Legal 500
Country Comparative Guides 2026

Egypt
TMT

Contributor

ADSERO-Ragy
Soliman & Partners

Ragy Soliman

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

Dr Ahmed Abdelgawad

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

Darah Zakaria

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

Hana Koptan

Associate | hana.koptan@adsero.me

Habiba Tarek

Associate | habiba.tarek@adsero.me

Laila Shaaban

Junior Associate | laila.shaaban@adsero.me

Egypt: TMT

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

Generally, proprietary rights in software and the associated materials to such software are protected under Law No. 82 of 2002 on the protection of Intellectual Property Rights (the "IP Law"). The IP Law grants protection to computer programs and databases (computer programs, data bases, software development) by classifying them as literary and artistic works.

Under IP Law, software is classified as a copyright, which is thus afforded protection. Copyright grants the author, or the rights holder, exclusive rights to use, reproduce, distribute, adapt, and publicly communicate the software. Copyright protection arises automatically upon creation, and while registration of the right is optional, it may aid in enforcement of the copyright in the event of any infringement.

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?

Article 138 of the IP Law stipulates that the author of a piece of work is the person who created the work, and as such, is considered as the rightful owner. Therefore, if a software developer or consultant creates software for a client without a written agreement assigning rights, the developer shall ultimately retain ownership of the software.

Proprietary rights may be evidenced by way of registration of the software. Registration does not create or transfer ownership, which remains vested in the author or rightful owner under the applicable provisions of the IP Law. Pursuant to Law No. 163 of 2023, the authority responsible for the deposit and registration of software and databases has been transferred from the Information Technology Industry Development Agency ("ITIDA") to the Egyptian Authority for Intellectual Property.

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

We note that there are no laws that specifically govern liability or harm caused by software or computer systems. The IP Law protects software as a copyrighted work but does not establish a liability regime for any damages caused by software/computer systems. Alternatively, liability is primarily governed under the general principles of Egyptian Civil Code No. 131 of 1948, which sets out provisions on contractual and tort liability, allowing affected parties to claim compensation in cases of negligence or breach of contract. In this respect, claimants must establish elements of fault, damage and causation.

Further, we note that 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.

Moreover, if harm arises from 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. Additionally, the Personal Data Protection Law No. 151 of 2020 (the "PDPL") shall also apply to protect personal data with respect to any incidents of unauthorised access or breaches to such data.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

Same as (4) above, the use or misuse of software is not governed under a single specific law. There are several laws that regulate use or misuse of software/computer systems, namely, The Anti-Cybercrime Law, and the PDPL.

Anti-Cybercrime criminalises 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. With respect to the PDPL, it regulates

the processing of personal data through software/electronic systems by imposing obligations on data controllers and processors on the lawful use (and misuse) of software/electronic systems involving use of personal data. It is important to note that both Anti-Cybercrime Law and the PDPL impose penalties such as fines and imprisonment for the violations.

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?

Aside from the abovementioned laws, with respect to cloud technology, the NTRA has issued a regulatory framework for Establishing & Operating Data Centers and Providing Hosting & Cloud Computing Services. This 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) (as detailed under the Data Centres section).

Further, we note that the general obligations for service providers under Anti-Cybercrime Law shall apply to any provider of cloud-based services, namely the following:

1. Retain specific system and user-related data for 180 days;
2. Keep stored data confidential, disclose data only pursuant to a judicial order, and implement security measures to protect data from unauthorised access or damage;
3. Make key information readily available to users and competent governmental authorities;
4. Provide the technical capabilities necessary for national security authorities to lawfully exercise their powers when requested; and
5. Ensure only the service provider, their authorized agents, and distributors responsible for marketing the services collect user data.

For cloud services and data-related aspects, the PDPL and its Executive Regulations shall apply in parallel, particularly when cloud services involve the processing, storage, or transfer of personal data, since cloud providers are treated as data processors/controllers that may only collect personal data under a license or permit for lawful purposes.

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 limitations of 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; (h) claims arising out of or in relation to artificial intelligence.

