EGYPT

Law and Practice

Contributed by:
Ibrahim Shehata, Hesham Kamel, Hana ElBarbary and Dima Mazen
Shehata & Partners

Contents

Shehata & Partners was founded in 1996 and is driven by a vision to provide unique legal services that cater to the business needs of corporate entities doing business in Egypt. Its core mission is to provide the most trusted and effective legal advice on both dispute resolution and corporate law in Egypt. The firm is result-driven and delivers exceptional services to clients across various practice areas and multiple industries. It continues to achieve the highest client satisfaction rates in the region due to the meticulous implementation of its client-centric approach.

Authors

Ibrahim Shehata is a partner at Shehata & Partners and has a decade of experience in the Egyptian market. He started off his career focusing on corporate law, where he successfully advised several multinational companies on doing business in Egypt, and has been involved in the Egyptian renewable energy market since 2014, developing niche expertise that makes him one of the leading lawyers in the field. He is also recognised as one of the key players in the entrepreneurial ecosystem, having worked with more than 60 start-ups. In this regard, Ibrahim has helped start-ups navigate the legal issues that always arise in this specific realm and guided them to be more investment-ready.

Hesham Kamel is an of counsel with over five years of experience in corporate matters. He has been an indispensable member of Shehata & Partners since the very beginning. He also has significant academic leverage, as he holds two master's degrees from the Sorbonne Law School, both specialising in the international rules governing business and trade. Hesham has closed several investment rounds with multiple start-ups, and has also been an integral part of multimillion-dollar investment projects in Egypt.

Hana ElBarbary is an associate at Shehata & Partners. She holds an LLB from Sorbonne University's Institut de Droit des Affaires Internationales (IDAI) as well as an LLB from Cairo University. She is currently advancing her expertise by pursuing a master's degree in international and European business law at Sorbonne University's IDAI. Hana has gained substantial experience in corporate and competition law at top-tier Egyptian law firms, where she has played an important role in navigating complex legal challenges and has contributed to significant cases in both fields.

Dima Mazen recently joined Shehata & Partners as a junior associate. She is a highly motivated corporate lawyer. She graduated fourth in her class from Ain Shams University's Faculty of Law (English section) and is currently pursuing her master's degree in private law. Before joining Shehata & Partners, she gained practical experience interning at top-tier law firms. Her experience also includes competing in international moot court competitions, including the Price Media Law Moot Court Competition at Oxford, as well as coaching mooting teams.

Shehata & Partners

Cairo Business Plaza Unit (204)
Fifth Settlement
New Cairo
Cairo
Egypt

Tel: +201022256100
Email: info@shehatalaw.com
Web: shehatalaw.com

1. Digital Economy

1.1 Key Challenges

Legal Framework

Telecommunications Law

The telecommunications sector is regulated by the Telecommunications Law. This law covers all telecommunications services, including:

- installation and operation of telecommunications networks;
- use of telecommunications equipment;
- provision of wired and wireless communications;
- connectivity, radio frequency, and broadband services; and
- information technology services.

Importance in the digital economy

The Telecommunications Law is crucial for the digital economy as it interacts with the regulatory framework for digital services through information technology. It also overlaps with other laws in the digital economy, such as the:

- E-Signature Law;
- Consumer Protection Law;
- Cybercrimes Law; and
- Media Law.

While these laws have their own legislation, their interplay with the digital market can be complex and unclear.

E-Signature Law

E-signatures and e-contracts are regulated under E-Signature Law No 15 of 2004 and its executive regulations issued by Ministerial Decree No 109 of 2005. The E-Signature Law established the Information Technology Industry Development Agency (ITIDA) to regulate and supervise e-signature activities in Egypt.

Enabling contract formation

The E-Signature Law allows technology use in contract formation by:

- recognizing e-signatures;
- establishing evidence standards for electronic contracts; and
- validating e-signatures and e-writing to create legal effects.

Previously, Egyptian evidence law did not recognise digital documents and digital signatures as legally effective.

Proof criteria (Article 18)

E-signatures, e-documents and e-writing must meet the following criteria:

- linked to the signatory only;
- controlled by the signatory; and
- modifications or replacements in the data must be detectable.

Verification and issuance

Service providers, licensed by ITIDA, handle the verification and issuance of e-signature certificates. These providers must comply with:

- data security systems;
- PKI management and security;
- secure custody systems for e-signature creation data and e-certificates; and
- ITIDA-approved contract service templates.

Data Protection Law

Egypt issued Data Protection Law No 151 of 2020 to align with international standards for online services and digital market transformation. The law upholds the data protection rights of individuals whose data is processed digitally.

Key definitions

- Personal data: any data identifying a person directly or indirectly, including name, voice, picture, ID number, online identifier, or any data determining a person's identity.
- Processing: any electronic operation involving personal data, such as collection, storage, display, transmission and analysis.
- Data subject: any individual whose personal data is processed electronically, enabling their identification.
- Electronic marketing: any technological means used to promote goods, services, or petitions addressed to specific persons.

