



Legislative Update Report: The Anti-Information Technology Crimes Law and Its Relation to Artificial Intelligence

Pursuant to Sultani Decree No. (61/2026) — effective as of 2 June 2026

Introduction

His Majesty Sultan Haitham bin Tarik issued Sultani Decree No. (61/2026) promulgating the Anti-Information Technology Crimes Law, which was published in the Official Gazette No. (1651) of 7 June 2026 and takes effect the day following its publication. This law replaces the previous law issued under Sultani Decree No. (12/2011), and comes in the context of keeping pace with rapid technological transformations, most notably the spread of artificial intelligence applications and social media platforms, and the emerging patterns of crime that accompanied them, which the previous legislation had not addressed.

This report aims to provide a comprehensive analytical reading of the aspects related to artificial intelligence and the digital environment in the new law, based on the official text published in the Official Gazette and the official media coverage issued by the Oman News Agency and government media outlets.

First: Government Entities Related to the Legislative Update

No official published statement has specifically identified the list of entities that participated in the preparatory work for drafting the draft law before it was presented to the Council of Oman and issued. However, the official text of the law and its constitutional issuance path clearly identify the entities with direct jurisdiction over its application and coordination:

- Ministry of Transport, Communications and Information Technology (the Ministry): the entity responsible for applying the provisions of the law, and the law grants it authority to coordinate with competent entities to obtain electronic data or information.
- Council of Oman: the draft law was constitutionally presented to it before issuance, as explicitly stated in the decree's preamble ("and after presentation to the Council of Oman").
- Public Prosecution and the competent court: the two judicial bodies authorized to issue the judicial order required for the Ministry to obtain electronic data.
- Cyber Defense Center (affiliated with the Internal Security Service): the law explicitly stated that its competencies are not affected, given its status as the national reference for cyber defense and protection of vital interests in the Sultanate's cyberspace.
- Government and non-government entities ("counterpart entities"), inside and outside the Sultanate: the law referred to them in general terms as parties with whom electronic data may be exchanged within the framework of investigating information technology crimes, without naming them specifically.

Note: The list of entities carrying the description "competent authorities" referred to in the law (such as the Telecommunications Regulatory Authority, the Ministry of Justice and Legal Affairs, the Public Prosecution, the Royal Oman Police, the Oman National CERT, and others) is usually determined later through implementing regulations or ministerial decisions subsequent to the law, and has not yet been issued as of the date this report was prepared. This report deliberately refrains from naming them unless



the Ministry has confirmed internal information about the entities that actually participated in the drafting, in which case it is recommended to include them accurately rather than relying solely on public sources.

Second: Legal Provisions Related to Artificial Intelligence

For the first time in Omani legislation, the new law includes explicit definitions of artificial intelligence and its systems, and includes "AI systems" as a component of the "information system" on which the majority of crimes provided for in the law are based. Below are the directly relevant provisions as they appear in Article (1) of Chapter One (Definitions and General Provisions):

Article (1) — Item 7: Definition of "Information System"

A set of computer programs, applications, social media platforms, or artificial intelligence systems prepared to create, process, and manage electronic data or information interconnected with one another over the information network.

Article (1) — Item 8: Definition of "Artificial Intelligence"

A field of computer science that focuses on developing techniques, algorithms, and systems that work on analyzing data and learning from it, and simulating some human cognitive abilities such as vision, language understanding, problem-solving, and decision-making. These systems can also perform certain tasks based on pattern analysis and deriving solutions from available data.

Article (1) — Item 9: Definition of "AI Systems"

Computer programs or devices that use artificial intelligence to perform specific tasks.

Practical effect of these definitions: since the term "information system" recurs in the drafting of most of the law's criminalization provisions (for example: "whoever uses an electronic site or an information system or a means of information technology..."), including "AI systems" within this definition practically means that all crimes covered by the law — from data trespass, to fraud and forgery, to content, extortion, and impersonation crimes — now also explicitly cover acts committed using artificial intelligence systems, without the need for a separate article for each use case.

