2115

13. Mohamed Farahat, *Coronavirus Trials in Egypt: Blurring the Lines Between Fake News and Freedom of Expression*, SMEX.

14. Freedom House, "Freedom On The Net 2024, Egypt", <https://freedomhouse.org/country/egypt/freedom-net/2024#B> Accessed 20/12/2024.

15. Ministry of Communications and Information Technology|ICT Indicators Bulletin, September 2025 Quarterly Issue, p.2. https://mcit.gov.eg/Upcont/Documents/Publications_4112025000_ICT_Indicators_in_Brief_September_2025.pdf

16. Data Reportal , *Egypt 2025*, <https://datareportal.com/reports/digital-2025-egypt>. Accessed 23 February 2026

17. Data Reportal , *Egypt 2024*, <https://datareportal.com/reports/digital-2024-egypt?rq=egypt>. Accessed 23 February

in 2025, up from 72.2%¹⁹ in 2024. In 2023, only 72.2% of the population was connected²⁰. According to the Speedtest Global Index, the speed of fixed broadband in Egypt in October 2025 was 91.25 Mbps, ranking 73rd globally out of 156 countries²¹, while it was 76.67 Mbps, ranking 81st globally out of 154 countries in November 2024²². In October 2023, it was 61.22 Mbps, ranking 83rd globally²³. In terms of mobile speed, it was 44.51 Mbps, ranking 83rd globally out of 104 countries by December 2025²⁴, while it was 38.29 Mbps, ranking 86th globally out of 110 countries by December 2024²⁵. According to Kepios, internet

users in Egypt increased by 12 million (+14.6%) between January 2024 and January 2025.²⁶ In 2024,²⁷ 99.89% of the population was covered by 3G mobile network, while 99.62% was covered by 4G mobile network.²⁸ Egypt is one of 14 countries in Africa where 5G networks are being tested and widely deployed.²⁹ Other African countries, including North African countries, still invest in 4G networks.³⁰ Egypt has achieved remarkable strides in connectivity and is among the leading countries on the continent in this regard. In the context of social media users, there were 50.7 million social media users in Egypt in January 2025, or 43.1% of the

2026

18. Data Reportal , Egypt 2025, <https://datareportal.com/reports/digital-2025-egypt>. Accessed 23 February 2026
19. Data Reportal , Egypt 2024, <https://datareportal.com/reports/digital-2024-egypt?rq=egypt>. Accessed 23 February 2026
20. Data Reportal , Egypt 2023, <https://datareportal.com/reports/digital-2023-egypt>. Accessed 23 February 2026
21. Speedtest Global Index , <https://www.speedtest.net/global-index>, October 2025. Accessed October 2025
22. Speedtest Global Index. Egypt's Mobile and Broadband Internet Speeds - Speedtest Global Index. Accessed October 2025
23. Speedtest Global Index. <https://www.speedtest.net/global-index/egypt#mobile>. Accessed October 2025
24. Speedtest Global Index, <https://www.speedtest.net/global-index/egypt#mobile>. Accessed October 2025
25. Speedtest Global Index. Egypt's Mobile and Broadband Internet Speeds - Speedtest Global Index. Accessed October 2025
26. Data Reportal , Egypt 2025, <https://datareportal.com/reports/digital-2025-egypt>. Accessed 23 February 2026
27. Figures of 2023 were not available during the time of writing this report.
28. Stasista, Digital & Connectivity Indicators – Egypt. <https://www.statista.com/outlook/co/digital-connectivity-indicators/egypt#:~:text=The%204G%20network%20coverage%20in,to%20amount%2099.89%25%20in%202024.>
29. Diplo Foundation , Status of internet access and connectivity in Africa. URL: https://www.diplomacy.edu/wp-content/uploads/2023/01/African-digital-foreign-policy_En.pdf. P,56 and 57.
30. Diplo Foundation , Status of internet access and connectivity in Africa, <https://www.diplomacy.edu/wp-content/>

total population.³¹ There were 45.40 million social media users in January 2024, representing 40% of the total population³². According to Statcounter, in the period from January 2025 to January 2026, 90.94% of the population was using Facebook³³, compared to 63.96% in November 2024³⁴. 2.7941% using Instagram by December 2025, while it was 21.3% in August in the same year.³⁵, and 18.57% in November 2024³⁶. By December 2025, 6.12% were using YouTube³⁷, down from 9.7% in November 2024³⁸. 1.07% used Twitter in 2025³⁹, down from 4.17% in 2024⁴⁰. It is very clear that there is a significant decrease between

2024 and 2025 in the use of social media, particularly Instagram, Twitter, and YouTube. There were no reported cases of internet shutdowns in 2025, but Freedom House reported that “the Brussels-based independent Egyptian media outlet, Zawia3, was blocked.”⁴¹

Privacy and Surveillance

As mentioned earlier, Egypt is a party to most of the international human rights binding treaties which emphasise and guarantee the rights to privacy and prohibit unlawful surveillance practices.

uploads/2023/01/African-digital-foreign-policy_En.pdf

31. Data Reportal , Egypt 2025⁴, <https://datareportal.com/reports/digital-2025-egypt>. Accessed 23 February 2026

32. Data portal <https://datareportal.com/reports/digital-2024-egypt?rq=egypt>. Accessed 23 February 2026

33. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026, <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026.

34. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

35. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026, <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

36. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

37. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026Jan 2025 - Jan 2026, <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

38. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 <https://gs.statcounter.com/social-media-stats/all/egypt>

39. StateCounter, Global State, Social Media Stats Egypt ,Jan 2025 - Jan 2026Jan 2025 - Jan 2026, <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

40. StateCounter, Global State, Social Media Stats Egypt , Nov 2023 - Nov 2024 <https://gs.statcounter.com/social-media-stats/all/egypt>. Accessed 23 February 2026

41. Freedom House, Freedom on the Net 2025, Egypt. URL:<https://freedomhouse.org/country/egypt/free->

Principle 40 of the African Commission on Human and Peoples' Rights' (ACHPR) 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa (the Declaration) states that "Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information and everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies".⁴² On October 25 2025, Egypt was one of North African States that signed the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes⁴³ (United Nations Convention against Cybercrime). Only four North

African States out of seven states signed the convention: Algeria, Morocco, Libya, and Egypt. It is worth mentioning that only 21 African countries out of 54 signed the convention.⁴⁴

Article 57 of the Constitution provides the protection to the right to privacy and this provision aligns with Principle 40 of the ACHPR 2019 Declaration and other international human rights treaties and standards. Article 57 states that "the right to privacy may not be violated, shall be protected and may not be infringed upon. Postal, telegraphic, and electronic correspondence, telephone conversations, and other means of communication are inviolable, their confidentiality is guaranteed, and they may not be confiscated, viewed, or monitored except by a reasoned judicial order for a specific period and in the circumstances specified by law."⁴⁵ The State is also committed to protecting citizens' right to use public means of communication in all its forms. It is not

[dom-net/2025#A](#) , Accessed 23/2/2026.

42. African Commission on Human and Peoples' Rights ,the Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019.

43. United Nations , Treaty collection.https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-VIII-16&chapter=18&clang=_en

44. United Nations , Treaty collection.https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=X-VIII-16&chapter=18&clang=_en

permissible to disrupt, stop, or deprive citizens of these rights arbitrarily. While this is regulated by law, other laws have provisions that undermine the right to privacy, as expounded later in this report. In terms of promoting children's digital safety and privacy online, Egypt adopted different laws seeking to protect children in general including in digital sphere such as children law no 12 of year 1996, Penal Code, cybercrimes law, data protection law, and law no 64 of year 2010 focused on combatting trafficking in persons.

In addition, Article 99 of the Constitution establishes the right to remedies and compensation for damage resulting from abuse of privacy: "any violation of personal freedom, or the sanctity of the private life of citizens, or any other public rights and freedoms which are guaranteed by the Constitution and the Law is a crime. The criminal and civil lawsuit arising from such crime shall not abate by prescription. The affected party shall have the right to bring a direct criminal action."⁴⁵ The right to remedy and compensation are guaranteed by the Constitution and also guaranteed under Article 163 of civil law. In particular,

there are many compensation claims submitted to Egyptian courts for breach of privacy with final judgement in favour of affected persons.

Article 25 of Law No. 175 of 2018 on Combating Information Technology Crimes criminalises the breach of the family's principles and values of Egyptian society and the violation of the inviolability of private life. It is punished by imprisonment for a period of not less than six months and a fine of not less than EGP50,000 (US\$1,600) and not exceeding EGP100,000 (US\$3,200).

The same Article includes some actions that constitute a breach of privacy, such as sending a large number of messages electronically to a specific person without their consent, granting data to a system or website to promote goods or services without their consent, or publishing, via the information network or by any means of information technology, information, news, pictures, and the like, that violate the privacy of any person without his consent, whether the published information is correct or incorrect. Article 26 of the same law added that "anyone who intentionally uses an information

45. Egypt, Constitution 2014 article 57

program or information technology to process personal data of others in order to link it to content that is contrary to public morals or to display it in a way that would infringe on his character or honour.” In the same context, Article 20 of Law No. 180 of 2018 regarding Regulating the Press, Media, and the Supreme Council for Media Regulation stipulated that “it is prohibited in any means of publication or broadcast to breach the private lives of citizens”.

In terms of surveillance practices in Egypt⁴⁷ according to Principle 41 of the ACHPR 2019 Declaration, states shall rely on it if it is “authorised by law, that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim”.⁴⁸ In the Egyptian context, community standards and ensuring national security are always used as justification for undertaking surveillance.⁴⁹ Under the regime of Hosni

Mubarak, surveillance practices were primarily focused on monitoring terrorist activities. However, the dynamics have transformed significantly in the aftermath of the 2011 revolution and subsequent political events, emanating from the pivotal role that social media played. Surveillance measures have expanded beyond tracking terrorist activities. Rigorous steps were implemented to regulate internet access and scrutinise online content. Legislation is used to ban websites, obtain personal data, abuse citizens’ right to privacy, and criminalise the right to freedom of expression through allegations of disseminating false news.⁵⁰

As already stated, Article 57 of the Constitution prohibits surveillance except when authorised by a judicial order, strictly for a defined duration, and in cases specified by the law. Article 71 of the Constitution stipulates that “it is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers

46. Constitution article 99

47. For detailed information about surveillance practices and related framework refer to Mohamed Farahat (2021), Egypt country report, in *Surveillance Law in Africa: a Review of Six Countries*, Brighton: Institute of Development Studies, pp.48-70. DOI: 10.19088/IDS.2021.059

48. African Commission on Human and Peoples’ Rights, *The Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019*.

49. OpenNet Initiative (September 2004). *A Starting Point: Legal Implications Of Internet Filtering*.

50. Mohamed Farahat (2021), Egypt country report, in *Surveillance Law in Africa: a Review of Six Countries*, Brighton:

and media in any way. In exceptional circumstances, they may be subject to limited censorship in times of war or general mobilisation”.⁵¹ However, the same laws contain specific provisions that grant powers to the authorities to block websites that are deemed a threat to national security.

