The Impact on Technological Innovations in Crime Prevention and Policing

Simran Biswas[1], Samiparna Ghosh[2], Anirban Bhar[3], Shyamapriya Chatterjee[4]

[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

[1] simranbiswas2003@gmail.com
[2] samiparna.ghosh2004@gmail.com
[3] anirban.bhar@nit.ac.in
[4] shyamapriya.chowdhury@nit.ac.in

ABSTRACT

New technological innovations have been developed to prevent crime and to improve the performance of the police, but we know about how and why certain innovations are adopted, and the consequences –both intended and unintended—of technology-driven solutions to the problem of crime.
Innovations in criminal justice technology can be divided into two broad categories, firstly hard Technology (new materials, devices, and equipment that can be used to either commit crime or prevent and control crime) and secondly, soft Technology (software programs, classification systems, crime analysis techniques, and data sharing/system integration techniques).
Crime prevention is a concept that has been applied to the problem of crime in a variety of methods. Understanding crime prevention requires an examination of both intentions and outcomes. Even broader is the definition of crime prevention when novel factors, such as the reduction of crime risk factors, are considered.
Changes in both technology of policing appear to be transforming local, state, and federal policing departments in a number of fundamental ways. Two recent reviews of technology and the police describe this transformation process, review the evidence of its impact on police practices and outcomes, and discuss the technological changes in policing for the public.
Research and evaluation should determine policy, according to the concepts presented in schools of public administration regarding the rational development of policy. That is hardly the case for the various types of hard and soft technology innovations, which challenges the new professionalism model of policing.
Recent changes in the technology area generally – and in the area of information technology in particular that they deserve special attention and critical review. It is important to consider new technology developed to support crime prevention generally because by focusing on innovations in only one area, we would likely miss the consequences – both intended and unintended.
Individual practitioners may have the knowledge and motivation to maximize the effectiveness of surveillance and crime-reduction technologies. In terms of the latter, this study especially highlights the negative impact of a lack of technical interoperability of different systems, and unclear guidelines and procedures.

Keywords: *Technological innovations, Crime prevention, Police practices, Technical interoperability.*

1. INTRODUCTION

Crime is cunning; it puts an angel in front of every devil. ~ German Proverbs

Public agencies are required to innovate at an ever-increasing rate in order to keep up with technological advancements. New technological innovations have been developed to prevent crime and enhance police performance, but we know surprisingly little about how and why certain innovations are adopted, as well as the consequences – both intended and unintended – of technology-driven solutions to the problem of crime. This article examines a broad variety of new technological innovations with applications in the fields of crime prevention in general and crime control (by police) in particular.

Given the significance of this issue to the future of policing and crime prevention, it is not remarkable that both the public and academic communities are discussing it. However, these are typically dominated by a concentration on the philosophical and theoretical aspects of technological innovation in the field. With a preponderant emphasis on the repercussions for society as a whole, there is a paucity of research that examines the topic from the perspective of practitioners and discusses the effects on those who actively employ these technologies.

2. INNOVATION AND PRACTITIONER PERSPECTIVES –BEYOND THEORETICAL ISSUES

The first important question to answer is why it is essential to focus on the practical aspects of the deployment of new SOSTs, particularly the perspectives of practitioners. Although discussing broad, often philosophical issues of security versus privacy and questions of individual rights is essential, it rarely provides direct insight into how new technologies are actually used on the ground, and therefore possibly into the types of outcomes that can be anticipated. When scrutinizing issues of surveillance and crime prevention, the voices of those who work in the field and employ new technological solutions on a daily basis are frequently absent from the discussion. As such, this article does not attempt to discuss the broader issues that frequently evoke images of a surveillance state and "big brother" in public discourse. A controversial example is the use of facial-recognition technologies for law enforcement and security purposes. The heated debate surrounding the deployment of facial recognition around a large multimodal transport hub in London (Sabbagh, 2019) and the trials conducted by the Metropolitan Police Services of London between 2016 and 2020 are only the top of the iceberg (Bradford et al., 2020; Fussey and Murray, 2019).