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 matters of 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 considered a common practice in Egypt, and as such, it is not governed specifically under any Egypt-specific legislation. Typically, source code escrow is 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. As such, validity and remedies rest on general Egyptian Civil Code contract principles and the terms of the escrow agreement itself.

9. 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 governed by a standalone legislative framework. Instead, outsourcing transactions and arrangements fall within the scope of multiple generally applicable laws, depending on the nature of the services being outsourced. Where personal data is processed as part of the outsourced function, the PDPL shall apply with respect to processing activities, which imposes requirements on the processing and cross-border transfer of personal data.

Further, Anti-Cybercrime Law places specific obligations on service providers, including requirements relating to the protection of information systems and retention of certain user data and traffic logs (as outlined under Q.5 above).

10. 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.

Egypt does not have a specific statutory regime protecting employees where the services they perform are transferred to a third-party IT outsourcing provider. However, in case the services transferred include personal data, then the PDPL will apply in this regard. Employers, as controllers, are subject to several obligations under the PDPL and ER. 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.

Additionally, the PDPL requires that explicit consent must be obtained from employees prior to the processing or disclosure of any of their personal data. If any personal data is to be transferred outside Egypt, the law imposes additional conditions, including that the recipient jurisdiction offers an adequate level of data protection, and subject to obtaining a valid license/permit from the PDPC.

We note that additional details with respect to compliance and implementation are set out below in the 'Data Protection' section.

11. 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 activities and services are governed in Egypt by the Telecommunications Law No. 10 of 2003 (the "Telecom Law"), which regulates the entire telecommunications sector; including:

- The establishment of the 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 Telecom Law, the telecommunications sector is further regulated through the decrees issued by the NTRA, and 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 telecommunications operators and Decree No. 667 of 2017 regulating the penalties to be imposed by the NTRA for breach of telecommunications licenses.

Finally, sector-specific requirements are further elaborated by the Guidelines issued by the NTRA on specific topics, such as the Guidelines elaborating the Regulatory Framework for Establishing Operating Data Centers and Providing Hosting and Cloud Computing Services.

12. 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 licenses are strictly regulated in Egypt. The NTRA has the broad authorities to review and issue such licenses. The Telecom Law provides the 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:

1. License for the provision of telecommunications infrastructure services. There is only one licenses currently issued to Telecom Egypt;
2. 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;
3. 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;
4. Licenses for the provision of internet services;
5. License for the establishment, operation and lease of international cables;
6. License for satellite telecommunications services;
7. License for the establishment and operation of telecommunications towers;
8. License for the establishment and operation of data centres and provision of cloud services; and
9. License for the provision of Internet of Things (IoT) 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.

13. 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 Constitution (2014), which provides 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 Telecom Law, provide expansive exceptions for national security purposes. Telecom 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 PDPL further complicates this framework, as it exempts personal data processed by national security entities from its provisions. 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 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.

14. Telecommunications – Please summarise the principal laws (present or impending) that impose cyber security and/or operational resiliency obligations applicable to the operation of telecommunications infrastructure and/or provision of telecommunications services.

There is no consolidated statute imposing cybersecurity and operational-resilience obligations on the telecommunications sector. These obligations arise from a combination of the Telecom Law, the Anti-Cybercrime Law, as well as the regulatory frameworks and controls issued by the NTRA. In this respect, the Anti-Cybercrime Law is the principal statutory instrument, as it requires such providers to retain and store users' data continuously for at least 180 days. Such data includes subscriber identification data, the content of the service's system, communication traffic data and terminal data, together with any additional data specified by the NTRA.

Providers must also secure the systems and data under their control and cooperate with the competent authorities. Article 4 of the Anti-Cybercrime Law established the National Centre for Computer and Network Emergency Response (EG-CERT) within the NTRA, which provides incident response, early warning and technical coordination for Egypt's telecommunications and critical information infrastructure.

