

# LONDA 2023

DIGITAL RIGHTS AND INCLUSION IN AFRICA REPORT



## EGYPT

---

Published in April 2024

Report produced by Paradigm Initiative

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 © 2024 Paradigm Initiative**

374 Borno Way, Yaba, Lagos, Nigeria

Email: [media@paradigmhq.org](mailto:media@paradigmhq.org)

[www.paradigmhq.org](http://www.paradigmhq.org)

2



# CREDITS

**Country Report:**

Mohamed Sayed Mohamed Farahat

**Editorial Team:**

'Gbenga Sesan  
Hlengiwe Dube  
Nnenna Paul-Ugochukwu  
Thobekile Matimbe

**Translators:**

Paper Bag Africa

**Copy Editor:**

Sabine Matsheka

**Design & Layout:**

Kenneth Oyeniya



# Egypt

## EXECUTIVE SUMMARY

## 4

This report is an evaluation of the state of digital rights in Egypt throughout the year 2023 and serves as complementary to the Londa Egypt report published in 2021.<sup>143</sup> 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 findings of this report highlight that while the current legal framework safeguards the digital rights and rights of internet users, it paradoxically serves as a foundation for digital rights abuses and a means to restrict the digital civic space. The report employed both analytical and qualitative research methodologies. Secondary data was gathered through an extensive literature review, delving into the primary themes discussed within. The review encompassed various sources, including academic books, research

reports, and articles. The proposed recommendations advocate 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 digital rights. It is also imperative to formulate executive regulations (bylaws) 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.

# Introduction

Egypt is a North African country with an estimated population of 112,716,598 in 2023.<sup>144</sup> In 2023, 41.3% of the total population lived in urban areas and 58.5% of the total population reside in rural areas. The country is party to several international human rights binding 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 be aligned with existing international human rights laws and standards.

In relation to connectivity, Egypt ranked third in Africa after Morocco and Seychelles. A noteworthy 80.75% of the populace is actively engaged as internet users.<sup>145</sup> By January 2023 41.4% of the population were social media users.<sup>146</sup> Notably, the growth rate of ICT sectors surged to approximately 16.3% in the fiscal year 2022/2023.<sup>147</sup> 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.<sup>148</sup> Egypt also enacted national security and anti-terrorism laws. However, rather than primarily safeguarding digital rights, this legislative framework has often been utilised to restrict the civic space. Regrettably, the implementation of these measures has also had adverse consequences on media freedoms.<sup>149</sup>

Moreover, in the aftermath of the COVID-19 pandemic, Egypt continues to grapple with dissemination of false information in its various manifestations such as misinformation and disinformation.<sup>150</sup> It is, therefore, evidently imperative to adopt an access to information legislation to guarantee the proactive dissemination of credible information to the public by relevant stakeholders. Generally, there was no significant improvement in the digital rights situation in Egypt in 2023 juxtaposed with the developments observed over the preceding five years. According to Freedom House, Egypt's score for internet freedom in 2018 was 28 out of 100 in 2019, 26 out of 100 in 2020, 27 out of 100 in 2021 and in 2023, 28 out of 100.<sup>151</sup> 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 the legislation or its execution.

This report examines the state of digital rights and digital inclusion in Egypt during 2023. It covers the dynamics of internet freedom, right to privacy, surveillance, online expression, data protection, the universal service fund and AI regulation.

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

145 Statista, Share of internet users in Africa as of January 2023, <https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/#:~:text=As of January 2023%2C Morocco had an internet,percent%2C followed by Egypt with approximately 81 percent.>

146 Datareportal, Digital 2023, Egypt. <https://datareportal.com/reports/digital-2023-egypt>

147 Egypt , State information Service, <https://www.sis.gov.eg/Story/191377/ICT-Sector?lang=en-us>

148 Mohamed Farahat, (2021). Egypt Digital Rights And Inclusion, LONDA, Paradigm Initiative,. <https://paradigmhq.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.,

149 Miral Sabry AlAshry (2022) A critical assessment of the impact of Egyptian laws on information access and dissemination by journalists, Cogent Arts & Humanities. P. 1. DOI: 10.1080/23311983.2022.2115

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

151 Freedom House, "Freedom On The Net 2023, Egypt", <https://freedomhouse.org/country/egypt/freedom-net/2023> .

Accessed 1/1/2024.

