Need to Amend Prevention of Electronic Crime Act 2016 (PECA)

Editorial

Kaukab Jamal Zuberi
Chief Editor

Electronic evidence has become an essential tool for solving white and blue collar crimes. However, due to bottle necks in the system, extensive use of digital evidence has yet to be seen in the country. Lack of awareness, quantum of cybercrimes, lack of qualified personnel, lack of awareness in judiciary and legal community, absence of proper procedures to collect digital evidence and presence of sole authority to collect evidence in the hands of one investigating agency are some of Prevention of Electronic Crime Act (PECA) was passed in 2016 and created new offences to prosecute perpetrators using technology to commit crimes. PECA explains the investigation agency and power to investigate as follows:

Establishment of Investigation Agency:

The federal Government may establish or designate a law enforcement agency as the investigation agency for the purpose of investigation of offences under this Act. Section 30 of the Act is referred to in this context. "**Power to Investigate**: Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act, provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation team Comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force."

Due to the wide range of new offences introduced in the Prevention of Electronic Crimes Act (PECA) it is almost impossible for an investigation agency to cater all the investigations through one investigative agency. Moreover, it is also not possible for other law enforcement agencies to wait for the bureaucratic procedures of creating a JIT and involving an authorized officer of the investigation agency, authorized under this PECA. At some occasions, timely actions are extremely important to take. For example, searching the house of the alleged member of a terrorist organization, the Anti-Terrorist Force finds a laptop, which is suspected to be used in cyber terrorism, should they wait for the creation of JIT to create images of the hard drive and get vital information out of it through proper digital forensic procedures. It should be noted that the terrorist should be presented in front of the court of law in 24 hours to take the physical remand. Another example can be a house of a suspect who was asking the ransom after kidnapping a child. Should the related police department wait for the creation of JIT before confiscating the mobile phone and start working on the information available to locate the alleged kidnapper.

Moreover, the use of term "dishonest intentions" in PECA creates ambiguity and provides advantage to the accused. Reference is given to the following sections of PECA:

Section 3: "**Unauthorized access to information system or data:**
"Whoever **with dishonest intention** gains unauthorized access to any information system or data shall be punished with imprisonment for a term, which may extend to three months or with fine, which may extend to fifty thousand rupees or with both."

Section 4: **Unauthorized copying or transmission of data:**
"Whoever **with dishonest intention** and without authorization copies or otherwise

transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both."

Section 5: **Interference with information system or data:**
"Whoever **with dishonest intention** interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with impoundment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

Clauses 6,7,8 are included in clause 10 which describes the offences treated as Cyber Terrorism. Therefore, the prosecutors now have to prove dishonest intention of the accused to prosecute under these sections."

Section 6: "**Unauthorized access to critical infrastructure information system or data:**
"Whoever **with dishonest intention** gains unauthorized access to any critical infrastructure information system or data shall be punished wd1 imprisonment which may extend to three years or with fine which may extend to one million rupees or with both."

Section 7: "**Unauthorized copying or transmission of critical infrastructure data:**
"Whoever **with dishonest intention** and without authorization copies or otherwise transmits or causes to be transmitted any critical infrastructure data shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to five million rupees or with both."

Section 8: "**Interference with critical infrastructure information system or data:**
"Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical informal ion system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both."

Section 23:
"Spoofing: Whoever **with dishonest intention** establishes a website or sends any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be an authentic source commits spoofing."

(2) "Whoever commits spooling shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both."

Section 6,7 and 8 are also mentioned in Section 10 which defines Cyber Terrorism.

National Response for Cyber Crime Center is the department of Federal Investigation Agency which is responsible for investigating cybercrimes and supporting other law enforcement agencies in solving electronic crimes. Poorly equipped laboratories, lack of trained human resources and neglected standard operating procedures and industry standards have resulted in back log of tens of thousands of cases to be investigated by this department. It is difficult to understand how will they be able to cater the needs of other law enforcement agencies.

There is a dire need to upgrade the laboratories of NR3C, increase number of qualified staff and bring necessary changes in PECA to cover the loopholes (some of them are mentioned here and some are not due to the potential effects on the ongoing investigations/case). Until then, it is expected that the number of unsolved cases will keep on increasing in NR3C and the general public suffering will increase in the hands of cyber criminals.