حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

Digital Transformation in Palestine

A Rights-Based Readiness Assessment of Emerging Digital Public Infrastructure

November 2026



7amleh - The Arab Centre for the Advancement of Social Media

Digital Transformation in Palestine

A Rights-Based Readiness Assessment of Emerging Digital Public Infrastructure

November 2026

Author: Dr. Mohammed Alshurafa

Design: Qafzeh - Marketing, Digital, and Production

This version is licensed under the following International License: Attribution-NonCommercial-NoDerivs 4.0 International

To view a copy of the license, please visit the following link:

https://creativecommons.org/licenses/by-nc-nd/4.0

Contact us:

Email: info@7amleh.org

Website: www.7amleh.org

Find us on social media: 7amleh

Table of Contents

1 Executive Summary 4

2 Data and Methodology 8

2.1 Purpose and Audience 8
2.2 Method and Evidence Base 8

3 Palestine's Emerging Digital Public Infrastructure 12

4 Human Rights Analysis of Palestine's Digital Transformation Readiness 17

4.1 Legal, Institutional and Governance Readiness 17
4.2 Human Rights, Transparency, Accountability and Inclusive Innovation 17
4.3 Human Rights within National Digital Policy 20
4.4 Infrastructure, Resilience and Structural Constraints 26

5 Conclusion 28

6 Practical Roadmap and Targeted Recommendations 30

6.1 Immediate Priorities: 0-12 Months 30
6.2 Medium-term Priorities: 1-3 years 31
6.3 Long-term Structural and Reconstruction Priorities 33

1 Executive Summary

Palestine is moving beyond isolated digitisation projects towards an integrated digital public infrastructure. This transition is guided by the Digital Palestine Agenda 2030[1], the Digital Government Strategy 2024–2029[2], and the Ministry of Telecommunication and Digital Economy (MTDE) Strategy 2025–2027[3], which prioritise digital government, integration between government systems, inclusion, infrastructure, and emerging technologies. Key developments include the Hukumati e-government service platform, the National Data Carrier and UXP/X-Road data-exchange architecture, iBuraq and e-wallet services, and the framework for electronic transactions and trust services. Other initiatives include the E-Shiraa electronic procurement platform, telecommunications and cybersecurity reforms, plans for a government-wide digital identity alongside iDplus, and a national direction on Artificial Intelligence (AI).

This report assesses Palestine's readiness for digital transformation through a human rights lens. It examines the legal, institutional, technical, and governance foundations supporting current initiatives and their implications for privacy, data protection, freedom of expression, equality and non-discrimination, accessibility, due process, effective remedy, transparency and public participation. It identifies both rights-supporting provisions and areas where broad powers, weak institutional independence, incomplete implementation or legal uncertainty may expose people to exclusion, surveillance, arbitrary restriction or decisions they cannot effectively challenge.

The assessment draws on desk research, a structured review of Palestinian laws, draft laws, Cabinet decisions, policies and regulatory instructions, and 10 interviews with stakeholders from government, technology, telecommunications, civil society, professional bodies and academia. The legal and policy review distinguishes binding legislation from draft provisions and administrative policies and assesses

1 Council of Ministers, State of Palestine (2023) Council of Ministers Decision No. 13 of 2023 Approving the Palestine Digital Agenda 2030 [قرار مجلس الوزراء بالمصادقة على أجندة فلسطين الرقمية 2030م رقم (13) لسنة 2023م]. Ramallah: Council of Ministers.

2 Ministry of Telecommunications and Digital Economy (MTDE) (2024) Draft Digital Government Strategy 2024–2029 [2029–2024 مسودة استراتيجية الحكومة الرقمية]. Ramallah

3 Ministry of Telecommunications and Digital Economy (MTDE) (2025) Strategy of the Ministry of Telecommunications and Digital Economy 2025–2027 [2027–2025 استراتيجية وزارة الاتصالات والاقتصاد الرقمي]. Ramallah

each instrument against legality, necessity, proportionality, independent oversight, transparency, equality, accessibility and effective remedy.

The central finding is that technological and strategic development is outpacing the legal, institutional, and human rights safeguards required to govern integrated digital systems. Palestine, therefore, faces a readiness challenge rather than simply a technology-adoption challenge. Digital platforms, identity systems, data exchange and AI can improve access and efficiency, but they may also increase exclusion, surveillance, error, opaque decision-making and institutional dependency where governance, oversight and remedies remain weak.

The national policies are not purely technical. They recognise digital inclusion, accessibility, data protection, cybersecurity and equitable access. However, these commitments are generally framed as objectives of modernisation, service efficiency, and economic development rather than as enforceable human rights. The policies do not consistently establish independent oversight, human rights impact assessments, meaningful public participation, non-digital alternatives or effective remedies. Commitments to serve all sections of society must therefore be assessed against actual outcomes for people in Gaza, marginalised and remote communities, persons with disabilities, women, older people, children, low-income households and people without reliable connectivity, devices, documentation or access to digital payments.

The most significant gap concerns personal data protection. A draft Personal Data Protection Law was published for consultation and referred to the President in November 2025, but no comprehensive law had been enacted by 1 October 2026. Protections remain dispersed across the Basic Law and sectoral legislation. This is increasingly problematic as integrated government systems, digital identity and AI expand opportunities to link and reuse personal information. A draft Right to Information Law was also consulted on in late 2025. Although the legal direction is promising, essential accountability structures remain incomplete.[4] [5] [6]

4 Ministry of Justice, State of Palestine (2025) Draft Decree-Law on Data Protection [مشروع قرار بقانون بشأن حماية البيانات], third draft. Ramallah: Ministry of Justice.

5 7amleh – The Arab Centre for the Advancement of Social Media (2023a) Position Paper: Personal Data Protection Draft Law by Decree from a Human Rights-Based Perspective.

6 7amleh – The Arab Centre for the Advancement of Social Media (2023b) Procedural Guide to Palestinian Personal Data Protection in the Digital Space.

The Telecommunications Regulatory Authority has begun operating, while the National Cybersecurity Authority was established under Decree-Law No. 8 of 2026, and its Board was approved in July 2026. Decree-Law No. 17 of 2024 and the 2026 licensing regulation have also strengthened the legal basis for electronic trust services. However, these institutions require adequate independence, capacity, resources, procedures and public reporting to provide effective oversight.[7] [8] [9]

Digital payments are among the most mature elements of Palestine's emerging digital infrastructure. The Palestine Monetary Authority has expanded payment infrastructure through iBuraq and e-wallets. By January 2026, around 1.4 million e-wallet accounts were outstanding, including 1.07 million in Gaza, while monthly iBuraq transactions had reached approximately 3.5 million. In Gaza, however, this growth reflects the collapse of conventional banking and cash channels as much as voluntary adoption. Readiness must therefore include consumer protection, fraud prevention, affordability, cash access, connectivity and effective non-digital alternatives. [10] [11]

AI governance is relatively advanced at the policy level. A national AI team, policy and strategy were approved in 2023, while an ethics charter has been reviewed. However, the use of AI in significant public decisions requires binding rules governing legal authority, data sources, discrimination testing, transparency, meaningful human review, auditing, procurement, incident reporting and appeals. [12]

