Pakistan Journal of Criminology
Vol. 16, No. 01, January—March 2024 (711-714)

Digital Forensics and Criminal Investigations in Pakistan

Kamran Adil

I- The Conspectus

The law and sociology grow, in tandem, with the former following the latter. In this evolution of the two disciplines, criminology, the subset of sociology, is further branching off. A new discipline named as digital criminology is emerging. Professor Anastasia Powell, in her book (Digital Criminology) co-authored with Gregory Stratton and Robin Cameron defined digital criminology as an 'intersection of critical, cultural, and socio-technical theory and research'. Likewise, the law is responding to the technology especially to the artificial intelligence through legislative and administrative measures. On 15th December, 2023, the European Artificial Intelligence Act was passed by the European Parliament. Similarly, in Pakistan, the Computer Emergency Response Team Rules, 2023 (CERT Rules) under section 49 read with section 51 of the Prevention of Electronic Crimes Act, 2016 (PECA) were passed. On the data scene, the draft data protection law by the Ministry of Information and Technology has been prepared and is pending consideration for legislation. In policing, the data analytics will be used proactively as many new pieces of legislation contain provisions for data collection, retention and lawful use. For example, the Anti-Rape (Sex Offenders Register) Rules, 2023 under section 24 of the Anti-Rape (Investigation and Trial) Act, 2021 obliges the state to collect data about sex offenders. Similar provisions are available now for trafficking in persons and for migrants' smuggling related offences in Pakistan. In this background, there is need to study how different technologies are shaping state and law enforcement responses. One area of particular interest is the use of digital forensics in criminal prosecutions. The instant write up will explore the concept and will analyze its integration with the criminal justice system along with some recommendations.

II- Definiing Digital Forensics

Many terms are used interchangeably like computer forensics, electronic forensics and digital forensics. Are these terms synonymous or are there any differences. In his book, Cybercrime and Digital Forensics: An Introduction, Professor Thomas J. Holt distinguished between computer forensics and digital forensics. He noted that the computer forensics has now transformed into digital forensics. He defined computer forensics as:

"Computer forensics, a branch of the forensic sciences, refers to investigation and analysis of media originating from digital sources in an effort to uncover evidence to present in a court of law."

He noted that it is also known as dead box forensics as it involved examination of powered down computer components. On the other hand, digital forensics, as per him, is:

"Digital forensics refers to the analysis of digital evidence, which includes network forensics (internet traffic), computer forensics, mobile device forensics (e.g., cell phone), and malware forensics (e.g., viruses)."

He elaborated that it includes 'whole array of digital devices'.

With the new overarching nature of digital forensics, the discourse about typology of evidence into electronic, digital and information system will not be of much use. For working purposes, therefore, digital forensics is the catch-all term.

III- Digital Forensics and Criminal Investigations

Earlier when the PECA was enacted in 2016, the authority to investigate an electronic crime was vested solely in the Federal Investigation Agency (FIA). However, this has been revised due to ubiquitous nature of digital evidence in all forms of crimes. The Criminal Laws (Amendment) Act, 2023 (2023 Amendments) has amended the PECA and has declared that the offences under the law shall be cognizable under section 30 of the Act (meaning thereby that provincial police organizations can now register criminal cases in relations to the offences). This mainstreaming of the PECA has far reaching effects as, more often than not, almost every criminal case now has a digital footprint. The 2023 Amendments have also added new list of offences to the PECA. These offences include online grooming, solicitation and cyber incitement (by inserting new section 22-A to PECA), commercial sexual exploitation of children (inserting new section 22-B to PECA), use of information system for kidnapping, abduction and trafficking in person (by inserting new section 22-C to PECA) and cyber bullying (inserting new section 24-A to PECA). In addition, incitement to terrorism/extremism, communication for money laundering and financing for terrorism through emerging technologies like crypto-currency and smart contracts primarily depend on electronic means that invariably call for collection, preservation and processing of digital evidence through digital forensics.