Requirements for data use and processing:

- setting out the rights of data subjects and lawful data processing cases;
- specifying the obligations of data processors, controllers and receivers;
- requiring express consent from data owners for data collection and processing;
- informing data owners of the purpose of data processing;
- implementing measures to secure and protect personal data; and
- imposing restrictions on direct electronic marketing communications.

Prohibitions and permissions

- Direct digital marketing requires the data subject's prior consent.
- Marketing communication must include the sender's name, location and purpose, allowing the data subject to approve or reject it.

Personal data protection centre (PDPC)

The PDPC will be established under law to license and regulate data processing in Egypt, once the executive regulations become available.

Protection of sensitive information

The law provides additional protection for sensitive information, such as health, biometric and financial data, and criminal records. The collecting and processing of sensitive data require prior permission from the PDPC. Information relating to children is considered sensitive by default.

Cybercrimes Law

The Cybercrimes Law came into force on 15 August 2018, with executive regulations No 1699 of 2020. It regulates online activities and penalises unlicensed online activity and content violations, such as unauthorised access to sites or private accounts, and exceeding authorised access limits.

Service provider obligations
Service providers must:

- keep and store records of information systems or technology for 180 days;
- maintain the confidentiality of stored data;
- not disclose data without a justified judicial order; and
- secure data and information to preserve confidentiality and prevent damage.

Coverage
The Cybercrimes Law covers offences related to the digital economy, including violations of confidentiality, integrity, and availability of computer data, computer-related offences, and privacy infringements.

Fintech Law
Law No 5 of 2022, known as the "Fintech Law", came into effect in February 2022. It aims to include the non-banking sector in the digital market and encourage a cashless society. The Financial Regulatory Authority (FRA) supervises and regulates non-banking financial activities.

Key definitions
- Non-banking activities: financial markets and tools supervised by the FRA, including capital markets, insurance, real estate finance, financial leasing, factoring, SME financing, and consumer finance.
- Financial technology: modern technology used in the non-banking financial sector to support financial services, financing, and insurance activities through applications, software, digital platforms, AI, or electronic records.

Licensing requirements
Companies in non-banking financial activities using financial technology must do the following:

- determine direct and indirect shareholding structure and related parties;
- provide necessary technological infrastructure, IT, and security means; and
- limit activities to those specified in the FRA-issued licence.

New Banking Law
Egypt issued the New Banking Law No 194 of 2020, replacing the old Banking Law No 88 of 2003, to integrate the banking system into the digital economy. The law introduces digital banks, cashless payments, payment service providers, payment systems operators, cryptocurrency, and e-money.

Financial technology and electronic payments
The Central Bank of Egypt (CBE) permits financial technology and electronic payment services, including:

- payment aggregators and facilitators;
- payment services using prepaid cards; and
- standards for contactless payments.

Licensing and regulations
The New Banking Law sets out licensing conditions and the main rules for operating payment systems, defining:

- payment systems – means and procedures for settling funds electronically;
- financial technology – technology-based business, applications or financial products; and
- payment services – services related to account information, payment orders, and operations, including issuing and managing payment tools and electronic money.

Licensing requirements

Natural and juristic persons must obtain a CBE licence to operate payment systems or provide payment services. This requirement also applies to payment system providers (PSPs) and payment system operators (PSOs) targeting Egyptian residents from abroad.

Record preservation

Licensed service providers must preserve electronic copies of registries, contracts, correspondence, commercial papers and banking transaction documents. These copies have the same legal value as original documents if preserved, processed and retrieved according to CBE guidelines (Article 203).

Key Challenges

Although Egypt has witnessed a number of efforts to support growth of the digital market, in practice, some challenges remain, as discussed here.

Regulatory framework

- Multiple regulatory authorities: The digital market involves various authorities based on the digital activity type. There is no consolidated E-Trade Law or authority regulating all e-commerce fields, leading to enforcement issues.
- Outdated legislation: The E-Signature Law, issued in 2004, is outdated given the current technology market's development.
- Unclear legislative platform: Egypt lacks clarity in handling e-commerce, especially regarding electronic transactions, liabilities, rights, and burden of proof.
- Slow e-government framework: The slow enactment of an e-government regulatory framework hinders integration with the commercial digital market, especially locally.

The 2017 national e-commerce strategy with UNCTAD highlighted these issues and the need for legislative improvements, such as intermediary liability, e-procurement, and data protection enforcement. The Data Protection Law's application remains unclear without an established licensing body and executive regulations.

Intellectual property

- Lack of specific protection: The IP Law does not provide specific protection for IP and copyrights in digital markets. It remains unclear which authority protects IP rights in the digital economy.
- Registration requirement: To gain legal protection under the IP Law, trade marks and IP rights must be registered.
- Enhancement needs: Enhancements include granting ITIDA authority to investigate infringements via an online complaints system, and training officers for electronic evidence procurement.

1.2 Digital Economy Taxation

The tax application regime in the digital market and e-commerce is complex. Key challenges include identifying the permanent establishment (PE) subject to tax, determining tax liability, and enforcement.