These developments remain constrained by Palestine's lack of sovereign control over telecommunications. The Gaza genocide began when only 2G mobile services were available in the territory, while the 2026 Gaza Rapid Damage and Needs Assessment estimated US$200.7 million in ICT damage, US$346 million in losses and

7 Ministry of Telecommunications and Digital Economy (MTDE) (2026) 'Launch of the Telecommunications Regulatory Authority [انطلاق أعمال هيئة تنظيم قطاع الاتصالات]'.
8 State of Palestine (2024) Decree-Law No. 17 of 2024 on Electronic Transactions and Trust Services [قرار بقانون رقم (17) لسنة 2024م بشأن المعاملات الإلكترونية وخدمات الثقة]. Ramallah: State of Palestine
9 State of Palestine (2026) Decree-Law No. 8 of 2026 on the National Cybersecurity Authority [قرار بقانون رقم (8) لسنة 2026م بشأن الهيئة الوطنية للأمن السيبراني]. Ramallah: State of Palestine.
10 World Bank, United Nations and European Union (2026) Rapid Damage and Needs Assessment: Gaza Strip, April 2026. Washington, DC: World Bank.
11 World Bank, United Nations and European Union (2026) Rapid Damage and Needs Assessment: Gaza Strip, April 2026. Washington, DC: World Bank
12 Ministry of Telecommunications and Digital Economy (MTDE) (2023b) National Artificial Intelligence Policy and Strategy. Approved by the Council of Ministers on 19 June 2023.

the destruction of 81 per cent of sector assets.[13] In the West Bank, Israeli approval for 4G was announced in January 2026, but Jawwal and Ooredoo were still preparing for its launch in August. [14] Readiness, therefore, cannot be separated from spectrum restrictions, equipment access, territorial fragmentation, energy constraints and the reconstruction of Gaza's communications infrastructure. [15]

The report concludes with practical recommendations for rights-respecting digital transformation in Palestine. These include stronger data-protection legislation and independent oversight, clear governance and data-sharing rules, mandatory impact assessments, accessible services and effective non-digital alternatives, transparent complaint mechanisms and safeguards for high-impact AI. The recommendations also address telecommunications access, cybersecurity, institutional capacity and resilient services for Gaza and other underdeveloped areas.

13 World Bank, United Nations and European Union (2026) Rapid Damage and Needs Assessment: Gaza Strip, April 2026. Washington, DC: World Bank.
14 Reuters (2026). Israel approves upgrade to 4G mobile services to Palestinians in West Bank.
15 International Telecommunication Union (ITU) (2024) 'Resolution 1424: Assistance and Support to Palestine for Rebuilding its Telecommunication Sector', in Resolutions and Decisions of the Council 2024. Geneva: ITU.

2 Data and Methodology

2.1 Purpose and Audience

The purpose of this report is to provide a useful reference for other public bodies, private-sector implementers, civil society organisations and development partners. The report asks not only what is being developed, but also whether the necessary legal, institutional, technical and governance conditions exist for these systems to operate safely, inclusively, accountably and consistently with Palestine's human rights obligations. It assesses whether human rights are embedded throughout the design, development, procurement, implementation, and oversight of digital systems, rather than being addressed only after harm occurs. Particular attention is given to privacy and data protection, freedom of expression, equality and non-discrimination, accessibility, due process, public participation, and effective remedy, as well as whether digital transformation serves people in Gaza, marginalised and remote communities, persons with disabilities, women, children, older people and those facing financial, technological or documentation barriers.

2.2 Method and Evidence Base

The assessment combines desk research, a structured review of legal and policy instruments and 10 stakeholder interviews. Documentary evidence was used to identify the formal legal, regulatory, and strategic foundations of digital transformation, while interviews were used to clarify implementation, institutional responsibility, practical safeguards, and the gap between formal commitments and lived experience. The assessment reflects the legal, policy and implementation evidence available up to the final cut-off date of 1 October 2026. The documentary review covered binding legislation, regulations and instructions, as well as adopted and draft policies, strategies and institutional frameworks. Distinguishing between these instruments is important because they carry different levels of legal authority and enforceability.

Table 1 presents the principal instruments reviewed in the assessment.

#	Name	Status	Legal nature
1	**Telecom Law # 37 for the year 2021 (Include latest amendments)**	Adopted (But will be (amended	Legal legislation
2	**MTDE new assigned Tasks by Cabinet 2024**	Adopted	Legal legislation
3	**Electronic Transactions and Trust Services Act 2024**	Adopted	Legal legislation
4	**Cybercrime Law 2018 (Include latest amendments)**	Adopted	Legal legislation
5	**Data Protection Law - Draft v3 2025.pdf**	Draft	Legal legislation
6	**Electronic Government Services System Law 2023**	Adopted	Legal legislation
7	**Interconnection Instructions 2007**	Adopted	Instructions
8	**Instructions on Competition Safeguards in the Telecommunications Sector 2011**	Adopted	Instructions
9	**Information Security Management System 2020**	Adopted	Instructions
10	**Information security policy**	Adopted	Policy
11	**Digital Government Strategy (2024-2029)**	Adopted	Strategy
12	**Public policy for the telecommunications sector (2026-2028)**	Adopted	Policy
13	**Public Policy for the Information Technology Sector 2026-2028**	Adopted	Policy
14	**Competition Law - 2025**	Adopted	Legal legislation
15	**Palestine National Blockchain Policy - project outline v1.030 - Draft - 2025**	Draft	Policy Framework
16	**Radio and Television Station Licensing Instructions 2018**	Adopted	Instructions
17	**Instructions for offers, telecommunications services, and promotional advertisements for 2020**	Adopted	Instructions
18	**Type Approval Instructions 2017**	Adopted	Instructions

19	**Instructions regarding the registration of subscriber data for mobile communication services 2009**	Adopted	Instructions
20	**Guidelines for using frequencies within short-range devices 2022**	Adopted	Instructions
21	**Instructions for regulating value-added services 2016**	Adopted	Instructions
22	**Mobile Number Portability Regulation 2019**	Adopted	Instructions
23	**Draft National Policy for Digital Accessibility in Palestine 2025**	Draft	Policy
24	**Digital Development Plan - Palestine V1**	Adopted	Policy
25	**National AI Strategy**	Adopted	Strategy
26	**National AI policy**	Adopted	Policy
27	**AI Ethical Charter**	Draft	Instructions
28	**Data Classification policy**	Adopted	policy
29	**Data Management policy**	Draft	policy
30	**API Governance Policy**	Draft	policy
31	**Cloud computing first policy**	Draft	policy
32	**The Right to Access to Information Law**	In the Final Adoption Step	Legal legislation
33	**Open Data policy**	Draft	policy
34	**Membership with OIC-Cert**		Cybersecurity Partnerships
35	**Instructions for Digital Asset Management Standards for the Public Sector No. (1) of 2024**	Adopted	policy
36	**Council of Ministers Decision No. (13) of 2023 Approving the Palestine Digital Agenda 2030**	Adopted	Policy
37	**Strategy of the Ministry of Telecommunications and Digital Economy 2025-2027**	Adopted	Policy

Table 1: Palestinian Legal, Regulatory and Policy Framework for Digital Transformation

The table demonstrates that Palestine has developed a substantial body of legislation, instructions, policies and strategies relating to digital transformation. However, the existence of an instrument does not establish that it provides adequate human-rights protection or that it has been effectively implemented. Draft policies and legislation were therefore distinguished from adopted instruments, while non-binding strategies and ethical frameworks were not treated as equivalent to enforceable legal duties.

