

Chapter 18

Cyber Vulnerabilities of Informal Workers in India

Antu Rani Majumdar, Assistant Professor, Swami Vivekananda University, Dr. Malay Adhikari, Assistant Professor, Amity University, Kolkata and Prof. (Dr.) Pradeepta Kishore Sahoo, Principal, Law College Durgapur.

Abstract

The rapid digitalisation of labour markets has transformed the nature of work, extending technological systems into informal and contract-based employment. While these developments promise efficiency, transparency, and inclusion, they simultaneously expose workers to emerging cyber vulnerabilities. This chapter examines the paradox of informal workers in the digital age, where informal and contract workers become increasingly visible through data collection yet remain legally unprotected. It argues that cyber risks such as data exploitation, identity theft, algorithmic wage manipulation, workplace surveillance, and online harassment are structurally embedded within contemporary labour arrangements.

Adopting a socio-legal approach, the chapter critically analyses the limitations of existing legal frameworks, including the Code on Social Security, 2020, the Code on Occupational Safety, Health and Working Conditions, 2020, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, highlighting their fragmented and inadequate response to worker-centric cyber harms. It further explores how power imbalances, digital illiteracy, and the absence of accountability in contract labour arrangements exacerbate these vulnerabilities.

The chapter contends that cybersecurity must be reconceptualised as a labour rights issue rather than merely a technological concern. It calls for an integrated regulatory framework that recognises digital safety as part of working conditions, ensures employer accountability, and protects the informational privacy and dignity of workers. By bridging the gap between cyber law and labour law, this study contributes to the evolving discourse on digital labour governance in India.

Keywords: *Informal Labour, Cyber Vulnerability, Data Protection and Algorithmic Control*

1. Introduction

The changes witnessed in labour markets over the last decades have been strongly influenced by the growth of gig economy and contract labour. Technology has changed the way people participate in labour markets as labourers have an opportunity to engage in flexible employment and perform their tasks under contracts without necessarily being formally employed. Although this change has presented economic gains, it has also deprived the participants of some benefits that would be available in case of permanent employment. The main issue with contract labour and informality in labour markets is that neither of these categories enjoys a number of benefits, such as health insurance, leaves,

job stability, and protection under labour laws. Participation of informal labour in economic activity is crucial; however, it goes unnoticed, which is why this type of labour is labelled “informal.”⁴⁵⁸

Invisibility in this case not only refers to the economic marginalization of such people, but also involves invisibility in the cyberspace domain. Given that such people have to rely on digital technology to secure jobs and perform tasks, cybersecurity becomes a significant concern for them. Irrespective of the role one plays, be it a cab driver who needs to seek customers through online platforms, a person who arranges deliveries using apps, a freelancer who finds clients through websites, or a domestic helper who seeks jobs online, digital technology becomes a crucial platform for earning a livelihood.⁴⁵⁹ But at the same time, the need to use digital technology opens the door to several cybersecurity issues. In the absence of any knowledge about digital technology and without any assistance from any institution, such people become highly susceptible to phishing, scams, identity theft, and other forms of cybercrime.

Moreover, the workplace in the platform system can involve gathering and analyzing large amounts of data about workers' behaviour and personal information. The degree of control by the informal workers over the collected data, its management, and accessibility is minimal. The algorithm behind the task allocation, the evaluation of workers' performance, and wage determination is very obscure and makes the workers vulnerable to exploitation, monitoring, and even blocking of their accounts. It follows that cybersecurity cannot be regarded as only a technical problem.

Considering the above discussion, therefore, it is apparent that a dire need for action exists. It is necessary to formulate measures that ensure that the digitalization era takes into consideration the protection of informal workers. Ensuring that informal workers have their cyberspace protected is necessary to ensure the protection of worker rights via measures that ensure that this is accomplished. This will ensure that digitalization does not result in even greater inequalities but instead promotes the objectives of inclusiveness.