November 2025 witnessed the emergence of a new criminal procedures law no 174 of 2025 as a new legal tool to close the civic space in Egypt and promote surveillance practices. The law gives prosecutors the authority to issue surveillance orders for communication services, including social media, for an indefinite period. The law will enter into force on October 1 2026, in accordance with Article (Sixth) of promulgating provisions of the law. This new development constitutes a clear abuse of digital rights and promotes closure of the civic space.

Article 80 of the above-mentioned law clearly states the following: “A member of the Public Prosecution (Prosecutor) - after permission from the judge - has

the power to order the interception of wired and wireless communications, social media accounts and applications (including their various non-public content), electronic mail (email), text, audio, or video messages on phones, devices, or any other technological means, and to seize the containing media/devices; or make recordings of conversations that took place in a private location, whenever such action is deemed beneficial for the discovery of the truth in a felony or a misdemeanor punishable by imprisonment for a period exceeding three months. The order must be for a period not exceeding 30 days. The order may renew it for one or more similar periods”. The new law reinforces surveillance for an indefinite period even in cases of not serious crimes.

Article 117 of the same law added that “Chief Prosecutor (Ra’ees Niyaba) or higher, shall have the authority, in the investigation of felonies stipulated in Chapters I, II, II bis, III, and IV of Book Two of the Penal Code⁵², in addition to the powers prescribed for the Public

[Institute of Development Studies, p.48. DOI: 10.19088/IDS.2021.059 p.48.](#)

51. [Constitution article 71](#)

52. [The Chapters from I to IV in Book Two of the Penal Code of Egypt address offences directed against persons and nature, beginning with crimes of Homicide, Wounding, and Battery/Assault \(Chapter I\), followed by Intentional Arson \(Chapter II\). This is succeeded by offenses such as Causing Abortion \(or Inducing Miscarriage\) and Manufacturing Substances Injurious to Health \(Chapter III\), and finally, Indecent Assault and Corruption of Morals](#)

Prosecution, to issue a reasoned order for a period not exceeding 30 days, to:

Intercept and monitor wired and wireless communications, social media accounts and their various non-public content, electronic mail (email), text, audio, or video messages on phones, devices, or any other technological means;

1. Seize the containing media/devices;
2. Or make recordings of conversations that took place in a private location, whenever such action is beneficial for the discovery of the truth

The order referred to in the first paragraph of this Article may be renewed for one or more similar periods”.

Article 80 and 117 of new criminal procedures law no 174 of 2025 legally establishes a provision for surveillance for an indefinite period of time, not only for published content but also for private conversation, without clear safeguards to avoid abuse of privacy rights.

Article 1 of the Cybercrimes Law No. 175 of 2018 defines national security as everything related to the independence, stability, and security of the homeland

and anything linked to affairs of the Presidency, the Ministry of Defense and General Intelligence. The term ‘national security’ is vague and shrouded in ambiguity. The lack of clarity in defining national security bestows unfettered discretionary powers upon the authorities, allowing them to decide which actions may pose a threat to national security. Although the Constitution prohibits surveillance practices without a judicial order, the different laws provide the legal basis for surveillance, such as Telecommunications Regulation Law No. 10 of 2003, Personal Data Protection Law No. 151 of 2020, Anti-Terrorism Law No. 94 of 2015, Anti-Cyber and Information Technology Crimes no. 175 of 2018, and Emergency Law no. 162 of 1958.⁵³ On the basis of the information already provided, it can be asserted that the existing laws exhibit a partial alignment with international human rights standards at a superficial level. However, the same laws contain provisions that undermine digital rights.

(Chapter IV). These Chapters pertain to direct aggressions/offences against individuals and their public and private property.

53. Mohamed Farahat (2021), Egypt country report, in *Surveillance Law in Africa: a Review of Six Countries*, Brighton: Institute of Development Studies, pp.53-56. DOI: 10.19088/IDS.2021.059 And , Mohamed Farahat , Mohamed

Irrespective of the Egyptian legal framework, which to some extent protects the right to privacy, the actual practice witnessed served as abuse to this fundamental right, and demonstrates that the existing legal framework was used to justify the digital surveillance. For instance, according to Thomson Reuters Foundation, 6,000 surveillance cameras were deployed in the new administrative capital⁵⁴. According to People in Need, “Digital censorship was evident, in the period between May 2023 and May 1 2024, there were five instances where digital platforms were blocked, further restricting access to information and limiting journalistic freedom.⁵⁵” In the same context, and according to Freedom House, “Egyptian governments use Sandvine devices to block websites and monitor, prevent, or tamper with connections”⁵⁶. The flagship product of Sandvine “is deep packet inspection (DPI) which is a common tool used by ISPs and

telecom companies to monitor traffic and prioritize certain types of content, however it is also used to divert traffic away from sites or social media platforms and into dead ends, effectively censoring them.⁵⁷” According to WIRED, “In February 2024, the US Department of Commerce added Sandvine to its Entity List, effectively blacklisting it from doing business with American partners due to the fact that the company’s technology was used in mass web monitoring and censorship in Egypt contrary to the national security and foreign policy interests of the United States.⁵⁸”

Online Freedom of Expression

The ACHPR 2019 Declaration stresses the importance of both rights and states that “[t]he respect, protection and

Farahat, Egypt Digital Rights and Inclusion 2020 report, LONDA, Paradigm Initiative <https://paradigmhq.org/wp-content/uploads/2021/05/lr-Egypt-Digital-Rights-Inclusion-2020-Report.pdf>

