COMPREHENSIVE POLICY ANALYSIS OF CAMBODIA'S DIGITAL TRANSFORMATION

A rights-holder centred analysis under Oxfam's Rights in a Digital Age (RiaDA) framework

This report examines whether Cambodia's digital transformation agenda is accompanied by protections for the rights of the people it affects. It draws on a review of thirty national laws, policies and strategies, twenty key informant interviews and four focus group discussions, and sets out thirty recommendations addressed to the government bodies concerned.

This research was written by Adrienne Ravez-Men as part of the Recentering the Civic Internet Through Partner Engagement (ReCIPE) project, co-funded by the European Union. The research reports are written to share research results, to contribute to public debate and to invite feedback on development and donor humanitarian policy and practice. They do not necessarily reflect Oxfam and donor policy positions. This publication was co-funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

This publication is copyright but the text may be used for the purpose of advocacy, campaigning, education and research provided that the source is acknowledged in full. The copyright holder requests that all such use be registered with them for impact assessment purposes. For copying in any other circumstances, or for re-use in other publications, or for translation or adaptation, written permission must be secured from Oxfam.

Published 15 October 2026 by Oxfam in Cambodia
©All rights reserved.

Oxfam in Cambodia
The Point, 3F, No. 113C, Mao Tse Tung Blvd., Tuol Svay Prey I,
Being Keng Kang, Phnom Penh, Cambodia.
(855) 23 885 412 / (855) 23 885 413
info.cambodia@oxfam.org
www.cambodia.oxfam.org

RECIPE Recentering The Civic Internet Through Partner Engagement
Co-funded by the European Union
CCC Cooperation Committee for Cambodia / Comité de Coopération Pour le Cambodge
OXFAM

ACKNOWLEDGEMENTS

Oxfam in Cambodia thanks the people who took part in the key informant interviews, the focus group discussions and the validation workshop of 10 September 2026, for their time and for sharing their experience. We thank the Khmer-speaking research team who facilitated the focus group discussions, and the Cooperation Committee for Cambodia (CCC) for co-organising the validation workshop. We also thank [names and roles of Oxfam staff who reviewed the report] for their comments on earlier drafts. This research was carried out as part of the Recentering the Civic Internet Through Partner Engagement (ReCIPE) project, co-funded by the European Union.

Contents

1. Executive summary 5
2. Introduction and background 7
2.1 The assignment 8
2.2 Context 8
2.3 Rights-holders at the centre 9
2.4 Scope 9
2.5 Structure of this report 9
3. Methodology 10
3.1 Analytical framework 10
3.2 Desk review and policy mapping 10
3.3 Primary qualitative research 10
3.4 Thematic analysis and triangulation 11
3.5 Strategic recommendations and prioritisation 11
3.6 Validation 12
3.7 Consent, transparency, data management, attribution and confidentiality 12
4. The national policy landscape 13
4.1 The policy framework 13
4.2 Comparison with international and regional standards 14
4.3 SWOT analysis of the policy environment 16
5. Pillar-by-pillar analysis 17
5.1 Access and Equity 17
5.2 Security and Digital Civic Space 18
5.3 Responsible Data Use and Privacy 20
5.4 Automation and the Future of Work 21
5.5 Governance 22
5.6 Findings outside the framework 24
6. Inclusion and systemic barriers 25
6.1 Gender 25
6.2 Rural communities 25
6.3 Indigenous communities 25
6.4 People with disabilities 26
6.5 Across the four themes 26

7. Conclusions 27
8. Recommendations 29
8.1 Where to begin 29
8.2 Recommendations by pillar 30
8.3 Focus of the policy brief 32
9. Limitations and areas for further research 34
9.1 Extending the findings 34
9.2 Evidence gaps to investigate 34
9.3 Disputed findings to test 35
10. Annexes 36

ABBREVIATIONS

AE	Access and Equity (RiaDA pillar)
AI	Artificial intelligence
ASEAN	Association of Southeast Asian Nations
AW	Automation and the Future of Work (RiaDA pillar)
CCC	Cooperation Committee for Cambodia
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
CRPD	Convention on the Rights of Persons with Disabilities
DP	Responsible Data Use and Privacy (RiaDA pillar)
EU	European Union
FGD	Focus group discussion
GV	Governance (RiaDA pillar)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
ILO	International Labour Organization
KHQR	Cambodia's common QR code standard for payments
LGBTQIA+	Lesbian, gay, bisexual, transgender, queer, intersex, asexual and other people of diverse sexual orientations and gender identities
QR code	Quick response code
R-[pillar]-[number]	Reference of a recommendation, for example R-AE-2, the second recommendation under Access and Equity
ReCIPE	Recentering the Civic Internet through Partner Engagement, a project co-funded by the European Union, under which this study was commissioned
RiaDA	Rights in a Digital Age, Oxfam's analytical framework
SC	Security and Digital Civic Space (RiaDA pillar)
SIM card	Subscriber identity module card
SWOT	Strengths, weaknesses, opportunities and threats
UN	United Nations
UNDRIP	United Nations Declaration on the Rights of Indigenous Peoples
UNESCO	United Nations Educational, Scientific and Cultural Organization

FOREWORD

Cambodia is digitising its economy, its government services and its society quickly. Payments, registration for public services, work and access to information increasingly happen online. These changes can widen access to services and opportunities. They also raise questions about who is reached, how personal data is protected, how people can speak freely online, and what happens to workers as tasks are automated.

Oxfam in Cambodia commissioned this study to understand whether the laws and policies guiding this transformation protect the rights of the people it affects. The study uses Oxfam's Rights in a Digital Age framework. It brings together a review of thirty Cambodian laws and policies, interviews with people who work on digital policy, and discussions with people who use digital services every day.

Several of the most important laws are still being drafted, including those on personal data protection, digital government and cybercrime. This gives government, civil society and the private sector an opportunity to build rights protections into them before they are adopted. The recommendations in this report are offered as a contribution to that work. We hope they will support dialogue between government and civil society, and we look forward to discussing them with our partners.

1. EXECUTIVE SUMMARY

Oxfam in Cambodia commissioned this policy analysis as part of the Recentering the Civic Internet through Partner Engagement (ReCIPE) project, co-funded by the European Union. The study asks whether Cambodia's move to digitise its economy, government and society comes with protections for the rights of the people it affects. It uses Oxfam's RiaDA framework, which looks at digital policy through five pillars: Access and Equity; Security and Digital Civic Space; Responsible Data Use and Privacy; Automation and the Future of Work; and Governance.

The study was carried out in five phases.

Phase	What was done
Desk review and policy mapping	Thirty Cambodian laws, policies and strategies on digital matters were reviewed. Each was compared with eighteen international and regional standards, such as United Nations human rights treaties and ASEAN frameworks, to see where Cambodian policy meets them and where it does not yet. The results were summarised as strengths, weaknesses, opportunities and threats (a SWOT analysis).
Primary qualitative research	Twenty people who work on digital policy or see its effects were interviewed: government officials, legal experts, development partners, private companies and civil society organisations. Four focus group discussions were organised with people who use digital services: young adults and first-time users, rural and peri-urban women, and older people.
Thematic analysis	What the documents said was compared with what people said in the interviews and focus groups. This produced 68 findings, each marked according to how far the sources agree.
Strategic recommendations	Thirty recommendations were written, each answering a gap found in Cambodian law or policy. They were ranked by how serious the harm is if nothing changes, whether the moment to act is now, and whether existing bodies can make the change.
Validation and finalisation	The findings and draft recommendations were discussed with stakeholders at a workshop on 10 September 2026, and their feedback was used to finalise them.

Cambodia policy framework has a large set of digital laws and policies, led by two long-term frameworks: the Digital Economy and Society Policy Framework 2021-2035 and the Digital Government Policy 2022-2035. Digital payments are the area where Cambodia comes closest to international good practice. Bakong, the payment system of the National Bank of Cambodia, and KHQR, a single QR code standard that works across banks, have brought payment services to people who live far from a bank branch. The laws that would protect people's rights most directly are still in draft: the laws on personal data protection, digital government, cybercrime and cybersecurity.