2. Understanding informal worker

The informal labour force, therefore, can be defined as those kinds of labour that are essential in the process of producing goods and services in the economy, yet they lack any official acknowledgment in the system of recognition. The term 'informal labour' refers to that kind of labour force which lacks both recognition and appreciation from any official policy or law formulated by the government.⁴⁶⁰

⁴⁵⁸ VV Giri National Labour Institute, *Gig and Platform Workers: Vision Towards Social Protection in India* (VVGNI 2021).

⁴⁵⁹ National Commission for Enterprises in the Unorganised Sector (NCEUS), *Report on Conditions of Work and Promotion of Livelihoods in the Unorganised Sector* (Government of India 2007).

⁴⁶⁰ Kunal Sen and Ravi Kanbur, 'Informality in India: Causes, Consequences and Policy Responses' (2015) *Indian Journal of Labour Economics*.

This is because informal labour includes those kinds of productive labourers like domestic labourers, street vendors, homeworkers, etc.

In addition, another aspect that contributes to informal employment is the lack of an employment agreement outlining terms of employment. Without evidence backing their allegations, the employers can alter payment rates, number of working hours, and duties allocated to the worker at will with no fear of any repercussions whatsoever. In this respect, informal employment shields the employer or his agent from any possible consequences of their actions. One of the problems encountered by workers engaging in informal employment is the issue of job insecurity. The workers have no guarantee they will be able to secure similar jobs in the coming day. They are engaged on either a daily basis or based on piece work. Conversely, during formal employment, individuals are able to access various social security services including medical services and compensation for injuries. Carefulness is going to be vital when it comes to planning, since if such people have an accident or get ill, they will be well prepared to deal with it. This implies that it would be difficult for them to plan their future life as a result of the unpredictability of the economy.

Informal workplace conditions may also be as a result of lack of protection. Many laws relating to work are written in the assumption that formal employment has occurred. Informal workers thus are not covered by law since they do not work within its realm. Even if there exist laws that cover informal employees, it remains difficult for such people to use the laws since they are rarely implemented.

However, in the case of the employee group under discussion, the application of the technology involves only consumption of information and not participating in the process. They have no knowledge regarding the techniques of negotiations related to the use of the digital technology and the power dynamics that exist in negotiating the use of the digital technology at their workplace. The process of negotiation is even more difficult for them because there are no organizations like trade unions to fight their cause.⁴⁶¹

3. Digitalization and the Informal Workforce

Indeed, technology has brought about various implications on the labour market, particularly for people who depend on the informal economy for their living. Due to the presence of technology inventions like mobile phones, mobile money transfers, software programs, and identity verification systems, people have been able to get jobs and make some money. It is important to point out that the shift in power relations within the labour market has been facilitated by these developments.

3.1. Platform-Based Work and Algorithmic Control

There is no doubt that gig labour should be mentioned as an example of the effects of digitalization. The intermediary role of the platforms will consist in bringing together people who want to perform

⁴⁶¹ Internet Freedom Foundation, *Privacy and Data Protection in India: Issues and Challenges* (IFF Report).

tasks and people who require these tasks to be performed.⁴⁶² Generally, the people providing their services will be regarded as independent contractors and not their employees.

This kind of work would surely be extremely easy to perform, considering the factor of digitization. However, aside from the advantage mentioned above, some problems arise when it comes to digitization in relation to this type of work. This is due to the fact that the processes involved, such as task assignment, assessment, and remuneration for the effort expended, have become automatic. In addition, individuals performing this kind of digitized task do not truly understand how it operates. Furthermore, there is always the possibility of blocking the user account.

3.2. Digital Payments and Financial Exposure

There have been numerous changes in the life of informal employees due to the adoption of digital money transaction systems. It is because of the existence of digital wallets as well as other forms of digital money transaction services like fast money and online banking that make it possible for informal workers to act without necessarily carrying any cash. Digital money transaction systems not only facilitate access to money for informal employees but also makes it possible for them to engage in financial transactions.