Diverse duties are utilizing data-driven technologies that have emerged as a result of the datafication phenomenon. Social media mining, sentiment analysis, and natural language processing are examples. At various stages of the criminal justice system, these technologies now inform decision-making. For instance, experimental algorithmic tools can influence police operational decisions to enhance a police force's decision-making, including how to allocate policing resources (Mastrobuoni, 2020; Oswald et al., 2018). In a number of nations, police services are utilizing new data-driven technologies for intelligence and surveillance-driven policing (Bennett Moses and Chan, 2018). The technologies, which are sometimes developed through collaborations between academics, the state, and non-state actors, also have an impact on other criminal justice services. In the criminal justice system, they can determine the intensity of interventions, parole decisions, and prison security classifications (e.g., Ministry of Justice, 2019). The technologies automate a combination of administrative data from criminal justice services and/or big data from other sources in order to execute their duties.

This demonstrates that technological innovation in policing and crime prevention is not some far-off scenario, but rather a necessity that dictates routines and daily activities for practitioners. Indeed, digitalization and technological innovation play a central role in the Policing Vision 2025 published by the National Police Chiefs' Council (2016) and the Metropolitan Police Service (2017a, 2017b), which emphasizes that more must be done in the coming years to capitalize on the operational benefits of technological advances. This demonstrates how important it is to move beyond wide philosophical discussions and investigate questions of practical realities in the deployment of new technologies for crime prevention and law enforcement.

The public's support for crime-reduction measures fluctuates over time and is frequently influenced by major events. Deployment of new surveillance technologies or the introduction of new surveillance powers, for example, frequently occurs in the aftermath of tragedies or mass-casualty events, when the perceived need for increased security among the population is greatest (Dinev et al., 2008; Thompson et al., 2020), or as a means of coping with otherwise scarce resources through automation (Joh, 2019; Leese, 2021; D Wilson, 2019). In contrast, public support is at an all-time low following data leaks and surveillance controversies such as the Snowden revelations (Hintz and Dencik, 2016; Lischka, 2017; Murata et al., 2017). As a result, the introduction of more technology-oriented security policies and increasingly intrusive SOSTs has elicited two primary responses in the majority of nations, ranging from those who support increased surveillance in the name of (national) security and efficiency to those who argue that restrictions are undemocratic, unjustified, or merely ineffective (Tsoukala, 2006). This dichotomy stems from the age-old debate between security and privacy. Frequently, this debate is framed as a cost–benefit dilemma and a trade-off between security improvements obtained through better SOSTs and privacy (Pavone and Esposti, 2012; Pavone et al., 2016).

3. METHODOLOGY

Methodology refers to your research project's overarching strategy and justification. It entails researching the methods used in your field and the underlying theories or principles to develop an approach that matches your goals. The authors examine a vast array of new technological innovations with implementations in the fields of crime prevention and (police) crime control. They then evaluate the available research on the intended and unintended effects of each type of new technology on crime prevention and police performance.

3.1 Data search criteria

We concentrated on academic literature retrieved via the citation indexing service Web of Science (WoS), which indexes the text and metadata of the majority of peer-reviewed academic journals, books, abstracts, conference papers, reports, and other pertinent literature. We searched for 'topics', a category that includes titles, abstracts, authors, and keywords. These search terms were used: OR (mining AND 'criminal justice') OR (mining AND policing) OR (artificial AND 'criminal justice') OR (artificial AND policing) OR (machine AND 'criminal justice') OR (machine AND policing) OR (algorithm* AND 'criminal justice') OR (algorithm* AND policing). The keyword search returned 1773 results, which became 1330 once we refined the search using the exclusion criteria set out further below. All titles, abstracts, and associated metadata from our search results were exported. Two researchers then manually screened the abstracts a second time to improve interrater reliability. The objective was to evaluate relevance, as keyword queries are notorious for producing false positives. After this manual screening, 493 abstracts were chosen for in-depth examination.