The findings below are grouped under the five pillars of Oxfam's RiaDA framework. They draw on two sources: the review of thirty Cambodian laws and policies, and what respondents expressed in the interviews and focus groups.

Access and Equity:

- Almost everyone who took part in the focus groups owns a smartphone. Beyond paying by QR code, however, most use almost no other digital service.
- Mobile internet costs about one dollar a week, and the poorest households weigh this against food and transport.
- Some government apps only work on recent phones.
- None of the laws and policies reviewed requires public digital services to be usable by people with disabilities.

Security and Digital Civic Space:

- Journalists, activists, leaders of Indigenous organisations and young people said they hold back from saying what they think online.
- The draft cybercrime law would make it a crime to publish content seen as harming the country's sovereignty, its stability or its moral and cultural values, with a penalty of one to three years in prison. The draft does not define these terms.
- People who are harassed or abused online have no clear place to report it where someone is available to respond.

Responsible Data Use and Privacy:

- Cambodia does not yet have a law protecting personal data. The current draft law would place data protection under the Ministry of Post and Telecommunications rather than an independent authority, and it would not apply to ministries and other public bodies.
- In practice, many people ask phone shops, technicians or relatives to set up their accounts, and these helpers often keep the passwords. This shows the need for digital literacy training that covers privacy and account security, so that people understand the risks and can make informed choices.

Automation and the Future of Work:

- None of the laws and policies reviewed protects people who find work through apps or who work in the informal economy.
- Workers' organisations described production lines that once needed about twenty workers and are now run by one machine operator.
- No ministry or agency is responsible for following how digital technology is changing work.

Governance:

- None of the civil society and community groups consulted had been asked for their views before a digital policy was adopted.
- When consultation does happen, it usually comes late, once the text is almost final. No independent body checks how digital laws affect people's rights.
- The people interviewed could not name a way to complain about a digital service, or have a decision reviewed, that works in practice.

When it comes to inclusion, digital policy targets are set for the population as a whole, so no one measures who is being left out. Respondents said women are rarely involved when policies are designed and decided. None of the laws and policies reviewed addresses the situation of Indigenous communities.

The draft laws on personal data protection, digital government and cybercrime, and the draft national strategy on artificial intelligence, are still being prepared. They can still be amended to include protections this report recommends, such as a body that decides complaints about personal data, minimum requirements for government online services, and a judge's approval before anyone's data is accessed or intercepted.

For people's rights to be protected in practice, three steps are needed:

- adopting these drafts with rights safeguards;
- putting the commitments already made into practice, with targets that show who is reached;
- setting up bodies that oversee digital laws and handle complaints, with safeguards to protect from retaliation people who raise concerns or report rights violations.

Until then, many people protect themselves by using digital services less, and national adoption figures do not show this.

PRIORITY RECOMMENDATIONS

The study makes thirty recommendations. Each answers a gap in Cambodian law or policy and is addressed to the government body able to act on it. Nine are the most pressing: the harm they address is serious, and the law or system concerned is being decided now. The nine are:

- **The draft cybercrime law (four recommendations):** define the vague terms the draft uses to decide what content is a crime, such as "sovereignty", "instability" and "moral and cultural values"; narrow the offences of publishing "non-factual" or defamatory content, and remove prison sentences for defamation; require a judge's approval before the authorities preserve, copy or seize a person's data; and require a judge's approval for interception, with investigations led by the prosecutor rather than a government committee.
- **Personal data (three recommendations):** issue interim guidance on handling personal information until the data protection law is adopted; require phone operators and online services to explain, in Khmer, what they do with the identity documents people give when they register; and apply to government bodies the same data protection rules the draft law sets for companies.
- **Government online services:** set minimum requirements every service must meet before launch: it works on the phones people actually use, it is in Khmer, it can be used by people with disabilities, it collects only the personal data needed to provide the service, and staff are available to help.
- **Digital laws and policies:** before each draft is adopted, assess its effect on people's rights. The assessment should look at each group separately, such as women, Indigenous communities and people with disabilities, and at people who belong to several of these groups at once. Once the law or policy is in force, a standing group that includes civil society and affected communities should review how it is applied.

2. INTRODUCTION AND BACKGROUND

2.1 The assignment

Oxfam in Cambodia commissioned this study as part of the Recentering the Civic Internet through Partner Engagement (ReCIPE) project, co-funded by the European Union.[1] The study asks whether Cambodia's move to digitise its economy, government and society comes with protections for the rights of the people it affects, so that rights are not left behind as technology changes. It uses Oxfam's RiaDA framework, which looks at digital policy through five pillars: Access and Equity; Security and Digital Civic Space; Responsible Data Use and Privacy; Automation and the Future of Work; and Governance.

The findings will be discussed with Cambodian civil society organisations, including at the provincial network meetings of the Cooperation Committee for Cambodia (CCC). They will also be shared with the Digital Rights Working Group, government agencies and Oxfam's regional networks.[2]

2.2 Context

Two long-term frameworks set the direction of Cambodia's digital transformation: the Cambodia Digital Economy and Society Policy Framework 2021-2035 and the Cambodia Digital Government Policy 2022-2035.[3][4] The terms of reference for this study describe Cambodia as entering Phase 2 (2026-2030) of its digital agenda, in which digital systems are to be joined up across finance, agriculture and public services.[5] Figures published by UNESCO in 2024 show that in 2020, 32 per cent of the population had basic digital skills, 5 per cent had intermediate skills and 1 per cent had advanced skills.[6] According to the Cambodia Socio-Economic Survey 2023, 95.5 per cent of households own a mobile phone[7].

Several of the laws that would protect people using digital technology are still drafts. They include the laws on personal data protection, digital government, cybercrime and cybersecurity, and the national strategy on artificial intelligence.[8] This report uses the latest version of each draft available to the study, and gives its date wherever it is cited.

---

[1]Oxfam in Cambodia (2026) 'Terms of Reference: Consultancy to Conduct a Comprehensive Policy Analysis of Cambodia's Digital Transformation', Phnom Penh: Oxfam in Cambodia.

[2]Ibid.

[3]Royal Government of Cambodia (2021) 'Cambodia Digital Economy and Society Policy Framework 2021-2035', prepared by the Supreme National Economic Council, Phnom Penh: Royal Government of Cambodia.

[4]Royal Government of Cambodia (2022) 'Cambodia Digital Government Policy 2022-2035', prepared by the Ministry of Post and Telecommunications, Phnom Penh: Royal Government of Cambodia.

[5]Oxfam in Cambodia (2026) op. cit.

[6]UNESCO (2024) 'Cambodia Launches its First Competency Framework on Digital, Media and Information Literacy to Empower Citizens in Today's Digital Society', 2 July 2024, https://www.unesco.org/en/articles/cambodia-launches-its-first-competency-framework-digital-media-and-information-literacy-empower (last accessed 28 September 2026).

[7] National Institute of Statistics (2024) 'Report of Cambodia Socio-Economic Survey 2023', Phnom Penh: Ministry of Planning, section 10.7.

[8]The drafts consulted are the Draft Law on Personal Data Protection (unofficial translation, version dated 31 July 2026); the Draft Law on Digital Government (version dated 21 June 2025); the Draft Law on Cybercrime, Draft V.1, prepared by

2.3 Rights-holders at the centre

The study focuses on the people affected by digital change, referred to in this report as rights-holders. They include women, informal and platform workers, rural and peri-urban communities, young adults and first-time users, older people, people with disabilities, Indigenous communities, LGBTQIA+ people and civil society organisations. The findings show that the groups with the least access to services and to decision-making, such as rural women, older people, Indigenous communities and people with disabilities, are also the most exposed to the harms of digital change, such as scams, online abuse and exclusion from online services. What they said about using digital services, and about the problems they face, is treated as evidence of how well current policy protects them.

2.4 Scope

The study has four parts: a review of Cambodia's national digital policies, summarised in a SWOT analysis; a comparison of these policies with regional and international standards; interviews and focus group discussions; and an analysis of all the evidence under the five RiaDA pillars. It ends with recommendations, which were discussed with stakeholders at a validation workshop on 10 September 2026. After the workshop, the findings and recommendations were revised using the feedback received, as recorded in Annex F. The results are presented in this report and in a separate four-page policy brief for policymakers and civil society organisations.