54. Thomson Reuters Foundation, CCTV cameras will watch over Egyptians in new high-tech capital, 4 January 2023.

55. People in Need, Report: Violations of journalist and media rights in Egypt (May 2023 - May 2024), Published: Sep 20, 2024. <https://www.peopleinneed.net/report-violations-of-journalist-and-media-rights-in-egypt-may-2023-may-2024-11862gp>

56. Freedom House, Key Developments, June 1, 2023 - May 31, 2024. https://freedomhouse.org/country/egypt/freedomnet/2024#footnoteref15_SkY8W4xsgQfWO6slCXHW5-YXwAktvCYGYMgBYfXwANI_nhebWdJe4puP

57. WIRED, Dictators Used Sandvine Tech to Censor the Internet. The US Finally Did Something About It, Feb, 2024. <https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/>

fulfilment of these rights is crucial and indispensable for the free development of the human person, the creation and nurturing of democratic societies and for enabling the exercise of other rights". This segment of the report underscores the correlation between freedom of expression and the right to access information. When both rights are guaranteed without undue restrictions, it contributes to combating the spreading of false news while promoting freedom of expression, including the right to engage in constructive criticism of government policies.

Despite the surveillance practices outlined earlier, it is essential to underscore the constitutional assurance of freedom of expression. Article 65 guarantees freedom of thought and opinion and all individuals have the right to express their opinions through various means of expression and publication, including digital platforms. However, Article 102 (Bis) of the Penal Code criminalises broadcasting false news, statements, or rumours, particularly if such actions are considered to potentially disturb public security, spread terror among people, or jeopardise public interest. While the

legitimacy of criminalising the publication of false news is acknowledged, the existing legal framework does not define the parameters of what constitutes harm to public security and interest. Moreover, article 19 of Law No. 180 of 2018, regulating the Press, Media, and the Supreme Council for Media Regulation, prohibits the publication of false news, incitements of violations of the law, promotion of violence or hatred, and discrimination between citizens. It also forbids publication of content that endorses racism or includes an abuse of the honour of individuals, cursing or slandering them, or insulting religions. Article 4 of this law also restricts the publication of content that contradicts the Constitution. In this regard, it explicitly prohibits the promotion of activities that encourage legal violations, contravene the professional code of honour, disrupt public order, or undermine public morals. The Article also prohibits the propagation of content that fosters discrimination, violence, racism, or hatred. Evidently, the aforementioned provision exhibits legal deficiencies characterised by the utilisation of ambiguous terms like "public order" and "public morality." It also fails

58. WIRED, Dictators Used Sandvine Tech to Censor the Internet. The US Finally Did Something About It, Feb, 2024. <https://www.wired.com/story/sandvine-us-sanctions-egypt-internet-censorship/>

to specify actions deemed as detrimental to the honour of individuals. The lack of precision raises concerns regarding the clarity and enforceability of the provision, warranting a careful reassessment to enhance its legal robustness and effectiveness. Also, the absence of a well-defined legal framework that distinguishes between misinformation and the lawful dissemination and unrestricted flow of information poses a significant challenge to the preservation of freedom of expression that is constitutionally guaranteed. The country's 2021 National Human Rights strategy that was developed by the government acknowledges "the lack of a legal framework regulating access to and circulation of official information, data, and statistics, albeit being a constitutional right".⁶⁰

Egypt is yet to enact an access to information law, a situation which is contrary to the aspiration enshrined under Principle 26 of the ACHPR 2019 Declaration. Therefore, dissemination of information that deviates from official government publications is consistently deemed a violation, constituting the offence of disseminating false

information.

New Open Data Policy

In October 2025, the National Council for Artificial Intelligence (AI) released the first "Open data policy"⁶¹ in the country. According to this policy, open data refers to the data maintained by the government and its goal is to establish the general framework for data openness in public institutions by defining the principles, guidelines, and responsibilities that ensure the consistent, secure, and effective sharing, management, and reuse of data, prior to the issuance of the Data Governance Law, its implementing regulations, and the accompanying data classification framework. This step may open the door to adopt access to information law. One of the important principles adopted by the policy is "availability, affordability, and ease of use." According to the policy, data should be available and easily accessible to the average citizen, regardless of their technical skills or geographical location; and data should be discoverable and machine-readable. In addition to that,

59. African Commission on Human and Peoples' Rights, *The Declaration of Principles of Freedom of Expression and Access to Information in Africa 2019 Principle 1*

60. Egypt, Supreme Standing Committee for Human Rights, *National Human Rights Strategy (2021)* p31 <https://sschr>.

the policy establishes an “Interim Joint Committee for Data Accessibility” as a central body responsible for data governance ensuring the protection of data by reviewing it and coordinating the disclosure process across ministries and public entities.

2025 witnessed several actions taken based on the above-mentioned laws which target content creators and ‘Online Opinion Expressers’ (OOE). For instance, “On Tuesday, July 22 2025, Al-Azhar’s official Facebook page published a statement by Sheikh Ahmed Al-Tayeb, the Grand Imam of Al-Azhar, strongly condemning Israeli attacks on the Gaza Strip and calling for urgent action to save residents of the Strip from starvation. The statement was mysteriously deleted minutes later. Multiple sources confirmed the deletion came under political pressure from powerful state agencies⁶²”.