Under the Telecom Law, the NTRA is mandated to safeguard the security and resilience of telecommunications networks and services, which form part of Egypt's critical information infrastructure, and it imposes cybersecurity and business-continuity obligations through licence terms and sector-specific guidelines (including those governing data centres and cloud services). The NTRA's National Cybersecurity Controls (issued in 2023) set out, among other things, incident-response and escalation requirements, including obligations to report cybersecurity incidents promptly to the competent national response centre.

Most recently, the NTRA's Regulatory Framework for Providing Cybersecurity Services entered into force in August 2025. It defines the regulatory requirements for entities providing or using cybersecurity services, mandates adherence to technical and organisational standards, requires the use of certified providers and the prompt notification of cybersecurity incidents, and establishes procedures for registering and certifying cybersecurity service providers. It also identifies the critical infrastructure sectors to which these requirements apply.

The Egyptian Supreme Cybersecurity Council (ESCC), established by Prime Minister's Decree No. 1630 of 2016, is responsible for formulating and overseeing the national cybersecurity strategy and for approving the classification of critical communications and information infrastructure across all sectors, including telecommunications. The current National Cybersecurity Strategy covers the period 2023–2027.

Finally, the PDPL imposes general data-security obligations – requiring appropriate technical and organisational measures to protect personal data. This applies to telecommunications operators in their capacity as controllers or processors of personal data.

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 principal standards, as follows:

- The Egyptian Organizations for Standards and Quality: The organization enjoys broad authorities in connection with setting the Egyptian standards for different fields;

- 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
- The NTRA: As the regulator of the telecommunications sector in Egypt, the NTRA has the broad authority in regulating the market which includes 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 PDPL 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 regime 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.

The principal law governing data protection in Egypt is the PDPL, together with its Executive Regulations.

The PDPL establishes the general legal framework for the protection of personal data in Egypt. It regulates the collection, processing, disclosure, retention, transfer and security of personal data, and sets out the main obligations of data controllers and processors. These include lawful processing, transparency, consent, data subject rights, data security, breach notification, sensitive personal data, direct electronic marketing, cross-border transfers, and licensing and permit requirements administered by the PDPC.

The PDPL ER supplement and operationalise the PDPL by setting out the procedures and practical requirements needed to implement the law. In particular, they activate the role of the PDPC as the competent supervisory authority, including its powers to issue licences, permits and accreditations, oversee compliance, approve data subject rights mechanisms, and conduct inspections and enforcement.

Additionally, they also introduce detailed rules on licensing and permits, including for cross-border transfers, direct electronic marketing and visual surveillance in public places. Furthermore, the PDPL ER introduce practical compliance obligations, including maintaining electronic records of processing activities, appointing and registering a data protection officer (DPO), notifying personal data breaches, and complying with specific requirements for children's data. They also regulate cross-border data transfers by requiring prior PDPC authorisation and, where applicable, the appointment of a local representative or agent in Egypt by foreign controllers.

Moreover, while they do not constitute legislative text per se, the PDPC has published several guidance documents intended to further explain the application of the PDPL in practice. These guidelines are intended to provide additional detail, clarify ambiguities, and assist controllers and processors in understanding and implementing their obligations under the Egyptian data protection framework.

While the PDPL is the principal law governing the protection of personal data in Egypt, other laws impose broader confidentiality obligations in relation to data generally. In particular, the Anti-Cybercrime Law requires service providers to preserve the confidentiality of stored data and prohibits its disclosure except pursuant to a reasoned order issued by the competent judicial authority.

Similarly, the Telecom Law imposes confidentiality obligations in relation to telecommunications activities and provides for penalties in the event of breach.

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?

Fines for breaches of the PDPL range from EGP 50,000 (approx. USD 975) to EGP 5,000,000 (approx. USD 97,465), depending on the nature and severity of the violation. Certain breaches may also carry imprisonment. This applies to:

(a) any person who violates the provisions relating to licences, permits or accreditations required under the PDPL;

(b) any data holder, controller or processor which collects, discloses, transfers, processes, stores or otherwise handles sensitive personal data without the data subject's consent or outside the legally permitted cases; and

(c) any person who violates the cross-border personal data transfer provisions under the PDPL.

