Legal 500
Country Comparative Guides 2025

Egypt
TMT

Contributor

ADSERO-Ragy
Soliman & Partners

Ragy Soliman

Managing Partner, Co-Head of M&A and Capital Markets | ragy.soliman@adsero.me

Dr Ahmed Abdelgawad

Partner, Co-Head of M&A and Capital Markets | ahmed.abdelgawad@adsero.me

Darah Zakaria

Counsel, Head of TMT | darah.zakaria@adsero.me

Nourhan Hatem

Managing Associate | nourhan.hatem@adsero.me

Habiba Haitham

Junior Associate | habiba.haitham@adsero.me

Hana Koptan

Junior Associate | hana.koptan@adsero.me

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Egypt.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Egypt: TMT

1. Software – How are proprietary rights in software and associated materials protected?

In Egypt, proprietary rights in software and related materials are protected under Law no. 82/2002 on the protection of Intellectual Property Rights (the "**IP Law**"). Said law protects computer programs and databases (computer programs, data bases, software development), categorizing them under literary and artistic works.

The IP Law classifies software as a copyright. Copyright grants the author or rightsholder exclusive rights to use, reproduce, distribute, adapt, and publicly communicate the software. Protection is automatic upon creation, and registration of the right is optional but may aid in enforcement.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Generally, Article 138 of the IP Law stipulates that the author of a piece of work is the person who created the work and thus is considered the owner by virtue of the law. Therefore, if a software developer or consultant creates software for a client without a written agreement assigning rights, the developer retains ownership of the software.

Proprietary rights may be granted by way of registration of the software in the Information Technology Industrial Development Agency ("**ITIDA**"). Anyone may register a software in ITIDA, however, with reference to enforcement, the ultimate ownership belongs to the author of the software. Registration aids in strengthening claims of authorship, but does not transfer or create ownership.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Whilst there are no specific laws that govern harm or liability caused by software or computer systems, such issues are governed through a combination of legal frameworks. The **Civil Code No. 131 of 1948** provides the basis for contractual and tort liability, allowing affected parties to claim compensation in cases of negligence or breach of contract.

In B2C context, the **Consumer Protection Law No. 181 of 2018** (the "**Consumer Protection Law**") may apply, holding suppliers accountable for damage caused by defective software or digital products. Additionally, if harm arises from cyber incidents such as data breaches or unauthorized access, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 (the "**Anti-Cybercrime Law**") is applicable, particularly where personal data or IT systems are compromised.

4. Software – To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

While there are no specific laws dedicated solely to governing the use or misuse of software, The Anti-Cybercrime Law serves as the primary legislation regulating such activities. The law criminalizes a wide range of offenses involving software and digital systems, including unauthorized access to networks or devices, illegal copying, modification, or deletion of data, the distribution of harmful software (such as viruses and malware), digital piracy, and the use of software for fraud, or other unlawful purposes. Violators may face substantial penalties, including fines and imprisonment.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

There is no standalone legislation that comprehensively governs software transactions or cloud services.

For cloud services and data-related aspects, the Anti-Cybercrime Law and the Personal Data Protection Law No.151/2020 (the "**PDPL**") may apply, particularly when cloud services involve the storage, processing, or transfer of personal data. Further, the National Telecom

Regulatory Authority (**NTRA**) has issued a regulatory framework for Establishing & Operating Data Centers and Providing Hosting & Cloud Computing Services. his regulation sets out licensing requirements, data hosting obligations, and security standards for providers operating cloud and hosting infrastructure in Egypt. It applies to entities offering cloud services from within Egypt and seeks to ensure compliance with national security and data protection standards. Registered entities can provide cloud computing services either through fully owned data centers, or through data centers rented from a licensed Public Data Center Provider (**PDCP**).

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, it is common practice in Egypt for software vendors to limit their financial liability in software transactions, including both licensing and SaaS agreements. Such caps are typically subject to negotiation between the parties. Under the Egyptian Civil Code, such limitations or liquidated damages clauses are generally enforceable, provided they do not involve gross negligence or fraud.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

There are no specific regulations or legislation that mandate what may be excluded from a contractual liability cap in software related transactions. In line with the Civil Code, contractual limitations of liability are enforceable unless they relate to gross negligence or fraud, which cannot be waived or limited.

In practice, the mentioned areas are often excluded from the general liability cap or treated with heightened liability. These exclusions reflect risk allocation norms in negotiated agreements and are generally upheld under Egyptian law, provided they do not conflict with public policy or mandatory legal provisions.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Source code escrow is not yet common in Egypt and is typically arranged on a contractual basis where needed.

