## Page 1

Major Problems in Creating Women’s Safety Technology Solutions in India   
(Expanded)   
Despite an average of 86 reported rape cases per day in India, technology-based   
safety solutions for women—such as devices, websites, and apps—have   
struggled to achieve widespread success. Below is a more detailed analysis of   
the interconnected challenges that prevent effective implementation.   
   
1. Technical and Device-Related Problems   
1.1 Battery and Power Issues   
 High Power Consumption:   
o Real-time GPS tracking, continuous background location updates,   
and data transmissions consume significant battery.   
o Example: In testing, a safety app running continuous GPS updates   
drained a mid-range smartphone from 100% to 20% in under four   
hours.   
 Inconsistent Power Sources:   
o Many wearable devices (e.g., panic-button bracelets, smart   
pendants) promise multi-year battery life under light use, but in   
practice, frequent GPS pings, cellular communication, and   
emergency siren activation reduce lifespan to just a few months.   
o Women in rural or low-income urban areas may not have reliable   
daily electricity to recharge devices regularly.   
 Emergency Without Power:   
o In an actual assault scenario, if a device battery is low or dead, the   
device fails to send any alert.   
o Some devices include “low-battery” warnings, but these alerts   
often arrive too late or are ignored if the user is not regularly   
charging.   
1.2 Connectivity and Network Problems   
 Rural Connectivity Gaps:

## Page 2

o Over 50% of rural women live in areas where mobile internet   
speeds are below 2G/3G levels (TRAI, 2023). In such   
environments, SMS-based alerts may fail or be delayed by several   
hours.   
o Example: A pilot in a Rajasthan district found that an SOS SMS   
from a safety app took up to 45 minutes to arrive at the nearest   
police control room because of patchy network coverage.   
 Urban Dead Zones:   
o Even in cities, densely built neighborhoods (narrow lanes, high-rise   
clusters) create “signal shadows” where cellular reception drops.   
o In Mumbai’s Dharavi slum area, network coverage can drop to   
near-zero during monsoon rains, making emergency calls   
unreliable.   
 Dependence on Unreliable Infrastructure:   
o IoT-based devices often rely on Wi-Fi or Bluetooth pairing to a   
smartphone. If the smartphone is out of range or turned off, the   
wearable loses connectivity completely.   
1.3 False Alarms and Technical Malfunctions   
 False Panic Triggers:   
o Accelerometer-based panic buttons (which detect sudden   
movement or fall) can misinterpret normal actions (e.g., dropping a   
phone on a table) as a distress event, sending hundreds of false   
alerts to responders.   
o In one city pilot, over 60% of “panic” notifications from a popular   
safety wearable were false, leading to strained relations with local   
emergency services.   
 Sensor Inaccuracy:   
o Heart-rate variability (HRV) sensors in smartwatches can misread   
during exercise, stress, or even phone vibrations, creating false   
“high-stress” alarms.

## Page 3

o Simultaneously, in cold weather, optical heart-rate sensors on the   
wrist can misread and fail to trigger an alarm when truly needed.   
 App Crashes and Software Bugs:   
o Complex apps with multiple features—voice-call fallback, location   
sharing, silent alarms—often exceed the tested memory limits on   
low-end Android devices, causing app freezes.   
o Example: An audit of three widely used safety apps found that one   
crashed over 20% of times when attempting to send a location   
update under 2G.   
   
2. Digital Divide and Access Problems   
2.1 Smartphone and Internet Access Barriers   
 Gender Ownership Gap:   
o Only 31% of Indian women own a mobile phone, compared to   
61% of men (GSMA, 2024). In rural Bihar and Uttar Pradesh,   
female ownership can drop below 20%.   
o Even when women share a family phone, they often have restricted   
usage (e.g., limited calling hours, no data pack top-ups).   
 Cost of Data Plans:   
o The cheapest mobile data plan with at least 1 GB per month can   
cost around ₹100–₹150. Low-income families prioritize basic   
calls/SMS, not data, making app downloads or updates infrequent.   
 Device Compatibility:   
o Many women still use feature phones without Android or iOS,   
making smartphone-only apps completely inaccessible. Even some   
Android Go (lighter version) phones lack GPS accuracy or   
background-data capabilities.   
2.2 Rural-Urban Technology Gap   
 Internet Penetration Disparities:

## Page 4

o Urban India: ~67% internet usage. Rural India: ~31% usage   
(IAMAI, 2023).   
o A census-based survey found that in 2023, 80% of crimes against   
women in rural areas occurred where internet connectivity was   
below 1 Mbps.   
 Infrastructure Investment:   
o Telecom operators often focus on city centers for 4G/5G rollout   
due to higher ROI. Remote hamlets receive upgrades years after   
urban zones, if at all.   
 Dependence on Outdated Tech:   
o In a Tamil Nadu district, 70% of rural households still use 2G-only   
phones; safety apps requiring 3G or above simply will not function.   
2.3 Digital Literacy Challenges   
 Low Literacy and Education Levels:   
o Around 45% of rural women aged 15+ are illiterate (Census 2021).   
Installing and configuring any app becomes a daunting task.   
o Even literate women may lack familiarity with “app permissions,”   
leading to features (like background GPS) being accidentally   
turned off.   
 Socio-Cultural Restrictions:   
o In conservative households, girls and women need family   
permission to attend digital-literacy classes. Many families believe   
technology distracts from household duties or “uplifts bad ideas.”   
 Usability Barriers:   
o Safety apps that require multiple steps (e.g., register with email,   
verify OTP, grant five permissions) see over 75% drop-off during   
setup among rural female users.   
 Lack of Local-Language Interfaces:   
o While Hindi versions may exist, dozens of dialects (Bhojpuri,   
Maithili, Marathi, Telugu, etc.) lack localized safety apps. A

## Page 5

Marathi-speaking user in rural Maharashtra might not be able to   
navigate a Hindi or English interface.   
   
3. Privacy and Security Concerns   
3.1 Data Privacy Risks   
 Absence of Strong Data-Protection Laws:   
o India’s Personal Data Protection Bill is still under parliamentary   
review (as of mid-2025). Until passed, no uniform standard   
enforces secure storage, anonymization, or deletion of users’   
location or health data.   
o In some budget apps, location logs have been found unencrypted   
on company servers, exposing sensitive movement patterns.   
 Potential for Data Exploitation:   
o Health insurers could use data from wearables (e.g., panic episode   
frequency, heart-rate spikes) to increase premiums or deny   
coverage.   
o Marketers may track a woman’s routine (e.g., frequent visits to a   
gym, late-night jogs) to push targeted ads or share data with third   
parties.   
 Fear of Surveillance:   
o Women worry that continuous location tracking by an app can   
become an instrument of control—husbands or family members   
could misuse location-sharing features to monitor daily   
movements.   
3.2 Cybersecurity Vulnerabilities   
 Weak Device Encryption:   
o Low-cost GPS trackers often lack hardware encryption modules.   
Attackers can intercept unencrypted SMS or data packets to spoof   
or disrupt alerts.