3.2 Data exclusion criteria and research limitations

We focused on content published within the last eleven years (January 2009 to December 2019) to reflect the period during which the big data phenomenon has expanded rapidly. In addition, to make qualitative analysis more manageable, we focused our queries on terms commonly found in the academic literature pertaining to datafication and data-driven technologies in criminal justice. We acknowledge that the dataset utilized has several limitations. First, it is important to note that a limitation of our data collection method is that WoS indexes the text and meta-data of the majority of relevant material, but some journals, books, and conferences, for example, may be missed. In this regard, we consider our research exploratory and valuable as a starting point for a discussion on sociotechnical imaginaries and digital capital in the context of data-driven technologies for crime prevention and control. Despite the fact that bibliometric evidence indicates that the coverage of WoS databases is competitive in the social sciences (Martn-Martn et al., 2018), additional research should consider other databases in order to assure a more comprehensive coverage. In addition, we acknowledge that abstracts do not convey the whole story (especially considering that abstracts in various disciplines are written in vastly different ways), and that a proper meta-analysis on the subject at hand would be advantageous. Yet, as acknowledged in the literature, abstracts are of fundamental importance for screening academic publications, to the extent that the necessity and urgency to improve abstract reporting have been widely discussed (see, e.g., Guo and Iribarren, 2014; Saint et al., 2000) – as a result, we believe abstracts provide essential information for our analysis. We only considered English-language studies and reports, which is another limitation of this research that must be acknowledged. Even though English has become the lingua franca for researchers, we acknowledge that our language restriction (which was imposed due to resource limitations) may have led to some bias in the results; for example, we may have overlooked essential research with a more local or regional focus.

3.3 Data Analysis

We utilised a thematic synthesis method to analyse and present the data. First, the data were imported into NVivo 11 (software for managing and organising unstructured information) for coding. We applied codebook thematic analysis, which is a structured approach to coding that includes reflexive elements (Braun et al., 2019). In accordance with this strategy, the main themes (conceptualised as domain summaries or main 'nodes' in NVivo) and the majority of sub-level nodes (child nodes) were determined in advance of full analysis, but they were subsequently compared and revisited within the context of the abstracts as analysis progressed (see Table 1 for a summary of the nodes). Obviously, there is some overlap between some of the identified sub-codes (consider, for example, the division by discipline); when creating categories, we aimed to strike a balance between being sufficiently fine-grained for analytical purposes and maintaining sufficient accuracy in light of the information available in the WoS database. Besides assisting us with qualitative analysis, NVivo allowed us to quantify the number of times each code was used across the sampled abstracts. A complete audit trail was maintained, and the two authors collaborated on data codification and interpretation.

4. REVIEWS

The aim of this research was to gain insights into the planning, procurement and use of new security technologies for policing. Complementing studies that have analyzed policy documents or measured the success or failure of outcomes, this work focuses on practitioners and the issues they face in day-to-day operations. Furthermore, official record keeping, position papers or policy documents do not tell us much about the precise tactics and strategies of their deployment or capture more informal interactions and processes (Beyers et al., 2014). Another caveat of simple policy analysis lies in the fact that, in some instances, the official position of the organization may differ from that of those directly working on the issue (Beyers et al., 2014).

A review of the research on implementation and impact of technological innovations in crime prevention and policing was conducted by James Byrne and Gary Marx [1]. They found that new technological innovations have been developed to prevent crime and to improve the performance of the police, but we know remarkably little about how and why certain innovations are adopted, and the consequences –both intended and unintended—of technology-driven solutions to the problem of crime.

According to a review of the research on implementation and impact of technological innovations in crime prevention and policing by James Byrne and Gary Marx, there are two general types of technological innovations that can be identified: information-based technologies (which we will refer to here as soft technology) and material-based technologies (which we will refer to here as hard technologies).

Soft technology innovations include new software programs, classification systems, crime analysis techniques, and data sharing/ system integration techniques. Hard technology innovations include CCTV, street lighting, citizen protection devices (e.g. mace, tasers), metal detectors, ignition interlock systems (drunk drivers), threat assessment instruments, and risk assessment instruments.