Nonetheless, although it is true that there arise some benefits from this transition, some challenges associated with this very transition revolve around exposing the informal labour force to different forms of danger. Indeed, since the informal labourers get their money using the technological method, they open themselves up to different dangers, especially hacking.⁴⁶³

3.3. Online Identity Systems and Data Dependence

Moreover, the mandatory use of digital IDs for accessing services not only at the office but also at government departments has also brought the informal workers into the digital age. It is important to have IDs, biometrics, and accounts on mobile devices to access the digital platform.

On the contrary, while these tools may have been quite useful in ensuring that verifying information and reducing paperwork was easy, the reality is that they end up being tools for gathering data on people. The people working in the informal economy do not know how their data is being managed.⁴⁶⁴ Dependence on digital identity can therefore become a double-edged sword facilitating access while simultaneously increasing exposure to data misuse.

⁴⁶² V V Giri National Labour Institute, *Gig and Platform Workers: Vision Towards Social Protection in India* (VVG NLI 2021).

⁴⁶³ The Cashless Revolution *The Cashless Revolution: China's Reinvention of Money and the End of America's Domination of Finance and Technology* (Oxford University Press 2020).

⁴⁶⁴ Re-Engineering India *Re-Engineering India: Technology Solutions for the World's Largest Democracy* (Penguin Books India 2015).

3.4.Role of Digital Literacy

Another factor worth mentioning that adds complexity to the situation is that of digital illiteracy. Indeed, it can be said without exaggeration that the informal workers will be completely unfamiliar with any form of digital technology before undertaking their job. This implies that such people have no clue as to:

- Distinguishing legitimate emails from phishing emails.
- Making sure that their personal data remains secure.
- Safely logging into their accounts.
- Devising solutions to digital conflicts.

Without this foundational knowledge, workers are unable to safeguard themselves against cyber threats. Digital tools, instead of empowering them, can become instruments of exploitation.

4. Structural and Institutional Challenges

The cybersecurity dangers faced by informal and contractual employees go further than personal risks because of their connection to systematic vulnerabilities within the system as a whole. The cybersecurity threats posed to informal and contractual employees can be linked to systematic failure, which has led to these employees being marginalized in cyberspace.

4.1. Digital Illiteracy and Knowledge Gaps

The second issue that emerges regarding the process of adoption is connected with the lack of digital skills among the workers. On the one hand, the workers should learn to operate in the digital space and become accustomed to performing certain tasks online and earning money online due to their lack of skills, but not as a result of being well-prepared. In spite of the fact that nowadays most individuals make transactions and use different services via smartphones and applications, they know very little about creating secure passwords, two-factor authentication, protecting themselves from cyber threats, and securing personal data.

Specifically, since workers are unaware of such threats as sending OTP codes, clicking on malicious links, and installing malware, they are vulnerable to various types of cyber-attacks.

4.2. Absence of Accessible Grievance Redressal Mechanisms

Another key issue that emerges is the absence of an effective channel through which such complaints can be filed. In the informal sector, employees are unaware of how to file a complaint with regard to cyber-fraud, cyber identity theft, and cyber harassment. There may be a cybercrime help line, but it would not be easily accessible to them.⁴⁶⁵

⁴⁶⁵ Centre for Internet and Society, *Privacy, Security and Digital Inclusion in India* (CIS Report).

Apart from that, the process of receiving compensation for the damages suffered is both time-consuming and demanding, which explains why workers do not take this route. In most cases, people who fall victim to cybercrimes prefer to accept their destiny rather than fighting back for justice, since it would be less troublesome.

4.3. Informality and Lack of Employer Accountability

The employment contract is a cause of cyber-crime through a number of lenses. It must be noted that certain obligations lie on the employer's part when it comes to maintaining secrecy concerning confidential information and creating a safe work environment for the worker. However, the employment contract loses its relevance and essence when the employer-worker relationship remains informal in nature and the duties of the former towards the latter are nonexistent.