For cloud-based software (SaaS), similar protections are often addressed through service level agreements (SLAs) and other contractual commitments.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

Egypt does not have a dedicated export controls that apply to software transactions. However, general export rules overseen by the Ministry of Trade and Industry may apply when dealing with strategic or sensitive technologies. That said, the import and use of encryption tools or cybersecurity-related software may require prior coordination with the NTRA or other national security authorities.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

IT outsourcing is not regulated by a singular, dedicated law; rather, it falls within the scope of multiple existing legal frameworks. Key among these is the PDPL, which imposes requirements on the processing and cross-border transfer of personal data, as outlined under Q.17

In addition, Anti-Cybercrime Law places specific obligations on service providers, requiring the implementation of robust security measures to safeguard systems and networks against breaches. Service providers may be held liable for unauthorized access, data breaches, or failure to report cyber incidents in accordance with the law. They are also required to retain user data and activity logs for a legally prescribed period (180 days).

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

In case the services transferred include personal data, then the PDPL will apply in this regard. Under said law, the employer (as the data controller) remains primarily responsible for ensuring that any processing of employee personal data is carried out lawfully, and for specific, legitimate purposes; and in a manner that guarantees the privacy, confidentiality, and security of the data.

Further, personal data must not be retained for longer than necessary to fulfill the intended purpose of processing. Both data controllers (employers) and processors (third-party IT providers) are required to implement all necessary measures to prevent unauthorized access, misuse, or harm to the data subject; in this case, the employee.

Additionally, the PDPL requires that explicit consent must be obtained from employees prior to the processing or disclosure of their personal data. If such data is to be transferred outside Egypt, the law imposes additional conditions, including that the recipient jurisdiction offers an adequate level of data protection.

In reference to transfers to third parties, the PDPL allows for the transfer of personal data outside of Egypt to jurisdictions, subject to certain conditions, as outlined under Q.17.

Nonetheless, key aspects of the PDPL remain unclear or unenforceable at this stage, as set out below in the 'Data Protection' section.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

Telecommunications is governed mainly in Egypt by Telecommunications Law No. 10 of 2003 (the "**Telecommunications Law**"). The Telecommunications Law regulates the entire telecommunications sector; including:

- The establishment of the National Telecommunications Regulatory Authority "NTRA" as the regulator of the telecommunications sector in Egypt;
- Laying down the licensing regime for establishment of telecommunications networks and provision of telecommunications services; and
- Regulating the relationship between the operators of telecommunications service providers.

In addition to the Telecommunications Law, the telecommunications sector is further regulated through two other types of decrees:

a. Decrees issued by the NTRA. Those are mainly technical and regulatory in nature; and
b. Decrees issued by the Minister of Telecommunications.

The most important decrees issued by the Minister of Telecommunications are Decree No. 128 of 2006 regulating the dispute resolution mechanism between operators and Decree No. 667 of 2017 regulating the penalties to be imposed by the NTRA for breach of telecommunications licenses.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

Telecommunications is a highly regulated sector in Egypt. The NTRA enjoys broad authorities to regulate the sector. The Telecommunications Law has provided for licensing requirement for the provision of all telecommunications services to be issued from the NTRA. The Board of the NTRA is entrusted with determining the licenses to be issued and the framework and the terms for issuing said licenses.

The main telecommunications licenses issued by the NTRA; include:

a. License for the provision of telecommunications infrastructure services. There is only one licenses currently issued to Telecom Egypt;
b. License for the establishing and operating international telecommunications gateway. There are currently two licenses issued, one for Telecom Egypt with full fledge scope to cover all customers in Egypt whether Telecom Egypt's customers or customers for other operators and the other for E& with limited

scope to cover the later's customers only;
c. Licenses for the provision of mobile telecommunications services. there are currently four mobile operators in Egypt. The NTRA requires obtaining a new license for each generation of technology. The NTRA has recently issued 5G licenses for the four operators;
d. Licenses for the provision of internet services;
e. License for the establishment, operation and lease of international cables;
f. License for satellite telecommunications services;
g. License for the establishment and operation of telecommunications towers;
h. License for the establishment and operation of data centres and provision of cloud services; and
i. A recently introduced license for the provision of Internet of Things services.

