

The 2026 Cybercrime Law of Oman and Digital Governance

Abdulwahab Abdullah Al-Maamari^{1,*} and Mukhammad Ali Turdialiev²

^{1.} Faculty of Law, Isra University, Queen Alia International Airport Road, Amman 11710, Jordan

^{2.} Department of Private International Law, Tashkent State University of Law, Uzbekistan; m.turdialiyev@tsul.uz

* Correspondence: abdulwahab.almaamari@iu.edu.jo

Abstract: On 1 June 2026, Royal Decree No. 61/2026, replaced the Sultanate of Oman's fifteen-year-old Cybercrime Law (Royal Decree No. 12/2011) with a substantially expanded statute governing digital conduct. The Decree 61/2026 modernizes Oman's technical cybercrime framework only incrementally, but expands liability for online expression, most visibly through Article 20's prohibition on "misleading information" and content deemed to undermine public order. Current research examines the new law's structure, its treatment of technical and content-based offenses, and its penalty architecture, situating the reform within Oman's obligations under international human rights instruments. The article situates the law within the broader regional pattern in which cybercrime statutes are deployed less against hacking than against dissent, and is a set of doctrinal and drafting recommendations aimed at narrowing the law's most indeterminate provisions.

Keywords: digital governance; cybercrime law of Oman; Offence; human rights

1. Introduction

Oman has digitally transformed since 2010, marked by expanding digital infrastructure, the widespread adoption of information technology across government and private sectors, and the deep integration of digital services into everyday life. This transformation has generated substantial opportunities for economic growth and social development while simultaneously exposing individuals, institutions, and the state to an evolving range of cyber threats. Cybercrime legislation is being increasingly implemented in the domestic legal orders of Gulf states, simultaneously addressing genuine technical threats of data breaches, ransomware, network intrusion and the regulation of online speech. On 1 June 2026, His Majesty Sultan Haitham bin Tarik issued Royal Decree No. 61/2026 promulgated a new Law on Combating Cybercrime, which entered into force the day after its publication in Official Gazette No. 1651 on 7 June 2026 (Lexis Middle East 2026; Gulf Centre for Human Rights 2026). The decree repeals Royal Decree No. 12/2011, Oman's original cybercrime statute, and voids any conflicting regulation (Lexis Middle East 2026).

The reform occurred when Oman's digital-speech record is being observed. Civil society organizations were urging the government to bring the 2011 law into conformity with international human rights standards, citing prosecutions of journalists and activists for online expression (Ismail 2026). The response is not liberalization but expansion. The new law retains previous provisions of scrutiny and added new categories of liability, including provisions addressing encryption and the protection of state officials from online criticism (Ismail 2026; IFEX 2026). Current study maps that expansion, situates it against Oman's technical cybersecurity objectives, and evaluates the resulting statute against comparative and international benchmarks.

2. Legislative History

Oman's original cybercrime statute, Royal Decree No. 12/2011, remained functional for nearly fifteen years and was, repeatedly invoked against online speech (Ismail 2026). A series of prosecutions were observed under the 2011 law's provisions on personal expression and "misuse of social media." In July 2025, the Omani Centre for Human Rights and Democracy and the Gulf Centre for Human Rights to Oman's Universal Periodic Review, which called on the state to align the 2011 law with international standards (Ismail 2026). Decree 61/2026 preserves statute's speech-related provisions and adds new liability, including the criminalization of encryption in defined circumstances, expanded provisions concerning calls for legal or constitutional reform, protections shielding the Sultan, the judiciary, and foreign heads of state from online criticism, and a provision permitting legal guardians to monitor the digital activity of women and minors in their charge (Ismail 2026; IFEX 2026). Local legal commentators and regional human rights bodies alike have characterized the resulting statute as restrictive of expression (Gulf Centre for Human Rights 2026).

Citation: Abdulwahab Abdullah Al-Maamari and Mukhammad Ali Turdialiev. 2026. The 2026 Cybercrime Law of Oman and Digital Governance. *Legal Research & Analysis* 4(2), 38-41. <https://doi.org/10.69971/lra.4.2.2026.194>



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>.

3. Architecture of the 2026 Law

Decree 61/2026 substantially enlarges the cybercrime statute in sheer volume. The 2011 law was a comparatively compact instrument, the 2026 law comprises sixty-two substantive articles addressing, among other things, artificial intelligence and synthetic media manipulation (Madasari 2026). The law preserves a bifurcated design separating "technical" offenses, directed at unauthorized access, data interference, and system disruption from "content" offenses directed at prohibited categories of online expression (Decree Blog 2026).