Documentary analysis alone could not establish how these instruments operate in practice. Therefore, 10 interviews were used to test formal claims, clarify current implementation, and identify safeguards, constraints, and experiences that were not evident in published documents. The interviews included senior representatives and experienced stakeholders from the MTDE, the Palestine Monetary Authority, and the national payments ecosystem; government cybersecurity and e-government functions; technology and telecommunications practice; education; academia; digital innovation; and digital-rights policy. They clarified the implementation status, institutional responsibilities, practical safeguards, service adoption, capacity constraints, and the differences between formal policy and lived experience. Institutional descriptions were triangulated against documentary sources where possible, while stakeholder perceptions were treated as evidence of experience, trust and implementation gaps. The interviews covered four broad perspectives, as shown in Table 2.

Public-sector implementation and policy	Interview 5, 7, 8, 9, 10
Financial infrastructure and payments	Interview 2
Technology and education practice	Interview 3, 6
Academic and user perspectives	Interview 1, 4

Table 2: Interview summary

3 Palestine's Emerging Digital Public Infrastructure

Palestinian policy increasingly treats digital government as an integrated national programme rather than a collection of isolated projects. The Digital Palestine Agenda 2030, Digital Government Strategy 2024–2029 and MTDE Strategy 2025–2027 emphasise interoperable systems, digital identity, electronic payments, open data, inclusion, resilience and AI.[16] [17] [18] Although these policies recognise equitable access, accessibility, data protection, cybersecurity and participation, these concerns are generally framed as conditions for successful digital development rather than as enforceable human rights. This distinction is important because connecting government systems can improve efficiency and access while also magnifying errors, exclusion and misuse across multiple institutions.

Hukumati serves as the principal public-service layer through a unified portal that offers single sign-on, electronic payments, and cash payment options. Interview 8 reported approximately 128 services, 70,000 registered users, and 9,000 completed paid service requests, although adoption remained below initial targets. Public awareness and routine use remain uneven, indicating the need to publish performance and complaint data by service, location and accessibility need (Interviews 4). Hukumati is connected to the National Data Carrier, through which 55 institutions reportedly exchange information using encryption, written authorisation and server-level permissions. However, technical security does not replace legal governance. Public rules are still needed to regulate the purposes of data exchanges, minimisation, retention, correction, onward sharing, auditing, and reporting (Interviews 3, 8, and 9).

Interoperable services also require reliable identification and authentication. iDplus uses facial biometrics, identity documents, and Ministry of Interior records. Yabous[19] shows how this identity system is used in practice. The Ministry of Finance describes

16 Council of Ministers, State of Palestine (2023) Council of Ministers Decision No. 13 of 2023 Approving the Palestine Digital Agenda 2030 [قرار مجلس الوزراء بالمصادقة على أجندة فلسطين الرقمية 2030م رقم (13) لسنة 2023م]. Ramallah: Council of Ministers. Available at: https://mjr.ogb.gov.ps/Decrees/ViewText/33525/

17 Ministry of Telecommunications and Digital Economy (MTDE) (2024) Draft Digital Government Strategy 2024–2029 [مسودة استراتيجية الحكومة الرقمية 2024–2029]. Ramallah

18 Ministry of Telecommunications and Digital Economy (MTDE) (2026) 'Launch of the Telecommunications Regulatory Authority [انطلاق أعمال هيئة تنظيم قطاع الاتصالات]'.

19 Yabous Finance is a Ministry of Finance and Planning application for authorised public employees. It operates as a closed payment system where balances can be used to pay approved billers but cannot be withdrawn as cash or transferred outside the system. https://www.pmof.ps/internal.php?route=yabous

it as a closed government payment application for authorised public employees to pay approved billers. Interview 2 explained that employees register through iDplus and can use credited balances to pay participating service providers. Interview 1 observed that digital records make it easier to measure uptake and trace payments, while raising concerns about access to financial information and public trust. These accounts point to a need for clear rules on what information the Ministry of Finance, identity providers, and billers can access, as well as accessible routes for correcting errors or disputing payments. Electronic signatures remain under development pursuant to Decree-Law No. 17 of 2024 and the 2026 licensing regulation. Before digital identity becomes a gateway to essential services, institutions should disclose their legal basis, data practices, retention periods, accessibility arrangements and appeal routes (Interviews 1, 3, and 6)[20] [21].

Digital payments are among Palestine's most mature shared systems. E-Sadad, iBuraq, the Mawtini switch, e-wallets and point-of-sale terminals connect 13 banks and five payment companies. Interviewee 2 reported approximately 50,000–60,000 daily E-Sadad transactions and 60,000 point-of-sale terminals.[22] In Gaza, reliance on digital payments has increased due to cash shortages, making fraud protection, transparent fees, accessible interfaces, consumer redress, and non-digital alternatives particularly important[23]. Electronic procurement is another developing component. E-Shiraa was launched in June 2026 to cover procurement from planning and tender publication through contract management and reporting. Its contribution to transparency depends on whether information is timely, searchable, and complete; interfaces are accessible; and complaint mechanisms function effectively[24]. These systems form part of a wider landscape that includes government information systems, cybersecurity institutions, postal infrastructure, digital access initiatives, and capacity-building programmes.

Table 3 maps the principal services and initiatives identified in the Digital Government Strategy, distinguishing planned initiatives from those that were subsequently confirmed operational.

20 Council of Ministers, State of Palestine (2024) Decision on the Functions and Responsibilities of the Ministry of Telecommunications and Digital Economy, Ramallah: Council of Ministers.
21 Ministry of Finance and Planning. Yabous Finance: An official government financial application.
22 State of Palestine (2022) Decree-Law No. 41 of 2022 on National Payments [قرار بقانون رقم (41) لسنة 2022م بشأن المدفوعات الوطني]. Ramallah: State of Palestine.
23 World Bank (2026) Economic Update on the West Bank and Gaza, May 2026. Washington, DC: World Bank.
24 E-Shiraa: The Palestinian Government Procurement Portal. Available at: https://www.shiraa.gov.ps/en-us

Area	Digital service/ initiative	What it provides
Citizen and business services	Hukumati (حكومتي)	Unified online portal for government-to-citizen and government-to-business services. At the time of the strategy, it provided 28 services, including 15 paid services, with Single Sign-On and online payment.
	Single Sign-On (SSO)	One account/identity to access multiple government services rather than separate logins for each ministry.
	Electronic payment through Hukumati	Allows citizens to pay fees for government services electronically.
Government data exchange	National Data Carrier – UXP/X-Road	Secure exchange of information between government databases so citizens do not have to repeatedly provide the same information. In 2023, it supported 60 integrated services across 12 institutions: 32 G2G and 28 C2G services.
	Zinnar interoperability framework	Common standards for how government institutions structure and exchange information.
Identity and trust	Electronic authentication and signatures	Development of electronic authentication, electronic signatures, digital certificates and government trust services.
	Digital identity – planned	The strategy proposes a trusted digital identity that can uniquely identify citizens when accessing government services. This was a strategic initiative rather than a fully implemented service at the time of the report.
Public procurement	Unified electronic government procurement system	Digitisation of procurement from planning and tendering through contract monitoring and payment. The report describes this as being developed to cover government institutions and municipalities.

