Technology at the Service of the Criminal Justice System

The flare-up of the internet and the increasing use of digital cameras and cell phone cameras have given perpetrators additional means to execute their intention of exploiting other human beings for their own profit. It is common to use chat rooms, message boards, peer-to-peer file-sharing servers, news groups, and specialized websites. Recent studies have demonstrated the increasing establishment of “cyber-sex dens” where some children may be sexually abused and the images beamed via a webcam on to the internet for a price, which payment is often made by a credit card via an internet connection. Additionally, alternative payment markets such as “Bitcoin” can be utilized for payments.”

Former President Barack Obama stated that, “We are turning the tables on the traffickers. Just as they are now using technology and the internet to exploit their victims, we’re going to harness technology to stop them.”

Technology is a tool that has been used by traffickers to advertise and coordinate the sale of victims. The advertising/selling process has been shifted from the “street corner” to the “digital room”, changing, consequently, the physical and legal risks involved in this process. In the media stratosphere, for example, there are many more traces of the interaction of perpetrators and victims, creating, thus, generating data which can be used later by law enforcement.

The solution presented by Mark Latonero includes integrating human experts and computer-assisted technologies. “Researchers developed a computer prototype to locate and extract or “scrape” the information appearing on the websites, then collect and store the aggregate data for analysis. Sites of interest were identified by the FBI and included for monitoring. A number of online classified and social networking sites were targeted, such as Backpage sites in dozens of U.S. cities and a number of explicit websites and forums known for trafficking activity. Information scraped from the sites includes all text, dates, and photograph.” Therefore, automated data collection is a first step towards effective cyber-trafficking investigation. Similarly, natural language processing, facial recognition and mapping technologies and

---


methods are being employed by cyber-trafficking investigators.4

Computer science researchers at the University of California, Berkeley have developed new tools to identify sex trafficking rings, making them easier for law enforcement to target and prosecute. The new technique, developed by a team including PhD candidate Rebecca S. Portnoff, combines two distinct approaches to solving that problem. First, the team created a machine-learning filter that finds stylistic similarities between ads for sex services posted to sites like Backpage.com. The second step comes via the payment method for sex ads, Bitcoin, and its public blockchain, which records all transactions, providing evidence of a larger organization and likelihood of trafficking. Therefore, those linkages could be used to subpoena further records from Bitcoin wallet services, or to expand on sting operations conducted using phone numbers or other contact information listed in the ads.5

The tool developed by Dr. Rebecca S. Portnoff’s team will help not only the investigation of potential traffickers but also “support prosecution efforts in an arena where money moves with rapidity across financial instruments and disappears from the evidence trail”, says Carrie Pemberton Ford at the Cambridge Centre for Applied Research in Human Trafficking.6

Additionally, software programs such as MEMEX have been “designed to help law enforcement officers and others to do investigations online and pursue human traffickers”. Digital forensics and electronic evidence provide new opportunities, but also new challenges. Given the issue of digital traces, there are also opportunities to engage new partners, including technology companies and financial institutions, to coordinate with law enforcement.8

India is also taking steps towards curbing this new menace. Cybercrime has been understood as unlawful acts wherein the computer is either a tool or a target or both.

According to Maharashtra’s Director General Information and Publicity, Mr. Brijesh Singh, the State is able to make use of recent technology such as link-analysis of calls, biometrics for facial recognition, and a fibre optical network: Crime and Criminal Tracking Network System (CCTNS). CCTNS is a project under the Indian government for creating a comprehensive and integrated

4 Ivi, at 29
8 Danah Boyd, Heather Casteel, Mitai Thakor and Rane Johnson, op. cit. at 7
system for effective policing through e-Governance. This network system includes a nationwide online tracking system by integrating more than 14,000 police stations across the country. The project has been implemented by the National Crime Records Bureau.

Furthermore, the Cabinet Committee on Economic Affairs also decided to implement an Integrated Criminal Justice System (ICJS) by 2017. It will be done through integrating CCTNS with e-Courts, e-prisons, forensics and prosecution - which are the key components of the criminal justice system.

The implementation of ICJS will: i) ensure a quick data transfer among different pillars of criminal justice system, which will not only enhance transparency but also reduce processing time; ii) enable national level crime analytics to be published at increased frequency, which will help the policy makers as well as lawmakers in taking appropriate and timely action; and iii) enable pan-India criminal/accused name search in the regional language for improved inter-state tracking of criminal movement.


A major amendment was made in 2008 when it introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource" and, amongst other changes, also introduced penalties for child pornography. Section 92 of IT Act has also introduced changes to the Indian Evidence Act, 1872 (Evidence Act). Section 3 of Evidence Act now foresees that "Evidence "means and includes (...) (2) all documents including electronic records produced for the inspection of the Court, such documents are called documentary evidence." Sections 65-A and 65-B were also added. The latter deals exclusively with the admissibility of the electronic record that due to technological grounds can be admitted only in the manner specified therein.

The Supreme Court of India has interpreted the above provisions of the Evidence Act and the IT Act in a way that any electronic evidence provided must be supported by a certificate in compliance. Reliance is placed on the decisions of the Supreme Court in Anvar P.V. v. P.K. Basheer & Ors., in Mukesh and Ors. v. State for NCT of Delhi and Ors. and also in Sanjay Singh Ramrao Chavan v. Dattatray Gulabrao Phalkar, Calcutta High Court in Abdul Rahaman Kunji v. the State of West Bengal, Delhi High Court in Ankur

10 Mukesh and Ors. v. State of NCT of Delhi and Ors., available at MANU/SC/0575/2017
Lex Lata

Chawla v. CBI\(^3\) and also in Jagdeo Singh v. the State and Ors.\(^{14}\), such as AHTU and cyber-trafficking units, to conduct appropriate investigation and consequent arrests. It is our opinion that this would lead to an effective and successful apprehension of evidence that, in turn, the courts would be able to rely upon in order to pronounce a judgment of conviction.

In the above mentioned decisions, the Courts have ruled on the admissibility of electronic evidence, as secondary evidence, provided that it can be corroborated by primary evidence. In example, the Court in Ankur Chawla v. CBI\(^5\) relied on the testimony of the witness that downloaded and printed the e-mail which was sufficient to prove the electronic communication by virtue of Section 65-B read with Section 88-A of Evidence Act. On the other hand, in Jagdeo Singh v. the State and Ors., while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without certificate under Section 65-B of Evidence Act, the court ruled such evidence inadmissible.

It seems clear from the above that “specific training and an in-depth specialization of law enforcement authorities, in example how to recognize trafficking in persons’ indicators [within a trafficking ring network which is using new technologies for sexual exploitation], (...) is required in order to conduct adequate and accurate investigations and prosecutions of cases of trafficking in persons”\(^{16}\) and appropriate collection of electronic evidence that would be able to stand alone in a court of law as primary evidence.

It is, therefore, evident that further steps need to be taken, especially specific training of law enforcement authorities as well as delegated authorities and specialized units

---

\(^3\) Ankur Chawla v. CBI, available at MANU/DE/2923/2014

\(^4\) Jagdeo Singh vs. the State and Ors., available at MANU/DE/0376/2015

\(^5\) See Note 13 supra

\(^6\) Supra note 1, at 337

For more details visit [www.ijmindia.org](http://www.ijmindia.org)

Contact Research and Development, International Justice Mission, Mumbai at mumbai@ijm.org