Article (36) — Paragraph 6 (Chapter Six: Content Crimes / Crimes Affecting the Family and Society)

This paragraph is considered the provision most directly linked to the risks of digital manipulation (Deepfake) and content tampering resulting from AI techniques. It reads:

Making any modification or manipulation to an audio or visual clip, or to an image of another person, with the intent of defamation, insult, or portraying them in a manner that would prejudice their reputation or dignity.

This paragraph falls within Article (36), which criminalizes violations of the privacy of individuals' or families' personal lives, and is punishable by imprisonment for a period of not less than three months and not more than three years, and a fine of not less than 1,000 Omani riyals and not more than 5,000 Omani riyals, or by either of these two penalties.



Paragraphs (1) and (5) of the same article are related to the same context; they criminalize eavesdropping on and recording audio or visual material without a legal right, and tracking the geographic locations of others — patterns of infringement that are increasingly being committed or facilitated through AI tools and applications.

Third: Broader Coordination Powers with Data-Protection Competent Authorities

This power appears in Article (4) of Chapter One, and its full text reads:

Without prejudice to the competencies of the Cyber Defense Center, and in the event there are sufficient grounds for the occurrence of an information technology crime, the Ministry may, in coordination with the competent authorities, obtain electronic data or information from counterpart entities and other government and non-government entities inside the Sultanate of Oman and abroad, based on a judicial order issued by the Public Prosecution or the competent court, as the case may be.

What this provision practically means:

- The entity holding the power: The Ministry of Transport, Communications and Information Technology, and not any other investigating body acting alone.
- Activation condition: the existence of "sufficient grounds" indicating the probable occurrence of an information technology crime — meaning the power is not absolute, but is tied to an existing criminal suspicion.
- Judicial safeguard: The Ministry may not obtain data except based on a judicial order issued by the Public Prosecution or the competent court, which provides prior judicial oversight over the use of this power.
- Scope of "competent authorities" and "counterpart entities": this includes government and non-government entities inside and outside the Sultanate of Oman, without naming them explicitly in the text of the law; it is practically expected to include entities such as the Royal Oman Police, the Public Prosecution, and the sectoral entities concerned with data (such as the telecommunications and financial-sector regulatory bodies), in addition to their international counterparts through international judicial and security cooperation channels.
- Explicit exception: the law states that this does not affect the competencies of the Cyber Defense Center (the national reference entity for cyber defense and protection of vital interests in cyberspace, affiliated with the Internal Security Service), meaning that the Ministry's new power is complementary to, and not a substitute for, its role.

Fourth: Objectives of the Legislative Update

According to the official coverage by the Oman News Agency (Oman) picked up by government newspapers upon the law's issuance, the new law comes to achieve the following objectives:

- Strengthening national digital security.
- Protecting society from emerging electronic crimes.



- Ensuring the confidentiality and integrity of electronic data and information.
- Providing legal protection for digital evidence.
- Achieving legal deterrence through the enactment of deterrent penalties for crimes committed using information technology means.

A reading of the legal text itself adds implicit objectives reflected in the law's structure, most notably:

- Keeping pace with technical development: by introducing definitions that did not exist in the 2011 law, such as artificial intelligence and its systems, social media platforms, digital evidence, and electronic payment means.
- Expanding the scope of criminalization: moving from 6 chapters in the previous law to 9 chapters comprising 62 articles in the new law, including newly introduced chapters such as crimes organized via information technology, electronic-payment-means crimes, and expanded content crimes.
- Closing the legislative gap between the legal text and the reality of use: so that acts committed via AI tools and systems do not remain outside the scope of criminalization on the pretext that they are not explicitly stated.

Fifth: The Nature of the Digital Environment Shaped by These Updates

The digital environment shaped by the new law can be described, from a legal standpoint, as a more regulated and clearer environment, characterized by the following:

- An environment legislatively recognized as one in which AI systems are an actual component of cyberspace, no longer a technical novelty outside the scope of legislation.
- An environment in which social media platforms are listed comprehensively within the "information system," reflecting the fact that a large share of today's digital crimes are committed through them.
- An environment that elevates the value of "digital evidence," giving it a dedicated definition and a special chapter (Chapter Four) that criminalizes withholding or tampering with it, which enhances the reliability of litigation in technical cases.
- An environment that tightens protection of individuals' digital privacy against tools for recording, tracking, and digitally editing images and clips (Article 36), which directly touches on the misuse of generative AI tools.
- An environment that enables institutional and judicial cooperation between the Ministry and competent authorities, locally and internationally, for exchanging data within a judicially regulated framework, rather than unregulated bilateral dealing.
- An environment that balances openness to modern technology tools and freedom of legitimate use, on one hand, with strict legal deterrence against their misuse, on the other, through a clear gradation of penalties according to the severity of the act and the harmed party (individual, governmental, or financial).

