Criminal Justice and Human Rights: Finding the Balance

Bikash Chandra Das

Apr 21, 2026

Abstract

Although the title refers to criminal justice and human rights, the article's main discussion focuses on the expansion of cybercrime in Bangladesh and the challenges this creates for law enforcement and digital security. It describes the transition from physical crimes such as theft, robbery, and violence toward hacking, online fraud, identity theft, phishing, cyberbullying, misinformation, and mobile-banking scams. The post explains how increasing internet penetration and digital payment systems have created new opportunities for offenders and exposed individuals and financial institutions to greater risk. It also discusses government responses, including cybercrime legislation, specialized police units, digital investigation capacity, and efforts to strengthen cybersecurity. At the same time, the article notes controversy surrounding digital-security laws, particularly concerns that broad legal powers can affect freedom of expression. Low digital literacy is identified as another major weakness. The article ultimately emphasizes stronger technical capacity, public education, updated legal frameworks, cybersecurity training, and international cooperation as necessary for a safer digital environment.



The history of crime in Bangladesh, as in most nations around the world, has undergone a tremendous change whereby criminal acts that were previously pursued in the traditional ways are now the sophisticated and unseen world of cybercrimes. In a nation where stealing, robbery, and murder have been well known, the emergence of the digital technologies and the internet has created new types of crime that pose new challenges to the criminal justice system and the law enforcement agencies. This paper will discuss the shift between traditional and cybercrime in Bangladesh, considering the reasons of the shift, the influence that cybercrime has had on the community, and what measures are currently being undertaken to address this menace that is on the rise.

Traditionally, a criminal environment in Bangladesh was shaped by physical crimes. Stealing, beating, killing, and other violent crimes were widespread, and the fuel was various factors, such as poverty, social inequalities, and political instability. The imperfect criminal justice system was structured to deal with such kind of crimes and was implemented by law enforcement agencies and judicial system, which was devoted to investigations, gathering of evidence and crime scenes. Gradually, however, the fast technological development and the extensive use of digital platforms started changing the process of crime realization, and the nation had to deal with a new set of issues concerning cybercrime.

Cybercrime which is a criminal activity that is characterized by computer usage, network, and the internet began in Bangladesh in the late 1990s and early 2000s. Some of the earliest forms of cybercrime in the country were characterized by relatively easy cybercrime as hacking, intrusion into systems, and internet fraud. They were commonly committed by persons or small gangs of technologically-sophisticated criminals who compromised weak systems, such as government systems, commercial organizations and

personal accounts. The domain of cybercrime was narrow in the early years and it was considered to be a challenge that affected big organizations and individuals who had high-value targets.

Nevertheless, with the increased internet penetration in Bangladesh and the further integration of digital technologies into the daily lives of its population, the character of cybercrime changed. The growing popularity of online fraud and identity theft remains one of the most important events in the emergence of cybercrime. Hackers started to use the vulnerabilities in the system of online payments, shopping sites, and banking facilities to rob the unsuspecting people of money and personal information. Criminals got even more possibilities to use the vulnerability of the system by introducing mobile banking and digital payment systems, including bKash and Rocket.

Phishing attacks that involve the fraudsters posing as trusted organizations and persuading people to disclose their personal data like credit card numbers and passwords also became common. These are scams that are conducted over emails or text messages and had a wide range of victims, the old and the young internet users. Most victims were in most instances duped into clicking dangerous links or giving personal information that was subsequently exploited to either enrich themselves or identity theft.

The social media sites also turned into a nest of cybercrimes, as the number of online harassment, cyberbullying, and fake news and misinformation proliferated. The internet gave people the freedom of anonymity, which increased their ease of attack other individuals with ill motive without any immediate repercussion. Online hate speech and defamatory content has become a big problem as these practices do not only violate the right of individuals; it is also associated with the proliferation of fake information, which tends to have political or social motives.

Cyber crime has been especially susceptible to the financial sector in Bangladesh. With the widening and availability of mobile banking services, crooks started to take advantage of loopholes in these services and use them to execute fraudulent dealings. In other cases, social engineering techniques were applied by the scammers to manipulate people to send money to the fraudulent accounts, whereas in other cases, the malware was used to obtain unauthorized access to the bank accounts. The impacts of these crimes have seen victims suffer millions of dollars and have led to a question of whether digital financial systems are secure.

The Bangladesh government has been trying to deal with the escalating menace of cybercrime by enacting laws and regulations. The prescription of the Digital Security Act in 2018 is one of the most significant measures that have been taken to combat different forms of cybercrime, such as hacking, online defamation, and cyberterrorism. The legislation was aimed at empowering the cybersecurity system of the country and making sure that cybercriminals are not exempt in their activities. The law has however been controversial and critics have claimed that it has been applied to curtail free speech and attack political dissent.

Nonetheless, the law is an important move to counter cybercrime in Bangladesh.

Besides the legislative action, the government has also attempted to enhance its digital era law enforcement capacity. In the police force, specialized units dealing with cybercrime cases have been set up and there has been an effort to augment the capacity of the law enforcers to detect and prosecute cybercrimes. Nevertheless, there are still difficulties in terms of training, resources, and coordination among agencies, especially because cybercriminals are getting more advanced in their methods.

The issue of the general population not being digitally literate is one of the greatest problems of combating cybercrime in Bangladesh. In most cases, particularly on the rural setting, people are not very conversant with internet security and how they can safeguard themselves against internet thieves. This ignorance exposes individuals to phishing attacks, identity fraud and other internet frauds. Lack of proper population education on digital security makes the situation even worse since people are not usually aware of the danger, not to mention the fact that they do not take simple measures to secure their personal information.

With the growth of digital technologies, the Bangladesh cybercrime is expected to spread even wider. There are also new kinds of cybercrime being formed like ransomware attacks where, criminals encrypt the data of victims and then require them to pay a certain amount of money to release it, which is already being practiced globally and is set to be a big danger to the emerging digital economy of Bangladesh. Moreover, the growing adoption of the Internet of Things (IoT) gadgets, including smart household appliances and smart cars, presents new opportunities to cybercriminals to use. Soon, as Bangladesh is becoming increasingly digitally integrated, it is important to be ahead of all emerging threats and make sure that individuals and organizations are ready to protect themselves against cyberattacks.

Although there are these challenges, there is hope on the future. One of the good things in the ever-increasing cybercrime menace is the emergence of the cybersecurity industry in Bangladesh as a result. The need to ensure the safety of their digital infrastructures has led to the high demand of cybersecurity professionals and solutions as businesses and government agencies realize the necessity of addressing this issue. Institutions of higher learning and technical institutions are also starting to offer degree programs and training opportunities in cybersecurity and this has been of assistance in creating a pool of qualified workers who can respond to the increasing cybersecurity demands in the country. Also, to solve the issue of cybercrime, governments, law-enforcement agencies, and even individual companies should engage in international cooperation because cybercriminals may work internationally.

Bangladesh has experienced the shift of crime to cybercrime, thus, indicating the revolutionary nature of technology on society. Although cybercrime is a challenge that brings a lot of difficulties, it brings opportunities to develop in the cybersecurity industry, create jobs, and education in the digital field. The increasing awareness of online security, investing in cybersecurity infrastructure, and making legal

frameworks flexible to the continuously evolving digital environment will help to ensure that the population of Bangladesh is not exposed to the risks of cybercrime. The balance that the country will maintain between innovation and cyber security will be very vital towards ensuring that the future of the country as far as digital aspects are concerned is safe and successful.