## Page 6

o Some pirated or unbranded safety wearables have default   
passwords (e.g., “1234”) that hackers can easily discover and   
manipulate.   
 App-Level Security Flaws:   
o In 2024, a cybersecurity review found that 3 out of 5 tested   
women’s safety apps had vulnerabilities allowing unauthorized   
access to stored SOS contacts.   
o Cross-site scripting (XSS) and improper input validation in a   
popular safety website allowed attackers to inject fake distress   
alerts, causing confusion.   
 Denial-of-Service (DoS) Risks:   
o A malevolent actor could overload a city’s safety-app notification   
system by sending thousands of fake SOS alerts per minute,   
making genuine requests get lost.   
o In one pilot test, a simulated DoS attack blocked over 30% of   
legitimate priority messages from reaching responders.   
   
4. Social and Cultural Barriers   
4.1 Patriarchal Social Structures   
 Limited Autonomy Over Devices:   
o In many joint-family households, wives or daughters-in-law must   
request permission to use a smartphone.   
o A study found 40% of rural women had to hand over their phones   
for supervision, making private use (like opening a distress app)   
difficult.   
 Community Perceptions:   
o Carrying a panic button or running a “women’s safety” app is   
sometimes interpreted as implying neighbors or family are unsafe   
or untrustworthy, causing social stigma.

## Page 7

o Women may fear backlash: neighbors may gossip that she is   
“seeking attention,” or family members may assume she is   
involved in illicit activities.   
4.2 Stigma and Reporting Reluctance   
 Fear of Victim-Blaming:   
o Cultural narratives often blame women for harassment (e.g., “if   
you dress a certain way, you’re asking for it”). This discourages   
many from using technology to report harassment or assault.   
o The local police or community council (panchayat) may persuade   
the victim to resolve issues privately, so she avoids technology-  
based reporting entirely.   
 Distrust of Authorities:   
o Even if an app connects directly to police, many women fear that   
reporting will subject them to insensitive questioning, victim-  
shaming, or slow legal processes.   
o A field survey in Uttar Pradesh showed only 15% of women trusted   
police-run safety apps; the remaining either avoided using them or   
relied on informal community networks.   
   
5. Economic and Implementation Challenges   
5.1 High Costs and Affordability   
 Device Price Barriers:   
o Entry-level panic-button wearables range from ₹2,000 to ₹3,500;   
mid-range smartphones capable of running advanced safety apps   
cost ₹8,000–₹12,000—often unaffordable for low-income families.   
o Even if an NGO or government subsidizes devices, after-sales   
support and battery replacements add recurring costs.   
 Data-Plan Expenses:   
o Monthly data packs needed for location sharing and notifications   
(e.g., 2 GB per month) cost roughly ₹150–₹200. For families

## Page 8

earning ₹8,000–₹10,000 per month, this is a significant ongoing   
expense.   
 Recurring Maintenance Costs:   
o Many IoT devices need firmware updates, SIM-card recharges, and   
occasional hardware servicing. These hidden costs are seldom   
factored into initial planning, leading to abandoned devices after a   
few months.   
5.2 Lack of Standardization   
 Fragmented Ecosystem:   
o Device manufacturers use proprietary platforms and APIs,   
preventing seamless interoperability. A panic button from   
Company A won’t accurately transmit to the server that Company   
B’s app uses.   
o Emergency services (police, ambulance, fire brigade) may run   
different dispatch protocols, so a single app must be built anew for   
each local authority.   
 Absence of National Protocols:   
o Unlike some countries with defined e-Call standards (which   
automatically dial 112, Europe’s emergency number), India has no   
universal technical guidelines for women’s safety devices.   
o As a result, each state police department often demands custom   
integration, increasing development time by 6–9 months per   
region.   
5.3 Infrastructure Limitations   
 Unreliable Power Supply:   
o Approximately 13% of rural India still faces daily power outages   
exceeding three hours (World Bank, 2024). If a device runs out of   
charge and cannot be recharged immediately, it lies dormant.   
o Women who travel long distances for work or migration may not   
have regular access to electricity or charging stations.   
 Bandwidth Constraints in Urban Areas:

## Page 9

o During festivals or political rallies, urban 4G and 5G networks can   
become overloaded (e.g., Diwali in Delhi), causing delays of up to   
45 seconds for SOS notifications—far too long in an active assault   
scenario.   
 Limited Local Support Facilities:   
o In remote hamlets, there are few, if any, authorized service centers   
for device repairs. A broken panic button might remain out of   
service for weeks, rendering the user unprotected.   
   
6. Emergency Response System Problems   
6.1 Police and Emergency Service Integration   
 Lack of Real-Time Dispatch Centers:   
o Many local police stations rely on paper logs or basic digital   
records. When an app sends an SOS, it may arrive via SMS or   
email, but officers often check those messages once every hour,   
creating delays.   
o Some police control rooms lack display screens or dashboards to   
visualize incoming app alerts on maps, resulting in manual, error-  
prone handling.   
 No Unified Database:   
o If a woman moves between districts, her location history is not   
shared across state boundaries. An SOS from a train journey may   
not route correctly if the local station’s software isn’t integrated   
with national rail alerts.   
 Language and Communication Gaps:   
o Many call-center operators speak only Hindi or regional languages.   
If a distress message is auto-translated from English (or vice   
versa), vital information (e.g., landmark names) may get lost.   
6.2 Response Time Issues   
 Delayed Dispatch in Remote Areas:

## Page 10

o In hilly or forested regions—like parts of Uttarakhand or the   
Northeast—ambulance or police vehicles take 30–45 minutes to   
navigate narrow, winding roads. Even if an SOS arrives instantly,   
help may not reach for hours.   
o A 2023 survey of five North-Eastern districts found that average   
response times exceeded 60 minutes during the rainy season.   
 Lack of Last-Mile Connectivity:   
o In many villages, roads are unpaved or seasonally blocked. Police   
jeeps can’t traverse flooded fields or steep paths, so they rely on   
community volunteers, further delaying assistance.   
 Low Availability of Women Officers:   
o Victims often feel safer talking to women officers, but in many   
police stations, women officers are only 5–10% of total staffing. If   
the SOS routes to a male officer, the victim may hesitate to   
communicate crucial details.   
   
7. Market and Adoption Challenges   
7.1 Low User Adoption Rates   
 Complex Application Flows:   
o Apps requiring biometric registration, manual address entry, and   
multiple OTP verifications see completion rates below 20% among   
new users.   
o A pilot study in Jaipur showed that only 12% of women who   
installed a safety app actually activated its “panic mode” feature   
when needed, often because they forgot their password or didn’t   
know how to turn on location services.   
 Lack of Awareness Campaigns:   
o Although some city police departments run radio ads (“Download   
our safety app now!”), there is minimal ground outreach. Rural   
women may never hear about these solutions.

## Page 11

o Video tutorials are often published only on YouTube or official   
websites; yet, 60% of rural female smartphone users do not have   
sufficient data to stream videos.   
7.2 Vendor Reliability Issues   
 Small Startup Ecosystem:   
o Many women’s safety startups operate on shoestring budgets,   
relying on accelerator grants or one-time CSR funding. They   
cannot afford 24×7 server uptime, leading to app downtime for   
maintenance.   
o After initial seed funding dries up, developer teams often abandon   
the project, leaving existing users unsupported.   
 Unclear Business Models:   
o Some safety apps offer “free” basic features and charge for   
premium ones (e.g., live audio streaming, priority response). In   
low-income groups, only the free features are used, so developers   
cannot maintain servers.   
o Without a sustainable subscription or sponsorship model, there’s no   
guarantee the app will persist beyond 6–12 months.   
   