# Country Analysis

## Internet Access

As reported by the International Telecommunication Union (ITU), in 2022, mobile telephone subscriptions encompassed 93% of the Egyptian population.<sup>152</sup> In November 2023, the percentage soared to 96.73%.<sup>153</sup> Subscribers numbered 102.77 million in March 2023<sup>154</sup>, and this figure increased to 103.74 million by November.<sup>155</sup> Only 10% of the population has a fixed broadband telephone subscription,<sup>156</sup> while 65% maintained active mobile broadband subscriptions in 2022.<sup>157</sup> This notably surged to 73.07% by November 2023.<sup>158</sup> As of 2022, the international bandwidth per Internet user was (71 kbit/s). According to the Speedtest Global Index, the speed of fixed broadband in Egypt by October 2023 was 61.22 Mbps, ranking 83<sup>rd</sup> globally.<sup>159</sup> Regarding internet connectivity, as of 2022<sup>160</sup>, only 72 % of the population was connected.<sup>161</sup> In terms of mobile network coverage, in 2022<sup>162</sup> 100 % of the population was covered by 3G mobile network, while 98% of the population was covered by 4G mobile network during the same period.<sup>163</sup> Egypt is one of 14 countries in Africa where 5G networks are being tested or widely deployed.<sup>164</sup> Other African countries, including North African countries, still invest in 4G networks.<sup>165</sup> Egypt has achieved remarkable strides in connectivity and is among the leading countries on the continent in this regard.

## 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 the unlawful surveillance practices. Principle 40 of the African Commission on Human and Peoples' Rights's 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa states that

152 International Telecommunication Union (ITU), (2022), The Digital Development Dashboard, Egypt. P1. [https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd\\_EGY.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_EGY.pdf)

153 Ministry of Communications and Information Technology, ICT Indicators in Brief December 2023 | Monthly Issue. P.2. [https://micit.gov.eg/Upcont/Documents/Publications\\_1512024000\\_ICT\\_Indicators\\_in\\_Brief\\_December\\_2023\\_15012024.pdf](https://micit.gov.eg/Upcont/Documents/Publications_1512024000_ICT_Indicators_in_Brief_December_2023_15012024.pdf)

154 Ministry of Communications and Information Technology. (2021-2022). Survey of ICT usage in household and individuals. Retrieved from [https://micit.gov.eg/Upcont/Documents/Publications\\_1272023000\\_ICT\\_Indicators\\_Quarterly\\_Bulletin\\_Q1\\_2023.pdf](https://micit.gov.eg/Upcont/Documents/Publications_1272023000_ICT_Indicators_Quarterly_Bulletin_Q1_2023.pdf)

155 Ministry of Communications and Information Technology, ICT Indicators in Brief December 2023 | Monthly Issue. P.2 [https://micit.gov.eg/Upcont/Documents/Publications\\_1512024000\\_ICT\\_Indicators\\_in\\_Brief\\_December\\_2023\\_15012024.pdf](https://micit.gov.eg/Upcont/Documents/Publications_1512024000_ICT_Indicators_in_Brief_December_2023_15012024.pdf)

156 International Telecommunication Union (ITU), (2022), The Digital Development Dashboard, Egypt. P1. [https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd\\_EGY.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_EGY.pdf).

157 International Telecommunication Union (ITU), (2022), The Digital Development Dashboard, Egypt. P1. [https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd\\_EGY.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_EGY.pdf)

158 Ministry of Communications and Information Technology, ICT Indicators in Brief December 2023 | Monthly Issue. P.3 [https://micit.gov.eg/Upcont/Documents/Publications\\_1512024000\\_ICT\\_Indicators\\_in\\_Brief\\_December\\_2023\\_15012024.pdf](https://micit.gov.eg/Upcont/Documents/Publications_1512024000_ICT_Indicators_in_Brief_December_2023_15012024.pdf)

159 Speedtest Global Index. <https://www.speedtest.net/global-index/egypt#mobile>

160 Figures of 2023 were not available during the time of writing this report.

161 International Telecommunication Union (ITU), (2022), The Digital Development Dashboard, Egypt. P2. [https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd\\_EGY.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_EGY.pdf)