IV- Analysis and Recommendations

Foregoing legal developments and notes from the field show that digital forensics will have to be accorded primacy and will be central to mainstream criminal justice processes. Keeping in view the significance, following may be noted:

First, crime scene inspection and role of first police responder are regulated by Chapter XXV of the Police Rules, 1934. This chapter will have to be

re-written to include and allow for the concepts of first responder for digital evidence and for crime scene investigation imagining the role of dedicated officers with technical/digital capacities. Presently, it is being practiced in some districts and by select officers; for want of an updated and comprehensive legal framework, the initiatives are often challenged by defense lawyers. In order to provide legality to all police and prosecution actions vis-à-vis digital evidence, there is a strong need to redraft the Chapter XXV to cater for electronic and digital evidence;

Secondly, the police and prosecution must be trained to collect, preserve and present digital evidence in a court of law by including dedicated modules in their training programmes on digital forensics;

Thirdly, for prevention of crimes, police are using data that they collect and maintain for the Criminal Record Office (CRO) and the data and videos that they get from the safe city systems' cameras. They identify hotspots and try to develop indigenous capacity for facial recognitions. The use of these technologies for predictive policing must be put under some sort of oversight mechanism and should also be properly legislated upon to strike necessary balance between security and privacy;

Fourthly, there is a strong case for national and international cooperation for digital forensics as many a time, it will involve non-localized servers and cross-border intermediaries. This national and international cooperation is very bureaucratic and is subject to the rules of business of the federal and provincial governments and to the Mutual Legal Assistance (Criminal Matters) Act, 2020;

Fifthly, accreditation and standardization of digital forensic labs in the country is a must. Unlike the forensic science agencies in the provinces that have legal framework and are part of international accreditation systems, the digital/IT labs need to be brought under some sort of standardization regime. An added advantage of this accreditation will be that the digital forensics' experts would be got declared as experts under article 59 of the Qanoon-e-Shahadat Order, 1984 (law of evidence; hereinafter referred to as QSO); this legal device will be useful in shielding the appearance of experts in courts unnecessarily;

Sixthly, the admissibility of electronic/digital evidence has long been permitted under article 164 of the QSO. Recently, the scope of the article was expanded to include social media applications like WhatsApp, Facebook, Skype by rewriting the article 164 of the QSO through section 12 of the Criminal Laws (Amendment) Act, 2023. There is, however, need to improve the weightage of digital evidence, which is still treated, at best, secondary in nature;

Seventhly, the preservation and storage of digital evidence as case property of criminal cases requires amendments in Chapter XVII of the Police

Rules, 1934 that regulates the record maintenance and chain of custody system in the criminal justice system. The digital media and forensic reports emanating out of these are to be handled professionally and all possibilities of editing/manipulation/deep fakes have to be ruled out;

Eighthly, other investigation agencies like the Anti-Narcotics Force, the National Accountability Bureau, the Pakistan Customs (while investigating smuggling related offences) and the provincial departments vested with lawful coercive powers must be trained in digital forensics;

Ninthly, better capacity of organizing digital forensics in criminal cases is likely to be of universal value for Pakistan as cross-border and cross-jurisdictional transmission of evidence will be easy, especially in terrorism cases;

Finally, the cybersecurity mechanisms must be integrated with the criminal justice processes. The latest CERT Rules are only focused on the preventive cybersecurity paradigm; the detective and restitution driven aspects must be incorporated into the CERT Rules and seizure of property acquired through electronic processes like e-banking, virtual assets and smart contracts must be added to the tools available to the law enforcement apparatus and for cross-border/international communication and cooperation.

The above stated points are not exhaustive by any means, but do provide a point of departure for further work in this dimension. Indigenous measurement of cybercrime and cyber related incidents has to be organized as at the moment, there is no singular nodal point to deal with the census of these instances.