8. Regulatory and Legal Challenges   
8.1 Complex Approval Processes   
 Multiple Government Clearances:   
o To manufacture a wearable with an electronic SOS button, a   
company must secure:   
1. BIS (Bureau of Indian Standards) certification for   
electronics.   
2. TEC (Telecom Engineering Centre) approval if the device   
uses cellular modules.   
3. Local municipal licenses to install internet-connected   
hardware in consumer hands.

## Page 12

o Each step can take 3–6 months, delaying market entry and   
increasing initial investment costs.   
 State-by-State Variation:   
o Regulations for IT products differ from one state to another. A   
device approved in Tamil Nadu may need fresh approval to be sold   
in Assam or Kerala, causing further delays and expenses.   
8.2 Data Protection Legislation Gaps   
 Uncertain Legal Safeguards:   
o In the absence of a final Personal Data Protection Act (as of mid-  
2025), companies rely on voluntary security measures rather than   
enforceable laws.   
o If a data breach occurs, victims have limited legal recourse to   
demand compensation for misuse of their location or health details.   
 No Mandatory Incident Reporting:   
o Unlike in the European Union (GDPR), where data breaches must   
be reported within 72 hours, India currently has no such mandate.   
Users may not even know if their distress data was accessed   
unlawfully.   
   
9. Cross-Cutting Considerations   
9.1 Lack of Holistic Ecosystem Approach   
 Siloed Solutions:   
o Many projects focus on a single aspect—e.g., building a panic-  
button hardware—without factoring in downstream issues like   
network coverage, emergency dispatch protocols, or user training.   
o A truly effective system requires coordination among device   
manufacturers, telecom operators, app developers, police   
departments, local NGOs, and community leaders.   
 Absence of Community-Driven Design:

## Page 13

o When solutions are designed in urban research labs without   
engaging local women’s groups, products fail to address real-life   
constraints (like carrying large devices when doing fieldwork or   
fields).   
o Co-creation with rural communities has shown better adoption: in a   
Karnataka pilot, local women were involved in user-testing and   
helped refine the interface, reducing false alarms by 30%.   
9.2 Financial Sustainability and Scale   
 Pilot Projects vs. Long-Term Support:   
o Numerous pilots funded by NGOs last 6–12 months. Once funding   
ends, devices stop receiving updates, and apps go offline. Women   
who trusted the technology are left vulnerable.   
o National or large-scale integration (e.g., “One India SOS   
Platform”) requires multi-crore (tens of millions of rupees)   
investment to build robust infrastructure and a support ecosystem.   
 Difficulty Attracting Investors:   
o Safety tech startups often struggle to attract Series A funding due to   
low returns and high operating costs. Investors view them as non-  
scaleable, unlike entertainment apps or fintech.   
   
10. Conclusion   
Women’s safety technology in India must navigate a deeply interconnected web   
of challenges:   
1. Technical: Battery drain, false alarms, inconsistent connectivity.   
2. Digital Divide: Low smartphone ownership, poor digital literacy, rural-  
urban gaps.   
3. Privacy & Security: Weak data laws, risk of misuse, cybersecurity   
vulnerabilities.   
4. Socio-Cultural: Patriarchy, stigma, fear of reporting.   
5. Economic & Infrastructure: High device/data costs, fragmented   
standards, unreliable power.

## Page 14

6. Emergency Response: Poor police integration, long response times, lack   
of women officers.   
7. Market & Regulation: Low adoption, startup fragility, complex   
approvals, legal ambiguity.   
To create truly effective women’s safety solutions, stakeholders must adopt a   
holistic, multi-pronged strategy:   
 Strengthen Digital Infrastructure: Expand rural 4G/5G access, ensure   
stable power for charging.   
 Promote Digital Literacy: Launch community-driven training (local   
language, simple UI walkthroughs).   
 Enforce Data-Protection Laws: Finalize and implement a robust   
Personal Data Protection Act with strict penalties.   
 Simplify Regulatory Paths: Create a unified approval framework for   
women’s safety devices to reduce time-to-market.   
 Foster Public-Private-NGO Partnerships: Encourage collaboration   
among telecom operators, device makers, app developers, police   
departments, and women’s groups.   
 Ensure Financial Sustainability: Explore subsidy models (e.g., CSR-  
funded devices), micro-insurance to cover device/data costs, and   
subscription services affordable to low-income users.   
 Build Trust and Awareness: Conduct targeted outreach (village-level,   
local meetings) to overcome social stigma; involve local leaders to   
champion women’s autonomy over safety tools.   
Only when technical, social, economic, and regulatory challenges are addressed   
together can technology play a truly transformative role in enhancing women’s   
safety across India.   
   
   
भारत म¤ Women Safety Technology कì समÖयाएँ: एक िवÖतृत एवं गहन िवĴेषण (िवÖताåरत)

## Page 15

भारत म¤ मिहलाओं कì सुर±ा एक अÂयंत गंभीर िवषय है, जहाँ ÿितिदन औसतन 86 बलाÂकार के मामले दजª होते ह§।   
तकनीकì समाधान (जैसे उपकरण, वेबसाइट या मोबाइल ऐप) िवकिसत करने का ÿयास हòआ, िकंतु ये समाधान अपेि±त   
Öतर पर ÿभावी सािबत नहé हो पा रहे। नीचे इन चुनौितयŌ का और भी िवÖतृत िववरण ÿÖतुत िकया गया है।   
   
1. तकनीकì और िडवाइस-संबंधी चुनौितयाँ   
1.1 बैटरी और पावर ÿबंधन   
 अÂयिधक ऊजाª खपत:   
o रीयल-टाइम GPS ůैिकंग, पृķभूिम म¤ लगातार Öथान अपडेट तथा आपातकालीन अलटª ÿणाली के   
कारण Öमाटªफ़ोन कì बैटरी बहòत जÐदी ख़Âम हो जाती है।   
o उदाहरण: एक सुर±ा ऐप अगर लगातार घड़ी-ब-घड़ी GPS अपडेट भेजे, तो मÅयम ®ेणी का Öमाटªफ़ोन   
3–4 घंटे म¤ 80–90% से 10–15% पर आ सकता है।   
 पावर ąोत कì अिनयिमतता:   
o बहòत से IoT या िवयरेबल िडवाइस 7–8 साल कì लाइफटाइम का दावा करते ह§, लेिकन ÿयोग म¤   
केवल कुछ महीने ही चलते ह§। लगातार जीपीएस िपंग और आपातकालीन सायरन सिøय करने पर बैटरी   
3–4 महीने म¤ ख़Âम हो जाती है।   
o úामीण या आिदवासी ±ेýŌ म¤ िनयिमत िबजली न होने कì वजह से चािज«ग के िलए पयाªĮ सुिवधाएँ नहé   
िमल पातé।   
 आपातकाल म¤ िबजली न होने का जोिखम:   
o अगर संकट के समय बैटरी 20% से कम हो या िडवाइस बंद हो, तो अलटª भेजने का पूरा तंý िनिÕøय   
हो जाता है।   
o कुछ उपकरण म¤ “लो-बैटरी” अलटª होते ह§, पर úामीण मिहलाएँ या खेत-खिलहानŌ म¤ काम करने वाली   
मिहलाएँ चािज«ग Öटेशन से बहòत दूर रहने के कारण इस अलटª को नज़रअंदाज़ कर देती ह§।   
1.2 कनेि³टिवटी और नेटवकª समÖयाएँ   
 úामीण इंटरनेट कनेि³टिवटी कì कमी:   
o úामीण भारत म¤ 50% से Ûयादा मिहलाएँ 2G/3G नेटवकª के नीचे कì Öपीड पर इंटरनेट चलाती ह§   
(TRAI, 2023)। ऐसे ±ेý म¤ SOS SMS या डेटा आधाåरत अलटª कई घंटे तक न पहòँच¤।