Information and transparency	Open Government Data Portal	Makes government datasets available electronically for public access, research, innovation and transparency. The report says datasets from more than 39 government entities had been published.
Emergency services	Unified 911 Emergency Response Centre	Digital/centralised emergency-response service bringing together civil defence, ambulance and police services.
Postal services	Palestinian Postal Code System	Digital geographic addressing system assigning unique codes to buildings and locations to improve public and private service delivery.
	EOS parcel-tracking system	Allows tracking of parcels from selected international/Chinese online stores and provides information about parcel location and delivery status.
Access and inclusion	Digital Access Points	Proposed use of around 100 post offices as assisted one-stop access points where people can obtain help accessing e-government services.
	National Digital Accessibility Policy	Intended to ensure digital services in government, health, education, commerce and other sectors are accessible, including to persons with disabilities.
Cybersecurity	PALCERT	Government computer emergency-response service dealing with cybersecurity incidents, security monitoring, threats and vulnerabilities.
	National Cybersecurity Authority	An institutional mechanism is proposed in the strategy to regulate and coordinate cybersecurity across the government and other sectors.
Government infrastructure	National Data Centre and Government Private Cloud	Hosting infrastructure for government systems and services; 10 ministries were already using the private cloud by the end of 2022.

	Central Government Email	Secure centralised email infrastructure for government institutions, designed for up to approximately 45,000 accounts.
Business / ICT sector	ICT companies platform	Digital directory/platform covering ICT and postal-sector businesses, designed to connect firms with programmes and initiatives and increase their visibility. The strategy reported 1,723 establishments on the system.
Digital skills and the economy	TechStart	Supports Palestinian technology companies, employment, skills, market access, and investment.
	Million Programmers initiative	Digital-skills initiative teaching programming and technology skills to children and young people.

Table 3: Principal Digital Government Services, Infrastructure and Strategic Initiatives in Palestine

The range of initiatives demonstrates the breadth of Palestine's digital-transformation programme. It also shows why readiness cannot be assessed solely by the existence of individual platforms. As these services become increasingly connected, weaknesses in identity management, data governance, accessibility, cybersecurity or complaint mechanisms may affect multiple institutions and services simultaneously. The following section, therefore, assesses whether the wider legal, institutional, and human rights framework is capable of governing this interconnected ecosystem.

4 Human Rights Analysis of Palestine's Digital Transformation Readiness

This section examines whether Palestine's expanding digital ecosystem is supported by coherent legislation, capable institutions, accountable governance, effective rights protections and resilient infrastructure. The assessment focuses on privacy, surveillance, freedom of expression, accessibility, non-discrimination, transparency, effective remedy and equitable access to essential services.

4.1 Legal, Institutional and Governance Readiness

Palestine has developed a substantial legal and policy framework covering telecommunications, competition, electronic government, electronic transactions, trust services, cybersecurity, information security, accessibility, AI and data governance. The 2024 Cabinet decision also assigns MTDE broad responsibilities for digital-economy policy, infrastructure, cybersecurity, digital assets, licensing, competition and user protection. The framework is therefore more developed than a narrative of legal absence would suggest. Its principal weakness is fragmentation. Although instruments have different legal statuses, oversight responsibilities overlap, and several important protections remain in draft policies rather than binding legislation.

The following chart budget demonstrates that digital inclusion is recognised as a distinct strategic objective, with approximately NIS 10.17 million allocated across 2025–2027. However, the largest allocation is directed towards digital infrastructure. This is understandable given Palestine's connectivity and reconstruction needs, but infrastructure expenditure does not automatically produce equitable access. Implementation reporting should therefore demonstrate who benefits from the expenditure, which barriers are removed, and whether inequalities related to geography, disability, gender, age, and income are reduced.

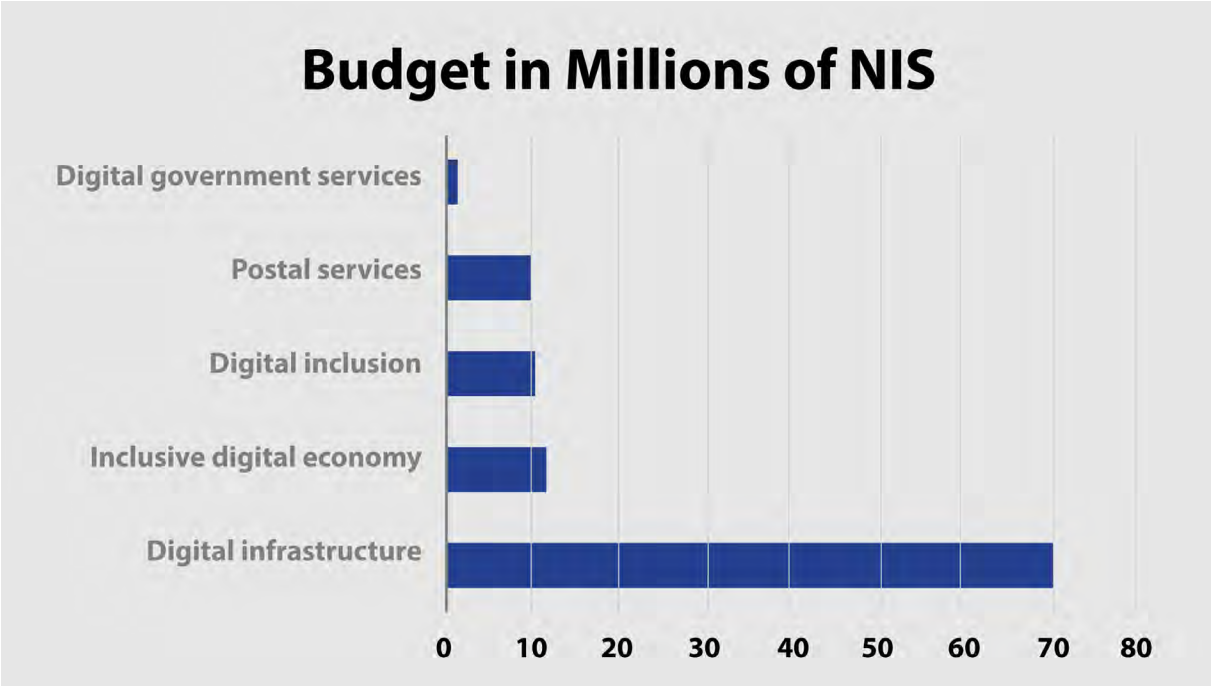


Chart 1: MTDE planned budget by strategic objective

Source: MTDE Strategy 2025–2027. Figures are planned allocations, not actual expenditure[25]

The telecommunications framework supports universal service, competition, affordability, communications confidentiality and complaint rights. The 2007 Interconnection Instructions and 2011 Competition Safeguards Instructions reinforce non-discrimination, infrastructure sharing and controls on market dominance. Their effectiveness nevertheless depends on regulatory independence and enforcement. Interview 5 highlighted the institutional context directly: "Governmental and financial weakness is another major challenge. Even when efforts within institutions are combined to achieve fundamental changes, the financial situation remains an obstacle." Staff losses, financial constraints and the imbalance between government institutions and powerful market actors can therefore weaken enforcement even where formal rules exist.