Sixth: Expected Impact of the Legislative Updates



Below is an analytical reading of the expected impact of these updates across a number of areas, based on the content of the legal provisions themselves and the official context announced for the law's objectives:

1. Information Security

The law strengthens the national digital security framework by expanding the scope of criminalization to explicitly cover acts committed by means of AI systems and social media platforms, alongside tightening penalties for crimes of breaching government and banking systems and data (Articles 10 and 11). It also establishes institutional integration between the Ministry, the Cyber Defense Center, and judicial authorities, which reduces jurisdictional duplication and enhances the speed of response to cyber incidents.

2. Data Protection

The law provides a higher level of legal protection for personal and government data, through an explicit classification of "electronic data or information" and "government data" (Article 1, Item 4), and a tightened penalty if the data violated is of a personal nature (Article 5). It also grants a regulated legal framework for exchanging data between official entities locally and internationally (Article 4), balancing the need for criminal investigation with privacy safeguards via the requirement of judicial authorization.

3. Investment

From the standpoint of the business environment, the clarity of the legal framework governing information technology and AI crimes contributes to raising the degree of legal certainty for investors and companies operating in the technology, telecommunications, and digital entrepreneurship sector, as it precisely defines the criminalized acts and the penalties attached to them (Chapter Seven). It also strengthens the confidence of consumers and international partners through stronger protection of data and intellectual property in the Omani digital environment (Article 51) and electronic payment means. In return, this requires companies — particularly those developing or using AI systems — to review their practices to ensure compliance with the new obligations.

4. Digital Innovation

The law sends a clear legislative signal that innovation in the field of artificial intelligence and digital technologies is embraced within legal recognition, not excluded from or left in a legislative vacuum, which supports the stability of national digital policies linked to the goals of the National Program for Artificial Intelligence and Advanced Digital Technologies and Oman Vision 2040. At the same time, the law sets clear limits on the misuse of these technologies (such as deep fakes, impersonation, and information fraud), thereby establishing the principle of "responsible innovation," which balances encouraging the development of new technical solutions with protecting individuals and society from their risks.



Conclusion

The Anti-Information Technology Crimes Law issued under Sultani Decree No. (61/2026) represents a qualitative shift in the Omani legislative framework for cyberspace — not merely in terms of the quantitative expansion in the number of articles and chapters, but more importantly through integrating artificial intelligence as a legally defined and embedded concept within the definitional foundation on which all crimes provided for in the law are based. This legislative approach — based on a comprehensive technical definition rather than dedicating separate articles to each emerging technology — grants the law greater flexibility to keep pace with future developments in this field without the need for repeated amendments.

It is recommended to monitor the issuance of the implementing regulations or complementary ministerial decisions to the law, which are expected to more precisely determine the intended competent authorities referred to in Article (4), and the practical coordination mechanisms between the Ministry and counterpart entities locally and internationally.

Sources

- Sultani Decree No. (61/2026) promulgating the Anti-Information Technology Crimes Law — Official Gazette No. (1651), 7 June 2026, published on the official portal for Omani legislation, Qanoon.om
- Oman Official Newspaper: "The Anti-Information Technology Crimes Law.. An Integrated Legislation and Broader Protection for Society," 7 June 2026
- Al Roya Omani Newspaper: "The Anti-Information Technology Crimes Law Strengthens National Digital Security and Protects Society from Electronic Crimes," quoting the Oman News Agency, 1 June 2026
- Shu'oon Wataniya website: "Details of the Sultani Decree Promulgating the Anti-Information Technology Crimes Law," 7 June 2026
- Sultani Decree No. (64/2020) establishing the Cyber Defense Center and issuing its statute — Qanoon.om