2.5 Structure of this report

Section 3 explains how the study was carried out, including how consent, data and the identity of participants were handled. Section 4 describes Cambodia's digital laws and policies and compares them with international and regional standards. Section 5 presents the findings under each pillar, followed by findings that fall outside the five pillars. Section 6 looks across the pillars at gender, rural communities, Indigenous communities and people with disabilities. Section 7 sets out the conclusions. Section 8 presents the recommendations and explains how those in the policy brief were chosen. Section 9 sets out the limits of the study and areas for further research.

The full recommendations are in the annexes. A separate four-page policy brief presents the main findings and recommendations for policymakers and civil society organisations.

the Cybercrime Law Formulation Working Group of the Council of Ministers, unofficial translation, identified by government sources as the current draft, https://data.opendevelopmentcambodia.net/en/laws_record/draft-cybercrime-law (last accessed 28 September 2026); the Draft Law on Cybersecurity (draft of 2 September 2022, as analysed in Access Now and International Commission of Jurists (2023) 'Legal Analysis: Cambodia Draft Law on Cybersecurity'); and the Draft National Artificial Intelligence Strategy 2025-2030 (June 2025).

3. METHODOLOGY

3.1 Analytical framework

The study uses Oxfam's RiaDA framework at every stage, from the review of documents to the recommendations.[9] The framework has five pillars:

- **Access and Equity:** whether people can actually use digital technology, meaning it is available, affordable, known about, accessible and easy to use, and whether they have a say in the technologies that affect them.
- **Security and Digital Civic Space:** free expression, privacy and anonymity online, safety from online violence, and the freedom of civil society to operate online.
- **Responsible Data Use and Privacy:** how personal data held by government bodies and private companies is protected.
- **Automation and the Future of Work:** how automation and work arranged through digital platforms affect workers' rights.
- **Governance:** how open and accountable the development, use and regulation of digital technology are.

3.2 Desk review and policy mapping

Thirty national laws, policies and strategies were reviewed; they are listed in section 4.1. For each one, the review recorded which body is responsible, whether it is in force or in draft, which version was read, and which RiaDA pillars it concerns. Each was then compared with eighteen international and regional standards, including United Nations human rights treaties, UNESCO guidance and ASEAN frameworks. The results were summarised in a SWOT analysis of strengths, weaknesses, opportunities and threats (section 4.3).

3.3 Primary qualitative research

Twenty key informant interviews were held in July and August 2026 with people who work on digital policy or see its effects. They came from five groups: government officials and policymakers; legal and regulatory experts; United Nations agencies and development partners; private companies; and civil society and digital rights organisations, including media. The interviews followed a set of guiding questions, took place in person or online, and were conducted in English or Khmer.

Four focus group discussions were organised with rights-holders: young adults and first-time users (FGD-01); rural and peri-urban women, in three sessions (FGD-02); and older people (FGD-04). Indigenous communities (FGD-03) took place as key informant interviews instead and are analysed with the interviews. The research team led the discussions in Khmer.

[9] Oxfam in Cambodia (2026) op. cit.

3.4 Thematic analysis and triangulation

All interview notes, discussion notes and documents were sorted under the five RiaDA pillars. For each topic, what the documents said was compared with what interviewees and focus group participants said. This comparison, called triangulation, produced 68 findings. Each finding was given one of four labels:

- **Confirmed:** all the sources that cover the topic agree (the review of laws and policies and the interviews and focus groups corroborate each other).
- **Framework gap:** the finding comes from the interviews or focus groups only, because none of the laws and policies reviewed covers the subject.
- **Mixed or disputed:** the sources give different accounts, and the report explains the difference.
- **Evidence gap:** no source could establish the point, so it remains a question for further research.

31	26	4	7
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Of the 68 findings, 31 are confirmed, 26 are framework gaps, 4 are mixed or disputed and 7 are evidence gaps. Within each pillar, findings were ranked by how relevant they are to the research questions, how often they come up across sources, and how much they matter for rights-holders and for policy.

Each gap in Cambodian law or policy was also classed by type: a missing or unclear rule (legal), a commitment not put into practice (operational), a missing body or a body without the mandate needed (institutional), or poor coordination between bodies (coordination). Findings that do not fit any of the five pillars are reported separately in section 5.6.

3.5 Strategic recommendations and prioritisation

For each priority gap, the relevant laws and policies were read again to check that the gap is real. Some gaps were confirmed, some narrowed and some dropped. One recommendation was then written for each confirmed gap, saying what should change and why. Each recommendation also records the type of action, who is affected, the Cambodian policies it refers to, the international standards that support it, the body that should act and the timeframe (Annex D). The recommendations were then ranked by three criteria.

Criterion	What it measures
Human rights risk	How serious the harm is if the gap stays open, and how many people it affects.
Urgency	Whether the moment to act is now, for example because a draft can still be amended.
Feasibility	Whether existing powers and bodies can make the change.

3.6 Validation

The findings and the 27 draft recommendations were presented at a validation workshop on 10 September 2026. Participants gave feedback on cards, through an online form and in open discussion, and all of it was gathered in one record. Participants raised four subjects that the draft recommendations did not cover. Each was checked against Cambodian laws and policies, and three became new recommendations, bringing the total to thirty. Annex F records each workshop input and what was done with it.

3.7 Consent, transparency, data management, attribution and confidentiality

Consent: Before each interview or discussion, participants were told that the study is independent, carried out for Oxfam as part of the ReCIPE project, co-funded by the European Union; that taking part is voluntary and that they could skip any question or stop at any time; and that nothing they said would be linked to their name or their organisation. Interview recording and transcription were conducted with participants' prior consent, with additional safeguards for sensitive interviews, including no retained audio recordings and automatic data deletion after 12 months.

Transparency: Participants were told what the study is for and how their input would be used. The findings and draft recommendations were then presented back to stakeholders at the validation workshop.

Data management: All material was kept in a single secure repository, organised by type of respondent, research question and pillar. Names and other identifying details were removed, and only the information the study needed was kept.

Attribution: Findings are reported by type of respondent, for example "workers' organisations" or "young adult participants", and never by name or organisation. Some respondents said their views were personal, and these views are not presented as the position of their organisation. Where an account is sensitive, or naming even the type of respondent could put someone at risk, it is not attributed at all.

Confidentiality: Where a personal account is sensitive and only a few people could have given it, the finding is used but the details that could identify the person are left out.

Safeguarding: Discussions were led with care for people's safety, especially on sensitive subjects such as online gender-based violence and surveillance.

Use of AI and Digital Tools: Digital tools and custom AI-assisted workflows were used to support documentation, evidence organisation, language review and report formatting, in line with the principles of the European Commission's *Living Guidelines on the Responsible Use of Generative AI in Research*.

4. THE NATIONAL POLICY LANDSCAPE

4.1 The policy framework

The desk review covered thirty national laws, policies and strategies: 22 already adopted and 8 still in draft or being developed. It also covered one further draft found during the review, the Data Governance Policy 2025-2035. The table groups them by subject.

Subject	Laws and policies reviewed
Overall frameworks	Cambodia Digital Economy and Society Policy Framework 2021-2035; Cambodia Digital Government Policy 2022-2035
Digital government and data	Draft Law on Digital Government; Draft Law on Personal Data Protection; Draft Cloud Priority Policy 2026-2035; Strategy for the Development of E-Services for Business 2025-2028; Sub-Decree on Digital Signatures; and the additional Draft Data Governance Policy 2025-2035
Security	Draft Law on Cybersecurity; Draft Law on Cybercrime; Law on Combating Online Scams
Technology, artificial intelligence and innovation	Digital Technology Roadmap 2023; Draft National Artificial Intelligence Strategy 2025-2030; Science, Technology and Innovation Policy 2020-2030; Cambodia Science, Technology and Innovation Roadmap 2030; Research and Development National Blueprint 2022
Skills, literacy and education	Policy and Strategy on ICT in Education 2018; Roadmap for Digital Skills Development in Cambodia 2024-2035; Competency Framework on Digital, Media and Information Literacy, 2nd edition, 2024; Masterplan on Technology and Enterprise for Rural Youth 2021
Financial technology and payments	Cambodia Financial Technology Development Policy 2023-2028; National Bank of Cambodia Fintech Regulatory Sandbox 2019; Bakong White Paper 2020; KHQR Standard for Retail Payments 2022; Prakas on Digital Asset Service Providers 2024; Draft Crypto-Asset Service Provider Licensing Framework; Digital Securities Sandbox and Guidelines 2024
Commerce and trade	Law on Electronic Commerce 2019; Law on Consumer Protection 2019; Law on Competition 2021; Digital Trade Policy, in development

The two overall frameworks were prepared by the Supreme National Economic Council and by the Ministry of Post and Telecommunications.[10] The National Council for Digital Economy and Society coordinates their implementation. One of its committees, the Digital Government Committee, is led by the Minister of Post and Telecommunications.