In addition to financial sanctions, certain breaches may also result in imprisonment, even where the applicable fine is lower than EGP 5,000,000 (approx. USD 97,465). The most serious imprisonment sanction under the PDPL is imprisonment for a period of not less than six months. This applies to:

(a) any person who prevents an employee of the PDPC, who has judicial enforcement authority, from performing their duties; and

(b) any data holder, controller or processor which collects, processes, discloses, makes available or transfers electronically processed personal data without legal authorisation or the data subject's consent, where the act is committed for material or moral gain, or with the intent of exposing the data subject to risk or harm.

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

There is no prescribed requirement under Egyptian law for technology contracts to refer to external data protection regimes. In practice, the relevant data protection provisions will depend on the location of the data subjects, the parties involved, the nature of the processing activities, and whether the arrangement has an international element.

Historically, certain technology contracts in Egypt, including data processing and data sharing agreements, referred to the GDPR as the governing or benchmark data protection framework. This was largely due to the limited practical enforceability of the PDPL before the issuance of its Executive Regulations and the activation of the PDPC.

However, following the issuance of the PDPL ER, the application of the PDPC, and the expected practical enforcement of the Egyptian data protection regime after the grace period for compliance ends on 31 October 2026, the PDPL is likely to be referenced more frequently in technology contracts related to Egypt. Where a technology contract involves the processing of personal data relating to Egyptian nationals or persons residing in Egypt, the PDPL should be addressed as the primary applicable data protection framework, considering its territorial and extra-territorial scope. The PDPL also extends to non-Egyptians outside Egypt where the relevant act is criminalised in the country in which it was committed, and the relevant data subject is Egyptian or a foreigner residing in Egypt.

External regimes, such as the GDPR, may still be referenced where relevant, including in cross-border arrangements, multinational group contracts, or where EU data subjects are involved. However, such regimes should not replace references to the PDPL where the processing concerns Egyptian data subjects or individuals residing in Egypt.

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

a brief explanation of the general purpose of those laws.

The principal cybersecurity legislation in Egypt is the Anti-Cybercrime Law, together with its executive regulations. It is primarily aimed at addressing cyber offences and protecting information technology systems, networks and data. It criminalises a wide range of conduct, including unauthorised access to information systems, unlawful interception of data, attacks on websites or accounts, misuse of electronic payment tools, online fraud, and the creation or use of fake websites, accounts or emails. The Anti-Cybercrime Law also imposes obligations on service providers relating to data retention, confidentiality, privacy of stored data, and cooperation with competent authorities. The executive regulations further set out technical security standards for systems and services, including requirements relating to secure protocols, encryption standards and antivirus processes.

At a strategic level, the ESCC is responsible for developing and overseeing Egypt's national cybersecurity strategy and approving the classification of critical communications and information infrastructure across all sectors. The current National Cybersecurity Strategy 2023–2027 aims to strengthen the security and resilience of Egypt's cyberspace and information infrastructure, enhance readiness against cyber threats, support secure digital transformation, and promote cooperation between public and private sector stakeholders.

Together, the Anti-Cybercrime Law, its executive regulations and the National Cybersecurity Strategy reflect Egypt's wider approach to cybersecurity, which combines criminal sanctions, technical standards, service provider obligations, strategic oversight and sector-specific regulation.

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?

Fines for breaches of the Anti-Cybercrime Law range from EGP 10,000 (approx. USD 195) to EGP 20,000,000 (approx. USD 390,000), depending on the nature and severity of the breach. Certain breaches may also carry imprisonment, ranging from a minimum of three months to aggravated imprisonment.

The maximum financial sanction under the Anti-Cybercrime Law is a fine of not less than EGP 5,000,000 and not exceeding EGP 20,000,000. This may apply to any service provider which fails to implement a decision issued by the competent criminal court ordering the blocking of a website, link or content that constitutes an offence under the Anti-Cybercrime Law, threatens national security, or endangers the country's safety or national economy, where such failure results in the death of one or more persons or causes harm to national security.

