The Daily Star
FOUNDER EDITOR: **LATE S. M. ALI**

Human traffickers must be stopped

Report on continued trafficking to Malaysia raises concerns

It is appalling to learn about the ordeal of victims of human traffickers lured with the promise of jobs in Malaysia. A report in this paper gives horrific accounts of those who have returned after paying hefty fines and being detained in Thai jails. The question is, why—despite an MoU signed by Bangladesh and Malaysia on the recruitment of Bangladeshi workers, effective till 2026—are such illegal activities still occurring? There are obviously loopholes in the system, with the potential collusion of traffickers with state officials allowing exploitation and rights violations.

The brokers and travel agents are the prime culprits in this scenario. According to experts, they manage to get immigration clearance by bribing a section of officials. The immigration department is responsible for reporting if individuals do not return after the expiry of the stipulated time in tourist visas, which is often used to traffic people. Reportedly, brokers first take jobseekers to Sri Lanka and Nepal, after which they are taken to Vietnam and Cambodia and then snuck into Thailand, before being transported to Malaysia. There have been reports in the international media of Bangladeshis being arrested in these countries, which also creates a negative image of our workers.

Against this backdrop, it is imperative to have an efficient mechanism to monitor and prevent irregularities by travel agencies and airport immigration. After failed attempts to traffic individuals via sea routes that have led to hundreds of deaths, trafficking syndicates are now using other routes. The government must take decisive steps to break these syndicates. Migrant workers are also duped into receiving fake work visas which results in them becoming undocumented workers. The arrests of some corrupt Malaysian officials over foreign workers' quota and other allegations of corruption in recent years show that the Malaysian authorities are trying to clamp down on corruption within the system. Bangladesh government, too, must take similar measures. Both governments must ensure that only the number of migrant workers stipulated in the quota go to Malaysia to work legally and with their safety ensured.

Bangladesh government also must initiate vigorous awareness campaigns so that prospective job seekers, no matter how desperate they are, know the traps laid by devious brokers and travel agents and refrain from risking their lives in the hope of a job abroad. Finally, the government must live up to its promise of providing jobs to young people so that the financial anxiety that drives them to take enormous risks is eliminated.

Cancer control needs better planning

Rising cancer cases have emerged as a big concern

We're alarmed by a recent report of the World Health Organization (WHO), published ahead of the World Cancer Day on February 4, that paints a grim picture of cancer in Bangladesh. With the number of cancer patients steadily increasing, the country faces the daunting prospect of more than doubling the new cases recorded in 2022 by the time it reaches 2050. This demands immediate attention and action from the policymakers, medical authorities, and citizens.

Currently, despite the increasing burden of cancer, Bangladesh's response is plagued by a number of challenges and inadequacies. Key among them is the lack of a national cancer control strategy that will encompass detailed action plans, robust cancer registration and screening systems, standardised treatment and vaccination protocols, and so on. Bangladesh also lacks national data on cancer, hindering efforts to develop effective intervention strategies. Currently, experts say, only some hospital-based data are available. But that is not enough. We must prioritise the collection and analysis of epidemiological data to better understand the scope of this disease within our borders, and the government must play a leading role in this regard.

It also has to address the general lack of awareness about the risks of cancer. Experts have identified several key contributing factors, such as consumption of adulterated and junk food, sedentary lifestyle, pollutions, use of tobacco and alcohol, etc. Late screening—a common occurrence—can also exacerbate the risk of fatalities. All these issues need to be addressed if we want to reduce the risks of cancer. And nothing short of a strong commitment will be enough in this fight given the struggle we're witnessing across the world. Reportedly, there were an estimated 20 million new cancer cases and 9.7 million deaths in 2022. The WHO predicts that in 2050 the number of new cancer cases globally will reach 35 million, about 77 percent higher than the figure in 2022.

The path ahead is clearly daunting but we must confront it head-on. We urge the authorities to treat the threat of cancer with the seriousness that it deserves.

COMMUNICATION SURVEILLANCE VS RIGHT TO PRIVACY

Where do our laws stand?

Md Saimum Reza Talukder
teaches cyber law at the School of Law in BRAC University.

MD SAIMUM REZA TALUKDER

The right to privacy is widely regarded as one of the fundamental rights inherent to every individual. Several international and regional human rights agreements have acknowledged this right as non-negotiable and mandatory. Examples of this recognition include the Universal Declaration on Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the European Convention on Human Rights (Article 8), the American Convention on Human Rights (Article 11), and the Arab Charter of Human Rights (Article 21).

A pertinent question may arise: what precisely is the right to privacy? Lawyers Samuel D Warren and Louis Brandeis described the term "right to privacy" in December 1890, defining it as the "right to be left alone." In his 1967 book *Privacy and Freedom*, lawyer and political scientist Alan F Westin provided a definition of privacy as the "voluntary, temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve."