The 2023 Government Electronic Services System Decree-Law provides a legal basis for secure, continuous services, confidentiality, payment transparency, complaints,

25 Ministry of Telecommunications and Digital Economy (MTDE) (2025) Strategy of the Ministry of Telecommunications and Digital Economy 2025–2027 [2027–2025 استراتيجية وزارة الاتصالات والاقتصاد الرقمي]. Ramallah: MTDE.

and the continued availability of pre-existing service routes. However, it does not establish comprehensive accessibility standards, an independent review or detailed rights concerning shared government data. This matters because Hukumati and the National Data Carrier connect services, identity, payments and institutional databases. The Hukumati official explained that readiness extends beyond connectivity: "The greatest challenge, however, is weak infrastructure. When discussing infrastructure, we do not mean only internet access and telecommunications. We also mean systems infrastructure, including firewalls, servers, backup systems, disaster-recovery systems, and related requirements" (Interview 8). The 2024 Electronic Transactions and Trust Services Decree-Law provides important protections concerning privacy, service quality, complaints, security breaches and continuity when providers cease operating. Nevertheless, the supervisory authority combines regulatory, licensing, inspection and complaint functions, while its board includes executive-government representatives. Institutional separation, published decisions, and external oversight are therefore necessary to protect independence and avoid conflicts of interest.

The most significant legislative gap remains the lack of comprehensive personal data protection. The 2025 draft contains purpose limitation, data minimisation, access, correction, deletion, portability, breach notification, objection rights and restrictions on automated decisions. It also requires impact assessments and data-protection officers in higher-risk settings. These protections should be retained, but the law should establish a specialised and independent authority, narrow exemptions for criminal investigations and public-sector sharing, and strengthen protections for children, biometric data and affected individuals. Article 13 of the draft also requires the authority to determine objections within 15 days, but treats administrative silence as a rejection, while judicial appeal remains available. This risks delaying effective remedy. Article 25's data-sharing exceptions should likewise be subject to legality, necessity, proportionality, documentation and independent review.[26]

Cybercrime legislation protects users and systems against unauthorised access, fraud, interference and exploitation. However, broad content offences and extensive powers relating to surveillance, retention, compelled disclosure, and website blocking pose risks to privacy, journalism, and freedom of expression. These powers require

26 Ministry of Justice, State of Palestine (2025) Draft Decree-Law on Data Protection [مشروع قرار بقانون بشأن حماية البيانات], third draft. Ramallah: Ministry of Justice.

precise thresholds, judicial authorisation, minimisation, time limits, transparency reporting and effective challenge mechanisms. Institutional cybersecurity capacity is developing. GovSOC monitors security logs, Hukumati infrastructure and connected government systems. Interviewee 9 stressed the importance of implementation: "We have an Information Security Policy and an Information Security Management System, both approved by the Council of Ministers in 2021. We tell institutions that they must follow and implement these policies to achieve at least a basic level of security." Nevertheless, cybersecurity must remain connected to data protection, transparency and remedy rather than being treated solely as technical system protection.

4.2 Human Rights, Transparency, Accountability and Inclusive Innovation

Digital transformation can improve access to services while also expanding surveillance, exclusion and administrative control. One private-sector practitioner captured this tension: "Digital transformation is not only about making life easier. Even an educated person examining digital transformation may see it as a double-edged sword" (Interview 3). Human-rights compliance must therefore be assessed through the actual design and implementation of systems, not merely through general policy commitments. Privacy protections currently vary across sectors. The Electronic Government Services System Decree-Law protects information submitted through government platforms, while telecommunications legislation protects subscriber information and the secrecy of communications. The draft Data Protection Law would create a broader framework, but it remains unenacted. A consistent and enforceable privacy baseline should apply across Hukumati, digital identity, payments, data exchange, telecommunications and AI. Digital identity illustrates the risks of connected systems. iDplus uses facial biometrics, scanned identity documents and Ministry of Interior records. Interviewees raised concerns about location access, financial visibility and the potential for tracking. Before digital identity becomes necessary for essential services, responsible institutions should disclose their legal basis, data fields, biometric practices, retention periods, security arrangements, accessibility testing and appeal routes.

Digital payments demonstrate both the benefits and dependencies of shared infrastructure. The payments representative explained: "Palestine has five licensed payment companies and 13 banks. Any government service connected to E-Sadad

becomes available to citizens regardless of the bank or electronic wallet they use" (Interview 2). This interoperability improves access, but dependence on electricity, connectivity, devices and digital identity can disadvantage people in Gaza, remote communities, low-income households, older people and persons with disabilities. Fraud protection, transparent fees, consumer redress and cash or assisted alternatives must therefore remain available.

Accessibility should be treated as a legal entitlement rather than a discretionary design feature. Interviewee 1 concluded: "Therefore, although some infrastructure exists, we are not yet fully capable of achieving complete digital transformation." Interviewee 6 similarly identified "the availability of technical resources in every household" as a central challenge. The Draft National Digital Accessibility Policy (2023) offers a strong foundation through its recognition of the Convention on the Rights of Persons with Disabilities and its engagement with disability organisations.[27] It should be adopted with funding, procurement requirements, independent testing and enforceable complaint procedures.

Digital inclusion also requires skills and meaningful participation. The digital-innovation representative emphasised that "Our most important resource is our human capacity. All groups need digital literacy, including older people, girls and women, and people living in remote areas" (Interview 7). Digital literacy should therefore accompany service development, supported by assisted access, low-bandwidth interfaces and non-digital alternatives.

Transparency and remedies remain fragmented. Telecommunications, Hukumati, trust services and the draft Data Protection Law provide separate complaint routes, but users may struggle to identify the responsible institution or escalate unresolved cases. Remedies should include reasoned decisions, realistic time limits, independent review, and powers to correct data, restore access, stop unlawful processing, and compensate for harm. Institutions should also publish service performance, complaints, impact assessments, procurement information and data-sharing registers. The government reports that human rights are incorporated into policymaking. Interviewee 10 highlighted that "Human rights are expressly considered and mentioned, although they are also embedded in the substance of

27 Ministry of Telecommunications and Digital Economy. The National Digital Accessibility Policy in the State of Palestine: A Consultative Workshop.

the policies." This commitment is important, but must be assessed against binding provisions, evidence of implementation, and available remedies. Public consultation should include publication of draft texts, stakeholder submissions, government responses and implementation updates.