Some examples of technological innovations in crime prevention are:

1. Digital Forensic Software: This type of software is used to find, recover and preserve digital evidence that's often associated with electronic crimes, such as credit card fraud or child pornography.
2. Information Sharing Technology: This technology allows law enforcement agencies to share information with each other in real-time. It helps to identify patterns and trends in criminal activity across different jurisdictions.
3. Virtual Reality Training: This technology is used to train police officers in high-stress situations without putting them in danger. It provides a safe environment for officers to practice their skills.
4. Facial Recognition Software: This technology is used to identify suspects by comparing their facial features with a database of known criminals.
5. Biometrics: Biometric technology is used to identify individuals based on their unique physical characteristics such as fingerprints, iris scans, or facial recognition.

These are just a few examples of the many technological innovations that have been developed for crime prevention and policing.

5. FUTURE SCOPE

Different technology-driven solutions and the potential adoption of contemporary smart pervasive, machine intelligence systems and miniature technologies for crime prevention have been considered and evaluated. As discussed previously, we believe that the use of short-range communication technologies as a crime-prevention tool has enormous potential. Together with current approaches, such as GPS monitoring, these technologies can be used to create a more robust proximity detection system, capable of detecting proximity in both interior and outdoor environments. Smart and short-range identifiers may be used to provide immediate access to information and to report emergencies. In recent years, as previously mentioned, a number of applications to report and collect evidence of emergency situations have been developed.

However, these apps commonly require the user to open the app and perform a specific action. Furthermore, violence detection scenarios in home or work environments, the use of a audio-based technologies appear to be preferred against that of CCTV cameras given the ubiquity, spherical field and lower privacy concerns exhibited by the former systems. As exposed, the use of audio signal processing along with machine learning techniques, allowing for applications such as speaker diarization, speech recognition, person identification and sentiment analysis, could be key to identify violent language as well as violent actions. From a technical viewpoint, standalone systems employing a single sensing technology exhibit distinct limitation. However, the combination of technologies, can be of great use to identify violent scenarios, which can lead to the prevention of further occurrences and therefore to the ultimate prevention of criminal activity.

6. CONCLUSION

In conclusion, not all situations or circumstances are identical, and there are no "one-size-fits-all" solutions. As a result, it is essential to investigate the diversity of offenders, victims, contexts of offending, and offending patterns in order to determine which solutions may work for whom and under what conditions. In addition to privacy, scalability, affordability, miniaturization, and personalization are important factors to consider when designing crime-prevention technologies. However, future work will include the conduct of focus groups with elements of co-design and co-creation, where the findings and conclusions of this paper will be further discussed and analyzed with end-user organizations and other groups of interest. By doing so, we hope to acquire a deeper understanding of the potential, limitations, and drawbacks of the technologies under discussion, as well as obtain expert feedback. Next, a number of prototypes of the selected crime prevention systems will be developed and implemented. The police have benefited from technology, which has enabled them to conduct criminal investigations more effectively. However, we cannot overlook the difficulties it has caused. Technology has significantly reduced manual labor and digitized data, making it easier to retrieve older files and understand a criminal's or accused's past. Even social media has contributed to our knowledge of an individual's past. Due to technological advancements, the criminal investigation procedure is now more transparent. Through technology, a connection between the public and the police is also made possible. It aids law enforcement in the protection of public safety and property. Complaints from the general public can be handled promptly and effectively. A strong partnership between the police and technology would expedite criminal investigations, substantially reduce crime, and aid in the maintenance of law and order. For improved and faster law enforcement, we must therefore continue to modernize our technology.

7. REFERENCES

[1]. Byrne, J.M., & Marx, G.T. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact.

[2]. https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/

[3]. https://www.orange-business.com/en/blogs/how-technology-helping-fight-against-crime

[4]. Antrobus, E., & Pilotto, A. (2016). Improving forensic responses to residential burglaries: Results of a randomized controlled field trial. Journal of Experimental Criminology, 12(3), 319–345

[5]. W. Pugh, “Concurrent maintenance of skip lists,” April1989. Tech. Report CS-TR-2222, Dept. of Computer Science, U. Maryland.