When it comes to remote employment, the online service providers replace the employer in the context of their mutual interaction and thus, any obligations they have towards the employee become binding and meaningless. Therefore, there is no sense of accountability remaining from the perspective of the online service provider, while the burden of obligations lies solely on the employee's part.⁴⁶⁶

4.4. Technological Inequality and Access Constraints

The technology gap creates more chances of cybercrime. The informal labour is forced to rely on less sophisticated devices such as low-cost cell phones and outdated software. Besides, they might have to share computers that do not have adequate security measures in place. The problem of not having secured internet and wireless services further complicates the situation especially when using free Wi-Fi services.

Moreover, because of their financial constraints, such informal labourers are unable to afford sophisticated technological devices as well as anti-virus programs.

5. Digital Vulnerabilities and The Precarity of Informal Workers

Digital vulnerabilities translate into economic loss, social harm, and legal exclusion, reinforcing the precarious position of such workers in the digital economy.

5.1. Gig Workers and Fraudulent Digital Interfaces

Delivery drivers, chauffeurs, and freelancers depend greatly on the use of mobile applications when they search for gigs that offer them income. This dependency may be abused by hackers since the trust that gig workers have on mobile applications can provide them with a loophole in gaining access to the gig workers' personal information.

⁴⁶⁶ Ministry of Electronics and Information Technology (MeitY), *Annual Report* (Government of India).

There have been instances wherein gig workers receive calls from fraudsters who pose as members of the platform that gig workers use. They trick the victims into signing in to a fraudulent website or updating their login details to install a new version of the application. This causes the gig workers to divulge their login details and even the one-time password.⁴⁶⁷

Algorithmic management in the gig economy is highly straightforward and ruthless. The vast majority of gig workers depend on their daily wages. Therefore, anything that would disrupt them negatively could include low morale, additional costs, or even the alteration of algorithms. The situation becomes much more complicated due to the lack of responsibility at the level of the platform. Once the gig worker is impacted by some form of misconduct on the part of the platform, he will not be able to recover his losses.⁴⁶⁸

It has become clear from the case of All India Gig Workers Union vs. Union of India, where there have been questions about the implementation of workers' rights and handling the pandemic situation. The matter of lack of accountability of such platforms, along with their arbitrariness regarding income earned by gig workers, has come to light.⁴⁶⁹

5.2. Domestic Workers and Fake Job Portals

Today, there are numerous individuals searching for work through online platforms and social media channels. Although these platforms provide the best opportunity for finding jobs, they are also the places where these individuals can be easily fooled by scammers.

The scammers would offer jobs that pay well and have acceptable working conditions, but these would come at a price in terms of application costs and personal data sharing. Some of these helpers could get involved in money laundering schemes, while others could become victims of human trafficking.

Due to the unsatisfactory nature of the method adopted for verifying such transactions and the ignorance among the employees, there will obviously be numerous cases of deception and frauds. This is because they don't fall under the organized sector, therefore not covered by any law. Privacy rights are included within the broader ambit of privacy rights as mentioned by K.S. Puttaswamy (Aadhaar) vs. Union of India. In supporting the constitutional validity of the Aadhar scheme in India, the apex court in its judgment states that the need for regulating the use of such information shall be proportionate. Employees using the Aadhar card as their mode of payment face various difficulties, including non-payment of salary due to mismatched biometrics and misuse of information.⁴⁷⁰

Rather, the increasing phenomenon of implementing surveillance management systems in digital companies poses grave issues regarding challenges to the freedom and independence of employees. The monitoring of surveillance can occur via methods such as surveillance on mobile applications, geo-tracking, and measuring performances, which form what is known as the "digital panopticon."

⁴⁶⁷ Telecom Regulatory Authority of India (TRAI), *The Indian Telecom Services Performance Indicators* (TRAI Report).

⁴⁶⁸ Unique Identification Authority of India (UIDAI), *Annual Report* (Government of India).

⁴⁶⁹ Aparna Ravi, 'Regulating the Gig Economy in India: Platform Work and Labour Rights' (2022) *NUJS Law Review*.

⁴⁷⁰ Janaki Srinivasan and others, *Digital Identity and Inclusion in India* (IT for Change 2018).