In addition to financial sanctions, certain breaches may also result in imprisonment, even where the applicable fine is lower than EGP 20,000,000. The most serious imprisonment sanction under the Anti-Cybercrime Law is aggravated imprisonment. This applies to:

(a) any person who intentionally causes a network belonging to a public legal entity or state-owned entity to shut down, be disrupted, suffer degraded performance, become jammed, obstructed or intercepted, or who unlawfully processes its data electronically;

(b) any service provider which fails to implement a decision issued by the competent criminal court ordering the blocking of a website, link or content that constitutes an offence under the Anti-Cybercrime Law, threatens national security, or endangers the country's safety or national economy, where such failure results in the death of one or more persons or causes harm to national security; and

(c) any person who commits any of the crimes stipulated under the Anti-Cybercrime Law with the intention of disturbing public order, endangering the safety or security of society, harming national security or the country's economic position, preventing or obstructing public authorities from performing their duties, disrupting the application of the Constitution, laws or regulations, or harming national unity or social peace.

22. Cybersecurity – Are there any cybersecurity regulatory frameworks in your jurisdiction which require registration for certain sectors or services?

Yes. The NTRA has issued the Regulatory Framework for the Provision of Cybersecurity Services in the Arab Republic of Egypt, which sets out the technical and regulatory requirements applicable to cybersecurity service providers. It requires entities providing cybersecurity services to third-party beneficiaries in Egypt to obtain a registration certificate from the NTRA. It also imposes obligations on registered providers, including maintaining confidentiality arrangements with

clients, complying with data retention requirements, and ensuring that relevant personnel satisfy the NTRA's accreditation requirements.

Companies that have acquired such registrations are published under the Register of Companies Approved as a Provider of Cybersecurity Services within the Arab Republic of Egypt, along with their authorized services and authorized customer categories.

23. Cybersecurity – Please summarise the regulatory framework for the reporting of cybersecurity incidents.

The main framework for reporting and responding to cybersecurity incidents in Egypt is EG-CERT within the NTRA. EG-CERT provides incident response, support, defence and analysis in relation to computer and information security threats and cyberattacks. It also cooperates with government bodies, financial institutions and other critical information infrastructure sectors, and issues early warnings regarding malware outbreaks and large-scale cyberattacks affecting Egypt's telecommunications infrastructure. EG-CERT provides both proactive and reactive incident-handling services.

In addition to EG-CERT, sector-specific reporting frameworks may apply. Where a cybersecurity incident involves a personal data breach, the PDPL requires controllers and processors, as applicable, to notify the PDPC within 72 hours of becoming aware of the breach. The notification must include, among other information, a description of the nature, causes and volume of the breach, the contact details of the DPO, the potential consequences of the breach, the mitigation measures taken or proposed to be taken, and any supporting documentation or additional information requested by the PDPC. Data subjects must also be notified within three days. Where the breach relates to national security, the PDPC must be notified immediately, and the PDPC must notify the competent national security authorities without delay.

Furthermore, where the cybersecurity incident relates to the financial or banking sector, the Central Bank of Egypt ("CBE") has established the Computing Incident Response Team for the Financial Sector (EG-FinCIRT). EG-FinCIRT provides dedicated channels for reporting cybersecurity incidents affecting the financial sector, including phishing, electronic fraud and other cyberattacks that may threaten the stability or security of financial and banking institutions.

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

There is currently no single dedicated regulator responsible for the comprehensive regulation of artificial intelligence in Egypt. However, the National Council for Artificial Intelligence (NCAI), established in 2019, is the main national advisory body responsible for AI policy direction and governance. The NCAI is responsible for issuing and overseeing the National AI Strategy, developing ethical AI principles, governance policies and standards, coordinating AI-related efforts across ministries, defining national priorities for AI applications, and supporting capacity-building initiatives.

In January 2026, the NCAI's mandate was expanded, and it became the National Council for Artificial Intelligence, Quantum Computing and Emerging Technologies, reflecting Egypt's broader focus on emerging technologies, including quantum computing and biotechnology.

Accordingly, while Egypt does not yet have a standalone AI regulator, the NCAI acts as the principal national body responsible for shaping AI governance and coordinating Egypt's approach to AI and emerging technologies.