Four of the drafts are the laws that would protect people most directly: the laws on personal data protection, digital government, cybercrime and cybersecurity. Until they are adopted, much of the

[10]Royal Government of Cambodia (2021) op. cit.; Royal Government of Cambodia (2022) op. cit.

protection promised in Cambodia's digital laws and policies is not yet in force. Annex A shows, for each law and policy, the pillars it concerns, the body responsible and its status.

4.2 Comparison with international and regional standards

Each of the thirty laws and policies was compared with eighteen international and regional standards. These include the main United Nations human rights treaties; the International Labour Organization Centenary Declaration on the Future of Work; the Global Digital Compact; UNESCO guidance on digital platforms and on the ethics of artificial intelligence; the UN Guiding Principles on Business and Human Rights; and the ASEAN frameworks on the digital economy, personal data protection and artificial intelligence. For each, the comparison notes whether Cambodian policy meets the standard, partly meets it, or does not yet address the subject. Annex B gives the full comparison. The main results by pillar are set out below.

Access and Equity: Digital payments are the area where Cambodian policy meets international good practice. The Bakong payment system, the KHQR payment standard and the Financial Technology Development Policy 2023-2028 are designed for people without bank accounts, rural populations and young people, and let them pay without going to a bank. Elsewhere, policies commit to inclusion in general terms but do not say how it will be achieved. Targets are set for the whole population and are not broken down by gender, location or disability, so they cannot show whether women, rural residents or people with disabilities are being reached. This does not yet meet the equality standard of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), to which Cambodia has been a party since 1992. No law or policy reviewed requires public digital services to be accessible to people with disabilities, as the Convention on the Rights of Persons with Disabilities (CRPD), which Cambodia ratified in 2012, requires. None addresses the situation of Indigenous communities, as the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) expects. UNDRIP is a non-binding declaration, which Cambodia voted to adopt in 2007.

Security and Digital Civic Space: The draft cybercrime law would punish with one to three years in prison any content "deemed" to harm the sovereignty and integrity of the Kingdom, to create insecurity or instability, or to damage moral and cultural values, as well as "non-factual" publications that slander government agencies (Article 28). None of these terms is defined. A prosecutor, not a judge, would authorise access to computers and the interception of communications, for up to four months (Article 20). Until an arrest is made, investigations would be led by the Secretary General of a National Anti-Cybercrime Committee chaired by the Prime Minister, instead of by the prosecutor (Articles 6 and 16).[11] The draft cybersecurity law, as analysed by Access Now and the International Commission of Jurists, would give a Digital Security Committee wide powers with no independent oversight.[12]

As drafted, neither law yet meets two international standards. Under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), to which Cambodia has been a party since 1992, any limit on free expression must be clearly set out in law and be necessary and proportionate. Under the Council of Europe Convention on Cybercrime (Budapest Convention), an international treaty open to all

[11]Draft Law on Cybercrime, Draft V.1, unofficial translation, op. cit., Articles 6, 16, 20 and 28.

[12]Access Now and International Commission of Jurists (2023) 'Legal Analysis: Cambodia Draft Law on Cybersecurity', 29 September 2023, analysis of the Draft Law on Cybersecurity dated 2 September 2022.

countries, investigative powers must come with safeguards such as supervision by a judge or another independent authority.

No law reviewed actively protects freedom of expression, assembly or association online. The only document that addresses freedom of expression and protection from unlawful surveillance is the Competency Framework on Digital, Media and Information Literacy, which treats them as skills to be taught rather than as rights. The Law on Combating Online Scams uses the ordinary criminal procedure, and does not hold people criminally liable if they were forced to take part in scam operations (Article 15).[13]

Responsible Data Use and Privacy: Several policies, including the Digital Government Policy and the draft strategy on artificial intelligence, promise to protect personal data and leave the details to the draft Law on Personal Data Protection. That draft gives people rights over their data close to those in ASEAN and European rules. Three points remain open. The law is not yet in force, and would apply only two years after it comes into force (Article 57). It places data protection under the Ministry of Post and Telecommunications rather than an independent authority (Article 4). And it does not apply to ministries and public bodies acting in their official role (Article 2).[14]

Other laws and policies that involve personal data at most require it to be kept secure. They set no rules on consent, on the purposes for which data may be used, or on the rights of the person concerned. Some require sensitive data to be stored in Cambodia, while the ASEAN Agreement on Electronic Commerce, which Cambodia has signed, commits member states to reduce barriers to cross-border data flows, with safeguards[15]. ASEAN's new Digital Economy Framework Agreement, concluded in May 2026, also covers these flows. No policy explains how these commitments fit together.

Automation and the Future of Work: Cambodian policy meets the part of the ILO Centenary Declaration that concerns skills, through the digital skills roadmap and the literacy framework. It does not yet meet the part that concerns protecting workers. No law or policy reviewed, in force or in draft, deals with the rights of people who find work through apps or who work in the informal economy. The draft strategy on artificial intelligence plans a study of how artificial intelligence will affect jobs (strategic measure 1.9), but sets no measure to protect workers in the meantime.[16]

Governance: Cambodia's digital laws and policies set up councils and committees, such as the National Council for Digital Economy and Society and the Digital Government Committee, to coordinate and deliver digital government and electronic services. What is less developed is how this work answers to the people it affects: publishing information, involving the public, independent oversight and ways to complain. These are the elements that the Global Digital Compact and the UN Guiding Principles on Business and Human Rights emphasise. The draft strategy on artificial intelligence is built around ethical principles, but sets no rules on accountability, bias or fairness in automated decisions of the kind found in the UNESCO Recommendation on the Ethics of Artificial Intelligence.

[13]Law on Combating Online Scams, unofficial translation dated March 2026, Article 15.

[14]Draft Law on Personal Data Protection, unofficial translation, version dated 31 July 2026, Articles 2, 4 and 57.

[15] ASEAN Agreement on Electronic Commerce, signed in Ha Noi on 22 January 2019, Article 7, paragraphs 4 and 6.

[16]Draft National Artificial Intelligence Strategy 2025-2030, June 2025, strategic measure 1.9.

4.3 SWOT analysis of the policy environment

Strengths	A full set of laws and policies, from the overall frameworks to sector strategies, with bodies to coordinate them. Working digital payment systems, Bakong and KHQR, that reach people without bank accounts. A draft data protection law close to international practice. Data protection built into the design of the e-services strategy for business and of Bakong. A literacy framework that names women, people with disabilities, Indigenous people and young people.
Weaknesses	Data protection depends on a law not yet in force. Inclusion is promised without measures or targets for particular groups. No protection for app-based and informal workers. Draft security laws focus on controlling expression and data rather than protecting them. Little transparency, public participation, independent oversight or means of complaint. Data protection placed under a ministry rather than an independent authority.
Opportunities	Adopting the data protection law with an independent authority, since many policies already rely on it. Adding rights safeguards to the drafts still open: the data governance policy, the cloud policy and the strategy on artificial intelligence. Using the ASEAN frameworks Cambodia already follows. Extending the digital payment model with targets for women, rural communities and people with disabilities.
Threats	The cybercrime and cybersecurity laws adopted as drafted. Digital identity, data-sharing and cloud systems rolled out before the data protection law applies. Conflict between keeping data in Cambodia and letting it cross borders. Gaps in rural connectivity, electricity, affordability and skills. Too few people with cybersecurity and data skills.