162 Figures of 2023 were not available during the time of writing this report.

163 International Telecommunication Union (ITU), (2022), The Digital Development Dashboard, Egypt. P1. [https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd\\_EGY.pdf](https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_EGY.pdf)

164 Diplo Foundation , Status of internet access and connectivity in Africa, <https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/internet-access-connectivity-africa/>

165 Diplo Foundation , Status of internet access and connectivity in Africa, <https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/internet-access-connectivity-africa/>

“[e]veryone 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”.<sup>166</sup>

Article 57 of the Constitution provides the protection to the right to privacy and this provision aligns with the 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.”<sup>167</sup> The State is also committed to protecting the right of citizens to use public means of communication in all its forms. It is not permissible to disrupt, stop, or deprive citizens of them arbitrarily. While this is regulated by law, other laws have provisions that undermine the right to privacy, as expounded later in this report.

In addition to the aforementioned article 57, article 99 of the Constitution establishes the right to remedies and compensation for damage resulting from abuse of privacy. The article 99 stipulates that “[a]ny 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 of such crime shall not abate by prescription. The affected party shall have the right to bring a direct criminal action.”<sup>168</sup> 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 50,000 Egyptian pounds (1600 US Dollars) and not exceeding 100,000 pounds(3200 US Dollars). 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 his 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 “[a]nyone who intentionally uses an information 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 the 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<sup>169</sup> according to principle 41 of the ACHPR 2019 Declaration, states shall use surveillance when 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”.<sup>170</sup> In the Egyptian context, community standards

## 7

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

167 Egypt , Constitution 2014 article 57.

168 Constitution article 99.

169 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

170 African Commission on Human and Peoples’ Rights, The Declaration of Principles of Freedom of Expression and Access to

and ensuring national security is always used as justification for undertaking surveillance.<sup>171</sup> 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.<sup>172</sup>

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 and media in any way. In exceptional circumstances, they may be subject to limited censorship in times of war or general mobilisation".<sup>173</sup> However, the same laws contain specific provisions that grant powers to the authorities to block websites that are deemed a threat to national security. 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.<sup>174</sup> 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.

## Online Freedom of Expression

The ACHPR 2019 Declaration stresses the importance of both rights and states that "[t]he respect, protection and 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".<sup>175</sup> This segment of the report underscores the correlation between freedom of expression and the right to access to 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

8

---

Information in Africa 2019.

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

172 Mohamed Farahat (2021), Egypt country report, in Surveillance Law in Africa: a Review of Six Countries, Brighton: Institute of Development Studies, p.48. DOI: 10.19088/IDS.2021.059 p.48.

173 Constitution article 71

174 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 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>

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



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 the Law No. 180 of 2018 Regulating the Press, Media, and the Supreme Council for Media Regulation prohibits 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, or cursing or slandering them, or insulting religions. Article 4 of this law also restricts 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 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”.<sup>176</sup>

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 which stipulates that the law shall guarantee the right of access to information. Therefore, dissemination of information that deviates from official government publications is consistently deemed a violation, constituting the offence of disseminating false information.

The laws above serve as mechanisms to restrict freedom of expression. In August 2023, Hisham Kassem, a prominent politician and news publisher, was arrested and detained on charges of libel and slander.<sup>177</sup> The allegations stemmed from Kassem’s critical Facebook posts directed towards a former Minister. Prosecutors referenced vague and broad terminology, like intentionally “disturbing the authorities.”<sup>178</sup>

## Data Protection

9 The Data Protection Law (DPL) No 151 of 2020 was enacted in 2020. Despite its enactment, the executive regulation of the data protection law is yet to be adopted. The undue delay in promulgating the regulation poses a significant obstacle to law enforcement, notably impeding the establishment of essential guidelines necessary for the proper execution and compliance with the provisions outlined in the legislation. According to articles 2 and 6(1) of the DPL, the consent of the data

176 Egypt, SupremeStanding Committee for Human Rights, National Human Rights Strategy (2021) p31 <https://sschr.gov.eg/media/gapb5bq4/national-human-rights-strategy.pdf>

177 Human Rights Watch , World Report 2024, events of 2023, P. 191. [https://www.hrw.org/sites/default/files/media\\_2024/01/World\\_Report\\_2024\\_LOWRES\\_WEBSPREADS\\_0.pdf](https://www.hrw.org/sites/default/files/media_2024/01/World_Report_2024_LOWRES_WEBSPREADS_0.pdf)