This continuous act of surveillance may be harmful to the fundamental rights of humans safeguarded by Article 21 of the Constitution of India in the case of *Francis Coralie Mullin v. Administrator, UT of Delhi*.⁴⁷¹

5.3. Gendered Cyber Harassment and Online Abuse

Nevertheless, the individuals employed within the informal sector remain vulnerable to a number of cybercrimes due to the fact that they use computers in order to behave professionally or advertise their services.

For example, when women use social networking sites or instant messaging services in order to market their products, they may be subject to harassment and intimidation from the consumers. Additionally, their personal data could be misused without their permission. These activities can have adverse implications but women cannot demand justice since they lack knowledge about the law.

6. Towards an Inclusive Cybersecurity Framework

The implementation of a cyber security framework that will ensure that the interest of the informal workers will be included must go beyond theory and seek ways through which such a measure can actually be enforced among the informal workers. The framework does not only have to reduce cyber risk, but it must achieve a shift in power dynamics within the digital economy dominated by the informal workers.

6.1. Digital Literacy and Awareness

A further point that needs consideration here is that digital literacy among informal and contractual workers cannot just be seen as a one-way learning experience. Rather, digital literacy must be considered an ongoing process that considers changes to technology, platforms, and also the issue of cybersecurity. The point is that in today's day and age, with informal and contractual workers becoming increasingly dependent on the mobile workplace, digital security emerges as a very important aspect of workers' rights.⁴⁷²

6.2. Localized and Contextual Training Design

It is imperative for the digital literacy training program to start from a practical base. The majority of the current digital literacy training programs are bound to collapse because they have taken a very impractical stance. It would help if the training incorporated situations which might arise in the utilization of digital tools such as fraudster calls made by customers, fraudulent job opportunities posted on social media platforms, phishing emails regarding payments, and UPI and OTP scam cases.

In terms of accessibility, it is not enough for the training to be translated into regional languages; it must also be accessible through other means of communication like visually and auditory-based communications. Examples of such training content include short films, infographics, and story-based

⁴⁷¹ The Age of Surveillance Capitalism *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

⁴⁷² Centre for Internet and Society, *Digital Literacy, Privacy and Inclusion in India* (CIS Report).

modules because most of the employees are uneducated. Micro-learning modules, which contain information for 2 to 5 minutes, will be appropriate alongside application-based communication.⁴⁷³

6.3.Behavioural Change Approach

Knowledge alone will not guarantee the employees' safety when performing online operations. For instance, even though the workers know everything that threatens their information security, they will still suffer from the effects of the circumstances due to their urgent need for money or because they have a habit of sending emails. Based on this reasoning, digital literacy should be able to cover the understanding of behavioural learning.

There are two approaches that could be used to address this challenge. First, the application can send text reminders to remind the employees that they have to safeguard their credentials and should never send any one-time passwords. Secondly, pop-up notifications can be placed on the screen to alert the workers that certain activities, such as sharing passwords, are unacceptable.

It is crucial to note that when designing these strategies, one fundamental issue must be considered. The problem relates to the economic insecurity of the employees. To this end, it is vital to ensure that the messages sent to the employees are friendly.

6.4. Recognition of Digital Labour Rights

One other aspect that should be taken into account during the process of reform is that of incorporating informal and gig workers as digital persons that should be accorded the legal rights under data security and cybersecurity legislation. At the moment, the legislation only views them as consumers and contractors.⁴⁷⁴

It is possible to achieve recognition in this regard through the following means:

- Control rights for the information produced by the workforce within the platform economy.
- Right to consent to how the information produced by them is used within the platform economy instead of consenting to the lengthy and difficult-to-understand terms and conditions of the agreement.
- The right to defend oneself against any form of abuse by algorithms, such as deactivating one's account, discriminatory task assignment, or automatic pay cut.

In summary, the above mentioned new perspective will bring about worker recognition within the digital labour market.

⁴⁷³ The Age of Surveillance Capitalism *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

⁴⁷⁴ Software Freedom Law Center, *Privacy, Surveillance and Data Protection in India* (SFLC Report).