Inclusion in the Tax System

Egypt has taken steps to include e-commerce in the tax system:

- Decree No 307 of 2020 created an e-commerce department to register e-commerce businesses for taxation;
- Executive Circular No 89 of 2021 requires that commercial and non-commercial activities be registered with the Egyptian Tax Authority (ETA), including:
  (a) e-commerce;

(b) audio-visual media content platforms; and
(c) publication and production of reading content.

Taxpayer Classification

The ETA classifies taxpayers into two categories:

- sole proprietorship (individuals); and
- companies (corporate).

Taxes Applied

E-commerce activities are subject to:

- revenue tax, which applies to direct income from online services; and
- value added tax (VAT), which applies indirectly to services rendered to customers.

1.3 Taxation of Digital Advertising

Digital advertising has gained significant prominence in Egypt, especially following the COVID-19 pandemic in 2020, which accelerated the shift towards online platforms. Recognising this growth, the ETA has intensified efforts to incorporate individuals and companies operating in all streams of e-commerce, including digital advertising, into the formal economy. The ETA's guidebook on the tax treatment of e-commerce explicitly identifies digital advertising as a taxable service.

Applicable Taxes

Digital advertising revenues in Egypt are subject to the following taxes:

- Income tax for individuals – individuals earning income from digital advertising activities are subject to income tax based on progressive tax brackets, as outlined in the Income Tax Law No 91 of 2005 and its amendments.
- Corporate income tax – companies engaged in digital advertising are liable to pay corporate income tax at a standard rate of 22.5%, calculated on their net taxable profits, in accordance with the same legislation.
- Value added tax (VAT) – digital advertising services are classified as taxable services under Value Added Tax Law No 67 of 2016. Consequently, they are subject to VAT at the prevailing rate of 14% once revenues reach or exceed EGP500,000.

Ensuring Compliance With Tax Laws

To ensure compliance with Egyptian tax laws related to digital advertising, individuals and companies should undertake the following measures:

- Tax registration – register with the ETA to obtain a tax identification number for income tax purposes and a VAT registration certificate, if applicable.
- Accurate accounting records – keep comprehensive tax ledgers and accounting books that accurately reflect all transactions, revenues, expenses, and applicable tax deductions or credits, in accordance with Egyptian accounting standards.
- Timely tax declarations –
  (a) annual income tax returns: submit annual income tax declarations within the prescribed deadlines (for individuals, returns are typically due by 31 March each year; companies must file their returns within the four months after the end of their fiscal year); and
  (b) periodic VAT returns: file monthly VAT returns detailing the output tax collected from digital advertising services and any input tax credits.
- Electronic invoicing compliance – adhere to the ETA's electronic invoicing system by

issuing electronic invoices for all transactions, enhancing transparency and facilitating compliance monitoring.
- Regular financial audits – conduct regular internal audits to ensure accuracy in tax reporting and promptly address any discrepancies.

1.4 Consumer Protection

Consumer protection is crucial, particularly in B2C transactions in the digital market. Strong legislative and regulatory systems are essential for building trust between consumers and service providers.

Consumer Protection Law

The Consumer Protection Law No 181 of 2018 and its executive regulations (Decree No 822 of 2019) extended consumer protection to online contracts. Key terminologies include:

- Online contracting– offering, buying or selling products via internet platforms or other communication means.
- Advertiser – any person who promotes a commodity or service using media, including digital means.
- Supplier – any person engaged in commercial, industrial or professional business providing services to consumers, including through electronic means.

Consumer rights and measures

The Consumer Protection Law outlines various consumer rights and protections:

- right to disclosure of pre-contractual and post-contractual information;
- methods to restrict unfair impositions on customers; and
- processes to file complaints against digital economy operators through the Consumer Protection Authority (CPA).

Online contracting protections

Specific rights and protections for online contracts include:

- the right to obtain the necessary contract information;
- the right to confirm contract approval within seven days;
- the supplier's obligation to observe all duties and consumer rights in remote contracts; and
- the right to revoke the contract within 14 days of receipt.

Exclusions

The Consumer Protection Law does not cover:

- banking and financial activities;
- capital markets trade;
- newspaper subscriptions;
- flight ticket reservations; or
- hotel reservations.

Supervisory Authorities

The CPA enforces the Consumer Protection Law. The National Telecommunications Regulatory Authority (NTRA) supervises consumer protection in telecommunications services, setting guidelines and obligations for service providers.

Best Practices for TMT Companies

To handle consumer disputes effectively, TMT companies should:

- establish proactive call centres for prompt consumer support;
- provide accessible customer support to resolve issues quickly and enhance customer satisfaction; and

- demonstrate a commitment to upholding consumer rights in the digital economy.

1.5 The Role of Blockchain in the Digital Economy

In Egypt, cryptocurrency activities are strictly regulated under the New Banking Law No 194 of 2020. Article 206 prohibits the issuance, trading, promotion and operation of cryptocurrency platforms and electronic money without a Central Bank of Egypt (CBE) licence. Since no licences have been granted, engaging in cryptocurrency activities is effectively illegal without proper authorisation.

Impact on the TMT Sector

The stringent regulatory framework limits the incorporation of cryptocurrency services into digital offerings. TMT companies must avoid unlicensed cryptocurrency activities to prevent legal repercussions.