Oman's Ministry of Transport, Communications and Information Technology describes the law's stated purposes as strengthening national digital security, protecting the confidentiality and integrity of electronic data, reinforcing digital evidentiary protections, and safeguarding intellectual property in digital contexts (Times of Oman 2026). Structurally, Chapter Six of the law addresses content-related offenses across five sections, covering crimes against the state, offenses affecting family and society, online gambling, and the creation or operation of websites and accounts used for prohibited content (Times of Oman 2026). Chapter Eight addresses organized cybercrime, criminalizing the establishment of, participation in, or support for criminal groups that use information technology to commit offenses under the law. Chapter Nine sets out final provisions, including which offenses require a formal complaint, the liability of legal entities, and penalties for incitement, complicity, and conspiracy (Times of Oman 2026).

The law also references a Cyber Defense Center, whose competencies are addressed in Article 4 and whose establishment have separately documented under earlier decrees (Gulf Centre for Human Rights 2026). The Center's institutional role of straddling technical incident response and, by implication, content-monitoring functions reflects a broader regional tendency to consolidate cybersecurity and information-control functions within a single administrative apparatus.

4. Technical Offenses

Despite the law's expanded scope, its treatment of genuinely technical cybercrime changed comparatively little. Technical offenses of unauthorized access, data interference, system interference, and related conduct occupy only fourteen substantive articles in the new law, compared with thirty-three articles devoted to content offenses (Decree Blog 2026). The law's treatment of artificial intelligence, despite official framing to the contrary, amounts to limited textual acknowledgment rather than a substantive regulatory framework. The highest fine for a purely technical offense under Article 18 is 20,000 Oman rials with a reduction from the 50,000 rial maximum under the 2011 law (Decree Blog 2026).

Other reporting describes materially different figures, including maximum penalties reaching fifteen years' imprisonment and fines as high as 100,000 rials for offenses targeting government websites, critical infrastructure, or banking systems (Oman Tech News 2026). These divergences likely reflect differing offense tiers within a single, internally graduated penalty scheme. The statute's technical provisions were not the focus of the 2026 reform, and its most consequential penalty increases fall elsewhere (Decree Blog 2026; Oman Tech News 2026).

Article 12 of the new law criminalizes the possession, importation, sale, or trade of any device, software, password, or data that has been designed, developed, or modified for the commission of an offense under the law, or for the concealment of evidence of such an offense (Ismail 2026; IFEX 2026). To encompass ordinary security-research and penetration-testing tools, this provision is common to technical cybercrime statutes generally. Instruments capable of dual use are criminalized by reference to purpose or intent, a formulation that shifts substantial discretion to prosecuting authorities.

5. Content-Based Offenses

Article 20 criminalizes producing, storing, broadcasting, sending, or republishing material that undermines public order or public morality, or that constitutes rumors or misleading information, whether disseminated directly or indirectly (Ismail 2026; Gulf Centre for Human Rights 2026). The baseline penalty ranges from one month to three years' imprisonment with a fine of between 1,000 and 3,000 rials, rising to a term of three to ten years where the prohibited intent is deemed present (Ismail 2026). The provision as designed, in practice if not on its face, to reach internet activists and critical commentary on government policy, given the discretion it affords to internal security authorities in characterizing content as disruptive of public order or morality (Gulf Centre for Human Rights 2026).

The doctrinal difficulty with Article 20 is definitional. Terms such as "public order," "public morality," and "misleading information" are not self-limiting. Without a narrowing construction or an accompanying body of judicial interpretation, these function as open-textured standards capable of being applied to a wide range of protected expression, including political criticism, satire, and reporting on matters of public concern (Ismail 2026). Comparable formulations recur across cybercrime statutes in the wider South-west Asia–North Africa region, where such language is the operative basis for prosecutions unconnected to any technical misuse of computer systems (Ismail 2026).

The 2026 law introduces an expanded section addressing offenses framed as crimes against the state conducted through digital means. This section is oriented substantially toward content. It extends protection against online criticism to the Sultan, members of the judiciary, and foreign heads of state, and to attach criminal liability to online advocacy for legal or constitutional reform (Ismail 2026). Under Article 30, providing false or misleading information that damages state interests has a sentence of up to three years, separate from the general penalty structure of Article 20 (IFEX 2026).

