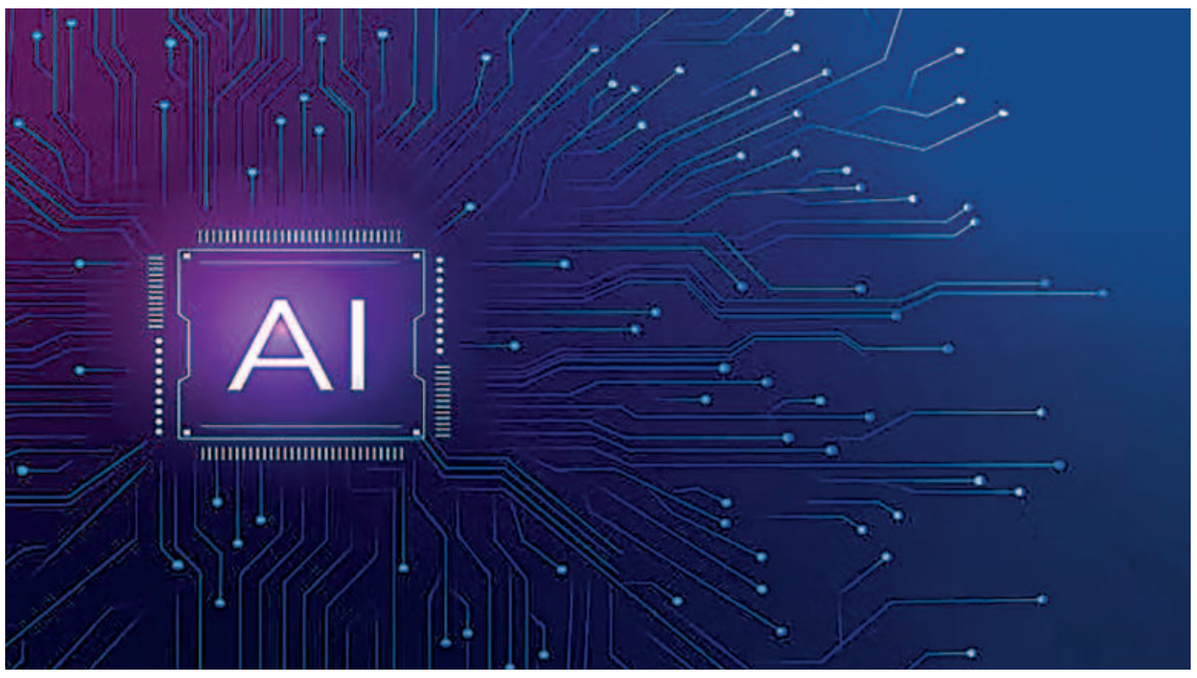
LAW VISION

WHEN ROBOTS GO ROGUE: Who's accountable in the digital workplace?

The World Day for Safety and Health at Work reminds us that technological progress must not come at the cost of human life. We cannot afford to be dazzled by AI and robotics without building the legal frameworks that keep them in check.

ROBAYET FERDOUS SYED

On April 28, the world observes the World Day for Safety and Health at Work—a day specified by the UN to reflect on how to make workplaces safer. The theme for 2025 is strikingly modern: "Revolutionizing health and safety: the role of artificial intelligence (AI) and digitalization at work." This theme speaks to a transformation already underway. Robots now carry out dangerous, repetitive tasks in factories. AI-driven platforms manage gig workers' schedules. Wearable tech monitors miners' heart rates in real time. Sensors can detect gas leaks before humans smell a thing. These technologies can save lives, boost productivity, and eliminate jobs that once led to deaths or injuries. Yet they also raise a troubling question: when something goes terribly wrong, who is to blame—the machine or the human behind it?