Blockchain Technology

While cryptocurrency use is heavily restricted, blockchain technology for non-currency purposes is not prohibited. TMT companies can use blockchain for secure data management and smart contracts, adhering to relevant data protection and cybersecurity laws.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

Data Protection Compliance

Cloud and edge computing services must comply with the Data Protection Law, which governs licensing, processing and securing personal data. Data subjects can file complaints for violations. The law excludes data with the CBE and entities regulated by the CBE, except remittance and exchange companies.

CBE Instructions (2019)

The CBE's instructions to protect customer interests include:

- maintaining data confidentiality;
- protecting customers in digital services; and
- duties of payment and digital service providers.

Complaints are handled by the CBE's customer protection unit.

Main Challenges

Cloud and edge computing face regulatory and practical challenges due to the lack of a clear regulatory framework and unissued executive regulations. This results in uncertainties in licensing, data protection enforcement, and rights enforcement.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

AI is set to bring significant changes to Egypt's economy and society. AI has the potential to revolutionise industries, increase productivity and drive economic growth by automating tasks, improving decision-making and fostering innovation.

Although a specific AI law is still under development, several existing laws contribute to AI governance in Egypt (see "Legal Framework" in **1.1 Key Challenges**).

Existing Laws Governing AI

National Council for Artificial Intelligence (NCAI)

Established in November 2019 by Decree No 2889, the National Council for Artificial Intelligence (NCAI) operates under the Ministry of Telecommunications, led by the minister. The NCAI is responsible for developing and managing Egypt's AI strategy, working closely with experts and stakeholders to ensure that AI initiatives align with national priorities and international best practices. The council's mandate includes fostering innovation, ensuring ethical standards, and driving sustainable growth in the AI ecosystem.

Egyptian Charter for Responsible AI

The Egyptian Charter for Responsible AI reflects the country's commitment to ethical AI practices. Aligned with the OECD AI Principles, the charter emphasises human-centred principles like accountability, fairness, safety, security, transparency and explainability. The charter aims to guide AI developers, enhance the attractiveness of investment, and empower citizens to advocate for responsible AI applications.

National Artificial Intelligence Strategy

In early 2025, Egypt introduced the second edition of its National Artificial Intelligence Strategy (2025–2030). This strategy sets clear guidelines for responsible AI use, fostering innovation and supporting integration across various sectors. By aligning with international standards and adapting them to the local context, Egypt seeks to position itself as a leader in AI development while ensuring ethical standards and sustainable growth.

Elements Relevant to AI Technology

Data protection and consumer protection

AI relies on collecting and processing large datasets to recognise patterns and make predictions. Under Egyptian law, any data collected and processed for AI purposes is protected. The Data Protection Law mandates that personal data must be collected for legitimate purposes, be accurate and secure, processed lawfully, and not retained longer than necessary. Similarly, the Consumer Protection Law requires suppliers to preserve consumer information, maintain confidentiality, and avoid unauthorised disclosure without explicit consent.

Intellectual property

While AI inventors can legally protect their patent rights under the Intellectual Property Law, AI machines themselves are not granted patent rights, as they lack legal personality. This raises intriguing questions about the ownership of inventions created autonomously by AI – an area not yet addressed in Egyptian law and still under global discussion.

Liability and insurance

Determining liability when an AI system causes harm can be complex. The Egyptian Civil Code holds guardians of mechanical devices responsible for damages unless these are caused by uncontrollable external factors. This suggests that AI developers or operators could be held liable if their AI systems cause predictable and preventable harm. Additionally, the Consumer Protection Law holds suppliers accountable for damages arising from product defects, improper use, or failure to take sufficient care.

Unaddressed issues in Egyptian law

Despite the existing legal framework, certain aspects of AI technology remain unregulated. For instance, Egyptian law does not specifically

address protections of a person's likeness or moral rights in relation to deepfake technologies. Similarly, there are no specific regulations concerning AI applications in transport, such as self-driving cars, commercial drones, or drone delivery services. As AI continues to advance, it is anticipated that legal provisions will evolve to address these emerging challenges and ensure comprehensive governance.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Vision 2030 and Smart Cities

In line with its Vision 2030, which includes establishing smart cities like the New Administrative Capital, Egypt has focused on the internet of things (IoT) services. In January 2022, the NTRA issued the first regulatory framework for IoT, advancing its growth and addressing related challenges.

IoT Definition and Framework

IoT involves using technical means for automatic communication between objects to exchange, analyse and process data. It includes devices and systems connected for data collection and sharing. The NTRA framework classifies IoT into five categories:

- consumer IoT apps – wearable devices and smart home systems;
- commercial IoT apps – intelligent transportation systems (ITS), surveillance and vehicle-to-vehicle (V2V) connections;
- industrial IoT apps – digital industrial control systems, smart agriculture and industrial monitoring;
- infrastructure IoT apps – smart city applications for monitoring environmental factors and managing resources; and
- government IoT services – applications for healthcare and public utilities (water, electricity, gas, transportation and education).