AI governance presents similar challenges. Palestine has adopted a national AI policy and strategy and developed an ethical charter with input from legal experts and civil society. The innovation centre also plans to use sandboxes for testing emerging technologies. However, policy ambition should not be confused with operational safeguards. High-impact AI requires a public register, clear legal authority, human rights impact assessments, discrimination testing, accessible explanations, meaningful human review, independent audit, and appeal. Sandboxes should test these safeguards rather than exempting projects from them.

4.3 Human Rights within National Digital Policy

The Digital Palestine Agenda 2030 and the MTDE Strategy 2025–2027 contain important human-rights-related commitments. They address digital inclusion, equitable access to services, data protection, cybersecurity, digital literacy and the needs of women, young people, persons with disabilities and marginalised communities. Nevertheless, the policies do not consistently adopt a human-rights-based approach. Privacy, equality, accessibility, and participation are generally presented as factors that support service delivery, public confidence, and economic development rather than as enforceable rights. The strategies do not systematically require human rights impact assessments, independent oversight, necessity and proportionality tests, public disclosure of data-sharing arrangements, non-digital alternatives or accessible complaint and appeal mechanisms. Their indicators also concentrate mainly on infrastructure, institutional outputs, service availability, skills, and adoption, rather than on exclusion, discriminatory effects, privacy violations, or the effectiveness of remedies.

Commitments to include all sections of society, therefore, require closer examination. Broad references to inclusion do not establish whether digital transformation adequately serves people in Gaza, displaced communities, Area C, refugee camps, remote locations, older people, children, low-income households, people without devices or official documentation, or individuals unable to use biometric identity

and digital-payment systems. A rights-based implementation framework should identify these groups explicitly, collect appropriately disaggregated data, involve affected communities in system design and preserve assisted and non-digital routes to essential services.

The central gap is therefore not the complete absence of human-rights considerations, but the limited conversion of general commitments into enforceable protections. The policies recognise several rights-related concerns, but they do not consistently specify who holds the corresponding rights, which institution bears responsibility, how implementation will be independently scrutinised or what remedy is available when harm occurs. Palestine's digital strategies may consequently be described as socially aware and increasingly inclusive, but not yet fully rights-based.

Assessing these policies requires distinguishing between recognising a human rights concern and providing the safeguards necessary to protect that right in practice. References to inclusion, accessibility, data protection, or participation are important, but they do not, by themselves, establish an enforceable entitlement, an accountable institution, or an effective remedy. Table 4, therefore, compares the positive commitments in the national policies with the remaining human rights gaps and the evidence needed to assess implementation.

Policy area	Positive policy commitment	Human-rights gap	Evidence needed
Digital inclusion	Broad commitment to inclusion and equitable access	Groups, barriers and enforceable entitlements are not consistently defined	Service use and completion by location, gender, disability, age and income
Accessibility	Persons with disabilities and accessible services are recognised	Accessibility is not consistently supported by binding standards, independent testing and remedies	WCAG testing, disabled-user participation, complaints and corrective action
Privacy and data protection	Protection of digital data is recognised as a strategic priority	Comprehensive legislation and sufficiently independent oversight remain incomplete	Data registers, impact assessments, breach reports and complaint outcomes

Digital identity	Identity systems support integrated services	Limited safeguards concerning biometrics, tracking, exclusion and alternative access	Legal basis, data fields, retention periods, biometric safeguards and appeals
Artificial intelligence	AI strategy, ethical direction and capacity building are included	Limited binding requirements for high-impact uses	AI register, discrimination testing, audits, explanations and human review
Freedom of expression	Digital content and cybersecurity are addressed	Limited examination of surveillance, blocking and restrictions on legitimate expression	Authorisation rules, transparency reports, challenges and judicial oversight
Public participation	Cooperation with civil society and other stakeholders is encouraged	Partnership does not necessarily provide meaningful rights-holder participation	Published consultations, submissions, responses and implementation updates
Transparency	Monitoring, indicators and periodic reporting are envisaged	Public disclosure duties are insufficiently detailed	Published indicators, budgets, procurement records, audits and impact assessments
Complaints and remedies	Some systems and sectors provide complaint routes	Routes remain fragmented, and independent escalation is unclear	Complaint numbers, resolution times, outcomes and corrective measures
Non-digital access	Some pre-existing service routes remain available	Policies do not consistently guarantee effective alternatives to digital systems	Evidence on paper, telephone, cash, assisted and face-to-face access
Emergency resilience	Infrastructure recovery and service continuity are recognised	Rights during outages, displacement and loss of documents receive limited detail	Continuity tests, low-bandwidth services, emergency access and Gaza-specific results

Table 4. Human-rights assessment of the Digital Palestine Agenda 2030 and the MTDE Strategy 2025–2027.

This comparison shows that the main weakness is not the complete absence of human-rights concerns, but their limited operationalisation. Several rights-related principles are recognised, yet they are not consistently translated into binding standards, independent oversight, measurable outcomes or accessible remedies. This limitation becomes particularly important when considering whether the broad commitment to include all sections of society addresses the distinct barriers experienced by specific population groups. Table 5 distinguishes groups explicitly named in policy from those addressed only indirectly or given limited attention. It also identifies where broad commitments need more specific measures, such as accessibility standards, affordable access, alternative ways to use essential services, and safeguards against surveillance and misuse of personal data.

Population group	Degree of recognition	Remaining concern
Women	Explicitly recognised	Limited gender-disaggregated indicators and limited attention to gender-specific digital harms
Young people	Explicitly recognised	Emphasis is mainly on skills, employment and entrepreneurship rather than privacy and participation
Persons with disabilities	Explicitly recognised	Accessibility standards, independent testing, procurement rules and remedies require stronger implementation
Marginalised communities	Broadly recognised	The category is not consistently defined by geography, income, displacement or service barrier
People in Gaza	Recognised through reconstruction and infrastructure priorities	Insufficient detail on prolonged outages, displacement, emergency access and non-digital alternatives
People in remote areas and Area C	Partially recognised through geographical inclusion	Limited location-specific targets, budgets and performance reporting
Low-income households	Recognised in the Digital Palestine Agenda	Affordability of connectivity, devices and service charges needs clearer measurement

Older people	Limited specific recognition	Digital-literacy support, assisted access and non-digital alternatives are insufficiently detailed
Children	Limited specific safeguards	Data protection, profiling, consent, age-appropriate design and AI risks require explicit attention
Refugees and displaced people	Limited explicit treatment as a distinct group	Loss of documents, unstable residence and interrupted connectivity may prevent access
People without smartphones or the internet	Indirectly addressed	No consistent entitlement to assisted, telephone, paper or face-to-face services
People without bank accounts or digital payments	Partially addressed through payment alternatives	Cash access, fees, failed payments, and consumer redress require stronger safeguards
People unable to use biometrics	Not adequately addressed	Alternative authentication and appeal routes should be guaranteed
Journalists, activists and human-rights defenders	Not treated as a distinct at-risk group	Surveillance, compelled disclosure, content restrictions and freedom of expression need stronger safeguards

Table 5: Assessment of who is included

The policies seek universal inclusion but do not yet demonstrate that every group can access digital services safely and equally. Explicitly naming a group is only the first stage of inclusion. A rights-based approach must also identify the barriers affecting that group, assign institutional responsibility, allocate resources, measure outcomes and provide an effective remedy when exclusion occurs. These inclusion gaps are closely connected to the wider weaknesses in transparency, accountability and remedy discussed below, because people cannot effectively challenge exclusion, data misuse or inaccessible services without clear information, identifiable institutional responsibility and independent complaint mechanisms.