6.5. Specialized Redressal Mechanisms

One of the main shortcomings of the present-day mechanism is that there exists no suitable platform for airing their complaints in case of any losses suffered owing to the online process.

One of the important aspects that need to be taken into account when considering the current legal structure is the lack of an effective procedure for dealing with complaints about cybercrimes against informal sector employees. These can include fraud, hacking, embezzlement of wages, identity theft, and other similar crimes.

In this respect, the other significant aspect will be the establishment of a grievance cell at the district and regional levels dealing with problems associated with cyberspace and serving the interests of the workers engaged in the gig economy. In this respect, it will become imperative to ensure that:

- The disputes pertaining to small amounts of money including UPI frauds and salaries are dealt with in a timely manner.
- The grievance cells are available to workers using mobile apps and toll-free numbers.
- The process has an easy access to banks and companies providing platforms for a speedy settlement of disputes.

It will be equally vital to ensure that the workers find it easier to file their grievances.

7. Platform Accountability (From Voluntary to Enforceable Responsibility)

Considering the increase in digital job opportunities, it is important to understand that these websites are not intermediaries anymore; they are quasi-employers. It is important, therefore, to regulate these websites, especially when it comes to accountability, because this will ensure that these sites take responsibility for cyber security.⁴⁷⁵

7.1. Algorithmic Transparency and Explainability

An essential element of platform accountability concerns the transparency of decisions made by algorithms that affect the livelihoods of those who rely on the services offered by these platforms. As it stands today, most gig and digital platforms use opaque algorithms to assign tasks, rate performances, and deactivate accounts.

It will be important for the right to an explanation of any decision that might have been made concerning the worker by the algorithm. These explanations shall entail:

- Explanation of the reasons for the modifications done on their scores
- The rationale for allocating certain tasks and assigning their priorities
- The reason certain accounts may have been either suspended or terminated by the platform

⁴⁷⁵ Uma Rani and Parminder Jeet Singh, 'Digital Labour Platforms and New Forms of Informality: The Case of India' (2020) *Indian Journal of Labour Economics*.

- The data fed to the algorithms that help make automatic decisions

In addition, there ought to be compulsion on the part of the platform to issue regular transparency reports on the operations of the algorithm and the type of data utilized.

7.2. Built-in Security by Design

However, there needs to be some proactivity in ensuring cybersecurity of the digital work systems apart from the reactivity of implementing these features where these will have been embedded in the process of designing. In this way, it will be possible for them to be included in the digital work system through the ‘security by design’ principle.⁴⁷⁶

A number of security features that should be considered are:

- Automated system that detects any fraudulent activity within the system, including those relating to payment, hacking into other accounts, or suspicious logins
- Increased measures of security, including MFA to prevent any unauthorized access to the system
- Security alerts on any suspicious payments, links, or identity verification

Such safeguards should not be optional add-ons but statutory compliance requirements, ensuring that digital labour platforms are designed with worker safety as a core structural principle rather than an afterthought.

7.3. Liability and Compensation Mechanisms

One of the major drawbacks of the present platform governance architecture is the lack of liability structures in case of any digital harm caused. This implies that the burden of all expenses will fall on the shoulders of the user, but in reality, it is the users who depend solely upon the platform system for their earnings.

Reforms should make it necessary for there to be some shared liability on the part of the platform specifically in instances where:

- There is exploitation of the vulnerabilities in the system for either accessing or committing fraud.
- Lack of responsibility on the platform results in data breach or compromise of accounts.
- Algorithmic or technical failures directly result in income loss

⁴⁷⁶ Rahul Matthan, ‘Beyond Consent: Data Protection and Platform Responsibility in India’ (2020) *Indian Journal of Law and Technology*.

In such cases, the platform should be in a position to offer compensation for the losses that arise from the above cases, particularly the loss of income through loss of wages, restoration of accounts, and financial help in the interim.⁴⁷⁷

7.4. Worker Representation in Governance

The implementation of governance through platforms will not yield positive results without the participation of workers within such systems. At present, almost all decisions relating to security and associated issues within the operations of platforms are made by corporate executives, who do not necessarily include workers.