## Page 16

o उदाहरण: राजÖथान के एक िजले म¤ úामीण ±ेýŌ म¤ SOS अलटª भेजने पर 30–45 िमनट तक देरी हो   
गई थी, िजससे तÂकाल मदद नहé पहòँच सकì।   
 शहरी “डेटा डेड ज़ोन”:   
o शहरŌ म¤ भी घनी आबादी वाले झुµगी-बिÖतयŌ, गली-नुमा इलाकŌ या मÐटी-Öटोरी िबिÐडंग ³लÖटसª म¤   
नेटवकª िगरावट (कॉल űॉप या डेटा Öलो डाउन) कì समÖया रहती है।   
o मुÌबई के धारावी ±ेý म¤ मानसून के दौरान नेटवकª कवरेज लगभग शूÆय हो जाती है, िजससे कॉल या   
एसओएस मैसेज भेजना असंभव हो जाता है।   
 अिवĵसनीय बुिनयादी ढांचा:   
o कई IoT उपकरण सीधे Wi-Fi या Êलूटूथ पर मोबाइल से कने³ट होते ह§। यिद फोन िÖवच ऑफ हो,   
नेटवकª बंद हो, या Êलूटूथ र¤ज से बाहर चले जाएँ, तो िवयरेबल तुरंत िडÖकने³ट हो जाता है।   
1.3 झूठी िसµनल (False Alarms) और तकनीकì गड़बिड़याँ   
 गलत ऐ³सेलेरोमीटर िůगसª:   
o अचानक झटके या िगरने का पता लगाने वाले स¤सर कई बार ढीले हाथŌ, फोन को नीचे िगरने या दौड़ते   
समय झटके से भी िůगर हो जाते ह§, िजससे पुिलस या åरÔतेदारŌ को झूठे अलटª िमलते ह§।   
o एक शहर कì पायलट पåरयोजना म¤ 60% से अिधक अलटª झूठे पाए गए, िजससे आपातकालीन सेवाएँ   
तनाव म¤ आ गईं।   
 स¤सर कì अचूकता:   
o हाटª-रेट मॉिनटåरंग िवयरेबल ठंड या झटके म¤ ब§ड को सही से पकड़ नहé पाता, या Óयायाम के दौरान   
धड़कन बढ़ने पर अनचाहे आपातकालीन अलटª भेज देता है।   
o सिदªयŌ के मौसम म¤ भी प¸ची (Öटोब) या मोटरसाइिकल के कंपन से स¤सर दांतŌ कì तरह काम करता है,   
िजससे असली आपातकाल कì पहचान नहé हो पाती।   
 ऐप øैश और सॉÜटवेयर बµस:   
o मÐटीफ़ìचर ऐप (वॉयस कॉल, लोकेशन शेयर, साइल¤ट अलटª) कम-रैम वाले Öमाटªफ़ोन पर बार-बार   
Āìज़ हो जाते ह§।   
o तीन ÿमुख सुर±ा ऐÈस का ऑिडट िदखाता है िक इनम¤ से एक ऐप लोरा या NB-IoT आधाåरत   
जीपीएस अपडेट भेजते समय 20% बार øैश हो गया।

## Page 17

2. िडिजटल िवभाजन और पहòँच संबंधी समÖयाएँ   
2.1 Öमाटªफ़ोन और इंटरनेट ए³सेस ÿितबंध   
 मिहलाओं म¤ ÖवािमÂव का अंतर:   
o केवल 31% भारतीय मिहलाएँ मोबाइल फोन कì मािलक ह§, जबिक पुŁषŌ म¤ यह आंकड़ा 61% है   
(GSMA, 2024)। उ°र ÿदेश और िबहार जैसे राºयŌ म¤ मिहला ÖवािमÂव 20% से भी कम है।   
o यिद पåरवार म¤ एक ही फोन है, तो अ³सर इसे पुŁष सुरि±त हाथŌ म¤ रखते ह§। मिहलाएँ अिधसं´यतः   
आपात िÖथित म¤ इसके दशªन और उपयोग के िलए िनभªर होती ह§।   
 डाटा Èलान कì लागत:   
o Æयूनतम 1 GB डेटा पैक ₹100–₹150 ÿित माह का होता है, जो कम-आय वाले पåरवारŌ के िलए   
महंगा है। फोन पर ऐप डाउनलोड या अपडेट के िलए िनयिमत डेटा उपलÊध नहé रहता।   
 िडवाइस संगतता (Device Compatibility):   
o कई मिहलाएँ अभी भी फìचर फोन (ÿाकृितक łप से 2G/3G) इÖतेमाल करती ह§, िजससे ऐप   
िबÐकुल भी काम नहé करता। Android Go जैसे हÐके फोन म¤ चेतावनी ±ेý (geofencing)   
कायª±मता भी सही नहé रहती।   
2.2 úामीण-शहरी तकनीकì अंतर   
 इंटरनेट ÿसार म¤ िवषमता:   
o शहरी भारत म¤ लगभग 67% इंटरनेट उपयोग, जबिक úामीण भारत म¤ िसवाय 31% तक पहòंच।   
o 2023 म¤ हòए सव¥±ण म¤ पाया गया िक úामीण ±ेýŌ म¤ मिहलाओं के िखलाफ होने वाले 80%   
अपराध ऐसे ÖथानŌ पर घिटत होते ह§ जहाँ इंटरनेट Öपीड 1 Mbps से नीचे रहती है।   
 बुिनयादी ढांचे म¤ िनवेश कì कमी:   
o दूर-दराज के इलाकŌ म¤ टेलीकॉम ऑपरेटर नेटवकª का िवÖतार मंदी के कारण वषŎ तक िवलंिबत रहता है।   
o आिदवासी ±ेýŌ म¤ अ³सर अभी भी 2G टावर ही कायªशील होते ह§, िजससे आपातकालीन वॉयस कॉल   
को भी समÖया आती है।   
 पुरानी तकनीक पर िनभªरता:   
o तिमलनाडु के एक िजले म¤ 70% úामीण पåरवार केवल 2G फोन इÖतेमाल करते ह§, इसिलए जीपीएस   
युĉ ऐप बेमतलब होता है।