Data Protection

IoT relies on data collection, exchange, analysis and processing (ie, data handling). Providers must implement measures to protect user data confidentiality per the NTRA IoT framework, which is subject to the Telecommunications Law and Data Protection Law. These laws ensure that data collected for IoT is protected (see "Legal Framework" in **1.1 Key Challenges**).

Cybercrimes Law

The Cybercrimes Law addresses IoT-related offences, including violations of data confidentiality, integrity and availability, as well as privacy infringements (see "Legal Framework" in **1.1 Key Challenges**).

Machine-to-Machine Communications

Machine-to-machine (M2M) communications involve connecting devices and transferring data between them, either wired or wirelessly. M2M applications are part of IoT services and are used by mobile phone providers and various companies through mobile networks or private networks (see "Legal Framework" in **1.1 Key Challenges**).

4.2 Compliance and Governance

See **4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection** .

4.3 Data Sharing

See "Legal Framework" in **1.1 Key Challenges** .

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Audiovisual services are regulated by the Media Law (Law No 180 of 2018) and its executive regulations (Prime Ministerial Decree No 418 of 2020). Licensing requirements are detailed in the President of the Supreme Media Council Decision No 26 of 2020.

The Media Law applies to all types of media, press, marketing content and broadcasting services, including audio, video, satellite, electronic media, marketing and internet platforms. Social media platforms and user-generated content are also regulated to track content and income for tax purposes.

Licensing Requirements

A licence from the Supreme Council for Media Regulation (SCMR) is required in order to operate audiovisual media services, and the prerequisites for audiovisual media services must be met.

Media institutions

Media institutions are defined as institutions managing media means, which include terrestrial and satellite TV channels, and wired, wireless and electronic broadcasting stations. A prior licence from the SCMR is required for incorporation or operation, and broadcasting from outside accredited locations needs SCMR approval.

Licence duties

A licence from the SCMR will outline the following duties for the licensee:

- service and technology – specify the type of service and broadcasting technology used;
- licence duration – define the duration of the licence;
- territory – indicate the geographical area covered by the licence;
- quality requirements – set the standards for quality of service; and
- intellectual property – address intellectual property rights and responsibilities.

Ownership

Egyptian nationals can own media means and websites. Prospective owners must not have committed dishonourable crimes or be deprived of political rights. Media companies must be incorporated with the following minimum authorised share capital:

- EGP50 million for TV, broadcasting and news channels;
- EGP30 million for specialised TV channels;
- EGP15 million for each radio station;
- EGP2.5 million for TV or digital TV channels; and
- EGP100,000 for online websites.

Foreigners are not allowed to own the majority of shares or acquire controlling rights in media institutions.

Website licensing

A website is a licensed electronic page, link or application presenting press, media or advertising content.

Establishing or operating websites requires a prior SCMR licence. Applicants must be Egyptian nationals and not have committed dishonourable crimes. Corporate entities need a minimum share capital of EGP100,000.

Foreign websites providing content in Egypt also require a prior licence from the SCMR.

Application process

Media services – applications must include:

- applicant's signature or legal representative;
- applicant's name, nationality and address;
- website or media means name, activity, financial resources, editorial and administrative structures;
- responsible broadcasting and programme manager's names, budget and broadcasting location;
- identification card (for natural persons) or commercial register (for juristic entities);
- newspaper website and broadcasting location;
- proof of fee payment (EGP250,000); and
- compliance with the SCMR code of ethics.

Websites – applications must include:

- commercial register and tax card;
- copies of ID cards of website owners;
- memorandum and articles of association (for juristic persons);
- directors' names, nationality and IDs;
- budget and financial statements (for juristic persons);
- trade mark registration certificate;
- undertaking to avoid transmitting illegal content;
- lease or title deed of management location, notarised; and
- proof of fee payment (EGP50,000).

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

This sector is primarily governed by the Telecommunications Law (see "Legal Framework" in **1.1 Key Challenges**), with additional regulations issued by the Ministry of Telecommunications and Information Technology, such as the Contraventions Regulations (Ministerial Decree No 667 of 2017) and Equipment Licensing Requirements (Ministerial Decree No 258 of 2003).

Telecommunications Services and Activities

These encompass various services and activities:

- fixed services – landline and data services, including internet connectivity and global peering services;
- wireless services – mobile networks, message services and value-added services;
- satellite services – telecommunications via satellite, global mobile communications by satellite and satellite broadcasting services;
- international services – establishing and operating international telecoms gateways;
- infrastructure leasing – establishing, operating and managing telecoms infrastructure, use of frequencies, and access to closed urban communities;
- telecommunications equipment – using, assembling and manufacturing telecoms equipment; and
- data hosting and cloud computing – cloud computing service providers and public data centres.

Licences and Permits

There are two types of authorisation required from the NTRA:

- licences – needed for establishing or operating telecoms networks, services, using radio frequencies, and passing international calls; and
- permits – required for importing, trading, manufacturing and assembling telecoms equipment.

Applicants must submit the relevant form to the NTRA, including:

- name and details of the applicant;
- proposed pricing;
- financial and operational plans;
- market analysis; and
- other NTRA requirements.