It is thus imperative that platforms ensure the involvement of workers in their policy-making processes, particularly through advisory boards or similar entities, which will aid:

- In ensuring the development of cybersecurity policies based on practical on-ground situations
- Building feedback mechanisms for the emergence of new risks
- The establishment of legitimacy within the process of governance

This cooperation allows the transition from regulatory to collaborative governance models.

The transition from self-regulation to mandatory responsibility of platforms would be important for the development of digital economy. Transparency of algorithms, the security-by-design concept, responsibility, and the involvement of representatives of the worker's voice give an opportunity for the platforms to rise above being merely service providers, but also assume the responsibility for defending the interests of the workers. This becomes crucial, as innovation must not substitute insecurity and inequality, especially absence of basic labour rights.

8. Institutional Support (Building an Ecosystem of Protection)

However, any form of protection of either informal workers or contractual employees working within the digital sphere would not be achieved through a fragmented approach. It would be important that such an approach be comprehensive and involve all aspects of support including the local aspect, the technological aspect, the regulatory aspect, and the corporate aspect. This would ensure that there is security in the digital environment equal to that found in the workplace.⁴⁷⁸

8.1. Decentralized Support Structures

It is absolutely essential that the present system should fail to create any sort of access point to educate and gig workers, who suffer from cyber crime at a grass-root level. In fact, most of them might be

⁴⁷⁷ NITI Aayog, *India's Booming Gig and Platform Economy* (Government of India 2022).

⁴⁷⁸ Aparna Ravi, 'Regulating the Gig Economy in India: Platform Work and Labour Rights' (2022) *NUJS Law Review*.

lacking in terms of knowledge, expertise, and even time to go to the central office of cybercrime and court.

As such, it becomes absolutely essential to create cyber assistance centers in different communities or localities, which include:

- Cyber community centers or cyber facilitation centers, in collaboration with the labour department.
- Cyber help desks, where the basic complaints of people related to cyberspace could be listened to.
- Mobile cyber assistance centers, through which assistance could be rendered to informal workers' organizations such as markets, construction sites, and transportation points.

The importance of such centers lies in the fact that they should be free, multilingual, and made possible through professionals. It is only through this method that less-educated labourers or those who do not know how to use computers can use such centers without relying too much on the conventional legal system.

8.2. Public-Private Partnerships (PPP Model for Cyber Protection)

Considering the multisectoral characteristics of digital labour, it becomes vital that the institution fosters collaboration between government agencies and the non-government private sectors. Public-private partnerships may play a pivotal role in implementing security measures that are scalable in nature.

- The telecom sector can offer automatic alerts with regard to any phishing attacks, scamming attempts, or even malicious hyperlinks.
- The banking and payments sector may develop easy-to-implement procedures for rectifying any fraud.
- The digital labour platform providers can provide risk data anonymously to the regulatory authorities for identifying any cyber fraud.
- NGOs may assist in awareness creation and grievances management.

The collaborative relationship facilitates sharing resources, technology innovations, and quick action, thus ensuring that the security of cyberspace does not rest in the hands of only the government.

8.3. Strengthening Cybercrime Infrastructure

The efficiency of these institutions depends greatly on the competence and effectiveness of the agencies tasked with enforcing the law and tackling cybercrime. However, despite their existence, the

existing structures do not take into consideration the vulnerabilities of the informal workers since they experience cyber-fraud all the time.⁴⁷⁹

- Training of police officers in dealing with cyber crimes concerning gig workers and informal cyber crimes relating to their employment with due regard and consideration
- Exclusion of the bureaucracy involved in the process of lodging complaints, which serves as a deterrent in filing complaints
- The process of responding promptly, particularly when cyber fraud occurs in finance, which is vital for daily subsistence and existence
- Cyber cells devoted to cases of cyber crimes in relation to labour

Additionally, integrating cybercrime reporting with labour departments and financial regulators can create a coordinated enforcement ecosystem, reducing fragmentation and improving recovery outcomes for victims.