With the exception of certain licenses e.g. mobile services, ISP, international gateways, the NTRA announces the regulatory framework for issuing the relevant license and its terms and qualified operators, with sufficient expertise, can apply for obtaining the relevant license.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Confidentiality of private communications is explicitly safeguarded under Egypt's **2014 Constitution**. Article 57 states clearly that private communications are inviolable and may not be intercepted or monitored except by a justified judicial warrant for a specified period and purpose, and only in circumstances stipulated by law. This constitutional protection establishes a robust principle that interception or monitoring must be judicially sanctioned, narrowly defined, and strictly necessary.

However, specific laws, notably the **Telecommunications Regulation Law No. 10 of 2003**, provide expansive exceptions for national security purposes. Article 64 of this law explicitly requires telecommunications service providers and operators to equip national security entities, at their own cost, with technical means to access communications and subscriber data necessary for these entities to perform their legally defined roles. The law does not explicitly mandate prior judicial authorization for national security-related requests, potentially creating tension with constitutional protections.

The **Personal Data Protection Law No. 151 of 2020 (PDPL)** further complicates this framework. While generally providing comprehensive safeguards for personal data, the PDPL explicitly exempts personal data processed by national security entities from its provisions under Article 3. This means that data access by national security agencies is subject to fewer transparency obligations and judicial safeguards, placing significant discretion in the hands of national security authorities, albeit still bound by the overarching constitutional requirements.

In practice, Egyptian law strikes a delicate balance between privacy protections outlined constitutionally and expansive statutory authorities granted to security and law enforcement bodies. Telecommunications operators must comply confidentially with national security demands, and individuals have limited practical avenues for challenging government data requests. The constitutional standard requiring judicial oversight remains critical as a potential legal safeguard, yet national security exceptions often operate with broader scope and less transparency.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

There are three main organisations that set principle standards, as follows:

1. The Egyptian Organizations for Standards and Quality: The organization enjoys broad authorities in connection with setting the Egyptian standards for different fields;
2. The International Telecommunications Union: Egypt is a member to the International Telecommunications Union and accordingly adopts the standards issued by the union. Further, it is standard in agreements between telecommunications operators to adopt such standards; and

3. The NTRA: As the regulator of the telecommunications sector in Egypt, the NTRA enjoys broad authorities in regulating the market; including, issuing general standards to be adopted by the different players in the sector.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Interoperability standards are crucial to Egypt's telecommunications and connected technologies sectors, underpinned by the Telecommunications Regulation and overseen by the NTRA. Egyptian law mandates non-discriminatory interconnection among providers through binding Reference Interconnection Offers (RIOs) and Service Level Agreements (SLAs), promoting fair competition and consumer choice. Mobile operators must adhere to internationally standardized GSM frequency bands, ensuring seamless device operation.

In specialized sectors like digital health, the Egyptian Health Information Exchange (EHIE) demonstrates the practical impact of interoperability standards, relying heavily on international protocols such as HL7 and FHIR. Compliance with Egypt's Data Protection Law No. 151/2020 further strengthens standards by imposing rigorous data protection obligations.

The NTRA's regulatory framework for IoT/M2M communications also emphasizes compliance with international technical standards, ensuring devices' compatibility and safety. However, regulatory frameworks for emerging fields such as connected and autonomous vehicles (CAVs) remain limited, leaving legal ambiguity around liability and driverless technologies. Nonetheless, smart city initiatives indicate growing regulatory interest and potential future legislation.

Finally, Egypt's cybersecurity strategy and Data Protection Law impose stringent security requirements, influencing interoperability standards and their implementation. Overall, Egypt's legal framework emphasizes compliance with international standards, non-discriminatory access, and robust cybersecurity, shaping technological innovation, fair competition, and consumer protection.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that govern data protection, including a brief explanation of the general purpose of those laws.

Data protection is mainly governed by the PDPL. The PDPL sets out general provisions for the protection of personal data, including provisions for data collection, sharing, storing and disposal of such data, providing that the same is processed in a legitimate manner and in compliance with the purposes for which it is collected. adopts very similar concepts to the European General Data Protection Regulation ("**GDPR**"). As is the case in the GDPR, "Personal Data" defined under the PDPL is given a broad meaning which effectively captures any information that can be used to identify a natural person either directly or indirectly. In addition, the PDPL outlines rules for transferring personal data to jurisdictions outside Egypt:

The PDPL allows for the transfer of personal data outside of Egypt to jurisdictions that do not have an equivalent level of protection, upon obtaining a license from the PDPC, subject to satisfying certain conditions including:

- If there is conformity between the nature of work of either of the Controllers or Processors, or unity between the purpose for which they obtain the personal data.
- If either of the Controllers or Processors, or the Data Subject, have a legitimate interest in the personal data.
- The level of legal and technical protection of personal data offered by the Controller or Processor abroad does not fall below the level of protection provided in the Arab Republic of Egypt.