Once obtained, the licences will specify the scope, duration, territory, quality of service, and secrecy of information.

Interconnectivity

Requirements

Licensed telecoms service providers must ensure the interconnection and integration of services. This includes disclosing technical specifications, ensuring non-discriminatory terms, and submitting data on harm caused by other networks.

Interconnection policy

This provides guidelines for reference interconnection offers (RIOs) and service level agreements (SLAs) with Telecom Egypt and other licensed providers. It covers regulatory, technical and economic aspects.

Security Requirements

Telecommunication Regulation Law

Under this law, telecoms entities must provide the NTRA with reports, statistics and information, excluding national security matters. They are under the oversight of national security agencies and the armed forces, facing penalties for non-compliance, including fines and imprisonment.

Law on Combating Information Technology Crimes

This imposes penalties for failing to block websites or links that threaten national security, with fines and imprisonment for non-compliance.

6.2 Net Neutrality Regulations

In Egypt, net neutrality is not explicitly codified, but existing regulations align with its principles. The Telecommunications Law requires service providers to offer non-discriminatory access, preventing practices like blocking or throttling of content. The NTRA enforces standards ensuring internet service providers (ISPs) adhere to minimum-quality service regulations, allowing users to access various services without unjustified degradation.

Although specific net neutrality rules are absent, the NTRA enforces guidelines preventing the blocking of legal content and ensuring fair competition. Additionally, the Data Protection Law influences how ISPs handle personal data, ensuring consumer protection and affecting internet traffic management.

Despite these measures, the lack of explicit net neutrality laws leaves room for issues like internet censorship or government website blocking. These actions, often related to national security or public morality, may restrict free and fair internet access. While the telecommunications sector strives for fairness and prevents anti-competitive practices, the absence of clear net neutrality provisions means there could still be potential for discriminatory practices, especially with the development of technologies like 5G and IoT.

6.3 Emerging Technologies

Emerging technologies like 5G, IoT, and AI are reshaping Egypt's telecommunications land-

scape by introducing new challenges, opportunities and regulatory requirements.

5G Networks

The implementation of 5G requires significant legal adaptation due to its impact on infrastructure, spectrum allocation, and cybersecurity. The NTRA must navigate the complexities of 5G spectrum allocation, ensuring a fair and efficient licensing process while minimising interference.

The development of 5G infrastructure demands increased density of mobile towers and small cells in urban areas, raising legal questions about zoning laws and permissions. Regulatory reforms are needed to support the smooth rollout of 5G technology. Additionally, 5G amplifies cybersecurity and data privacy concerns.

The Data Protection Law imposes new responsibilities on telecoms companies to protect users' data, while the Cybersecurity Law safeguards national infrastructure from cyber-attacks.

Internet of Things

IoT, heavily reliant on 5G, connects a vast array of devices, raising concerns over data security, privacy and device management. IoT devices must comply with the Data Protection Law, ensuring secure data handling and user consent for data collection. The growing use of IoT calls for updated cybersecurity regulations to take the vulnerabilities of numerous connected devices into account. Specific IoT security standards are necessary to prevent wide-ranging consequences as a result of data breaches or system failures.

Artificial Intelligence

AI in telecommunications, used for network optimisation, predictive maintenance, and enhancing customer service, presents legal challenges related to bias, accountability and transparency. The legal framework must ensure ethical AI use, with clear regulations for transparency in AI-driven decisions.

Egypt's National Artificial Intelligence Strategy aims to position the country as a regional leader by 2030, aligning with global best practices like the OECD AI Principles.

The Egyptian Charter for Responsible AI underscores the commitment to human-centred, accountable and transparent AI applications, potentially necessitating updates to laws like the Consumer Protection Law and Cybersecurity Law.

Impact on Competition and Market Regulation

The integration of 5G, IoT and AI impacts telecoms sector competition and market regulation. As 5G technology becomes widespread, new service providers and business models may emerge, potentially disrupting existing market structures.

Antitrust and competition laws may need to evolve to ensure fair competition and prevent monopolistic practices. Updates to the Telecommunications Law may be necessary to regulate new market entrants and promote innovation while safeguarding consumer interests.

Interaction With Fintech

Egypt's Fintech Law interacts with emerging telecoms technologies. Recognising AI's role in processing consumer data, the law is relevant in the context of 5G and IoT, enabling rapid data analysis and improving the efficiency of financial transactions. However, data privacy and algorithmic fairness concerns also arise.

Financial service providers must ensure compliance with telecommunications and data protection regulations to mitigate risks. The General Authority for Financial Supervision emphasises the need for responsible AI application in the financial sector, particularly with the use of AI in robo-advisers for investment.

Adaptations in Regulatory Framework

The Telecom Equipment Regulation Law and E-Signature Law will need to adapt to innovations in AI and IoT for digital identity verification, secure communications, and blockchain-based applications, challenging existing regulatory structures, especially around authentication and electronic contracts.

7. Challenges with Technology Agreements

7.1 Legal Framework Challenges

Technology agreements are recognised under Egyptian legislation in the context of the transfer of technology. To understand the challenges involved with transfer of technology agreements, it is important to first examine the related legal provisions. Transfer of technology agreements are dealt with under Trade Law No 17 of 1999.