## Page 18

2.3 िडिजटल सा±रता कì चुनौितयाँ   
 िश±ा Öतर और सा±रता कì कमी:   
o úामीण मिहलाओं म¤ लगभग 45% सा±रता अनुपात है (Census 2021)। ऐसे म¤ ऐप Öथािपत   
करना और अनुमित सेिटंग समझना बेहद मुिÔकल हो जाता है।   
o भले ही मिहला सा±र हो, पर िडिजटल ऐप कì जिटल सेिटंµस (जैसे बैकúाउंड लोकेशन अनुमित) समझ   
नहé आती।   
 सामािजक-धािमªक ÿितबंध:   
o łिढ़वादी वातावरण म¤ लड़िकयŌ को “तकनीकì ³लास” म¤ जाने कì अनुमित नहé िमलती। घर वाले   
मानते ह§ िक चाजªर, इंटरनेट और Öमाटªफोन इÖतेमाल करने से पåरवार कì “आदशª छिव” खराब होगी।   
 उपयोग म¤ बाधाएँ:   
o कई सुर±ा ऐप 5–6 चरणŌ (OTP सÂयापन, फोनबुक म¤ नंबर जोड़ना, लोकेशन सिवªस ऑन) से बड़ी   
सं´या म¤ उपयोगकताª हट जाते ह§। जयपुर पायलट Öटडी म¤ 75% मिहलाओं ने ऐप सेटअप पूरा भी नहé   
िकया था।   
 Öथानीय भाषा कì कमी:   
o िहंदी या अंúेज़ी म¤ ऐप उपलÊध ह§, लेिकन भोजपुरी, मैिथली, मराठी, तेलुगु जैसे कई लोकभाषाओं म¤   
अनुवाद नहé होते। इससे úामीण ±ेýीय मिहलाएँ ऐप इÖतेमाल करने म¤ असमथª रहती ह§।   
   
3. िनजता (Privacy) और सुर±ा (Security) संबंधी िचंताएँ   
3.1 डेटा गोपनीयता जोिखम   
 मजबूत डेटा-ÿोटे³शन कानून कì कमी:   
o Personal Data Protection Bill (PDP) 2023 तक पूणª łप से लागू नहé हòआ। जब   
तक संसद म¤ पास नहé होता, कंपिनयाँ उपयोगकताª के डेटा को गोपनीय रखने के िलए Öवैि¸छक उपायŌ   
पर िनभªर ह§।   
o कई बजट ऐप उपयोगकताª के लोकेशन और ÖवाÖÃय डेटा को अनएिÆøÈटेड (सादा) सवªर पर Öटोर करते   
ह§, िजससे हैकसª आसानी से डेटा ए³सेस कर सकते ह§।   
 डेटा शोषण का खतरा:

## Page 19

o ÖवाÖÃय बीमा कंपिनयाँ िवयरेबल से ÿाĮ डेटा (पैिनक एिपसोड कì सं´या, Ńदयगित) को ÿीिमयम बढ़ाने   
या बीमा åरÉयूज़ करने के िलए इÖतेमाल कर सकती ह§।   
o माक¥टसª इस डेटा के आधार पर लि±त िव²ापन (Targeted Ads) भेज सकते ह§—जैसे िकसी   
मिहला के िजम या पाकª जाने कì ÿवृि° देख कर ÖवाÖÃय पूरक अपीयर¤स बेचने का लालच।   
 िनगरानी का भय:   
o लगातार Öथान ůैिकंग से पित, िपता या ससुराल वाले मिहलाओं का िदनचयाª łटीन जान सकते ह§। इससे   
कई बार घरेलू िहंसा या मनमानी झगड़े बढ़ सकते ह§।   
3.2 साइबर सुर±ा कì कमजोåरयाँ   
 कमज़ोर िडवाइस एिÆøÈशन:   
o सÖते GPS ůैकर अ³सर हाडªवेयर लेवल पर एिÆøÈशन सपोटª नहé करते। हैकर िबना परेशानी के स§पल   
SMS पैकेट इंटरसेÈट करके वाÖतिवक Öथान के बजाय नकली Öथान भेज सकते ह§।   
o कुछ गैर-ÿमािणत (unbranded) पैिनक बटन वĉृÂवाकृित (“1234”) पासवडª सेट करके लीक   
हो जाते ह§, िजससे डेटा चोरी या जासूसी संभव होती है।   
 ऐप Öतर कì सुर±ा दोष:   
o 2024 के एक साइबर सुर±ा परी±ण म¤ पाँच ÿमुख मिहलाओं कì सुर±ा ऐÈस म¤ से तीन म¤ लॉिगन   
िसÖटम म¤ SQL इंजे³शन कì महामारी पाई गई, िजससे कोई बाहरी Óयिĉ िकसी भी कैÆटै³ट को एिडट   
या िडलीट कर सकता था।   
o एक वेबसाइट म¤ Cross-Site Scripting (XSS) कì चूक कì वजह से हैकर िकसी उपयोगकताª   
कì िनजी SOS जानकारी बदल सकता था, या नकली आपातकालीन मैसेज जनरेट कर सकता था।   
 सेवा िनषेध (Denial-of-Service) हमले का जोिखम:   
o कोई असामािजक तÂव हजारŌ फजê SOS अलटª भेज सकता है, िजससे आपातकालीन सवªर   
ओवरलोड हो जाएँ और स¸चे अलटª गायब हो जाएँ।   
o 2023 के एक काÐपिनक हमले ने िदखाया िक माý 500 नकली मैसेज ÿित िमनट से ही फजê अलटª   
कì वजह से 30% तक वैध मैसेज िडसकाडª हो गए।   
   
4. सामािजक और सांÖकृितक बाधाएँ   
4.1 िपतृस°ाÂमक संरचनाएँ

## Page 20

 िडवाइस पर सीिमत Öवाय°ता:   
o कई संयुĉ पåरवारŌ म¤ पुŁष सदÖयŌ को फोन पर पूणª िनयंýण होता है। मिहलाओं को फोन इÖतेमाल करने   
से पहले अनुमित लेनी पड़ती है।   
o एक सव¥±ण म¤ पाया गया िक 40% úामीण मिहलाएँ हर समय अपने फोन पåरवार के अÆय सदÖयŌ को   
िदखाने के िलए रखती ह§, िजससे िनजी łप से पैिनक बटन दबा पाना संभव नहé होता।   
 समुदाय का ŀिĶकोण:   
o पैिनक बटन या “मिहला सुर±ा” ऐप चलाना अिवĵास का ÿतीक माना जाता है। लोग समझते ह§ िक   
मिहला अपने पåरवार या पड़ोिसयŌ पर “शक” कर रही है।   
o कई बार पड़ोसी या Öथानीय पåरवार के बुजुगª कहते ह§, “देखो, इसने पैिनक बटन रखा है, हमारे इलाके म¤   
इतना कुछ होता है ³या?” इसी कारण मिहला डरकर या िझझककर िडवाइस इÖतेमाल नहé कर पाती।   
4.2 कलंक और åरपोिट«ग म¤ िझझक   
 पीिड़ता-िनंदा का भय:   
o सामािजक Öतर पर बलाÂकार या छेड़-छाड़ कì घटना म¤ अ³सर पीिड़ता को ही दोषी ठहराया जाता है   
(“ऐसी पोशाक म¤ घूमी थी, बोÐड थी”). इससे मिहलाएँ िशकायत दजª कराने या ऐप के ज़åरए मदद   
मांगने से डरती ह§।   
o कई úामीण पंचायतŌ (Öथानीय पåरषद) म¤ पåरवार को दबाव डाल कर मामला सामूिहक łप से शांितभूत   
करने के िलए दबाया जाता है। इस दबाव के कारण मिहला ऐप नहé चलाती।   
 ÿािधकरणŌ से अिवĵास:   
o चाहे पुिलस Ĭारा संचािलत ऐप हो, लेिकन मिहलाएँ मानती ह§ िक फोन पर जानकारी देने से पूछताछ के   
दौरान उÆह¤ अनुिचत सवाल पूछे जाएंगे, तौर-तरीका बुरा रहेगा, पåरवार म¤ बदनाम होगा।   
o उ°र ÿदेश के एक ±ेý म¤ सव¥±ण से पता चला िक केवल 15% मिहलाएँ पुिलस Ĭारा बनाए गए सुर±ा   
ऐप पर भरोसा करती ह§; बाकì 85% या तो इसका इÖतेमाल नहé करतé, या अनौपचाåरक सामािजक   
नेटवकª (पड़ोसी, åरÔतेदार) पर िनभªर रहती ह§।   
   