The Executive Regulations of the law, which have not been issued as of yet, are set to further specify the policies, procedures, regulations and standard criteria for collection, processing, retention and security of personal data, in addition to the establishment of the PDPC which is not yet operative. As such, currently, there is stark gap in enforcement with respect to the PDPL.

Further to the PDPL, Anti-Cybercrime Law outlines that service providers are under a duty to maintain the privacy of the data stored and not disclose it without a reasoned order from a relevant judicial authority.

Lastly, Telecommunications Law sets out an obligation to maintain privacy with respect to telecommunications related activities, and imposes penalties for infringement of its regulations.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Fine ranges for breach of the PDPL from EGP 50,000 – 5,000,000 depending on the nature of the breach, and/or potential imprisonment.

For example, the PDPL penalizes individuals who collect, process, disclose, grant access, or circulate personal data without the consent of the data subject, except in cases authorized by law. The relevant fine in this respect ranges between EGP 100,000 to 1,000,000.

The Penalty shall be imprisonment for a minimum of 6 months, and a fine ranging between EGP 200,000 and 2,000,000 in the event that the above is committed in exchange for obtaining a material or moral benefit or with the intention of exposing the data subject to danger or harm.

As another example, violating the provisions pertaining to cross-border transfers entails a penalty of a fine ranging between EGP 500,000 and 5,000,000 and imprisonment for a minimum period of three months, or by either of these penalties.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Whilst there is no set standard for inclusion of external data protection regimes in technology contracts, in practice, some technology contracts in Egypt, such as data processing / data sharing agreements frequently include reference to the GDPR as the governing piece of data privacy legislation. This often occurs specifically considering the current lack of enforceability with respect to the PDPL, as mentioned above in Q.(17), though, this does not negate that such agreements still refer to the PDPL, as they directly involve data subjects in Egypt. Aside from the GDPR, technology contracts typically refer to the relevant data protection regime that the data subjects are subject to (e.g. A data processing agreement that handles personal data of data subjects in the US shall include reference to US privacy laws).

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

Anti-Cybercrime Law sets out various provisions mainly pertaining to cyber-related offenses, such as unauthorized access, hacking, creation of fake accounts or websites, online fraud, prescribing criminal penalties such as fines and imprisonment. Anti-Cybercrime law further sets out obligations and duties for service providers, ranging from maintaining confidentiality and privacy of data. The executive regulations of Anti-Cybercrime Law further mandate technical standards for the security and functionality of systems, by way of example, through implementing secure protocols (HTTPS), encryption standards, and antivirus processes.

Further, the NTRA has issued a regulatory framework to govern the work of cybersecurity service providers by setting necessary technical and regulatory requirements for delivering these services in Egypt. Essentially, companies willing to provide cybersecurity services in Egypt must obtain a registration certificate from the NTRA, ensuring compliance with its rules and conditions. Moreover, the regulatory framework imposes obligations on service providers, such as maintaining confidentiality agreements with clients, data retention policies, and ensuring staff meet the NTRA accreditation requirements.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

Anti-Cybercrime Law imposes various sanctions for violations of its provisions, namely, fines ranging between a minimum of EGP 10,000 and up to potentially EGP 20,000,000, as well as imprisonment which may range from a minimum of three (3) months, and aggravated imprisonment, if it is proven that any violations were committed to disrupt public order, threaten order and safety, harm national security or the economy, obstruct public authorities, undermine the constitution or laws, or damage national unity or social harmony.

By way of example, anyone who unlawfully accesses or hacks a state or public system, account, website, or email, whether intentionally or by mistake, faces imprisonment for a minimum of two (2) years and a fine ranging between EGP 50,000 and EGP 200,000. If such crime has been committed with the intention to

unlawfully obtain government data, the fine increases to EGP 100,000 – 500,000. If the act causes damage, destruction, or alteration of data or systems, the penalty rises to imprisonment plus a fine ranging between EGP 1,000,000 and 5,000,000.