4.4 Infrastructure, Resilience and Structural Constraints

Digital transformation in Palestine is shaped by conditions beyond domestic policy control, including restricted spectrum, delayed mobile generations, equipment restrictions, territorial fragmentation and the destruction of infrastructure. An

academic interviewee summarised the position: "We therefore face many barriers to digitalisation. I believe the university, schools, and government are all trying, but we need time, funding, and better infrastructure" (Interview 4). The West Bank's delayed access to modern mobile technology has widened the gap between fixed and mobile connectivity. Limited spectrum, permit restrictions and indirect infrastructure routes increase costs, weaken competition and discourage investment. Digital services must therefore be designed for the networks and devices people actually possess, using low-bandwidth interfaces, realistic concurrency testing and assisted service routes.

Gaza presents the most severe test of rights-based readiness. Digital payments and distance education have helped maintain access during the crisis, but electricity loss, network destruction, device scarcity and disrupted banking systems have also exposed their fragility. Services that assume continuous electricity, reliable broadband, valid identity documents or normal banking conditions cannot be considered universally accessible.

Connectivity in Gaza is directly connected to the rights to life, information and humanitarian assistance. Reconstruction should therefore include redundant networks, emergency power, secure public-access points, interoperable standards and contingency arrangements. Any proposal for a shared, government-monitored network should also include strict limits on surveillance, independent governance, transparent access conditions, structural separation between network management and monitoring, and effective remedies.

The postal-code project's use of a national map rather than complete dependence on Google or Apple illustrates an effort to strengthen digital autonomy. Similar principles should guide cloud infrastructure, data hosting, identity, payments, and government systems: open standards, government control over encryption keys, supplier exit plans, redundancy, and protection against vendor lock-in.

Infrastructure resilience is therefore inseparable from human rights. A system cannot be considered ready merely because it functions under normal conditions. It must remain accessible, secure and accountable during outages, displacement, conflict and financial crisis. This requires investment not only in platforms and hardware but also in institutional capacity, local expertise, independent oversight and inclusive service alternatives.

5 Conclusion

Palestine is building important components of a modern digital state under extraordinarily constrained political, economic and infrastructural conditions. Hukumati, the National Data Carrier, electronic payment systems, cybersecurity monitoring, postal infrastructure and emerging identity and AI initiatives demonstrate meaningful progress towards integrated digital government. Several systems are already operational, simplifying access to services, supporting secure data exchange, expanding payment options and strengthening institutional coordination.

However, technological progress remains uneven and is outpacing some of the legal, institutional and human rights safeguards needed to govern interconnected systems. Institutional capacity varies across ministries, municipalities and sectors, while service availability does not necessarily translate into widespread or equitable use. Accessibility barriers, limited digital literacy, privacy and surveillance concerns, fragmented accountability and inadequate complaint mechanisms may prevent people from benefiting equally. Territorial fragmentation, occupation-related restrictions, unreliable electricity and connectivity, and the destruction of infrastructure in Gaza further constrain access and continuity.

The assessment, therefore, identifies a readiness challenge that extends beyond the availability of technology. Digital systems must have a clear legal basis, identifiable institutional responsibility, proportionate data practices, accessible service routes, effective security safeguards and independent oversight. People must also be able to understand how systems affect them, correct errors, challenge decisions, and obtain remedies. These requirements are particularly consequential for children, persons with disabilities, older people, low-income households, displaced communities and people facing weak connectivity or difficulties accessing identity documents and payment services.

Palestine's principal digital policies provide a foundation for addressing these concerns through their commitments to inclusion, accessibility, data protection, cybersecurity and equitable access. Yet these commitments are not consistently translated into enforceable entitlements, funded institutional responsibilities, measurable human rights outcomes or effective remedies. The next stage of digital transformation should

close this gap between policy ambition and protection in practice. Progress should be assessed through evidence of who can access services safely and affordably, who remains excluded, how personal information is used and whether institutions respond effectively when harm occurs.

Addressing these gaps requires a sequenced programme of action. Some protections can be strengthened immediately within existing systems, while others depend on sustained legislative reform, institutional development and investment. Structural constraints, particularly those affecting telecommunications access and Gaza's reconstruction, also require action beyond domestic digital-service reform. The recommendations that follow translate the assessment into immediate, medium-term and long-term priorities, linking the expansion of digital public infrastructure to the safeguards and capacities necessary for it to serve people safely, equitably and accountably.

6 Recommendations and Practical Roadmap

The report findings support a sequenced roadmap. Immediate measures should close the most consequential gaps in rights and accountability while improving the usability of systems already in operation. Medium-term reforms should strengthen institutions, workforce capacity, and shared standards. Structural recommendations should address the occupation-related and crisis conditions that domestic software reform cannot resolve.

6.1 Immediate Priorities: 0-12 Months

Priority action	Lead and partners	Why it matters	Timing
Enact a revised data-protection law with independent oversight and stronger safeguards for children, biometrics, breaches and automated decisions.	Government, President, ministries and civil society	Establishes enforceable rights across digital systems.	Immediate
Publish a digital public infrastructure governance charter and register for major government systems and high-impact AI.	MTDE and Cabinet	Clarifies ownership, purpose, data use and oversight.	months 0-6
Require data protection, human rights, and accessibility impact assessments for high-impact systems.	MTDE, the Justice Ministry and oversight bodies	Introduces safeguards before procurement and deployment.	0-12 months
Issue binding inter-agency data-sharing rules.	MTDE, Justice Ministry and data-governance authority	Regulates access, retention, correction, and onward sharing.	months 0-12
Adopt government-wide accessibility standards and preserve non-digital alternatives.	MTDE, public institutions and disability organisations	Prevents exclusion from essential services.	months 0-12
Publish service-level Hukumati performance and complaint data.	MTDE and service-owning institutions	Measures user experience and outcomes.	months 0-12

Adopt interim rules for high-impact public-sector AI.	MTDE, Cabinet and oversight bodies	Requires impact assessment, human review, audit and appeal.	months 0-12
Review cybercrime provisions on content, surveillance, disclosure, retention and blocking.	Justice sector, MTDE, legislature and civil society	Protects privacy, expression and due process.	months 0-12
Issue implementing rules for accessibility, data exchange, breach notification and independent complaints.	Cabinet, MTDE, oversight bodies and civil society	Converts general safeguards into enforceable duties.	months 0-12

Table 6: Immediate Priorities for Rights-Respecting Digital Transformation in Palestine

6.2 Medium-term Priorities: 1-3 years

Implementation of the MTDE Strategy 2025–2027 depends on whether planned financial commitments are converted into adequately resourced programmes and measurable outcomes. Planned expenditure increases substantially in 2026 and remains at a similar level in 2027. This creates a need for transparent reporting that distinguishes between allocated budgets, actual expenditure, completed activities, and resulting human rights outcomes. Chart 2 shows MTDE planned development and operational expenditure for each year in millions of NIS.