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

There is currently no specific legislation governing AI systems in Egypt. However, the deployment and use of AI may be subject to existing laws depending on the nature of the relevant system or the sector involved, including the PDPL, the Anti-Cybercrime Law, the Consumer Protection Law, the IP Law, and the Telecom Law.

Additionally, The Guide to Egypt's National AI Governance Framework (the "AI Governance Framework") provides non-binding guidance for the responsible development and use of AI systems in Egypt. While it does not constitute legislation, it sets out key principles intended to guide AI deployment, including human-centered use, fairness, accountability, transparency, safety, security, data protection, and risk management throughout the AI lifecycle. It also emphasises that AI should augment human capabilities rather than replace them, that measures should be adopted to identify and mitigate bias, particularly where vulnerable groups may be

affected, and that responsibility for AI outcomes should remain with natural or legal persons under effective human oversight.

26. 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 currently no binding laws or regulations in Egypt specifically governing the deployment or use of Large Language Models, generative AI or agentic AI. This may be addressed under future AI legislation; However, while proposals have been made for draft AI-related legislation, they are not expected to be enacted in the near future based on current parliamentary timelines and the government's drafting progress.

The AI Governance Framework, while non-binding, generally covers generative AI, Large Language Models and General Purpose AI. It applies a risk-based approach to AI systems, including copyright compliance and transparency requirements for chatbots and generative AI content, such as disclosure of machine interaction and labelling of AI-generated content.

27. 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 under Q.24 and Q.25 above.

28. 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?

Technology contracts in Egypt do not yet typically include detailed provisions dealing specifically with copyright, other intellectual property rights, or ownership of outputs in the context of AI systems. This is largely due to the absence of a clear statutory framework or judicial precedent in Egypt addressing the treatment of works created by, or with the assistance of, AI.

In practice, general intellectual property principles under the IP Law would remain relevant, including in relation to the protection of software and other copyrightable works. In addition, software may benefit from registration with ITIDA where applicable. These general protections may extend to AI software and systems, although they do not directly resolve questions relating to the ownership or copyrightability of AI-generated outputs.

The AI Governance Framework, while non-binding, recognises the distinction between human-authored and AI-generated works and indicates that further regulatory guidelines are expected to address the copyrightability of AI-generated content. It further recommends that General Purpose AI providers document training data provenance and copyright compliance and emphasises the protection of intellectual property and cultural data, particularly in relation to Arabic-language models and generative AI systems. This is intended to prevent unauthorised exploitation of Egypt's cultural, literary and media heritage and to ensure respect for content creators' rights.

29. 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 is not currently regulated under Egyptian law, and there is no specific legislation governing the use or development of blockchain infrastructure. However, blockchain applications, particularly those used in the financial sector, may fall within the scope of the CBE where they are used to deliver financial services, process payments, operate payment systems or manage electronic money. They may also fall within the scope of the Financial Regulatory Authority ("FRA") where they relate to non-banking financial activities, financial instruments or services subject to the FRA's supervision. The non-financial uses of blockchain remain unregulated under Egyptian law.

The Banking Sector Law No. 194 of 2020 (the "Banking Law") provides the main legislative framework for regulating and supervising Egypt's banking and financial sector. It grants the CBE broad powers to license and supervise banks, payment service providers and

electronic money activities. Although digital assets are not comprehensively regulated under the Banking Law, Article (206) restricts the issuance, trading, promotion and operation of platforms relating to cryptocurrencies, without authorization from the CBE.

The CBE has also issued several warning statements reaffirming its position on cryptocurrencies, warning against dealing in all types of cryptocurrencies due to the associated risks and the absence of any governmental guarantee, as well as reiterating that no licenses have been issued for such activities in Egypt.

30. 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.