Also, dealing (including but not limited to possession, sale, production, import, export) in any devices, programs, access codes, passwords, encryption keys, or similar data, without proper authorization, and with an intention to use the same to commit, facilitate, or conceal a crime under Anti-Cybercrime Law entails imprisonment for a minimum term of at least two years and a fine ranging between between EGP 300,000 and EGP 500,000.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

There are currently no dedicated regulatory bodies or authorities specifically established for the regulation of artificial intelligence in Egypt. The National Council for Artificial Intelligence (NCAI) is an advisory body responsible to prepare, formalize, approve and govern the implementation of the National Strategy for AI. The National Council is tasked with reviewing and potentially implementing policies, rules and frameworks that outline standards for responsible use of AI, through involvement of various stakeholders.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

There is no specific legislation regulating AI systems in Egypt, but existing laws such as the Consumer Protection Law, Anti-Cybercrime Law, PDPL, IP Law and Telecommunications Law will be relevant. Although Egypt does not yet have a standalone AI law, the National AI Strategy for 2025–2030 establishes a comprehensive roadmap for integrating AI across government and industry. The strategy emphasizes integrating AI into government operations, driving sector-specific advancements, and investing in skills, infrastructure, and ethical frameworks to ensure responsible and inclusive AI adoption.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

There are no specific binding laws or regulations specifically govern the deployment or use of Large Language Models and/or generative AI in Egypt. Though, this may be addressed following implementation of AI legislation in Egypt. At the current stage, many political parties in Egypt have taken the initiative of drafting potential legislations regulating AI. However, based on current parliamentary timelines and the government's drafting progress, we anticipate these bills will not be enacted in the near future.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

Currently, there is no specific legislation in Egypt requiring the inclusion of AI-related risk provisions in technology contracts, and their inclusion is not yet considered standard practice. Please see our response in Q.22 and Q.23 above.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Similar to AI-related risk provisions (as discussed under Q.25), technology contracts in Egypt do not yet typically include specific clauses dealing with intellectual property (IP) rights or the ownership of AI-generated outputs. This is largely due to the absence of any clear legal framework or judicial precedent in Egypt addressing how copyright or other IP laws apply to works created by or with the assistance of AI.

Applying the general provisions under IP Law, in addition to the IP registration provided under ITIDA, would be relevant for all kinds of software, and as such, extend to the protection of AI softwares and systems.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

Blockchain technology itself is not regulated under the current laws. There is no legislation that governs the use, development of blockchain infrastructure. However, blockchain applications – particularly those used in the financial sector – fall within the scope of the Central Bank of Egypt ("**CBE**") if they are used to deliver financial services, process payments, or manage electronic money. The non-financial uses of blockchain remain unregulated under Egyptian law.

ii) **Central Bank of Egypt Law No.194 of 2020** is a comprehensive legislative framework that modernizes Egypt's banking and financial sector, granting the CBE broad authority to regulate, supervise, and ensure the stability of financial institutions. It mandates licensing for all banks, payment service providers, and electronic money, While the Digital Assets are not fully regulated under the Banking law, Article 206 prohibits the issuance, trading, promotions, or operations of cryptocurrencies or electronic money without prior CBE authorization, with violations subject to imprisonment and fines ranging from EGP 1,000,000 to EGP 10,000,000.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

Currently, there is no standalone legislation in Egypt specifically dedicated to governing search engines or online marketplaces. However, the general rules, in addition to other regulations shall apply depending on the nature of the services provided, particularly in relation to consumer protection, advertising, and content regulation.

Key regulations include: i) Consumer Protection Law: Its general purpose is to establish rights for consumers and obligations for suppliers, including requirements related to transparency, fair advertising, return policies, pricing, and after-sales support.

ii) Media Law No. 180 of 2018 and its Executive Regulations (the "**Media Law**"): Said law primarily aims at regulating traditional and digital media platforms, and imposing content restrictions and licensing requirements for websites.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Social Media and online platforms in Egypt are primarily governed by several laws including: the Anti-Cybercrime Law, the Media Law, and the PDPL. These laws aim to regulate online content, combat cybercrimes, safeguard personal data.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Under Egyptian law, the maximum sanctions that may be imposed by regulators for breaches of online safety laws vary depending on the nature and severity of the violation. Under Anti-Cybercrime Law, the most severe penalties include fines of up to EGP 20 million and imprisonment of up to 15 years for grave offenses such as incitement to terrorism or threats to national security. Additional administrative sanctions may include website blocking and revocation of licenses. Under Media Law, violators may face fines of up to EGP 5,000,000 and imprisonment of up to 5 years. Meanwhile, the PDPL sets fines up to EGP 5,000,000 and imprisonment of up to 6 months for breaches involving misuse or mishandling of personal data. These sanctions are intended to uphold online safety, ensure legal compliance, and protect both public and individual interests in the digital space.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

We note that there is no specific law that directly governs spatial computing technologies (such as augmented reality (AR), virtual reality (VR), extended reality (XR), or the metaverse). This will be subject to the general principles of law, in addition to the Telecommunications Law and the PDPL, based on the function or effect of the technology.