Cambodia's strengths lie in access to payments, infrastructure and service delivery. The weaknesses and threats concern freedom of expression online, the protection of workers and enforceable data rights, where the relevant laws are still drafts or do not exist. Most opportunities involve adopting drafts that are already written and adding safeguards to those still being prepared.

5. PILLAR-BY-PILLAR ANALYSIS

This section presents the findings under each of the five pillars. Each finding comes from comparing three sources: the review of Cambodian laws and policies, the key informant interviews, and the focus group discussions. Within each pillar, findings are grouped by the label they received (section 3.4).

HOW THE FINDINGS ARE LABELLED

- **Confirmed:** all the sources that cover the topic agree (the review of laws and policies and the interviews and focus groups corroborate each other).
- **Framework gap:** the finding comes from the interviews or focus groups only, because none of the laws and policies reviewed covers the subject.
- **Mixed or disputed:** the sources give different accounts, and the report explains the difference.
- **Evidence gap:** no source could establish the point.

Each finding is summarised in one or two sentences. The detailed evidence behind every finding is in the findings synthesis matrix (Annex C). Section 5.6 presents the findings that do not fit any of the five pillars.

5.1 Access and Equity

This pillar has thirteen findings: eight confirmed, four framework gaps and one evidence gap.

8	4	0	1
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Confirmed findings

Use of digital services: Almost all focus group participants own a smartphone, but apart from paying by QR code, most use almost no other digital service.

Affordability: Mobile internet costs about one dollar a week. Interviewees said that for the poorest households, this competes with spending on food, transport and rent. In rural areas, the poorest fifth of the population consumes on average about 203,000 riels per person per month, so one dollar a week, about 17,000 riels a month, represents around 8 per cent of that amount[17].

[17] National Institute of Statistics (2024) 'Report of Cambodia Socio-Economic Survey 2023', Phnom Penh: Ministry of Planning, section 10.5.

Digital literacy training: Digital literacy training exists, but interviewees and participants said it rarely reaches factory workers, older people or women with household responsibilities, for example because sessions take place during working hours or last a full day.

Digital payment: Digital payments are where Cambodian policy meets international good practice. Even so, they do not yet reach many older people, rural women who work mainly at home or on farms, or small vendors who have no smartphone.

Inclusion targets: Policy targets are set for the population as a whole, not for groups such as women, older people, rural residents, people with disabilities or Indigenous communities. As a result, no one measures whether these groups are left out, and no institution is responsible for it.

Accessibility: Only one document reviewed, the draft Law on Digital Government, mentions accessibility for people with disabilities, and it does not make it a requirement.

Indigenous communities: None of the laws and policies reviewed addresses the situation of Indigenous communities, and almost no digital training or service is designed to reach them.

Gains from access: Where people do have access, they described real benefits, such as learning a trade from online videos and starting a business, and paying faster and more safely.

Framework gaps

Phone requirements: Some government apps only work on recent smartphones, and some bank accounts are blocked if they are not linked to the user's own phone number. No law or policy reviewed sets a standard for how easy public digital services must be to use.

Language: Some people cannot use services they have access to because the screens are in English, the Khmer used is technical, Khmer is not their first language, or Khmer screen-reading software for people with visual disabilities is limited.

Coverage: Remote, coastal and forest communities have little or no mobile signal, and interviewees said only about 12 per cent of schools have an internet connection.

Reach of government systems: According to interviewees, the government system for registering informal economy workers has reached about 700,000 of an estimated 7.5 million. No body was identified as responsible for making sure such systems reach the people they are built for.

Evidence gap

Rural access fund: Government interviewees named the Universal Service Obligation Fund, which mobile operators pay into, as the main tool for closing the digital divide. The study could not find out what the fund has paid for.

5.2 Security and Digital Civic Space

This pillar has fourteen findings: seven confirmed, five framework gaps, one mixed or disputed and one evidence gap.

7	5	1	1
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Confirmed findings

Undefined terms: Terms such as "national security" and "public order" appear across Cambodian laws without a definition. Interviewees saw this as the main risk, because the authorities can read these terms broadly when they apply the law.

Self-censorship: Journalists, activists, leaders of Indigenous organisations and young adults said they limit what they say online. Their reasons range from harassment by other users to fear of the criminal charges brought against critics.

Altered and shared images: When someone's photo is altered with artificial intelligence or shared without their consent, there is no official way to have it taken down. The only removal service identified is run by a non-governmental organisation.

Reporting online harm: There is no accessible place to report online harassment or abuse where someone is available to respond. People who do report it can be blamed, or treated differently because of their gender identity or sexual orientation.

Fraud: Phone and online scams succeed most often against people who cannot easily check whether a call or message is genuine, including people with disabilities, older people and Indigenous communities.

Penalties in the draft cybercrime law: The draft cybercrime law would make defamation punishable by prison. Interviewees said the existing Criminal Code punishes it with a fine only.

Authenticity of official messages: No rule sets how people can check that a message from a government body is genuine. Participants described an emergency storm warning issued with an AI-generated voice.

Framework gaps

Press law: Journalists are prosecuted under the Criminal Code rather than under the 1993 Press Law, whose revision has not been completed.

Account takeover: Social media and messaging accounts are often taken over by other people. This affects individuals, organisations and provincial administrations, and accounts no longer in use are a particular target.

Women in public life: Some women turn down leadership roles to avoid online abuse, and interviewees described attacks on women leaders as a known pattern.

Moderation in Khmer: Social media platforms do not appear to block the Khmer words used to abuse women and LGBTQIA+ people.

Measurement of online harm: Cambodia has not yet published national data on online gender-based violence, and there is no data at all on online harm against people with disabilities.

Mixed or disputed finding

Cybercrime law and expression: Legal and regulatory interviewees said cybercrime legislation is not related to the law on freedom of speech, and that citizens can express opinions and criticism freely within the law and public order. Other interviewees, and the review of the draft itself, found that its provisions could expose users and media to prosecution.

Evidence gap

Older people and civic space: No source covered how older people experience free expression, online harm or taking part in public life.

5.3 Responsible Data Use and Privacy

This pillar has twelve findings: six confirmed, five framework gaps and one evidence gap.

6	5	0	1
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Confirmed findings

Legal protection: Cambodia does not yet have a general law on personal data. Protection relies on scattered provisions in the Constitution, the Criminal Code, the Civil Code and sector rules, which are applied mainly in banking and finance.

Consent: People often accept terms and conditions without understanding them. Workers who find jobs through apps cannot refuse to hand over their identity card if they want to work.

Identity documents: People must show an identity document to register a SIM card or to sign up for apps, but they are told little about how it is used, stored or shared.

Regulator and complaints: There is no data protection authority yet. The draft law would place one under a ministry, and no body was found that currently handles complaints about the misuse of personal data.

Storing data in Cambodia and across borders: Some policies require sensitive data to be stored in Cambodia, while trade agreements commit Cambodia to letting data move across borders. No policy explains how the two fit together.

Protection by design: Two policies build data protection into their design from the start: the Strategy for the Development of E-Services for Business and the Bakong payment system.

Framework gaps

Passwords and account details: Many people ask phone shops, technicians or relatives to create their accounts, and these helpers often keep the passwords and account details.

Personal data already in circulation: Scammers use personal details that are already public or have leaked to make their calls and messages seem genuine.

Consultation on the draft law: Consultation on the draft data protection law appears to have reached very few organisations, with only a few days to respond.

Community and land data: No law or policy recognises the right of Indigenous communities to decide how information about their communities, land and natural resources is collected and used.

Security in the telecommunications sector: It is not possible to judge from published information how well telecommunications companies protect data. Interviewees described security practices that follow company rules rather than Cambodian regulation.

Evidence gap

Sharing or sale of customer data: People reported receiving marketing calls soon after buying a new phone number. The study could not establish whether, or how, customer information is shared or sold.

5.4 Automation and the Future of Work

This pillar has fourteen findings: four confirmed, seven framework gaps, one mixed or disputed and two evidence gaps.