Data Protection

The Data Protection Law (DPL) No 151 of

2020 was enacted in 2020. In November 2025, the Minister of Communication and Information Technology issued the law’s executive regulation⁶³, five years after the law was adopted, to complete the personal data protection legal and regulation framework in compliance with the provisions outlined in the legislation. The executive regulations of this law specify the policies, procedures, controls and standards for collecting, processing, preserving and securing this data. Data minimisation regulation in the law ensures that organisations collect, process, and retain only the personal data that is strictly necessary for the purpose for which it was collected. This provision is aligned with Article 22 of the African Union, African Convention on Cybersecurity and Personal Data Protection 2014 (Malabo Convention), which permits the retention of personal data until the fulfilment of the intended purpose for which the data were originally collected and processed.⁶⁴ However, Article 2 of the Cybercrimes Law No 175 of 2018 grants permission to service providers to retain and store user data for 180 days. This provision for data

gov.eg/media/gapb5bq4/national-human-rights-strategy.pdf

61. The National Council for Artificial Intelligence, Open Data Policy- Arab Republic of Egypt <https://ai.gov.eg/>

62. Law and Democracy Support Foundation e.V., Egypt: Escalating Hostility Toward Freedom of Expression Now Targets Regime Insiders, July 23, 2025. URL: <https://ldsf.info/blog/2025/07/23/23-07-25-1/>

retention contradicts the Data Protection Law. The Cybercrime Law does not include a provision that justifies personal data retention for that timeframe. The law should be amended to enhance transparency and incorporate a clear justification for data retention.

The Data Protection Law has provisions that regulate the processing of sensitive personal data. Article 12 prohibits the collection, transfer, storage, retention, processing, or disclosure of sensitive personal data except with authorisation from the “personal data protection centre”.⁶⁵ Except in cases authorised by law, written and explicit consent is required from the person concerned. Additionally, when processing children’s personal data, the consent of the guardian must be secured. Participation of a child in activities such as games, competitions, or any other engagements should not be contingent upon the provision of personal data beyond what is strictly essential for their involvement. Article 1 of the law defines sensitive data as data that discloses psychological, mental,

physical or genetic health, biometric data, financial data, religious beliefs, political opinions, or security status. In all cases, children’s data is considered sensitive personal data. Article 41 of the law states that “Any holder, controller, or processor who collects, makes available, circulates, processes, discloses, stores, transmits or saves sensitive personal data shall be punished by imprisonment for a period of not less than three months and a fine of not less than EGP500,000 (approximately US\$10) and not exceeding EGP five million (approximately US\$100000), or by one of these two penalties, without the consent of the data subject or in cases other than those legally authorised”.

In February 2025, the Economic Court of Alexandria ordered Orange Egypt to pay EGP 10 million in compensation to a woman whose personal data had been unlawfully compromised. The judgment arose after the company replaced the claimant’s SIM card without her consent, which led the court to award compensation for both material and moral damages⁶⁶

63. Minister of CIT, Ministerial decree No.816 of 2025 on 1 November, 2025. Al Wqaa El Masrya issue 244 Bis (A).

64. African Union, African convention on Cybersecurity and personal data protection 2014.

65. According to article 1 of personal data protection law No 151 of 2020, centre refers to the personal data protection centre.

66. Shehta and Partners, Legal Alert: Egyptian Court Judgment Tightens Enforcement of Privacy and Data Protection

Universal Service

Fund (USF)

According to GSMA Intelligence,⁶⁷ a Universal Service Fund (USF) is based on three principles: availability, affordability, and accessibility.⁶⁸ Egypt allocated a specific fund for accessing universal services, regulated by the Telecom Regulation Law no.10 of 200. Article 2 of that law stipulates that Telecommunication Services shall comply with the following rules:

1. Publicity of information;
2. Protection of free competition;
3. Provision of Universal Service; and
4. Protection of Users' rights.

Article 9 stipulates that the National Telecommunications Regulatory Authority (NTRA) is entitled to maintain an autonomous budget, adhering to

the guidelines outlined in its internal regulations and in conformity with the Unified Accounting System. This autonomy extends without any restrictions imposed by governmental rules or regulations. In 2005, the National Telecom Regulatory Authority (NTRA) established the USF.⁶⁹ The USF strives to provide essential telecommunication services to every citizen at reasonable rates.⁷⁰ There is no publicly available official record about the value of the USF in Egypt. According to some media reports, the USF started with an initial budget of EGP50 million, approximately US\$1 million.⁷¹ Moreover, the National Telecommunications Regulatory Authority (NTRA) has proposed and financed projects to establish, operate, and provide mobile phone services to 54 urban areas and 22 strategic roads throughout the Republic, with a total length of 3,100 km, and a total cost of EGP1,668,000,000

Laws, URL:<https://shehatalaw.com/law-update/legal-alert-egyptian-court-judgment-tightens-enforcement-of-privacy-and-data-protection-laws/> Accessed in 24/3/2026.

67. GSMA Intelligence is the global home of mobile market information, driven by our team of expert analysts and is the definitive source of mobile industry insights, forecasts, and research, used around the world.<https://www.gsmainelligence.com>.

68. GSMA, (2023). Universal service funds in Africa Policy reforms to enhance effectiveness, p.14. <https://www.gsma.com/subsaharanafrika/wp-content/uploads/2023/10/USF-Africa.pdf>.

69. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.3. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>

70. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.8. <https://www.tra.gov.eg/wp-content/>

(US\$ 54 million).⁷² Furthermore, the National Telecommunications Regulatory Authority (NTRA) has initiated measures to enhance the efficacy of fundamental communication services within the Sinai Peninsula. The initiative involves the funding, construction, and operation of mobile phone stations across 30 urban areas and along four critical roads with a total distance of 112 kilometres. This initiative will reportedly cost EGP513 million (US\$16,000,000), reflecting NTRA's commitment to advancing connectivity and infrastructure.⁷³

Available media reports indicate that in a meeting held in January 2023, with the Parliamentary committee responsible for telecommunication and information technology, the Chairperson of NTRA said that “[t]he Universal Service Fund bears three billion Egyptian pounds to provide telecommunications services in deprived areas and new roads at a cost of 1.8 billion Egyptian pounds, in addition to 1.2

billion to establish 592 stations in the first phase for a decent life Project (تأهيل عوالمهم / Decent life).⁷⁴ The aforementioned initiatives and allocated funds, aimed at addressing telecommunication and connectivity challenges, illustrate that the USF in Egypt is used to narrow the digital divide between urban and rural areas. Concurrently, these initiatives are focused on enhancing the affordability, accessibility, universality and availability of internet and telecommunication services. This is what is envisaged under Principle 41 of the ACHPR 2019 Declaration which requires States, in collaboration with other stakeholders, to adopt measures to ensure universal, equitable, affordable, and meaningful access to the internet without discrimination.⁷⁵

USF initiatives include upgrading existing road infrastructure linked to providing telecommunication services⁷⁶; the El Million Fadan Project which aims

[uploads/2020/11/Universal-Service-Policy.pdf](https://muhtwaplus.com/uploads/2020/11/Universal-Service-Policy.pdf)

71. <https://muhtwaplus.com/49705/2020/07/25/ال-م-دخ-ال-م-دق-ي-ت-ال-اص-ت-ال-ل-ي-م-و-ق-ل-ا-ز-ا-ه-ج-ل-ا/>

72. El Youm El Sabaa, accessed 13 /2/2024. <https://www.youm7.com/story/2021/12/8/ن-ع-هت-ف-ر-ع-م-د-ي-ر-ت-ا-م-ل-ك/>

73. El Youm El Sabaa, accessed 13 /2/2024. <https://www.youm7.com/story/2021/12/8/ن-ع-هت-ف-ر-ع-م-د-ي-ر-ت-ا-م-ل-ك/>

74. Sada El-Balad news , <https://www.elbalad.news/5594448>

75. ACHPR 2019 Declaration principle 41

to expand the agricultural sector by improving mobile coverage⁷⁷ and other national telecommunications and information plan projects such as public educational institutions and libraries, funding for Health Care Centers, services provided to the disabled, infrastructure of digital society and digital architecture, and a broadband project to increase the deployment of high-speed internet in Egypt to create jobs.⁷⁸ While acknowledging that the USF regulations focus on digital transformation to a considerable extent, it is imperative to propose recommendations to amend the existing framework so that it explicitly provides for regulating funds for digital literacy and awareness. The abovementioned initiatives contribute to filling the digital gap in Egypt, promoting economic development, and ensuring connectivity in urban and rural areas. As ICT is one of the core services of the government, it is always keen to allocate financial sources to improve.

Developments in

ICT and Emerging

Technologies

In 2025, Egypt ranked 51st globally in the Government AI Readiness Index, which places it as the first in Africa and North Africa sub-region, and third in the MENA region after Kingdom of Saudi Arabia and United Arab of Emirates, and before Qatar⁷⁹. Its rank was 65th globally in 2024⁸⁰, which means Egypt moved up fourteen places between 2024 and 2025. The country was ranked seventh in the MENA region in the same year and moved up four positions in 2025. This reflects the progress Egypt has achieved in the context of AI integration.

In November 2019, the Egyptian Cabinet approved the establishment of the National Council for Artificial Intelligence

76. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.17. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>

77. National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.17. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>.

78. National Telecom Regulatory Authority (NTRA), Universal Service Policy, pp.17-19.. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>, pp. 17-19.

79. Oxford Insights, Government AI Readiness Index,2025.p.61.

80. Oxford Insights, Government AI Readiness 2024, <https://view.officeapps.live.com/op/view.aspx?s->

(NCAI).⁸¹ At its inception, the primary task of the NCAI was the adoption of a National AI Strategy (NAIS). Subsequently, in July 2021, the NCAI adopted the Egypt AI strategy.⁸² At the point of adoption, it was envisaged that the strategy would be implemented in a phased approach until the end of 2022. In 2024, the strategy's execution remained in its initial stage, primarily attributable to the postponed launch. The goal of the initial phase is "to prove the value of AI in the different domains and build the foundations upon which to build AI at scale".⁸³ Although the Egyptian government adopted the national AI strategy⁸⁴ and established the NCAI, binding legislation on AI is yet to be enacted.

Regarding the influence of AI on privacy, Egypt enacted the previously stated cybercrimes and data protection laws in 2018 and 2022 respectively, providing a

framework that could be utilised, to some degree, for AI regulation, particularly in terms of privacy, combating arbitrary actions, unlawful surveillance and personal data protection. However, both laws are inadequate to completely regulate AI in Egypt as both laws tackle human acts and do not touch on actions committed by AI systems.

In 2023, the NCAI adopted the Egyptian Charter for Responsible AI (the Charter).⁸⁵ The main aim of the Charter is to ensure the ethical use, deployment and management of AI systems in Egypt.⁸⁶ The Charter also incorporates overarching principles such as fairness, transparency, a focus on human-centeredness, accountability, and the assurance of security and safety⁸⁷. In addition, the strategy acknowledges that "the existence of policies, regulations, and legislation to mitigate potential

rc=https%3A%2F%2Ffoxfordinsights.com%2Fwp-content%2Fuploads%2F2024%2F12%2F2024-GAIRI-data.xlsx&wdOrigin=BROWSELINK

81. <https://ai.gov.eg>

82. Egypt , AI strategy, [https://ai.gov.eg/Egypt National AI Strategy \(6-4-2021\)4.pdf](https://ai.gov.eg/Egypt%20National%20AI%20Strategy%20(6-4-2021)4.pdf)