A further set of provisions address conduct framed in terms of family and societal protection, including a guardianship provision permitting legal guardians to monitor the digital communications and activity of women and minors under their authority (Ismail 2026). While framed defensively as a child- and family-protection measure, such provisions can function as a legal safe harbor for the surveillance of adult women by male guardians, raising distinct concerns under both domestic family law and international non-discrimination norms (Ismail 2026). Chapter Six additionally addresses online gambling and the operation of websites or accounts dedicated to prohibited content, extending the law's reach to platform-level and intermediary conduct rather than individual expression alone (Times of Oman 2026).

6. Penalty and the Proportionality Problem

The relationship between offense severity and penalty severity of Decree 61/2026 raises concerns across its technical and content provisions. An individual who deliberately wipes data and disables the systems of a private hospital is subject, under Article 5, to a maximum sentence of one year. However, an individual who posts a single message containing misleading information during a public health emergency is subject, under Article 30, to a maximum sentence of fifteen years, i.e., fifteen times the maximum penalty for the underlying cyberattack (Decree Blog 2026). The highest fine attached to any technical offense in the law is 20,000 rials under Article 18, compared with a maximum fine of 500,000 rials for a non-technical, content-based offense under Article 55 (Decree Blog 2026).

This inversion, whereby expressive conduct is punished more severely than conduct causing direct, measurable harm to critical systems is difficult to justify on ordinary criminal-law principles of proportionality, which generally calibrate punishment to the gravity of harm caused and the culpability of the offender. The practical center of gravity of Decree 61/2026 lies in the regulation of online expression rather than in the deterrence of technical intrusion. This reading is reinforced by the law's own internal proportions: content offenses occupy more than double the substantive articles devoted to technical offenses (Decree Blog 2026).

7. Human Rights and International Law

Oman is party to the International Covenant on Civil and Political Rights (ICCPR) and a signatory to the Arab Charter on Human Rights, whose Article 32 guarantees freedom of opinion and expression and whose Article 21 prohibits arbitrary interference with privacy (IFEX 2026). Oman's accession to the ICCPR was followed, within a comparatively short interval, by legislation whose content provisions notably Article 20 raise tension with the Covenant's protections for expression, given their reliance on broad, discretion-conferring terminology rather than narrowly drawn, foreseeable categories of prohibited speech (IFEX 2026).

Under the ICCPR framework, restrictions on expression must satisfy a three-part test. They must be provided by law, must pursue a legitimate aim recognized under Article 19(3), and must be necessary and proportionate to that aim. Terms such as "undermining public morality" or "misleading information," without further statutory or judicial specification, sit uneasily with the legality requirement, which demands that a restriction be formulated with sufficient precision to allow individuals to regulate their conduct accordingly. The guardianship-monitoring provision raises analogous concerns under the Covenant's privacy protections and under international non-discrimination norms concerning the equal treatment of women, insofar as it formalizes differential digital oversight based on gender and guardianship status (Ismail 2026).

The Internal Security Service is the principal enforcement actor under the new content provisions, consistent with its role in earlier prosecutions under the 2011 law (Gulf Centre for Human Rights 2026). This continuity of institutional enforcement, combined with an expanded and more severely sanctioned content regime, characterizes the reform as a net contraction, rather than an expansion, of protected digital expression in Oman (Gulf Centre for Human Rights 2026).

Oman's 2026 reform is not an isolated development. Across the wider Southwest Asia–North Africa region, successive cyber-crime statutes have followed a broadly similar pattern: each new law is publicly justified by reference to hacking, fraud, and national-security threats, while its practical application falls disproportionately on journalists, activists, and ordinary social media users rather than on technical intruders (Ismail 2026). This pattern recurs regardless of the specific vocabulary used, whether framed as protecting "public order," combating "misleading information," or preventing the "misuse of technology" (Ismail 2026).

Decree 61/2026 is notable less for its novelty than for the degree to which it consolidates and extends an established legislative template. It has an expanded content-offense regime, official-protection provisions insulating heads of state and the judiciary from online criticism, and penalty structures that treat expressive offenses as more serious than technical ones. The law's new features, the criminalization of encryption in defined circumstances and the guardianship-monitoring provision are incremental additions to that template (Ismail 2026; IFEX 2026).

8. Policy Recommendations

Decree 61/2026 can be aligned with international free-expression and privacy standards without compromising its legitimate technical objectives. Article 20 and the analogous content provisions in Chapter Six should be narrowed through precise statutory definitions of "public order," "public morality," and "misleading information," ideally accompanied by an actual-harm or actual-malice threshold that distinguishes deliberate disinformation causing demonstrable harm from ordinary political commentary, satire, or good-faith reporting. Similarly, the penalty structure should be recalibrated so that offenses causing direct, quantifiable harm to critical infrastructure, financial systems, or personal data are punished at least as severely as expressive offenses, consistent with ordinary proportionality principles in criminal sentencing.