4	7	1	2
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Confirmed findings

Rights of platform and informal workers: No law or policy reviewed, in force or in draft, protects the rights of people who find work through apps or who work in the informal economy.

Decisions made through apps: Workers who find jobs through apps appear to have no way to challenge decisions the app makes about them, and the research did not identify a body that could review such decisions.

Current protection: No current rule protects workers from the effects of automation. Government interviewees said this protection would come through artificial intelligence regulation that is still being developed.

Responsibility for effects on work: No ministry or agency is responsible for following how digital technology affects work.

Framework gaps

Job losses in production: Workers' organisations described production lines that once needed about twenty workers and are now run by one machine operator.

Harder working conditions: Workers' organisations said the jobs that remain after automation are more intense, with constant monitoring and restricted breaks, and that the jobs most at risk are held mainly by women.

Online recruitment: Job applicants can be rejected because an online form is incomplete, with no way to correct it or ask why.

Small vendors: Small vendors without smartphones are losing customers as buyers switch to digital payment, and nothing has been put in place to help them.

Creative work: Artificial intelligence tools copy original work, voices and images without permission, and the creators lose credit and income.

Media jobs and protection of sources: Media organisations expect fewer jobs for junior staff, and journalists who use artificial intelligence transcription tools risk exposing their interview recordings and sources.

Unpaid online work: People who do work arranged online and are not paid have no known way to recover what they are owed.

Mixed or disputed finding

Pace of job losses: Workers' organisations in manufacturing describe large-scale job losses already under way. Representatives of informal workers do not expect most informal work to disappear soon. The two accounts concern different sectors.

Evidence gaps

Platform workers' own accounts: What is known about app-based work comes from organisations that represent or observe these workers. No app-based worker was interviewed directly.

Platform companies: The interview planned with a delivery app company did not take place.

5.5 Governance

This pillar has fifteen findings: six confirmed, five framework gaps, two mixed or disputed and two evidence gaps.

6	5	2	2
Confirmed	Framework gaps	Mixed or disputed	Evidence gaps

Confirmed findings

Consultation before adoption: None of the civil society and community groups consulted had been asked for their views before a digital policy was adopted. Four laws and policies were each consulted on in a different way.

Redress: None of the people consulted could name a way to complain or seek a remedy that works in practice. Interviewees described court cases that can take up to ten years and that do not pause the decision being challenged.

Groups left out of policy-making: Several groups have no way into digital policy-making, including the general public, provincial organisations, Indigenous communities, disability organisations and journalists outside Phnom Penh.

Oversight and impact assessment: Each digital law or policy is overseen by the same ministry that drafted it, and none appears to have been assessed for its impact before adoption.

Launch of public services: Government online services are launched without testing with users, without announcing when they will be available, and without staff to help. People who find that a service does not work the first time tend not to come back.

Coordination: Interviewees said the responsibilities of different ministries overlap and that no senior body coordinates digital policy across government.

Framework gaps

Timing of consultation: Consultation starts when a text is almost final, with notice ranging from 24 hours to one month.

Feedback on input: People who give input are not told what happened to it, and some organisations now submit less as a result.

Barriers to taking part: Cost, timing, limited capacity and the need for technical expertise keep many people out of consultation. The need for recognised experts particularly excludes women from the stages where policy is designed and decided.

Role of civil society networks: Provincial and community organisations hear about consultations through civil society networks, not through any government channel, and this depends on outside funding.

Consultation leading to change: One case was found where consultation led to a documented change: approval times for registering informal workers fell after workers' organisations raised the problem with the ministry concerned.

Mixed or disputed findings

Consultation on the artificial intelligence strategy: Government interviewees described an open public call for comments. Interviewees who took part said consultation came late, on an almost final text. Both accounts are accurate.

National data: Private sector and development interviewees said national data is out of date and scattered, while government interviewees pointed to published national assessments.

Evidence gaps

Consultation on policies and on laws: Government interviewees said consultation on policies differs from consultation on laws, but no document setting out this difference was found.

Redress in rural communities: The study could not find out what people in rural communities do when a digital service fails or they lose money.

5.6 Findings outside the framework

Six findings from the interviews and focus groups do not fit any of the five pillars.

Using less as self-protection: People protect themselves by using digital services less, closing accounts or avoiding certain subjects. In national statistics, someone who stops after one bad experience looks the same as someone who was never reached.

Effects on the mind and on relationships: Young adults and several interviewees described effects on concentration, mental health, critical thinking and relationships.

Children and shared phones: Many families share one phone with their children. Development interviewees reported children as young as nine being exposed to pornography and to people seeking to abuse them.

Environmental cost: Specialist organisations raised the environmental cost of digital technology.

How rules are made: Interviewees suggested testing new rules on a small scale before applying them nationally, and using incentives and adjustment periods rather than penalties alone.

Dependence on outside funding: Scrutiny of digital laws, support for people harmed online and the presence of marginalised groups in consultations all depend on outside funding, and stop when it ends.

NB: Several recommendations in this report involve civil society organisations in oversight, for example in reviewing how digital laws are applied. Fulfilling this role implies that civil society organisations have enough sustainable and independent funding. A challenge to this is the recent reduction in funding: Oxfam has noted that aid cuts have weakened Cambodian civil society organisations, with effects on citizen journalism, local radio and support for the Digital Rights Working Group. Therefore, sustainable and independent funding for civil society organisations is an important condition for putting these recommendations into practice.

6. INCLUSION AND SYSTEMIC BARRIERS

This section looks across the five pillars at four themes: gender, rural communities, Indigenous communities and people with disabilities.

6.1 Gender

Access: For rural and peri-urban women, whether they can pay for internet access is decided through the household budget and by agreement within the family. Training that lasts a full day does not suit women with household responsibilities, and screens in English exclude women who do not read English. Digital payments do not yet reach rural women who work mainly at home or on farms. Interviewees said many women avoid digital payment because there is no way to correct a transfer sent by mistake.

Online safety: Some women turn down leadership roles to avoid online abuse, and participants described personal photos altered with artificial intelligence and circulated. Social media platforms do not block the Khmer words used to abuse women and LGBTQIA+ people, and people who report online harm may be treated differently because of their gender identity or sexual orientation. Cambodia has not yet published national data on online gender-based violence.

Work: Workers' organisations said the factory jobs most at risk from automation are held mainly by women, while supervisory jobs go more often to men. They also said that restricted breaks on automated production lines affect women most.

Participation: Interviewees said women are invited to consultations but play little part where policy is designed, and are almost absent where it is decided. These stages call for recognised technical experts, who are more often men.

Policy: No law or policy reviewed sets targets for women. The Digital Government Policy refers to women mainly as people to be protected, rather than as users whose access should be measured.

6.2 Rural communities

Remote, coastal and forest communities have little or no mobile signal, and some people travel to a particular spot to get a connection. Internet access at about one dollar a week competes with basic needs in the poorest households. Training rarely reaches rural areas, because it is concentrated among organisations already working on digital issues. Provincial organisations cannot afford to travel to consultations, and information reaches organisations in Phnom Penh first. The study could not find out what rural people do when a digital service fails or they lose money.

6.3 Indigenous communities

None of the laws and policies reviewed addresses the situation of Indigenous communities. Khmer is a second language for many Indigenous people, mobile signal is often absent near protected forests, and some people borrow money to buy a phone. Some Indigenous community members with bank loans sent money to scammers, believing they were paying the bank.

Leaders of Indigenous organisations said they do not feel safe expressing their views online. Indigenous organisations also raised a shared concern about who controls information on their communities, their land and their natural resources. They are rarely invited to consultations on digital issues, and interviewees said they attend mainly when international partners require it.

6.4 People with disabilities

Only one draft law mentions accessibility for people with disabilities, and none requires it. Khmer screen-reading software remains limited, and many people do not know about the accessibility features already on their phones. People with visual disabilities have lost money to scam calls about loan repayments, and there is no data on online harm against people with disabilities. Disability organisations have not been invited to consultations on digital policy so far. No focus group included participants with disabilities.