Let's begin with some real examples. In 2023, a factory worker in South Korea was killed when an industrial robot mistakenly identified him as a box and crushed him. Investigations revealed lack of proper programming and sensor calibration. In Arizona, a self-driving Uber car killed a pedestrian in 2018. The safety driver was distracted, but the AI failed to recognise the woman as a person. Prosecutors debated whether the driver, Uber, or the algorithm was at fault. In Amazon's warehouses, AI-powered systems track worker productivity. Workers have complained that the system penalises them for taking restroom breaks. In some cases, this pressure has reportedly led to exhaustion, injury, and even heart failure. In 2024, a gas leak at a semi-automated dyeing factory in Bangladesh killed three workers after an unmonitored early warning system failed. These examples highlight the incredible potential—and the unprecedented risks—of AI and automation in the workplace.

Who is Responsible? Suppose a robot malfunctions or an AI system leads to a workplace fatality. Is it the fault of the software engineer who built it? The manager who deployed it? The company that owns it? Or is the AI itself—trained, adapted, and increasingly autonomous—the culprit?

The problem is that most legal systems don't yet have an answer. In countries like Bangladesh, there are no clear laws on liability when AI or robots cause harm. Courts are left to rely on existing tort and criminal law, which were built for human conduct—not autonomous machines.

At the center of this legal confusion are two competing schools of thought: Fiction Theory and Reality Theory. The fiction theory views AI, robots, and corporations as legal fiction—not real persons but tools created by humans. These entities can only act through real people. They have no conscience, no emotions, no "guilty mind" (or mens rea). Hence, if something goes wrong, it must be because a human erred. By this view, for a robot arm that crushes a worker, the fault lies with the factory supervisor or the programming team. An AI scheduling tool that drives workers to burnout, is in fact, a management policy issue. For digital sensor that fails to sound an alarm, its engineers are to be blamed.

This approach upholds human responsibility and avoids blaming "dumb" machines. But it also has loopholes. What if no specific human can be identified? What if an autonomous system, learning on its own, develops harmful behavior over time? Does that mean no one is responsible?

In contrast, the reality theorists argue that legal entities— such as corporations, and potentially AI systems are real actors with their own "will" and "body." Just as a company can be sued, fined, or even held criminally liable in some countries, so too could an AI system or robot be treated as a juristic person. Under this theory, AI systems could be held liable for causing injury or death, face fines or operational bans, or similarly, trigger compensation payouts from mandatory insurance schemes. A legal entity, like an AI-managed logistics firm, is no longer a tool but a collective actor. Just how a football team function as a unit, the AI system and its human "organs"—engineers, managers, users—operate together and can be blamed when required as a whole.

As workplaces around the world—including in Bangladesh—adopt automation, AI, and smart devices, governments must not lag behind. A few urgent steps are necessary to revolutionase workplace safety. First, policymakers must clarify whether and how AI and robots can be held liable, especially in sectors such as manufacturing, construction, and logistics. Second, just as drivers need auto insurance, companies deploying autonomous systems should be required to carry insurance that compensates victims of malfunctions. Third, all workplace AI systems should be subject to independent safety audits and required to pass usability and risk tests—just like elevators or pressure boilers. Importantly, laws must clearly establish who is responsible when harm occurs: the programmer, the operator, the company—or the AI entity itself. Finally, Occupational Safety and Health (OSH) laws need urgent revision to address risks unique to digital systems—like mental stress from surveillance, or ergonomic injuries from automated work pacing.

The World Day for Safety and Health at Work reminds us that technological progress must not come at the cost of human life. We cannot afford to be dazzled by AI and robotics without building the legal frameworks that keep them in check.

The writer is law faculty at Southeast University, Dhaka, Bangladesh.

REVISITING LAWS

CYBER SECURITY LAWS IN BANGLADESH: The ties that bind our past and present

REZOAN ASRAF

The cyber legal landscape of Bangladesh has witnessed a phase of transition in recent years, initially marked by the repealing of the controversial Digital Security Act (DSA), 2018 with the Cyber Security Act (CSA), 2023 and now replacing the Cyber Security Act with the Cyber Protection Ordinance (CPO), 2025. Even though every modification was presented by the government(s) as the betterment in the preservation of civil liberties alongside the protection of digital accessibility, legal experts and human rights activists have largely been concerned about there being mere re-labeling instead of substantive reforms.