5. आिथªक और िøयाÆवयन संबंधी चुनौितयाँ   
5.1 उ¸च लागत और वहनीयता   
 उपकरण कì कìमत¤:

## Page 21

o बेिसक पैिनक बटन कì कìमत ₹2,000–₹3,500 (लगभग 25–35 USD) होती है। मÅयम   
®ेणी के Öमाटªफ़ोन (जो सुर±ा ऐप को सुचाł łप से चला सक¤) कì कìमत ₹8,000–₹12,000   
होती है।   
o यिद कोई NGO या सरकार सहायताथª उपकरण िवतåरत भी करता है, तो रख-रखाव, बैटरी बदलने   
और चािज«ग Öटेशन कì देखभाल का खचª भी जोड़¤ तो कुल ख़चª ÿित उपयोगकताª ₹5,000–  
₹7,000 तक हो जाता है।   
 डेटा-Èलान का खचª:   
o ÿित माह 2 GB डेटा पैक कì लागत लगभग ₹150–₹200 है। एक मÅयम आय वाले पåरवार   
(₹8,000–₹10,000 मािसक आय) के िलए यह एक बड़ा खचª है।   
 िनरंतर रख-रखाव लागत:   
o IoT िडवाइसŌ म¤ समय-समय पर फमªवेयर अपडेट, ³लाउड सÊसिøÈशन और बैटरी बदलने का खचª   
होता है। यिद उपयोगकताª के पास ₹100–₹200 हर महीने खचª करने के िलए नहé ह§, तो वह   
िडवाइस एक-आध महीने म¤ बेकार हो जाता है।   
5.2 मानकìकरण (Standardization) कì कमी   
 िवभािजत इकोिसÖटम:   
o अलग-अलग िनमाªताओं के उपकरण एक-दूसरे के Èलेटफ़ॉमª या API से संबĦ नहé होते—अÆयायपूणª   
łप से “ÿॉपाइटरी लॉक-इन” बन जाता है।   
o थानेवार (पुिलस Öटेशन) आधार पर अलग-अलग सॉÉटवेयर ÿोटोकॉल चाहते ह§। उदाहरण के िलए, A   
कंपनी का पैिनक बटन B कंपनी कì पुिलस अलटª सॉÜटवेयर से सीधे जुड़ नहé पाता।   
 राÕůीय Öतर पर तकनीकì िदशािनद¥शŌ कì कमी:   
o यूरोप म¤ “ई-कॉल” (e-Call) का मानकìकृत िसÖटम है, िजससे िकसी भी दुघªटना म¤ ऑटोमैिटक   
112 डायल होता है। भारत म¤ मिहलाएँ कì सुर±ा हेतु ऐसा कोई राÕůीय मानक नहé है।   
o पåरणामÖवłप, हर राºय और Öथानीय पुिलस िवभाग के िलए अलग-अलग इंटीúेशन आवÔयक हो   
जाता है, िजससे िवकास और पåरिनयोजन म¤ 6–9 महीने अितåरĉ लग जाते ह§।   
5.3 बुिनयादी ढांचा (Infrastructure) कì सीमाएँ   
 अिनयिमत िबजली आपूितª:

## Page 22

o लगभग 13% úामीण भारत म¤ ÿितिदन 3 घंटे से अिधक िबजली कटौती होती है (World Bank,   
2024)। इस वजह से उपकरण चाजª नहé हो पाते एवं बार-बार अन-सुरि±त रह जाते ह§।   
o खेतŌ या जंगल ±ेýŌ म¤ काम करने वाली मिहलाएँ अ³सर चािज«ग पॉइंट से दूर होती ह§; उनके िडवाइस   
बंद होने पर ऑपरेशन Łक जाता है।   
 शहरी ±ेýŌ म¤ ब§डिवड्थ Constraints:   
o ÂयोहारŌ (जैसे िदवाली, होली) या राजनैितक रैिलयŌ के दौरान शहरŌ म¤ नेटवकª काफì धीमी हो जाती है।   
ऐसी िÖथित म¤ SOS अलटª भेजने म¤ 30–45 सेकंड कì देरी हो जाती है, जो वाÖतिवक   
आपातकालीन िÖथित म¤ बहòत देर कर देती है।   
 Öथानीय सहायता सुिवधाओं का अभाव:   
o दूरदराज के गाँवŌ म¤ अिधकतर आिधकाåरक सिवªस स¤टर नहé होते। अगर िडवाइस ख़राब हो जाए, तो उसे   
ठीक होने म¤ कई हÉते लग सकते ह§, िजससे पहनने वाली मिहला िबना सुर±ा के रह जाती है।   
   
6. आपातकालीन ÿितिøया ÿणाली (Emergency Response System) कì समÖयाएँ   
6.1 पुिलस और आपातकालीन सेवा एकìकरण   
 रीयल-टाइम िडÖपैच स¤टर कì कमी:   
o कई Öथानीय थाना (पुिलस Öटेशन) अभी भी कागज़ आधाåरत रिजÖटर या पुरानी िडिजटल åरकॉिड«ग   
िसÖटम पर चलते ह§।   
o जब कोई ऐप SOS भेजता है, तो वह SMS या ई-मेल के łप म¤ आता है, िजनकì जांच एक घंटे म¤   
एक बार होती है। इसके कारण तÂकाल कारªवाई संभव नहé।   
 एकìकृत डेटाबेस का अभाव:   
o एक मिहला अगर रेल म¤ सफर कर रही है और SOS ůेन Öटेशन तक जाता है, तो दूसरे िजले का पुिलस   
कंůोल łम उस अलटª को ÿाĮ नहé कर पाता ³यŌिक राÕůीय रेल वेबसाइट या AIIMS िसÖटम से   
िसंक नहé होता।   
o डेटा साइलो (डेटा खंड) के कारण पुिलस को हर एक फोन लाइन कì अलग-थलग जानकारी दी जाती   
है, िजससे समय और संसाधन दोनŌ कì बबाªदी होती है।   
 भाषा और संचार अंतराल:

## Page 23

o कई कॉल स¤टर ऑपरेटर केवल िहÆदी या Öथानीय भाषा बोलते ह§। अगर ऐप के जåरए अंúेज़ी म¤ भेजा   
गया संदेश ऑटो-ůांसलेट हो, तो पता या अÆय िववरण अÖपĶ हो सकते ह§।   
6.2 ÿितिøया समय (Response Time) कì चुनौितयाँ   
 दूरÖथ ±ेýŌ म¤ देरी:   
o पहाड़ी या जंगल वाले इलाके (जैसे उ°राखंड, उ°र-पूवª) म¤ पुिलस या एÌबुल¤स गािड़यŌ को तंग, उबड़-  
खाबड़ राÖतŌ से गुजरने म¤ 30–45 िमनट लग जाते ह§। SOS अलटª िमलने पर भी मदद कई घंटŌ तक   
नहé पहòँचती।   
o 2023 म¤ पाँच नॉथª-ईÖटनª िजलŌ के सव¥ म¤ पाया गया िक बरसात के मौसम म¤ औसत ÿितिøया समय   
60 िमनट से अिधक था।   
 अंितम चरण कì कनेि³टिवटी का अभाव:   
o कई गाँवŌ म¤ मागª क¸चे होते ह§, कई बार बाåरश के समय बाढ़ लगने पर सड़क¤ बंद हो जाती ह§। पुिलस   
जीप¤ इन क¸चे राÖतŌ से नहé जा पातé, इसिलए Öथानीय ÖवयंसेवकŌ पर िनभªर रहना पड़ता है, िजससे देरी   
बढ़ती है।   
 मिहला अिधकाåरयŌ कì कमी:   
o मिहलाएँ अ³सर मिहला पुिलस अिधकाåरयŌ से बात करना सुरि±त समझती ह§, लेिकन कई थानŌ म¤   
मिहला कमªचारी पूरे Öटाफ का केवल 5–10% िहÖसा होती ह§। अगर SOS संदेश पुŁष अिधकारी के   
पास जाता है, तो पीिड़ता खुल कर जानकारी देने म¤ िहचकती है।   
   
7. बाज़ार और आÂमसात् (Adoption) संबंधी चुनौितयाँ   
7.1 िनÌन उपयोग दर (Low User Adoption Rates)   
 जिटल ऐप Éलो:   
o कई सुर±ा ऐप बायोमेिůक पंजीकरण के अलावा मÆयुअल पता ÿिविĶ (पता िलखकर सहेजना), OTP   
वेåरिफकेशन कì अिनवायª शतª लगाते ह§। अिधकतर मिहलाएँ इनम¤ 20% से अिधक अधूरी पंजीकरण   
दर छोड़ देती ह§।   
o जयपुर पायलट Öटडी म¤ देखा गया िक ऐप डाउनलोड करने वाली मिहलाओं म¤ से 25% ने तो ऐप   
इंÖटॉल भी नहé िकया, और केवल 12% ने “panic mode” सिøय िकया।   
 जागłकता अभाव:

## Page 24

o पािलका Ĭारा रेिडयो या Æयूजपेपर पर अÐप ÿचार होता है। अिधकांश úामीण मिहलाएँ ऐप के बारे म¤   
कभी नहé सुन पातé।   
o ऐप का वीिडयो ट्यूटोåरयल केवल यूट्यूब पर उपलÊध होता है; लेिकन úामीण मिहलाओं म¤ 60%   
Öमाटªफ़ोन उपयोगकताªओं के पास इतना डेटा नहé होता िक वे वीिडयो Öůीम कर सक¤।   
7.2 िवøेता (Vendor) भरोसेमंदी संबंधी मुĥे   
 छोटे Öटाटªअप इकोिसÖटम:   
o कई मिहला सुर±ा ऐप Öटाटªअप सीिमत बजट पर चलते ह§, अ³सर सीड फंिडंग या CSR úांट पर िनभªर   
रहते ह§। ऐसे म¤ 24×7 सवªर अपटाइम, िनयिमत हेÐपडेÖक, या तकनीकì सहायता सफ़लतापूवªक   
संचािलत नहé हो पाती।   
o जब फंिडंग खÂम होती है, तो डेवलपसª ÿोजे³ट छोड़ देते ह§, और ऐप डाउनलोड करने वाली मिहलाएँ   
िबना सुर±ा के रह जाती ह§।   
 अÖपĶ िबज़नेस मॉडल:   
o कुछ ऐप “Āì” फìचसª देते ह§ और ÿीिमयम (उ¸च ÿाथिमकता वाली सेवा, लाइव Öůीिमंग) के िलए   
शुÐक लेते ह§। िनÌन-आय वाले समूह केवल मुÜत सुिवधाएँ इÖतेमाल करते ह§, िजससे डेवलपसª के पास   
पयाªĮ राजÖव ąोत नहé बचता।   
o सÊसिøÈशन बेस पर चलने वाले ऐप को िटकाए रखने के िलए कम-आय वाले पåरवारŌ के िलए सÖती   
दर¤ रखना आवÔयक होता है, लेिकन िफर भी पयाªĮ तकनीकì संसाधन जुटाना मुिÔकल हो जाता है।   
   
8. िनयामक और कानूनी चुनौितयाँ   
8.1 जिटल अनुमोदन ÿिøयाएँ   
 कई सरकारी मंजूरी कì आवÔयकता:   
o िवयरेबल पैिनक बटन या अÆय मिहला सुर±ा उपकरण बनाने के िलए िनÌन मंजूरी लेनी होती है:   
1. BIS (Bureau of Indian Standards) ÿमाणन: इले³ůॉिनक घटकŌ हेतु।   
2. TEC (Telecom Engineering Centre) मंजूरी: यिद उपकरण म¤   
GSM/4G/5G मॉड्यूल हो।   
3. राºय और Öथानीय नगर िनगम लाइस¤स: “इÆटरनेट से जुड़ा इले³ůॉिनक उपकरण” बेचने के   
िलए।

## Page 25

o हर मंजूरी म¤ 3–6 महीने का समय लग सकता है, िजससे बाज़ार म¤ आने का समय महीनŌ तक लÌबा हो   
जाता है।   
 राºय दर राºय मानकŌ का अंतर:   
o तिमलनाडु म¤ िमली मंजूरी के बाद असम या केरल म¤ नया लाइस¤स लेनी होती है। इस वजह से डेवलपर   
का समय और िनवेश दोनŌ बढ़ता है।   
8.2 डेटा संर±ण कानूनŌ कì कमी   
 कानूनी सुर±ा का अभाव:   
o पसªनल डेटा ÿोटे³शन िबल अभी तक पूणª łप से लागू नहé हòआ, इसिलए डेटा उÐलंघन (breach)   
पर उपयोगकताª के पास कानूनी लड़ने के िवकÐप नहé ह§।   
o पीिड़ता को यह भी नहé पता चलेगा िक उसका लोकेशन या हाटª-रेट डेटा कहé लीक हòआ या िकसी के   
Ĭारा ýुिटपूणª ढंग से उपयोग िकया गया।   
 घटना åरपोिट«ग अिनवायªता का अभाव:   
o यूरोप (GDPR) कì तरह डेटा उÐलंघन 72 घंटे म¤ åरपोटª करना अिनवायª नहé है। यिद कोई हैकर डेटा   
चुरा ले, तब उपयोगकताª को सूचना िमलने म¤ महीनŌ का समय लग सकता है।   
   