32. Quantum Computing – Please summarise the

principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

We note that there are no specific laws or regulations dedicated to quantum computing or quantum cryptography. This will be subject to the general principles under Egyptian law.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

The NTRA has recently required that all data centres operators in Egypt obtain a license from the NTRA for the establishment and operations of data centres. Each operator must, in addition to obtaining such license, register each data centre with the NTRA. The license regulates in general the services to be provided by the operator, the relationship between the licensee and its customers, restrictions on disposal of the data centres without prior approval from the NTRA. Further, the NTRA requires the registration of any entity that provides cloud services.

Given that the issuance of such license is relatively recent, the level of intervention by the NTRA in the operations of the data centres operators is yet to be tested in practice. However, it seems that the NTRA is adopting a lite approach to such intervention.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

The next three years are likely to see transformative changes in Egypt's technology law, driven by national strategic priorities, rapid digitalization, and alignment with global standards. The following are the top three predicted legal and regulatory developments:

1. Comprehensive AI Regulation and Governance

- Egypt is expected to enact a dedicated legal framework for artificial intelligence, currently under preparation as part of the National Artificial Intelligence Strategy (2025–2030). The expected legislation will address ethical, safety, accountability, and data governance issues, and create a regulatory body or authority tasked with overseeing AI deployment, standardization, and sector-specific applications.
- Emphasis will be put on responsible and secure AI, ensuring compliance with international best practices and fostering Egypt's ambition to become a regional AI hub. The framework will likely complement existing laws such as the Personal Data Protection Law No. 151/2020, Anti-Cyber and Information Technology Crimes Law, and sector-specific guidance (e.g., for fintech, digital health, and transport).

2. Expansion of Data Protection and Cross-Border Data Regulations

- Enforcement of the Personal Data Protection Law is expected to intensify, with possible updates to address cross-border data flows and cloud computing in response to Egypt's goal of attracting large-scale data centers and digital outsourcing.
- The regulatory framework will likely clarify the procedures for data transfers to and from Egypt, establish sector-specific compliance mechanisms (especially for digital health, financial services, and e-government), and expand on consent, security, and accountability requirements for both private and public sector entities.
- The Data Protection Center will play a more active role in oversight, licensing, and coordination with international regulatory bodies, positioning Egypt in line with global adequacy standards for data privacy.

3. Continued Modernization of Telecom and Digital Infrastructure Laws

- Legal reforms will continue to facilitate national digital transformation, building upon the Telecommunications Regulation Law No. 10/2003 and the latest NTRA regulatory frameworks. This will include updates to accommodate 5G deployment, expansion of IoT legal frameworks, and standards for smart infrastructure and connected services.
- Digitization of governmental functions, company registration, judicial procedures, and public services will be accelerated, necessitating new regulations for e-signatures, digital authentication, and electronic records. The law will prioritize accessibility, security, and interoperability of digital platforms to encourage investment and innovation.
- Telecommunication regulations will increasingly address competition, fairness, and transparency in licensing and service provision, supporting both domestic and cross-border digital services as outlined in Egypt's Vision 2030 and Digital Egypt initiatives.

Egypt's investment in digital transformation, AI, and data

economy is expected to result in substantial legal innovation, aligning regulatory frameworks with international standards, attracting global investment, and safeguarding consumer rights.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Based on our practical experience advising on technology contracts in Egypt, explicit provisions concerning sustainability, net-zero, or broader environmental commitments are not yet common practice. Most contracts are limited to statutory compliance rather than proactive or enforceable sustainability requirements. However, this may begin to shift as ESG awareness grows and more global clients seek alignment with international sustainability goals.

Contributors

Ragy Soliman
Managing Partner, Co-Head of M&A and Capital Markets
ragy.soliman@adsero.me

Dr Ahmed Abdelgawad
Partner, Co-Head of M&A and Capital Markets
ahmed.abdelgawad@adsero.me

Darah Zakaria
Counsel, Head of TMT
darah.zakaria@adsero.me

Nourhan Hatem
Managing Associate
nourhan.hatem@adsero.me

Habiba Haitham
Junior Associate
habiba.haitham@adsero.me

Hana Koptan
Junior Associate
hana.koptan@adsero.me