8.4. Inclusion through Design (Human-Centred Digital Infrastructure)

The inclusion of technology must also come into play when creating the technology so that the technology does not marginalize the very workers who utilize the technology. This means that the inclusion must become inherent in the architecture of the platform being used.

- Simplistic interface design that would prevent the technology from excluding workers with limited literacy levels
- Multi-language support for regional languages and voice-based interfaces for illiterate workers
- Ideas to make navigation easier by way of icon and voice-based navigational systems
- Safeguarding the workers with low literacy levels through simplified security systems with a fraud alert and simple authentication process

Nevertheless, most importantly, the systems should never make any assumptions about the prior technical knowledge of their users, and should design the process of safety in such a way as to be easy for them to understand and utilize.

On the other hand, the institutional response towards both digital workers and informal economy workers should stop being merely supportive and start being protective by incorporating local support, inter-sectorial collaboration, enforcement, and technology design into itself. When all four strategies are combined at once – decentralization, PPPs, cybersecurity, and human-centered design – the result becomes a highly effective institutional response framework that will protect the workers, not only themselves.⁴⁸⁰

⁴⁷⁹ Internet Freedom Foundation, *Cybersecurity and Data Protection in India: Gaps and Challenges* (IFF Report).

⁴⁸⁰ Ministry of Electronics and Information Technology (MeitY), *Digital India Programme: Annual Report* (Government of India).

9. Conclusion

The right cybersecurity approach is not to be considered just as an approach helping to protect the users of the system. In fact, there is an increasing number of informal workers, contractors using different platforms, technological supply chains and other services on a daily basis. Even though they play an important part in the process, their role is legally invisible. We have come up with the scenario where people using digital technology become defenseless. It becomes obvious that there is a need to make certain changes within the framework of cybersecurity policy. The traditional policy assumes that everyone should be concerned about his or her own cybersecurity when using the network. This way of tackling the problem is clearly doomed to failure as it refers to the uneducated people whose negotiating positions are far weaker than those of the platform owners.⁴⁸¹ However, a correct approach to cybersecurity cannot be viewed as something meant to help the users of the particular system. Rather, it is necessary to note that today many informal workers, contractors hired by several platforms, technological chains of production and other similar groups operate in various fields. Although these groups are crucial to this process, their participation goes unseen from the perspective of law. Regarding the situation at hand, one can say that the participants in this process using digital technologies have no security at all. Therefore, it is evident that some measures should be undertaken to deal with the issues associated with cybersecurity. To begin with, the traditional policy implies that every person should realize his or her problems regarding cybersecurity when working on the network. Nevertheless, such an approach would not bring the desired results as the members of this group are much less educated than the owners of the platforms are.⁴⁸² Another equally important group of stakeholders is civil society organizations, academic institutions, and advocacy groups. Apart from simply increasing awareness, this includes rights-based advocacy, policy monitoring, legal literacy education, and organizing workers. Such stakeholders act as intermediaries, ensuring that when there is any conversation taking place around policy development, it does not stay only within the realm of theory but takes into account the practicality of the situation in the workforce. What is even more important is the need to re-conceptualize the informal and contractual workforce as stakeholders within the same ecosystem. In effect, empowerment means that they should get the right knowledge of their rights and be involved in governance mechanisms. Last but not least, cybersecurity should be made a core element of an integrated and converged architecture that embraces labour rights, social protection, financial inclusion, and digital governance in order to address the inherent shortcomings of informal and gig workers. In other words, the idea of cybersecurity should change from self-protection to something more proactive, where cybersecurity is used in order to guarantee equality and inclusiveness in a way that ensures that digital transformation will not exacerbate inequalities but will help resolve them.

⁴⁸¹ Rahul Matthan, 'Beyond Consent: Data Protection and Platform Responsibility in India' (2020) *Indian Journal of Law and Technology*.

⁴⁸² Kunal Sen and Ravi Kanbur, 'Informality in India: Causes, Consequences and Policy Responses' (2015) *Indian Journal of Labour Economics*.