The CSA, passed in September 2023, was brought in amid increasing domestic protests and continuing international criticism of the DSA's repressive provisions. While promoted as a liberal response to calls for protecting digital rights, the CSA retained the problematic areas from the previous law. Notably, section 42(1)(d) of the CSA retained the DSA's notorious provision regarding arrest without warrant, in the case of "reasonable suspicion" which continued to pose threats to whistle-blowers, journalists, and dissidents. Section 29 also retained criminal defamation, a violation of international human rights standards that favor civil remedies over penal sanctions for defamation.

Although the Act made certain offenses bailable and capped maximum penalties, it did not address the fundamental flaws in the predecessor. The phrasing remained vague, judicial oversight continued to be lax, and enforcement continued to be under the control of potentially biased actors. Amnesty International's report in August 2024 labeled the CSA as a missed opportunity, noting that it failed to live up to the standards of Bangladesh's international human rights commitments.

Enacted on May 21, 2025, the CPO replaced the CSA and formed part of the interim government's expressed commitment to re-establish democratic credibility and freedom of expression following the controversially contested national elections earlier in 2024. On paper at least, the CPO introduces several promising reforms. First, the ordinance repeals nine contentious provisions of the CSA, including provisions restricting speech that is critical of the Liberation War, national leaders, and constitutional institutions. It also introduces judicial oversight in case of content removals ordered by the government. Courts are required to review these actions afterwards and restore the content if the removal is found to be unjustified.

Significantly, the CPO is the first South Asian legal instrument to refer to cybercrimes using artificial intelligence (AI), acknowledging the emerging and evolving threats of deepfakes, AI-generated dis- and misinformation, and autonomous hacking networks. It also criminalises online sexual harassment of women and children with stricter sentencing guidelines and an apparent attempt to make definitions clearer, although the language remains vague and overly broad, still leaving scope for misinterpretation and potential abuse.

Furthermore, the CPO also brought forth an ideological shift by proclaiming internet access as a civil right and embracing the worldwide digital rights movement that sees connectivity as indispensable for education, work, and civic life in general.

Despite these reforms, there are several structural problems that remain. Under section 35(1)(d) the CPO still has a version of section 42, empowering warrantless arrests in situations concerning threats to national security using cyberterrorism, yet subject to a new proviso of post-arrest judicial review. However, critics argue that the judicial review mechanism offers limited protection in practice, as the broad and undefined scope of cyber-attack may still facilitate arbitrary arrests. On top of that, defamation remains a criminal offense under Section 28 of the ordinance, where it still complicates its definition.

Finally, some argue that the promulgation of the ordinance by an interim, unelected government, not subject to parliamentary debate, undermines its democratic legitimacy. The process was not transparent and subject to public consultation as such, two important hallmarks of responsible lawmaking in a constitutional democracy.

The transformation from the DSA to the CSA and then again to the CPO reflects a process of reactive regulation rather than true legal reform. Real reform indeed demands more than a change in acronyms or redrafting of provisions. Structural change is necessary: clear definition of cybercrimes, unqualified judicial discretion for content control, robust safeguards for online journalism and whistleblowing, and regulation or criminalisation of hate speech under well-structured guidelines.

In the long run, the government must conduct inclusive law-making processes with technologists, journalists, legal scholars, civil society groups, and the wider public. Then only can Bangladesh expect to enact a cyber law protecting its virtual boundary without compromising the democratic values of openness, accountability, and individual liberty. Although the CPO 2025 is an advancement in some ways at least, it is not yet a transformative legal instrument that the people of Bangladesh including the human rights defenders have longed for.

The writer studies law at the University of Dhaka and is official contributor at the Law Desk.