Hence, it can be contended that privacy is subjective and should be individually determined by each person. Furthermore, it is imperative that an individual possesses the freedom to determine which specific information pertaining to themselves they wish to disclose. However, in the age of Big Data and the automated processing of personal data by artificial intelligence, it has become challenging for individuals (referred to as "data subjects") to determine which data pertaining to themselves may be considered private.

In the book titled *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Prof Shoshana Zuboff argues that our actions in cyberspace are being commodified and traded, resulting in the emergence of unsettling "behavioural futures markets." Technology corporations have realised that they possess a novel form of a valuable resource: our "behavioural surplus." Instead of curating and disseminating all human information, technology platforms exert complete control over its accessibility. Every online action, including our thoughts, words, and actions, is continuously monitored and exchanged for financial gain in emerging digital marketplaces that rely on predicting our everyday needs.

Communication surveillance, as defined by Privacy International, refers to "monitoring, interception, collection, preservation, and retention of information that has been communicated, relayed or generated over communication networks to a group of recipients by a third party." Privacy International additionally explained that the third party in question might be a law enforcement agency, an intelligence agency, a commercial corporation, or a criminal actor. Communication surveillance can occur on a mass scale, or it could be more intrusive and benign, like secretly installing Pegasus malware onto a digital device.

In turn, we are tracked and monitored by various political, governmental, commercial, and societal entities who remunerate the technological platforms for this access.

The consequences of exchanging our personal data in such trade can significantly erode democracy, freedom, ethics, and morality. In his book *The Net Delusion: The Dark Side of Internet Freedom,* journalist and social commentator Evgeny Morozov argues that authoritarian regimes are effectively using the internet to suppress freedom of expression, improve their surveillance methods, disseminate sophisticated propaganda, and distract their citizens by diverting them to irrelevant subjects on digital platforms. Despite journalist Andrew Sullivan's optimistic belief that "The revolution will be Twittered!" the Twitter Revolution in Iran and the Arab Spring ultimately failed. Similarly, the ongoing Ukraine war is witnessing an intense and sophisticated information war between the opposing factions, while authoritarian regimes worldwide have grown increasingly powerful.

Communication surveillance, as defined by Privacy International, refers to "monitoring, interception, collection, preservation, and retention of information that has been communicated, relayed or generated over communication networks to a group of recipients by a third party." Privacy International additionally explained that the third party in question might be a law enforcement agency, an intelligence agency, a commercial corporation, or a criminal actor. Communication surveillance can occur on a mass scale, or it could be more intrusive and benign, like secretly installing Pegasus malware onto a digital device. Communication surveillance can be done either by state actors or non-state actors.

The freedom of communication is an integral part of our freedom of expression, freedom of association, and the right to privacy. Knowledge of being under surveillance can result in altered behaviour, self-restraint, and either permanent or temporary social disengagement by someone. However, there are instances where communication surveillance is necessary for purposes such as criminal investigations, legal proceedings, safeguarding national security, and combating terrorism, child pornography, and hate speech. In these cases, state actors, such as law enforcement agencies, commonly refer to this practice as "lawful interception" (LI).

LI enables authorised persons, typically law enforcement agencies or intelligence organisations, to intercept communication between specific users. Nevertheless, LI is characterised by its precision, specificity, and adherence to legal procedures, distinguishing it from the concept of "mass surveillance." Edward Snowden, a whistleblower in 2013, exposed the fact that the NSA employed the PRISM programme to surreptitiously copy and retain internet traffic data without the permission of internet users. This programme was characterised by its lack of transparency, invasive nature, and large-scale operation. These days, the advent of open-source intelligence technology (OSINT) has facilitated the state government's use of mass surveillance due to our voluntary disclosure of personal data on various social media platforms.

Nevertheless, in light of the detrimental consequences of unchecked mass surveillance, various multilateral treaty bodies and civil society organisations have expressed their concerns. The UN special rapporteur on the right to privacy, in a report (A/HRC/40/63) issued to the UN Human Rights Council, asserts that surveillance, unless conducted in a lawful, reasonable, and necessary manner, constitutes violations of the right to privacy. Factors such as gender, colour, class, social origin, religion, and ideas, along with their expression, can contribute to the surveillance of persons in society and increase the likelihood of their privacy rights being violated.

VISUAL: **REHNUMA PROSHOON**

However, no multilateral treaty has been adopted regarding this matter yet. The nearest approximation to a formal agreement endorsing these resolutions was a collection of principles by various global civil society organisations in 2014, titled "International Principles on the Application of Human Rights to Communications Surveillance," commonly called the "Necessity and Proportionality Principles."