These agreements facilitate exchange of the technical know-how crucial for production, development or service provision. They encompass various forms, such as technical assistance, patents, utility models, commodity grants and licence agreements. By defining a transfer of technology agreement as a contract where technical know-how is exchanged for payment, the law provides a clear structure for these complex transactions.

Mandatory Provisions and Supplier Obligations

These agreements must be meticulously drafted in writing, detailing all relevant technical know-how. Suppliers hold significant responsibilities, including:

- providing essential information and technical services to ensure the technology's seamless operation;
- disclosing potential risks, legal obstacles, and compliance with local laws;
- guaranteeing the conformity of the technology and related documents with the agreement's terms; and
- ensuring the production of the commodity or performance of services as specified in the agreement.

These supplier obligations are default guarantees unless otherwise agreed in writing between the parties. Thus, it is crucial for parties to explicitly agree on specifications and guarantees.

Protection for Importers

The law protects importers from restrictive provisions that could limit their freedom to utilise or enhance the technology. Specific prohibitions include:

- mandating the acceptance of supplier improvements;
- restricting technology modifications;
- enforcing exclusive material purchases from the supplier; and
- restricting sales exclusively to the supplier.

Jurisdiction and Dispute Resolution

Disputes arising from these agreements fall under the jurisdiction of the Egyptian courts. Arbitration is permitted, but only if conducted within Egypt under Egyptian law. This provision

ensures that legal proceedings remain within the national framework, providing consistency and predictability in dispute resolution.

Guarantees and Liability

Article 85 emphasises the supplier's obligation to guarantee the conformity of the technology and its associated documents with the agreement's terms. This default guarantee becomes enforceable unless the parties explicitly agree otherwise in writing. Additionally, both parties are liable for any third-party damages resulting from the use of the technology, highlighting the importance of precise and comprehensive contractual terms.

Technology Services Requirements

Parties must consider technology services requirements, especially regarding consumers, data privacy and cybersecurity. Proper attention to consumer protection rights and cybersecurity requirements under Egyptian law is essential, as these aspects may involve liability or other implications. These requirements can vary based on the technology's use and related activities. For example, data secrecy and security in the banking sector are subject to additional requirements and stricter monitoring under applicable laws.

Confidentiality and Secrecy

Confidentiality is paramount in the transfer of technology agreements. Article 83 outlines the parties' roles in maintaining secrecy:

- importers must maintain the confidentiality of improvements they introduce to the technology (breaching this duty can lead to indemnification obligations); and
- suppliers are required to protect only the confidentiality of importer-introduced improvements.

It is essential for parties to review and clearly define their confidentiality duties and rights within the agreement. Additionally, considerations regarding intellectual property rights and protection factors are crucial to avoid potential disputes.

Termination and Amendment

Article 86 grants parties the right to seek termination or amendment of the agreement's terms five years after the agreement date. To avoid the default application of this provision, parties must explicitly agree on the duration and specific terms for termination or review within the contract. This foresight ensures mutual understanding and clarity on the agreement's lifespan and modification conditions.

Technology transfer contracts in sensitive sectors like banking and insurance are subject to additional regulations and guidelines from their respective competent authorities. These measures ensure the integrity, security and stability of financial systems are maintained throughout the transfer process. This includes strict data protection, cybersecurity protocols, and comprehensive risk assessments to mitigate the potential risks associated with new technologies.

7.2 Service Agreements and Interconnection Agreements

Considerations for Service Agreements

Key elements

In Egypt, telecommunications service agreements must comply with the Telecommunications Law and related regulations. Key elements to cover are:

- clear definitions of telecommunications services – categories include fixed services, wireless services, satellite services, international services, infrastructure leasing, tel-

ecommunications equipment, or data hosting and cloud computing services;
- licences and permits – obtaining the necessary authorisations from the NTRA is essential;
- agreement details – scope, duration, territory, quality of service, and confidentiality obligations should be specified in the NTRA licence; and
- compliance with equipment licensing requirements – essential for any telecoms equipment used.

Negotiating favourable terms

To negotiate favourable terms in telecommunications service agreements, companies should ensure:

- transparency and fairness – to clearly outline each party's responsibilities, technical specifications, pricing and operational plans;
- flexibility in technology use and development – to avoid restrictive clauses that could limit operational freedom;
- there are provisions for regular updates and improvements – to ensure the technology and services provided are kept up to date; and
- they have legal counsel – to help navigate negotiations to cover all regulatory and legal aspects effectively.

Considerations for Interconnection Agreements

When entering interconnection agreements, TMT companies must consider the following.

Regulatory compliance

- Ensure connectivity between users across different networks and services as mandated by the Telecommunications Law.
- Include protection measures to safeguard networks from interference or harm resulting from interconnection.
- Adhere to intellectual property rights and notify if there are any changes impacting services.

Technical specifications

- Detail interconnection points and standards for network management and fault recovery.
- Establish non-discriminatory terms to ensure fairness.