6.5 Across the four themes

THE SAME PATTERN FOR ALL FOUR GROUPS

Policy targets cover the population as a whole, so no one measures whether women, rural communities, Indigenous communities or people with disabilities are being reached. All four groups are targeted by scams in the same way, because many of their members cannot easily check whether a call or message is genuine. None had been consulted before a digital policy was adopted, and none could name a way to complain that works in practice. These are barriers the same groups already face outside digital services, in cost, language, access to decision-making and redress. Digital transformation therefore reinforces existing patterns of exclusion. Addressing them requires action on these barriers themselves, such as measures on cost, language, training and consultation, which are set out in the recommendations section of this report.

7. CONCLUSIONS

This section brings together the evidence in sections 4 to 6. It sets out where Cambodia's digital laws and policies already meet international rights standards, where existing laws and policies can be improved, and where new rules or bodies are needed.

Where Cambodian policy meets the standards: Digital payments are the area where Cambodian policy meets international good practice and works in practice. The Bakong payment system, the KHQR standard and the Financial Technology Development Policy reach people without bank accounts and rural populations, and participants described digital payment as faster and safer. Two documents also meet international standards in what they say. The draft Law on Personal Data Protection gives people rights over their data close to ASEAN and European rules, but it is not yet in force. The Competency Framework on Digital, Media and Information Literacy covers free expression, privacy and the inclusion of named groups, but it is guidance rather than a binding rule.

Where existing laws and policies can be improved: In several areas, a law or policy exists but does not yet meet the standard:

- policies promise inclusion, but their targets are not broken down by gender, location, disability or Indigenous status;
- the draft data protection law would place the data protection authority under a ministry, and would not apply to ministries and other public bodies;
- the draft cybercrime law would punish vaguely defined online content with prison and let a prosecutor, rather than a judge, authorise interception, while the draft cybersecurity law would give a committee wide powers without independent oversight, so neither yet meets Article 19 of the ICCPR or the Budapest Convention;
- the draft strategy on artificial intelligence sets out ethical principles but no rules on accountability, bias or fairness;
- consultation takes place, but it would reach more people if it started earlier, followed the same procedure each time and told participants what happened to their input.

Where new rules or bodies are needed: No law or policy reviewed yet provides:

- protection for people who work through apps or in the informal economy;
- a requirement that public digital services be accessible to people with disabilities;
- any provision for Indigenous communities;
- a way to have altered or intimate images taken down;
- a place to report online harm where someone responds;
- independent oversight or impact assessment of digital laws and policies;
- a way to complain or seek a remedy that works in practice.

Between policy and practice: The interviews and focus groups show that services and programmes that exist often do not reach the people they are meant for. Examples include digital literacy training; the registration system for informal economy workers, which has reached about 700,000 of an estimated 7.5 million; and government apps that only work on recent phones. Four of the laws that would protect people remain drafts, while digital identity, data-sharing and cloud systems are already being rolled out. In the meantime, people protect themselves by using digital services less: they stop using services,

close accounts, avoid certain subjects and, in the case of some women, turn down public roles. National adoption figures do not show any of this.

OVERALL ASSESSMENT

Cambodia has a complete set of digital laws and policies, and several drafts still being prepared can be amended to include the protections this report recommends. For people's rights to be protected in practice, three steps are needed: adopting these drafts with rights safeguards and preparing the rules that do not yet exist; putting the commitments already made into practice, with targets that show who is reached; and setting up bodies that oversee digital laws and handle complaints, with safeguards to protect from retaliation people who raise concerns or report rights violations. The recommendations in section 8 address each of these three steps.

8. RECOMMENDATIONS

The study makes thirty recommendations. Each answers a gap in Cambodian law or policy that was checked against the text of the laws and policies concerned. They are of five types:

- changes to a law or policy (8 recommendations);
- steps to put an existing commitment into practice (7);
- ways to hold decision-makers to account (6);
- measures to strengthen an institution (5);
- safeguards for groups at risk of being left out (4).

All recommendations are addressed to government bodies, which set the rules. Several also set obligations for private sector companies: mobile operators (R-AE-5, R-DP-2 and R-DP-6), online services (R-DP-2 and R-DP-6), and social media and messaging companies (R-SC-6). Eighteen recommendations can be acted on in the short term and twelve in the medium term. Annex D gives the full text of each recommendation: the gap it answers, who is affected, the Cambodian policies it refers to, the international standards that support it, the body that should act and the timeframe. Annex E ranks all thirty by human rights risk, urgency and feasibility.

8.1 Where to begin

NINE RECOMMENDATIONS TO BEGIN WITH

Nine recommendations are the most pressing, because the harm they address is serious and the law or system concerned is being decided now:

- R-SC-1 to R-SC-4: the four changes to the draft cybercrime law, on its undefined terms, on the offences of publishing non-factual or defamatory content, and on a judge's approval before a person's data is preserved, copied, seized or intercepted;
- R-DP-1: interim guidance on handling personal information until the data protection law is adopted;
- R-DP-2: information, in Khmer, about what happens to the identity documents people give when they register for a SIM card or an app;
- R-DP-4: data protection rules for ministries and other public bodies;
- R-AE-2: minimum requirements that government online services must meet before launch;
- R-GV-6: an assessment of each draft digital law and policy for its effect on people's rights, and a working group that reviews how it is applied once it is in force.

8.2 Recommendations by pillar

The recommendations are listed below by pillar, in order of priority within each pillar. The code in the first column, for example R-AE-2, is the one used in the annexes.

Access and Equity

Ref	Recommendation
R-AE-2	**Minimum requirements for government online services:** before launch, every government online service should work on the phones people commonly use, be available in Khmer, be usable by people with disabilities, collect only the personal data needed to provide the service, and have staff available to answer questions.
R-AE-4	**Cost of access and the universal service contribution:** mobile operators pay into a Universal Service Obligation Fund meant to extend access. Publish each year how this money is spent, with an independent audit made public, and involve civil society in deciding its priorities. Dedicate a clear share of the fund, for example 15 per cent, to Khmer-language assistive technologies and digital literacy for Indigenous and underserved communities.
R-AE-3	**Khmer-language screen reading software:** make the development of Khmer screen-reading software, which lets people with visual disabilities use phones and computers, a funded priority in national research and technology plans.
R-AE-7	**Provision in Indigenous languages:** recognise Indigenous communities as a group to be reached by digital training and public information, in their own languages.
R-AE-1	**Reach and design of digital literacy training:** publish guidance on using the national digital literacy competency framework to adapt training to each group, with targets for the groups currently reached least.
R-AE-5	**Clarity of internet pricing:** require mobile operators to present their prices in Khmer, in a way that lets customers compare offers.
R-AE-6	**How coverage is measured and targeted:** measure mobile coverage by land area as well as by share of the population, set targets on that basis, and name the communities still without a signal.
R-AE-8	**Testing and support when a service is launched:** test each government online service with the people who will use it before release, announce when it will be available, and publish the hours when help is available.

Security and Digital Civic Space

Ref	Recommendation
R-SC-1	**Undefined terms in the draft cybercrime law:** define in the law itself the terms that decide what content is a crime (Articles 3 and 28), such as "sovereignty and integrity", "insecurity", "instability" and "moral and cultural values", and state who decides whether content falls under them.

Ref	Recommendation
R-SC-2	**The offences of publishing non-factual or defamatory content:** define what counts as "non-factual" content, require proof that harm was caused, remove prison sentences for defamation, and make sure that reporting and comment on matters of public interest are not covered.
R-SC-3	**Preservation and copying of data held by companies:** require a judge's approval before the authorities order a company to preserve, copy or hand over a person's data, limit the use of that data to the investigation, and set when it must be deleted.
R-SC-4	**Access to and interception of a person's data:** require a judge's approval for interception, set rules on how intercepted data is stored and deleted, allow the person concerned to challenge the measure once informed of it, and keep investigations under the prosecutor rather than a government committee.
R-SC-5	**Where to report online harassment and abuse:** extend the police reporting service for online scams to online harassment and abuse, and train the officers who receive reports to deal with personal harm and to treat every person without blame and without regard to their gender identity or sexual orientation.
R-SC-7	**Online safety education for children and young people:** make online safety a required part of digital literacy teaching in schools and youth training, covering how to secure accounts, recognise scams and get help, with delivery targets and a way to measure them.
R-SC-6	**Moderation of abusive content in Khmer:** raise with the social media and messaging companies used in Cambodia the need to detect and remove abuse written in Khmer.