There is currently no standalone legislation in Egypt specifically governing search engines or online marketplaces. However, such services may be subject to general Egyptian law and sector-specific regulations, depending on the nature of the services provided, particularly in relation to consumer protection, advertising, content regulation and electronic contracting. Key relevant laws include:

(a) The Consumer Protection Law No. 181/2018 (the "CPL"), which establishes consumer rights and supplier obligations, including requirements relating to transparency, fair advertising, pricing, return policies, warranties and after-sales support. The CPL also includes specific provisions on distance contracting, which applies to contracts concluded remotely, including through the internet or other electronic means of communication; and

(b) The Media Law No. 180/2018 (the "Media Law"), which regulates traditional and digital media platforms and imposes certain content-related restrictions and licensing requirements for websites.

Accordingly, while search engines and online marketplaces are not regulated under a dedicated framework, their activities may be regulated indirectly depending on their functions, target users and the nature of the content, products or services made available through them.

31. 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?

Egypt does not rely on a single law to govern social media; there are several present and implemented laws that govern different aspects of social media and online platforms. These laws include:

Media Law: sets out the key framework for media regulation. The provisions of Media Law apply to all entities, institutions, and outlets of the press, media, and websites , with the exception of personal websites, personal mediums, or electronic accounts. The scope of Media Law addresses entities that are licensed within Egypt, in addition to offshore websites that are operating in Egypt. The Supreme Council of Media Regulation (SCMR) is the competent media authority as per the Media Law. It has powers to restrict content that is in violation of Media Law and its provisions, which may extend to blocking online platforms or restricting content.

Anti-Cybercrime Law: Sets out a framework that penalizes various cyber-offences including unlawful access to computer systems, online fraud, identity theft, and the dissemination of unlawful content, while also setting out obligations for service providers, requiring them to retain user data and cooperate with law enforcement.

PDPL: Key piece of legislation for the safeguarding and lawful processing of personal data. Establishes rules governing the collection, processing, and protection of personal data by legal and natural persons, including online platforms.

32. 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 Media Law, violators may face fines of up to EGP 5,000,000 and imprisonment of up to 5 years. For social media and online platforms, the SCMR may also commonly impose sanctions such as content takedown/removal, suspension of accounts or pages, and blocking of websites or platforms. Under Anti-Cybercrime Law, the most severe penalties include fines of up to EGP 20,000,000 and imprisonment of up to 15 years for grave offenses such as incitement to terrorism or threats to national security, additional administrative sanctions may also include website blocking and revocation of licenses. 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.

33. 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.

34. 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?

There are currently no specific laws or regulations in Egypt dedicated to quantum computing or quantum cryptography. Accordingly, they may be subject to the general principles of Egyptian law, including any applicable rules relating to cybersecurity, data protection, telecommunications, intellectual property and national security, depending on the relevant use case.

However, Egypt has begun to address quantum computing within its broader emerging technologies agenda. In January 2026, the mandate of the NCAI was expanded to include quantum computing and emerging technologies, reflecting Egypt's wider policy focus on advanced and emerging technologies, including quantum computing and biotechnology.

To that end, Egypt, represented by the Ministry of Communications and Information Technology ("MCIT"), also participated in the BRICS Quantum Technologies Forum, where it noted that Egypt's national quantum computing strategy is being developed under the supervision of the NCAI, and outlined its key pillars.

Accordingly, while Egypt does not yet have a dedicated legal framework for quantum computing or quantum cryptography, policy development in this area appears to be underway.

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

Yes. Data centres in Egypt are primarily regulated by the NTRA under the Regulatory Framework for Establishing and Operating Data Centres and Providing Hosting and Cloud Computing Services ("Data Centres Framework").

The Data Centres Framework is the main sector-specific framework regulating data centres, hosting services and cloud computing services in Egypt. Its applicability depends on the relevant activity, including whether the operator provides services inside or outside Egypt, operates a public data centre, provides hosting or cloud services, or serves internal users or third parties.

The framework distinguishes mainly between a Public Data Centre Provider (PDCP) Licence and a Cloud Service Provider (CSP) Registration. A PDCP Licence permits the licensee to establish and operate data centres and provide hosting services for itself or third parties, site rental services to customers in Egypt, and certain cloud computing services, subject to the applicable conditions. A CSP Registration applies to entities providing cloud computing services for internal use or to third parties in Egypt. Both the PDCP Licence and CSP Registration are issued for a term of 15 years.