83. Egypt AI strategy , p. 60.

84. Egypt , Egypt Artificial Intelligence Strategy. [https://ai.gov.eg/Egypt National AI Strategy \(6-4-2021\)4.pdf](https://ai.gov.eg/Egypt%20National%20AI%20Strategy%20(6-4-2021)4.pdf)

85. Egypt ,Egyptian Charter For Responsible AI <https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf>

86. Egypt ,Egyptian Charter For Responsible AI. p.1. <https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf>

87. Egypt ,Egyptian Charter For Responsible AI. pp..2-3. <https://aicm.ai.gov.eg/en/Resources/EgyptianCharterForResponsibleAIEnglish-v1.0.pdf>

misuse, whether ethical, legal, or socio-economic, can promote and enable the widespread adoption of AI solutions”⁸⁸. This is not yet the case. Egypt’s ethical use and deployment of AI systems is undermined by the lack of a national legal framework on AI.

One of the recommendations proposed in the strategy is to “communicate and coordinate with appropriate government bodies to issue laws and regulations when and where needed.”⁸⁹ This recommendation may be considered a call for the adoption of a regulation where the need arises. The question of adopting independent and specific AI laws and regulations may need more time because Egypt has recently commenced regulating AI by adopting a national strategy and Charter for responsible AI. In this stage, AI may be regulated by adding specific provisions to existing laws. In the same vein, as per media reports, the Parliamentary Committee on Communication and Technology has commenced deliberations on the adoption of AI-related regulations. The Committee Chairperson indicated that the

proposed regulation will not be a separate law. Instead, the plan is to introduce AI-specific provisions to the Cybercrimes Law No. 175 for 2018. This approach is the first step towards the establishment of precise regulations governing various facets of AI within the Cybercrimes Law. The imperative to regulate the utilisation of AI systems is strongly advocated for, whether achieved through the enactment of an independent law or the incorporation of targeted provisions into existing legal frameworks.

In January 2025, due to the rapid development of AI technology, the Egyptian government launched the second edition of the NAIS (2025-2030)⁹⁰. According to this Strategy, there are six strategic objectives the Egyptian State seeks to achieve by 2030: Ensure ethical and responsible AI use by establishing a comprehensive AI regulatory system, activate the ethical framework, and put a nucleus for a clear regulatory body, actively contributing to global efforts and playing an active role in AI different international fora;

1. Enhance quality of life and sectoral

88. Egypt , AI strategy, p.47. [https://ai.gov.eg/Egypt National AI Strategy \(6-4-2021\)4.pdf](https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf)

89. Egypt , AI strategy, p.47. [https://ai.gov.eg/Egypt National AI Strategy \(6-4-2021\)4.pdf](https://ai.gov.eg/Egypt National AI Strategy (6-4-2021)4.pdf)

90. National AI Strategy, 2nd edition, 2025 URL: [URL: https://ai.gov.eg/](https://ai.gov.eg/)

- efficiency through AI applications;
2. Ensure data accessibility and sharing by developing frameworks for national data governance and strengthening life cycle management of domestic data;
 3. 4. Build a robust scalable AI infrastructure and cloud services, innovate business models, and create a good digital foundation for the development of the AI industry with the support of infrastructure development;
 4. 5. Create a healthy AI ecosystem by supporting local startups, small and medium enterprises, and innovation efforts, and strengthening the investment of venture capital institutions in Egypt;
 5. 6. Strengthen the quantity and quality of local AI talents and experts.

In the reporting year, Egypt was subjected to the Readiness Assessment Methodology by UNESCO to check the readiness of Egypt to adopt AI in an ethical way.

Conclusion

While Egypt's current legal frameworks contain provisions aimed at safeguarding digital rights, their efficacy in upholding citizens' right to privacy is questionable. The absence of a precise definition outlining legitimate aims and reasonable grounds for surveillance poses a significant threat to digital rights. Moreover, the lack of clear criteria for identifying false news not

only undermines freedom of expression but also opens the door to potential abuse. Addressing these gaps is crucial to fortifying the protection of digital rights and privacy for the citizens of Egypt. Therefore, in light of the identified gaps, stakeholders must consider the recommendations proposed in this report.

Recommendations

Parliament should:



- Enact an access-to-information law and adopt human rights-based approaches to combat the publication of false information.
- Amend the Telecommunications Regulation Law and ensure the legitimacy of surveillance practices.
- Amend Article 2 of Cybercrimes Law No. 175 of 2018 requiring service providers to retain and store data for 180 days by including justifications for the six-month data retention period.
- Amend article 80 and 177 of Criminal Procedures Code no 174 of 2025 before it enters into force to ensure respect of the right to privacy, In particular, it is strongly needed to determine definite periods for surveillance practice for the purpose of investigation. Furthermore, to determine specific crimes which may be subject to surveillance practice for legitimate purposes.
- Enact laws regulating the use of AI systems and their deployment in alignment with the AI strategy.
- Introduce explicit regulations through a standalone law or as an integral component within existing legislation to strengthen the legal framework on privacy rights and their protection. A proposed adjustment involves amending the title of the personal data protection law to: “Privacy and personal data protection”. Additionally, emphasis should be placed on including a dedicated and comprehensive chapter solely focused on delineating the rights to privacy and the corresponding safeguards within the legal framework. This nuanced approach ensures a more robust and distinct coverage of privacy concerns, enhancing the overall efficacy of the regulatory measures.