178 Human Rights Watch , World Report 2024, events of 2023, P. 191. [https://www.hrw.org/sites/default/files/media\\_2024/01/World\\_Report\\_2024\\_LOWRES\\_WEBSPREADS\\_0.pdf](https://www.hrw.org/sites/default/files/media_2024/01/World_Report_2024_LOWRES_WEBSPREADS_0.pdf)

subject for processing and gathering the personal data is required in processing data. In addition, article 2 gives the data subject control over their data and allows them to delete it. The data subject has the following rights:

1. Knowing, accessing, or obtaining personal data held by any holder, controller, or processor.
2. Changing the prior consent to retain or process his personal data.
3. Correction, modification, erasure, addition or updating of personal data.
4. Allocate treatment within a specific scope.
5. Knowing of any breach or violation of his personal data.
6. Objecting to the processing of personal data or its results if they conflict with the basic rights and freedoms of the person concerned with the data.

In terms of transparency, the DPL is aligned with international standards in this regard, particularly article 13 of the Malabo Convention includes provisions regarding transparency requirements on data usage.<sup>179</sup> According to article 2 of the law a person has a right to know, access, or obtain their personal data. In addition, the data subject has a right to be informed of any breach or violation of their personal data. According to article 7 of personal data protection law, the data breach incident shall be reported to the data protection centre within 72 hours and in case that data is related to national security should be reported immediately. The data subject should be notified of data breach within the next three days after reporting the breach to the centre. Furthermore, article 3 emphasises the principle of legitimacy in collecting and processing the personal data. Article 3 stipulates conditions that should be met in the collection, processing and retention of personal data. These are:

1. Personal data is collected for legitimate, specific and declared purposes for the person concerned.
2. It must be correct, sound and secure.
3. To be processed in a lawful and appropriate manner for the purposes for which it was collected.

Data minimisation is one of the data protection principles guaranteed by article 3 of the data protection law. Article 3 emphasises that the collected data should not be kept longer than necessary to fulfil its specified purpose. The executive regulations of this law specify the policies, procedures, controls and standard 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 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.<sup>180</sup> 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 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

179 African Union, African convention on Cybersecurity and personal data protection 2104.

180 African Union, African convention on Cybersecurity and personal data protection 2104.

personal data except with authorisation from the “personal data protection centre”.<sup>181</sup> 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 for the aforementioned operations. 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 in the said activity. 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 500,000 pounds and not exceeding five million pounds, or by one of these two penalties, Without the consent of the data subject or in cases other than those legally authorised”.

### Universal Service Fund (USF)

According to GSMA Intelligence,<sup>182</sup> Universal Service Fund (USF) is based on three principles: availability, affordability, and accessibility.<sup>183</sup> 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.<sup>184</sup> The USF strives for the provision of essential telecommunication services to every citizen at reasonable rates.<sup>185</sup> There is no publicly available official record about the value of the USF, according to some media reports, the USF started with an initial budget of 50 million Egyptian Pounds.<sup>186</sup> 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 one billion and 668 million Egyptian pounds (54 Million US Dollars).<sup>187</sup> Furthermore, the National Telecommunications Regulatory Authority (NTRA) has initiated measures

181 According to article 1 of personal data protection law No 151 of 2020, centre refers to the personal data protection centre.  
 182 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>.  
 183 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>.  
 184 National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.3. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>  
 185 National Telecom Regulatory Authority (NTRA), Universal Service Policy, P.8. <https://www.tra.gov.eg/wp-content/uploads/2020/11/Universal-Service-Policy.pdf>  
 186 <https://muhtwaplus.com/49705/2020/07/25/الخدمات-الاسي-مؤهل-ازاجل/>  
 187 El Youm El Sabaa, accessed 13 /2/2024. <https://www.youm7.com/story/2021/12/8/عوفرل-ري-وطتل-علم-اشل-ال-ق-مدخل-ال-ق-ودن-ص-ن-ع-هتفر-عم-دي-رت-ام-لك/5571579>

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 of a total distance of 112 kilometres. The investment in this initiative amounts to 513 million Egyptian Pounds (16,000,000 US Dollars), reflecting NTRA's commitment to advancing connectivity and infrastructure.<sup>188</sup>