In addition to the Data Centres Framework, data centre operators may also need to comply with the PDPL where they process, store or otherwise handle personal data, with the scope of obligations depending on whether they act as a controller, processor or both. They may also be subject to confidentiality and security obligations under the Anti-Cybercrime Law, particularly where they qualify as information and communication technology service providers.

36. 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:

A. Comprehensive AI Regulation and Governance

- Following the publication of the AI Governance Framework, Egypt is expected to move towards the enactment of a dedicated and binding AI law. Such legislation would codify the principles and governance measures currently set out in the non-binding framework and establish enforceable obligations for the development, deployment and use of AI systems in Egypt.
- The introduction of binding AI legislation would reflect Egypt's efforts to align its regulatory framework with international developments and comparable legislative initiatives in other jurisdictions. It is also expected to support Egypt's ambition to become a regional tecnhology and investment hub by providing greater legal certainty while promoting responsible AI development.
- Any future AI law is expected to complement existing legislation, including the PDPL, the Anti-Cybercrimes and applicable sector-specific rules in areas such as telecommunications, financial services, healthcare and transport. Regulatory oversight may be coordinated at the national level by the NCAI, together with the relevant sectoral regulators.

B. Environmental Sustainability Requirements for Technology Infrastructure and Data Centers

- As Egypt continues to position itself as a regional and global hub for technology investment, cloud services and data-centre operations, it is expected to introduce legislation or regulatory standards addressing the environmental sustainability of technology infrastructure. Such measures may form part of a standalone framework for sustainable data centres or be incorporated into existing licensing, environmental, energy and technology-sector regulations.
- The framework may impose sustainability-related requirements on the construction and operation of data centres, including standards concerning energy efficiency, renewable-energy use, carbon-emissions measurement and reduction, water consumption, cooling systems, electronic-waste management, environmental reporting, certifications and technical standards.
- The adoption of such measures would support Egypt's efforts to attract international technology companies by bringing its regulatory environment closer to emerging global practices. Alignment with international sustainability trends would be important not only from an environmental perspective, but also to ensure that data centres established in Egypt remain commercially attractive to multinational operators, investors and customers that are subject to net-zero commitments, environmental reporting obligations and global sustainability standards.

C. Digital Platforms, Online Safety, and Platform Liability

- Egypt may introduce a more comprehensive framework governing social-media platforms and digital intermediaries. Such a framework could address platform responsibility for illegal or harmful content, the protection of minors, age-verification mechanisms, online advertising, complaint-handling procedures, transparency obligations and cooperation with public authorities.
- It may also establish clearer rules on platform liability, including the circumstances in which platforms may be held responsible for content, products or services made available by users.

The likelihood of further regulation is reinforced by recent parliamentary discussions concerning the protection of minors from harmful online content and the regulation of children's access to social-media platforms. During these discussions, the MCIT was involved in considering technical measures to strengthen child online safety, including proposals for child-specific SIM cards and controlled home-internet services incorporating content filtering, parental controls and age-appropriate access restrictions. These discussions indicate a broader policy direction towards imposing stronger child-safety and content-governance obligations on digital platforms and telecommunications providers. The introduction of a unified framework would address an existing regulatory gap, as platform conduct and liability are currently governed through several separate laws, such as the CPL, the Media Law, and the Child Law No. 126 of 2008, rather than a dedicated online-safety or digital-platform regime.

37. 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, express provisions addressing sustainability, net-zero targets or wider environmental commitments are not yet commonly included. Most contracts generally focus on compliance with applicable legal requirements, rather than imposing proactive or independently enforceable sustainability obligations. However, this position may gradually evolve as ESG considerations become more prominent and international clients increasingly require alignment with global sustainability objectives.

Contributors

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

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

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

Hana Koptan
Associate
hana.koptan@adsero.me

Habiba Tarek
Associate
habiba.tarek@adsero.me

Laila Shaaban
Junior Associate
laila.shaaban@adsero.me