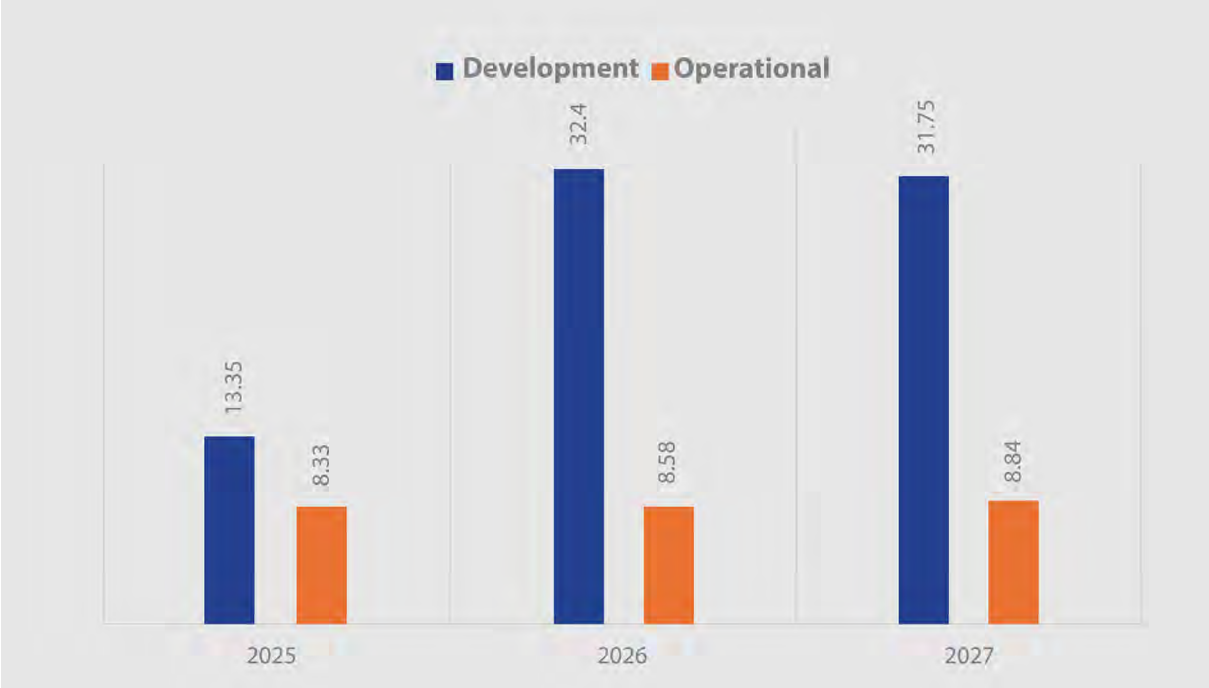


Chart 2: Annual distribution of the MTDE planned budget

Source: MTDE Strategy 2025–2027. Figures are planned allocations in millions of NIS[28]

The planned increase in development expenditure should be accompanied by sufficient operational funding for oversight, accessibility testing, cybersecurity, complaints, public participation and system maintenance. Otherwise, Palestine may develop new platforms and infrastructure without establishing the continuing institutional capacity required to protect rights and respond to harm. The following priorities focus on establishing these foundations.

» **Operationalise independent oversight.**

Ensure the Telecommunications Regulatory Authority, the National Cybersecurity Authority, and trust-services supervision have adequate staffing, budgets, published procedures, reporting duties, and clear coordination arrangements. A future data-protection authority should be institutionally independent and capable of supervising both public and private processing. Publish clear escalation arrangements linking service complaints, payment disputes, cybersecurity incidents, and data-protection complaints.

» **Institutionalise common architecture, data stewardship, and procurement controls.**

Create or formalise a cross-government architecture function to approve reusable components, interoperability standards, data-sharing agreements, and the procurement of high-risk technology. Each connected institution should appoint accountable data stewards, maintain data quality and access records, and plan for maintenance, staff retention, vendor exit, and legacy-system replacement.

» **Move from service counts to service equity indicators.**

Publish Hukumati registrations, completed and abandoned transactions, processing time, outages, accessibility testing, user assistance, complaints, closure times, and outcomes by service and location were lawful and safe. Use these data to redesign services and evaluate whether cash, assisted, telephone, paper, and low-bandwidth routes remain effective.

28 Ministry of Telecommunications and Digital Economy (MTDE) (2025) Strategy of the Ministry of Telecommunications and Digital Economy 2025–2027 [استراتيجية وزارة الاتصالات والاقتصاد الرقمي 2025–2027]. Ramallah: MTDE

» **Strengthen transparency by default.**

Enact a robust right-to-information framework and require the proactive publication of digital policies, procurement records, impact assessments, system registers, audit summaries, and major service incidents, while protecting legitimate security information.

» **Build participation into the digital public infrastructure lifecycle.**

Require structured consultation with civil society, disability organisations, older people, rural and remote communities, Gaza-based users, private implementers, educators, and affected professional groups before major systems are approved and at review points after deployment. Publish consultation submissions, government responses, and implementation status.

» **Create a national public-sector AI assurance function.**

This could sit within an appropriate independent or cross-government structure and should maintain the AI register, define risk tiers, approve high-impact assessments, set audit requirements and coordinate incident reporting.

6.3 Long-term Structural and Reconstruction Priorities

Palestine's digital transformation should be treated as a public-governance and human-rights project, not only a programme of technological modernisation. Investment in infrastructure must be accompanied by legal safeguards, independent oversight, inclusive design and sustainable local capacity. Long-term priorities should include:

» Treat telecommunications access as foundational public infrastructure by securing spectrum, modern equipment and resilient connectivity for digital public services.

» Embed digital rights into Gaza's reconstruction by requiring accessibility, security, emergency power, redundancy and service continuity in all digital infrastructure.

» Design for degraded conditions by providing low-bandwidth, assisted and contingency access during internet outages, electricity shortages or loss of devices and documents.

» Ensure donor financing supports governance and technology by funding legal

safeguards, accessibility, cybersecurity, public participation and local expertise alongside infrastructure.

» Embed human rights across digital systems by integrating privacy, freedom of expression, non-discrimination, accessibility and effective remedy into their design and operation.

» Strengthen independent oversight and participation by involving civil society and affected communities and ensuring access to independent complaints and remedies.

Contact Us:

info@7amleh.org | www.7amleh.org

Our Social Media Pages: 7amleh