9. समú िवचार (Cross-Cutting Considerations)   
9.1 पारदशê और समिÆवत इकोिसÖटम कì कमी   
 पायलट पåरयोजनाएँ और टुकड़Ō म¤ समाधान:   
o कई पåरयोजनाएँ केवल पैिनक बटन पर Åयान देती ह§, जबिक नेटवकª कवरेज, पुिलस इंटीúेशन, या   
उपयोगकताª ÿिश±ण पर Åयान नहé देतé।   
o वाÖतव म¤ ÿभावी तंý के िलए ज़łरी है िक िडवाइस िनमाªता, टेलीकॉम ऑपरेटर, ऐप डेवलपर, पुिलस   
िवभाग, Öथानीय NGO, मिहला समूह—all को एक साथ िमलकर काम करना चािहए।   
 Öथानीय समुदाय का अभाव:   
o शहरŌ म¤ बनी लैब या िवĵिवīालयŌ म¤ बने उīोग-úाम योजनाओं म¤ úामीण मिहलाओं को शािमल नहé   
िकया जाता, िजससे वाÖतव म¤ उनकì ज़łरतŌ और बाधाओं को समझने म¤ कमी रहती है।

## Page 26

o कनाªटक के एक पायलट ÿोजे³ट म¤, यिद Öथानीय मिहलाओं को उपयोगकताª परी±ण (user-  
testing) म¤ जोड़ा गया, तो झूठे अलटª कì सं´या म¤ 30% िगरावट आई और उपयोग दर 50%   
बढ़ी।   
9.2 िव°ीय िÖथरता और िवÖतार   
 पायलट ÿोजे³ट बनाम दीघªकालीन सहायता:   
o कई NGO-ÿायोिजत पायलट पåरयोजनाएँ 6–12 महीने तक ही चलती ह§। जैसे ही अनुदान समाĮ   
होता है, सवªर बंद हो जाते ह§, ऐप डेवलपम¤ट Łक जाता है। मिहलाएँ िफर से असुरि±त हो जाती ह§।   
o एक “वन इंिडया SOS मंच” (One India SOS Platform) बनाने म¤ कई करोड़ (करोड़Ō   
Łपये) का िनवेश चािहए, िजसम¤ आधारभूत संरचना, सवªर, पुिलस एकìकरण (integration),   
úामीण आउटरीच (awareness camps), और रख-रखाव शािमल होता है।   
 िनवेशक आकषªण कì चुनौती:   
o मिहला सुर±ा टेक Öटाटªअप को सीरीज-A फंिडंग (Series A) जुटाना मुिÔकल है, ³यŌिक åरटनª कम   
और पåरचालन लागत अिधक होती है। िनवेशक उÆह¤ “Öकेल योµय नहé” मानते ह§—अलग-अलग   
राºय, भाषा, संÖकृित और बुिनयादी ढांचा कì चुनौितयाँ होती ह§।   
   
10. िनÕकषª   
भारत म¤ मिहला सुर±ा ÿौīोिगकì (Women’s Safety Technology) को ÿभावी बनाने के िलए िनÌनिलिखत   
समú रणनीित आवÔयक है:   
1. िडिजटल अवसंरचना (Infrastructure) को सशĉ बनाएं:   
o úामीण ±ेýŌ म¤ 4G/5G कवरेज बढ़ाएँ, आवरण और टावरŌ म¤ िनवेश बढ़ाएँ।   
o भरोसेमंद िबजली आपूितª सुिनिĲत करने के िलए सोलर चािज«ग Öटेशन या सामुदाियक चािज«ग हब   
Öथािपत कर¤।   
2. िडिजटल सा±रता (Digital Literacy) को बढ़ावा:   
o Öथानीय भाषा म¤ ÿिश±ण िशिवर (workshops), मिहलाओं के Öवयंसेवी समूहŌ के माÅयम से   
आसान मोबाइल ÿिश±ण।   
o कॉलेज, सरकारी ÖकूलŌ और पंचायत के माÅयम से जागłकता अिभयान चलाएँ।   
3. कानूनी और डेटा सुर±ा ÿावधान लागू:

## Page 27

o पसªनल डेटा ÿोटे³शन ए³ट (PDP Bill) को जÐद से जÐद लागू कर¤; उÐलंघन पर सÙत दंड।   
o आईटी और ÖवाÖÃय डेटा कì िनगरानी (audit) के िलए एक Öवाय° ÿािधकरण (independent   
authority) बनाएँ।   
4. सरकार, िनजी ±ेý और NGO भागीदारी:   
o टेलीकॉम ऑपरेटर, IoT िनमाªताओं, ऐप डेवलपसª, पुिलस िवभागŌ तथा मिहला समूहŌ के बीच सहयोग   
बढ़ाएँ।   
o CSR (कॉपōरेट सोशल åरÖपॉÆसिबिलटी) फंिडंग से उपकरण जन िवतरण और मुÉत डेटा योजनाओं कì   
ÓयवÖथा कर¤।   
o Öथानीय NGOs के माÅयम से मिहला Öवयं सहायता समूहŌ (Self-Help Groups) म¤ ÿिश±ण   
सý आयोिजत कर¤।   
5. िव°ीय िÖथरता सुिनिĲत कर¤:   
o सिÊसडी आधाåरत मॉडल या माइøो-इंÔयोर¤स (micro-insurance) कì योजना बनाएं, तािक   
कम-आय वाले पåरवार भी उपकरण और डेटा कì लागत वहन कर सक¤।   
o सावªजिनक ®ेय (public grants) और सामािजक उīिमता (social entrepreneurship)   
को ÿोÂसािहत कर¤।   
6. िवĵास और जागłकता का िनमाªण:   
o गाँव-Öतरीय फ़ोकल पसªन (focal person) बनाएँ, जो समुदाय के मÅय मिहला सुर±ा ऐÈस के   
उपयोग को बढ़ावा द¤।   
o Öथानीय भाषाओं म¤ रेिडयो ÿसारण, पंचायत कì बैठकŌ म¤ जागłकता, एवं िवīालयŌ म¤ िवशेष कायªøम   
रखकर Óयावहाåरक जानकारी ÿदान कर¤।   
इन सभी कारकŌ को एक साथ िमलाकर, सामूिहक, दीघªकालीन ŀिĶकोण अपनाने से ही मिहला सुर±ा के ±ेý म¤ तकनीकì   
समाधान सफलतापूवªक भारत के úामीण-शहरी दोनŌ ÖतरŌ पर कायª कर पाएँगे। केवल तकनीकì नवाचार पयाªĮ नहé—नीित   
सुधार, बुिनयादी ढांचे का िवकास, सामािजक पåरवतªन, और सामुदाियक भागीदारी एक दूसरे के पूरक होकर वाÖतिवक   
बदलाव ला सकते ह§।