Bangladesh has enacted multiple laws that either authorise or may facilitate the legal interception and/or mass surveillance of telecommunication networks, digital devices, computer networks, and computer systems. According to Section 61 of the Bangladesh Telecommunication Regulatory Act, 2001 (BTRA), the inspector is authorised to inspect, make photocopies of, and retrieve data from a telecommunication system or equipment. According to Section 46 of the Information and Communication Technology Act, 2006 (ICTA), the controller has the power to grant permission to law enforcement agencies to compel any user or caretaker of a computer resource to decrypt any information stored on that computer resource. This authorisation is granted in order to protect the sovereignty, integrity, and security of Bangladesh, maintain friendly relations with foreign states, and uphold public order, among other reasons. According to Section 80 of the ICTA, a controller, authorised official, or a police officer of at least the level of sub-inspector has the authority to confiscate any device, such as a computer system or equipment, if there is suspicion that a crime, as defined under the ICTA, has been or is being committed.

According to Section 42 of the Cyber Security Act (CSA) 2023, a police officer of at least the rank of inspector is authorised to seize any computer, computer system, computer network, data, and information if there is suspicion that a crime under the CSA has been, is being, or is about to be committed. This can also be done if there is suspicion that evidence may be lost, deleted, altered, or made scarce. According to Section 45 of the CSA, the investigating officer has the authority to request information from individuals, entities, or service providers as part of the investigation.

According to Section 40 of the proposed Personal Data Protection Act, 2023 (PDPA), the "Bangladesh Data Protection Board (BDPB)" has the authority to request the "Data Fiduciary" and "Data Processor" to submit any personal data they possess. According to Sections 33 and 34, any person or any organisation, including law enforcement organisations, can be granted an exemption and further exemption from adhering to the data protection principles outlined in the PDPA. Consequently, there is a possibility that these two sections may be employed to support widespread surveillance and/or legal interception.

As per Section 15 of the proposed Bangla draft of the Over-The-Top Content Based Service Providing and Conduct Regulation, 2022, registered OTT platform service providers are required to retain content for a minimum of one year in the event of a complaint being filed against the specific content. However, based on Section 16 of the Bangla draft, the OTT Platform Registering Authority has the authority to take action in accordance with Section 8 of the Digital Security Act, 2018 (DSA). It should be emphasised that the CSA has replaced the DSA, and Section 8 of the DSA is identical to Section 8 of the CSA.

Therefore, from the aforementioned sections of the BTRA, ICTA, CSA, proposed PDPA and OTT policy, we can see a growing trend of curtailing, restricting, or taking down contents, and/or compelling data or information, and controlling access to data, by the decisions of the different executive organs of the states. These laws do not include adequate checks and balances against lawful interception and/or widespread surveillance. This is how the fundamental rights mentioned in Bangladesh's constitution—for example, freedom of assembly (Article 37), freedom of association (Article 38), freedom of thought, conscience, and of speech (Article 39), and privacy of correspondence and other means of communication (Article 43)—can be restricted by executive decision only.

Moreover, these particular sections of the aforementioned laws have not provided direct or clear provisions for checks and balances by other organs, like the judiciary, which goes against the spirit of the "separation of power." In addition, the laws in Bangladesh do not currently provide a clear definition of the "right to privacy." There is no existing personal data protection law in Bangladesh, with the exception of the PDPA—which the Cabinet has approved and is now waiting to be passed in parliament. However, the laws, as previously stated, permit interception and/or widespread communication surveillance without explicitly referencing concepts such as the "Necessity and Proportionality Principles." The Bangladeshi laws also do not adhere to the standards of legality, proportionality, and necessity as mentioned in the UN Human Rights Council study. These laws are framed from a "security" perspective rather than a "rights-based approach."

Hence, to ensure a delicate equilibrium between "lawful interception" and the "right to privacy," it is imperative to integrate the aforementioned international principles into the Bangladeshi context and expand the scope of Article 43 of the constitution.

The Daily Star Reg. No. DA 781 | **EDITOR & PUBLISHER: Mahfuz Anam** Printed by him on behalf of Mediaworld Ltd at Transcraft Ltd, 229, Tejgaon Industrial Area, editor@thedailystar.net | **EXECUTIVE EDITOR: Syed Ashfaqul Haque** | **Registered & Head Offices:** The Daily Star Centre 64-65 Kazi Nazrul Islam Avenue, Dhaka-1215 Phone: 09610222222 | **Newsroom:** Fax- 58156306 reporting@thedailystar.net | **Advertisement:** 01711623910 advertisement@thedailystar.net GPO Box: 3257 | **Subscription:** 01711623906 | thedailystar.net bangla.thedailystar.net/