The Government should:



- Incorporate digital rights explicitly into the National Human Rights Strategy.
- Refrain from infringing on digital rights like privacy and cease engaging in unauthorised surveillance.
- Enact legislation that promotes the ethical utilisation of artificial intelligence.
- Ratify the Malabo Convention.
- Facilitate access to Universal Service Fund information through official government websites.
- Enhance transparency and accountability by annually publishing comprehensive reports on the Universal Fund's activities and funded projects.
- Craft the USF reports to vividly highlight the significant progress achieved by the USF in narrowing the digital gap and addressing the digital divide. Illustrate the impactful strides made in fostering digital inclusion and reducing disparities.

The National Human Rights Council should:



- Engage in continuous monitoring of digital rights violations, document and propose policies and practices that uphold human rights.
- Aligning with their mandate, investigate all digital rights violations and, where necessary, refer violations for further investigation and judicial oversight.

Civil Society Organisations should:

- Enhance the skills of various stakeholders through comprehensive training programs.
- Strengthen the capability of legal professionals, with a particular focus on strategic litigation and the utilisation of international human rights standards in national court proceedings.
- Report any privacy breaches to the National Human Rights Council and other relevant judicial entities.
- Advocacy campaigns and activities against the new Criminal procedures law before its enter into force in October 2026.

Civil Society Organisations should:

- Enhance the skills of various stakeholders through comprehensive training programs.
- Strengthen the capability of legal professionals, with a particular focus on strategic litigation and the utilisation of international human rights standards in national court proceedings.
- Report any privacy breaches to the National Human Rights Council and other relevant judicial entities.
- Advocacy campaigns and activities against the new Criminal procedures law before its enter into force in October 2026.









Private Sector should:









- Ensure AI systems deployed for hiring or credit scoring, companies should audit these systems to ensure they don't discriminate against marginalized groups or specific geographic areas in Egypt.
- Adopt internal responsible AI guidelines.
- Ensure risk assessment took place before using AI systems.
- Raise awareness of their staff about the ethics of using AI systems and associated harm and risks and how to avoid and mitigate them..
- For companies using CCTV or employee monitoring software, provide clear "Privacy Notices" to staff.
- Ensure surveillance is used only for legitimate security purposes and is not intrusive to personal privacy.
- Adhere to data protection law and regulation and respect the privacy of employees and beneficiaries.
- Adhere to the transparency principle in using AI systems, cyber attacks which lead to breach the personal data and privacy of the staff and beneficiaries.









The Score Index

Egypt, 2025

1 = Totally non-compliant; 2 = Mildly compliant; 3 = Moderately compliant; 4 = Considerably compliant; 5 = Fully compliant

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Internet Shutdowns	P38(2)			Although Egyptian authorities resort to blocking some media websites, the Egyptian government did not disrupt access to the Internet and other digital technologies for segments of the public or an entire population.
Inexistent laws, policies and other measures to promote universal, equitable, affordable and meaningful access to the internet	P37			All laws, measures, and policies did not exclude some groups or include discriminatory provisions on gender or geographic bases. All existing policies and laws ensure the inclusion of all groups of society without any discrimination.
False News Criminalisation	P22(2)			False news is criminalised by different laws without clear criteria of what to consider as false news
Sedition Legislation	P22(2)			Sedition is criminalised by different laws, without criteria of what is considered sedition. Importantly, criminalisation of sedition is acceptable as long it is associated by specific criteria and clear definition. Neither declaration or other international instruments include clear criteria.

Indicator	ACHPR Principle	2024 Score	2024 Score	2025 Justification
Arbitrary Arrests and Harassments of the Media, HRDs and Citizens	P20 (1) & (2)			Although ,2025, witnessed a reduction in arbitrary arrest cases in comparison to 2024. 2025 witnessed a few cases of arbitrary arrest, and also witnessed the release of a number of imprisoned HRDs and citizens such as “Alaa Abdel Fatah”
Data Protection Legislation.	P42			Data protection law and its executive regulation were a adopted, the institutional framework was completed. As , in 2025 data protection authority has been established.
States interfere and require the removal of online content by internet intermediaries	P38 and P39(4)			Different legislation give rights to the government to request the regulatory authority to remove online content or entirely or block the website
Invasion of Privacy of Communications	P41			<p>Although surveillance is prohibited by the Constitution and other laws, there are laws allowing the surveillance of communication and in practice there is evidence of surveillance being used to close civic spaces as articulated in the report.</p> <p>In 2025, a new law has been passed furthering surveillance practices: Criminal procedures law no 174 of 2025</p>

Indicator	ACHPR Principle	2024 Score	2025 Score	2025 Justification
Failure by the government to proactively disclose and disseminate information digital technologies.	P29(3)	 3	 4	In 2025 Egypt adopted “Open Data Policy” to make all governmental data available for citizens, and the government considers it as a pre-step before issuing data governance law, and data classification framework. In addition, the Egyptian government established several platforms to disseminate information.
AI and Emerging Technologies national strategies	P29(3)	 5	 5	Since 2021, Egypt has had an AI national strategy and issued the Egyptian charter for responsible AI in 2023. Data Protection law, Cybercrimes law and other laws include some safeguards in case of misuse of AI
Adoption of specific child laws, policies and measures promoting children’s digital safety and privacy online	P37(5)	 3	 4	Egypt adopted different laws to protect children in general including in the digital sphere such as Children Law no 12 of 1996, penal code, cybercrimes law, data protection law, and law no 64 of 2010 to combat human trafficking
Digital Inclusion	P37(3)	 4	 5	The Universal Service Funds are addressing the digital divide and there are different government initiatives to address this gap

Total (out of 60):	2024: 32	2025 38
--------------------	----------	--------------------------



374 Borno Way, Yaba 101245, Lagos, Nigeria.
www.paradigmhq.org