Responsible Data Use and Privacy

Ref	Recommendation
R-DP-1	**Guidance while the data protection law is in preparation:** issue interim guidance on how organisations should handle personal information until the data protection law is adopted and applies.
R-DP-2	**Information about what happens to identity documents:** require phone operators and online services to explain in Khmer, when people register and afterwards, how their identity documents are used, stored and shared.
R-DP-4	**Personal data held by government:** apply to ministries and other public bodies the same data protection rules the draft law sets for companies.
R-DP-5	**Information about Indigenous communities and their land:** set out who decides how information about Indigenous communities, their land and their natural resources is collected and used, and give those communities a say in that decision.
R-DP-3	**Who decides complaints about personal data:** give the Personal Data Protection Unit created by the draft law the task of receiving and deciding complaints from people whose data has been misused.
R-DP-6	**Accounts linked to a phone number that is resold:** require operators to warn customers before a phone number is cancelled and again before it is resold, make the 90-day wait before resale a permanent rule, and require online services to check that the new holder of a number cannot open the previous holder's accounts.

Automation and the Future of Work

Ref	Recommendation
R-AW-1	**Employment status of platform workers:** clarify how the Labour Law applies to people who find work through apps, such as delivery and ride-hailing drivers.
R-AW-2	**Support for workers whose work changes because of digitalisation:** follow how digital technology changes jobs and working conditions on an ongoing basis, and publish the results.
R-AW-3	**Artificial intelligence and creative work:** the National Committee on Intellectual Property Protection, with the Ministry of Post and Telecommunications, should set out how creators can report work, voices or images copied by artificial intelligence tools, and how their reports will be handled.

Governance

Ref	Recommendation
R-GV-6	**Assessment and review of digital laws and policies:** before adopting any digital law or policy, assess and publish its likely effect on people's rights, looking at each group separately and at people who belong to several groups at once. Once it is in force, set up a working group, including civil society and affected groups, to review how it is applied, with funding set out in the law or policy so that civil society members can take part independently.
R-GV-1	**How consultations are run:** publish guidance setting out when a draft must be shared, how long people have to respond and who should be invited.
R-GV-5	**Knowing what data exists:** prepare a list of the data government bodies hold on digital access and use, showing who holds each dataset and when it was last updated.
R-GV-2	**Barriers of logistics and inclusion in consultation:** hold some consultations outside Phnom Penh or online, cover travel costs for provincial organisations, and invite organisations beyond those a ministry already knows.
R-GV-3	**Measuring how digital laws and policies affect people:** measure and report the results of digital laws and policies separately for women, rural communities, older people, people with disabilities and workers.
R-GV-4	**Period between adoption and entry into force:** leave time between the adoption of a digital law and the date it applies, so that it can be explained and guidance issued.

8.3 Focus of the policy brief

The four-page policy brief presents a selection of the thirty recommendations, organised by pillar. The selection draws on the ranking in Annex E, on the evidence from the research and on the discussion at the validation workshop. Five considerations guided it.

- **Priority:** seven of the nine most pressing recommendations listed in section 8.1 are in the first tier of the brief: R-SC-1 to R-SC-4, R-AE-2, R-DP-1 and R-GV-6. An eighth, R-DP-4, is in the second tier.

- **Decisions still open:** each selected recommendation concerns a law, policy or system that is still being decided: the draft cybercrime law, the draft data protection law, the draft Law on Digital Government (which covers requirements for online services and the Digital Government Committee), and the artificial intelligence regulation now being developed.
- **Strength of evidence:** most selected recommendations rest on confirmed findings. The others rest on problems that people described and that no Cambodian law or policy deals with.
- **One message per subject:** recommendations about the same law or the same body are presented together, so that each message speaks to one audience.
- **Coverage:** every pillar appears in both tiers. The first tier also includes R-DP-5, on Indigenous communities' say over information about their land, a concern raised by Indigenous organisations.

Tier 1 recommendations are the main messages of the brief, and Tier 2 recommendations follow them. The full text of each recommendation is in Annex D, its ranking in Annex E, and the evidence behind it in Annex C.

Pillar	Tier 1	Tier 2
Access and Equity	R-AE-2 Minimum requirements for government online services; R-AE-8 Testing and support when a service is launched	R-AE-1 Reach and design of digital literacy training
Security and Digital Civic Space	R-SC-1 to R-SC-4, the four recommendations on the draft cybercrime law, presented as one message	R-SC-5 Where to report online harassment and abuse; R-SC-6 Moderation of abusive content in Khmer
Responsible Data Use and Privacy	R-DP-1 Guidance while the data protection law is in preparation; R-DP-3 Who decides complaints about personal data; R-DP-5 Information about Indigenous communities and their land	R-DP-4 Personal data held by government
Automation and the Future of Work	R-AW-1 Employment status of platform workers; R-AW-2 Support for workers whose work changes because of digitalisation	R-AW-3 Artificial intelligence and creative work
Governance	R-GV-1 How consultations are run, together with R-GV-2 Barriers of logistics and inclusion in consultation; R-GV-6 Assessment and review of digital laws and policies	R-GV-3 Measuring how digital laws and policies affect people

9. LIMITATIONS AND AREAS FOR FURTHER RESEARCH

This section sets out the limits of the study and the research that could build on it.

9.1 Extending the findings

Sample: The study is based on twenty interviews and four focus group discussions, so its findings reflect the views of the people consulted. Research with larger groups of rights-holders, drawn directly from each group, would capture a wider range of views and show how widely the situations described here apply.

Remote communities: Research in remote, coastal, forest and Indigenous communities would add the views of people living furthest from services, where the gaps in mobile coverage and cost described in section 5 are greatest.

Laws and policies in draft: Several of the laws and policies reviewed are drafts, read in the latest version available to the study and dated where cited. Following them through revision and adoption would show whether the gaps identified here are closed before they take effect.

Documents not reviewed: The Constitution, the Criminal Code and the Civil Code were not part of the review, although interviewees said they contain some protections for personal data. Reviewing them would show how far existing law protects personal data and free expression until the new laws apply.

Data and infrastructure sovereignty: Cambodian policies use the term "data sovereignty" mainly to mean where data is stored, and several require sensitive data to be held in the country. Interviewees described protections, such as security audits in the telecommunications sector, that follow the rules of foreign parent companies rather than Cambodian regulation. Research on who sets and enforces the rules for data and digital infrastructure in Cambodia, including systems supplied or operated by foreign companies, would complement this study.

9.2 Evidence gaps to investigate

The study identified seven subjects that further research could develop.

Older people and civic space: how older people experience free expression, online harm and taking part in public life.

Platform workers: the conditions of work arranged through apps, as described by the workers themselves.

Platform companies: how delivery and ride-hailing companies describe their terms, how their apps make decisions about workers, and how workers are treated.

Rural access fund: what the Universal Service Obligation Fund has paid for, and who has benefited from it.

Customer data: whether, and how, customer information held by phone operators and online services is shared or sold.

Consultation on policies and on laws: whether a formal difference exists between consultation on policies and consultation on laws.

Redress in rural communities: what people in rural communities do when a digital service fails or they lose money.

9.3 Disputed findings to test

Four findings rest on accounts that differ, which further research could test.

Cybercrime law and expression: whether the draft cybercrime law, once adopted, changes what people say and publish online.

Pace of job losses: how quickly automation replaces workers in manufacturing compared with informal work.

Consultation on the artificial intelligence strategy: who took part in the consultation on the draft strategy, and at what stage of the text.

National data: how complete and up to date the national data on digital access and use is.

10. ANNEXES

The annexes below accompany this report.

- Annex A. Policy mapping matrix of the national instruments reviewed
- Annex B. Benchmarking matrix against international and regional instruments
- Annex C. Findings synthesis matrix
- Annex D. Recommendations Master Sheet
- Annex E. Prioritisation of the recommendations
- Annex F. Record of validation workshop inputs and the revisions they produced