The guardianship-monitoring provision should be revisited in light of its potential for discriminatory application, with consideration given to independent oversight mechanisms or its removal in favor of general child-protection provisions that do not differentiate by gender among adult family members. Prosecutorial guidance or implementing regulations should clarify the evidentiary standard for the state-protection and official-criticism provisions, distinguishing legitimate public-interest criticism of government conduct from conduct properly understood as defamation or incitement.

9. Conclusion

Current study relies primarily on official gazette notices, licensed legal databases (Lexis Middle East 2026; Lawrtal 2026; Decree 2026), and contemporaneous reporting and human rights analysis due to lack of peer-reviewed secondary literature. Readers requiring citation-ready statutory text for litigation or compliance purposes should consult the official Arabic text published in Official Gazette No. 1651 (7 June 2026) or a verified licensed translation. Royal Decree No. 61/2026 is the most significant reform of Oman's cybercrime framework since 2011. It modernizes Oman's technical cybersecurity architecture. In a substantially enlarged body of content-based offenses, punishing expressive conduct more severely than direct technical harm, and new provisions covering encryption, official protection, and guardianship-based digital surveillance extend state authority over online life. Whether the

law achieves its stated aims of strengthening digital security and protecting Oman's institutions will depend on implementation and how narrowly, or broadly, its most indeterminate provisions are construed by Omani courts and prosecuting authorities.

References

- Basatwar, Govindraj. 2026. Oman Cybersecurity Regulations & Compliance Guide. DoveRunner. [https://doverrunner.com/blogs/oman-cybersecurity-regulations-compliance-guide/](https://doverunner.com/blogs/oman-cybersecurity-regulations-compliance-guide/)
- Decree Blog. 2026. The Cybercrime Law of 2026: When Content Is Your Biggest Crime. Decree Blog. <https://blog.decree.om/2026/content-is-your-biggest-crime>
- Decree. 2026. Royal Decree 61/2026 Issuing the Cybercrime Law. Decree. <https://decree.om/2026/rd20260061/>
- Gulf Centre for Human Rights. 2026. New Cybercrime Law More Repressive Than Previous One. Gulf Centre for Human Rights. <https://www.gc4hr.org/new-cybercrime-law-more-repressive-than-previous-one/>
- IFEX. 2026. Under the Guise of Combatting Cybercrime, Oman's New Law Provides a Mechanism for Speech Control. IFEX. <https://ifex.org/under-the-guise-of-combatting-cybercrime-omans-new-law-provides-a-mechanism-for-speech-control/>
- Ismail, Zeinab. SMEX. 2026. Why Oman's New Cybercrime Law Has Little to Do with Cybercrime. SMEX. <https://smex.org/why-omans-new-cybercrime-law-has-little-to-do-with-cybercrime/>
- Lawrtal. 2026. Royal Decree No. 61/2026 Promulgating the Cybercrime Law. Lawrtal. <https://www.lawrtal.com/en/legislation/20128>
- Lexis Middle East. 2026. Oman Sultani Decree No. 61/2026 - On the Promulgation of the Cybercrime Law. Lexis Middle East. https://www.lexismiddleeast.com/law/Oman/SultaniDecree_61_2026/en
- LexisNexis Middle East. 2026. Oman: Sultan Haitham Issues New Cybercrime Law. LexisNexis Middle East Insights. <https://www.lexisnexis.com/blogs/ae-legal/b/insights/posts/oman-sultan-haitham-issues-new-cybercrime-law>
- Madasari, Mohammed Saud Al Madasari. 2026. Effective Reporting of Cybercrimes Crucial. Oman Observer. <https://www.omanobserver.om/article/1191715/opinion/international/effective-reporting-of-cybercrimes-crucial>
- Oman Tech News. 2026. Oman Enacts Landmark Cybercrime Law Under Royal Decree 61/2026 to Combat Modern Digital Threats. Oman Tech. <https://techoman.om/oman-enacts-landmark-cybercrime-law-under-royal-decree-61-2026-to-combat-modern-digital-threats/>
- Times of Oman. 2026. New Cyberlaw to Enhance Oman's Digital Security. Times of Oman. <https://timesofoman.com/article/172462-new-cyber-law-to-enhance-omans-digital-security>