Economic aspects

- Specify interconnection charges, payment terms, and billing procedures based on cost models approved by the NTRA.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Trust services, e-signatures, and digital identity schemes are regulated under the E-Signature Law and its executive regulations, which fall under the Telecommunications Law. The E-Signature Law, issued in alignment with Evidence Law No 25 of 1968 and Protection of Intellectual Property Rights Law No 82 of 2002, aims to regulate e-signatures and establish ITIDA to oversee e-signature services and electronic transactions.

Key Provisions of the E-Signature Law

In March 2021, ITIDA issued a general "Certificate Policy" guideline, establishing that ITIDA operates the Egyptian Root-CA, issuing certificates for certified service providers (SPs) for e-signatures and electronic seals. Licensed and certified SPs in Egypt include:

- The Egyptian Co. For Digital Signature & Information Security SAE (Egypt Trust);
- El Delta Electronic Systems;

- Fixed Misr; and
- Misr for Central Clearing, Depository and Registry (MCDR).

Fundamental Rights

E-signatures and electronic documents in civil, commercial and administrative transactions have the same evidentiary effect as written signatures and official documents under Egyptian evidence law, provided the conditions of the E-Signature Law are met. Copies of official electronic documents have the same evidential effect as the originals if backed up electronically.

Data Protection

The E-Signature Law enhances data protection for e-signatures. E-signature data and electronic information provided to a certified SP are confidential and must not be disclosed or used for unauthorised purposes.

Intellectual Property

The E-Signature Law supports IP rights, granting ITIDA the authority to register original copies of computer programs and databases to preserve IP rights and other associated rights.

Jurisdiction

ITIDA is responsible for licensing and supervising e-signatures by:

- issuing and renewing licences for e-signature services;
- setting e-signature system standards;
- handling complaints related to e-signature activities;
- providing technical advice on disputes and IT activities; and
- registering original copies of programs and databases.

ITIDA can revoke or suspend a licence if the certified SP violates licensing conditions.

Liability

Mutual obligations on ITIDA and certified SPs ensure the legally binding effect of e-signatures and electronic seals. Certified SPs must obtain relevant licences from ITIDA and use them within their scope, issuing digital certificates for e-signatures and seals. Certificates must not exceed the validity of the certified SP's licence. ITIDA must comply with the E-Signature Law and its executive regulations when licensing certified SPs.

9. Gaming Industry

9.1 Regulations

Gaming Regulations

There are currently no specific laws or regulations in Egypt that address the gaming industry. However, it is expected that the SCMR will play a key role in overseeing video games. The SCMR is currently drafting new legislation that will require any platform, including those offering video games, to obtain a legal licence before accessing mobile phone users. The goal of this regulation is to mitigate the spread of harmful content that may be associated with certain games.

Gambling Laws

Article 352 of the Egyptian Criminal Code prohibits traditional forms of gambling involving a physical place that could host clients. However, the legislative framework for online gambling remains unclear.

In-Game Purchases, Loot Boxes and Gambling

Currently there is no clear legislative framework for such matters, except to the extent that they could be subject to current laws and regulations

(see "Legal Framework" in **1.1. Key Challenges**). The SCMR's upcoming legislation may address these issues.

Age Ratings

Finally, there are currently no specific legal requirements for game developers in terms of age ratings and content restrictions. The SCMR's new regulations may introduce such requirements to ensure games are appropriate for different age groups and to prevent harmful content from being distributed.

9.2 Regulatory Bodies

See **9.1 Regulations** .

9.3 Intellectual Property

As explained in **9.1 Regulations** , there are currently no laws or regulations in Egypt related to the gaming industry.

10. Social Media

10.1 Laws and Regulations for Social Media

Social media platforms in Egypt are primarily regulated under the Data Protection Law. This law provides a comprehensive framework for protecting personal and sensitive data, imposing strict rules and safety measures on data processors and controllers, including social media platforms. Platforms must obtain clear consent from users and ensure secure collection, storage and processing of data (see "Legal Framework" in **1.1. Key Challenges**).

The SCMR also oversees digital content, including social media. The Media Law No 180 of 2018 extends to social media accounts that have at least 5,000 followers. Accordingly, it requires them to adhere to ethical standards similar to those of professional media. The SCMR can take action against violations, such as suspending or blocking accounts.

Key Legal Challenges

Data protection and cybersecurity

One major legal challenge is ensuring compliance with data protection laws. Social media platforms must implement robust cybersecurity measures to protect user data. The Data Protection Law mandates that data controllers and processors must obtain user consent and secure data, but enforcement can be challenging.

Intellectual property

Egypt's IP law is broadly worded, potentially extending to content shared on social media platforms. This can create ambiguity and difficulties in applying IP protections to social media content.

Data monetisation

Monetising user data while complying with data protection regulations presents another challenge. Platforms must balance the commercial use of data with the need to protect user privacy and obtain proper consent.

Age restrictions

There are no specific legal requirements for age ratings and content restrictions for social media platforms. The SCMR's regulations may address harmful content, but age-specific guidelines are not well defined.

10.2 Regulatory and Compliance Issues

See **10.1 Laws and Regulations for Social Media** .