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 pounds to provide telecommunications services in deprived areas and new roads at a cost of 1.8 billion pounds, in addition to 1.2 billion to establish 592 stations in the first phase for a decent life Project (قايح عورشم/ Decent life ).<sup>189</sup> 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.<sup>190</sup>

## USF Initiatives

**Roads Infrastructure National Project:** It is linked to providing telecommunication services. This project aims to enhance the existing road networks. Additionally, under this project, the basic telecommunications services must be available in these roads, and the universal service fund shall be responsible for the financing of this project for the benefit of the national economy and the Egyptian citizen.<sup>191</sup>

**El Million Fadan Project:** This project aims to expand the agricultural sector. According to the Egyptian universal service policy, “the availability of telecommunication services in these areas is one of the attractive factors for the success of this project and the universal service is responsible for funding the mobile coverage for these areas”.<sup>192</sup>

**National Telecom and Information Plan Projects:** These projects include:

- 1) Public educational institutions and libraries with an annual budget of 50 million Egyptian pounds to fund universal service for the eligible educational institutions and libraries;
- 2) Funding Health Care Centers accredited by ministry of health and located in rural areas;
- 3) Services Provided to the Disabled, according to USF's policy Universal service department targets the persons with disabilities (in Egypt and all citizens are entitled to access basic telecommunications services regardless of any type of disability);
- 4) Infrastructure of Digital Society and Digital Architecture, to construct a robust telecom

188 El Youm El Sabaa, accessed 13 /2/2024. <https://www.youm7.com/story/2021/12/8/>

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

190 ACHPR 2019 Declaration principle 41

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

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

infrastructure of Digital Society and Digital Architecture with high speeds and capabilities similar to those of the developed countries;

- 5) Broadband Project, this project aims to increase the deployment of high-speed internet in Egypt and support the development of the digital community for the purpose of creating jobs, encouraging the utilisation of information and communication technologies in various governmental sectors, thus improving the quality of life for citizens and reducing the digital divide between urban and rural communities”.<sup>193</sup>

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 November 2019, the Egyptian Cabinet approved the establishment of the National Council for Artificial Intelligence (NCAI).<sup>194</sup> At its inception, the primary task of the NCAI was the adoption of a national AI strategy. Subsequently, in July 2021, the NCAI adopted the Egypt AI strategy.<sup>195</sup> At the point of adoption, it was envisaged that the strategy would be implemented in a phased approach until the end of 2022. In 2023, 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”.<sup>196</sup> Although the Egyptian government adopted the national AI strategy<sup>197</sup> 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 and combat arbitrary and 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 expose actions committed by AI systems.

In 2023, the NCAI adopted the Egyptian Charter for responsible AI (the Charter).<sup>198</sup> The main aim of the Charter is to ensure the ethical use, deployment and management of AI systems in Egypt.<sup>199</sup> The Charter also incorporates overarching principles such as fairness, transparency, a focus on human-centeredness, accountability, and the assurance of security and safety.<sup>200</sup> In addition, the strategy acknowledges that “the existence of policies, regulations, and legislation to mitigate potential misuse, whether ethical, legal, or socio-economic, can promote and enable the widespread

193 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.

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

195 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)

196 Egypt AI strategy , p. 60.

197 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)

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

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

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

adoption of AI solutions”.<sup>201</sup> This is not the case yet. 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.”<sup>202</sup> 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 through adopting a national strategy and Charter for responsible AI. In this stage, AI may regulate through 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 provision 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.

---

201 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)  
202 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)

# ▶ Conclusion & Recommendations

## 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:

- » Enact an access to information law and adopt human rights-based approaches to combating 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.
- » Enact law regulating the use of AI systems and deployment, in alignment with the AI strategy.
- » Introduce explicit regulations either 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.

---

### National Human Rights Council:

- » 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.
-

---

**Government:**

- » Incorporate digital rights explicitly into the national human rights strategy.
- » Refrain from infringing on digital rights, such as privacy rights, and cease engaging in unauthorised surveillance.
- » Enact legislation that promotes 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.

---

**Civil Society:**

- » 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.
-





[www.paradigmhq.org](http://www.paradigmhq.org)

Copyright © 2024