7

The role of information systems in the prevention and detection of transnational and international crime

DIONYSIOS DEMETIS

Introduction

All around the world criminal activity remains at the forefront of governmental concerns, not only as a problem that distorts the very fabric of society within the confines of national jurisdictions, but also as a problem that cuts across national borders to exhibit a global dimension.[1] The international dimension of criminal activity remains critical and is generally characterized by a complexity that is unique and requires action on many different levels.[2] Criminals set out to mask their illegal activities and deliberately generate complexity as a means of concealment. In doing so, they exploit new developments in technology that assist them in achieving their ends. This criminality exhibits forms of innovation that stretch far beyond traditional criminal activity (e.g., drug and human trafficking) and manages to attach itself within the broader fabric of society by exploiting the very latest developments.[3] This evolution is necessary as criminals seek not only to escape arrest, prosecution and conviction, but also to enjoy the fruits of their criminality (mostly financial gains). Thus, they seek to develop ways of exploiting the various diffuse norms of social interaction (e.g., trust), financial modes of conduct (e.g., cash-based economies), technological and communication developments (e.g., Internet), and thereby minimize the possibility for detection. By limiting the resources that can be made available for prevention (or making them obsolete when

[1] J. Wolfensohn, 'Making the World a Better and Safer Place: The Time for Action Is Now', (2002) 22 *Politics* 118.
[2] S. Mohamed, 'Legal Instruments to Combat Money Laundering in the EU Financial Market', (2002) 6 *Journal of Money Laundering Control* 66.
[3] J Haines and P Johnstone, 'Global Cybercrime: New Toys for Money Launderers', (1998) 2 *Journal of Money Laundering Control* 317.

developing new criminal behaviour), they participate in this co-evolution actively; and this they achieve by generating complexity.

This dynamic is nothing really new, but the central role that technology has acquired in modern societies, particularly in the last decade, requires a more thorough look at how the spectrum of serious criminality changes in light of these developments. A more thorough investigation is also required in order to better understand how technology can be used to facilitate cooperation between different jurisdictions. Here another important issue is raised: in the fight against serious international crime, such as terrorism, or cross-border tax evasion, nation states have launched a number of initiatives for which citizen data are being stored in a centralized manner; jeopardizing this data can produce tremendous consequences and create adverse conditions leading to yet more crime. For instance, in the UK, two DVDs that contained a full copy of HM Revenue and Customs (HMRC) entire data of child benefits were lost en route to the National Audit Office in an unrecorded and unregistered package. The lost data affected 25 million people in the UK and jeopardized names, addresses, dates of birth of children, along with National Insurance numbers and bank details of their parents. Ultimately, this has exposed an entire generation to identity fraud. Should we treat these failures as singularities or as systemic occurrences for any large-scale centralized data project? The latter possibility seams more plausible due to the complexity behind these projects.[4]

In India, a project is underway to collect biometric data for the entire population with the aim of thwarting tax avoidance and corruption and securing a single identification scheme for the population. The government promotes the project, not only as a means to tackle corruption and tax evasion, but also as a way to provide particular benefits to the population from government funds and also gain access to banking services. While this massive effort seems to display a near complete disregard for the security risks related to the storage of biometric data in centralized databases,[5] it does

[4] After much debate in the House of Commons and the House of Lords, the biometric-enabled identity card scheme for the UK was halted for both financial reasons as well as doubts about the security of the systems and their potential effect to curb criminal activity by getting a firm grip on individual identity. See LSE, 'The Identity Project', Department of Information Systems, London School of Economics, (2005), available at http://csrc.lse.ac.uk/IDcard/default.htm.

[5] A very useful report to look at comes from the Future of Identity in the Information Society (FIDIS), which has examined the relationship between the Public Key Infrastructure and Biometrics. More can be found in the report: M. Gasson, M. Meints and K. Warwick (eds.), 'D3.2: A Study on Pki and Biometrics', (FIDIS, 2005) at 1–138.

demonstrate that technology is at the top of government agendas in an effort to bridge control of identity with financial crime (as well as other transnational crimes). This irresistible fusion between technology and tackling criminality is very important. It is usually predicated upon the assumed thesis of benevolent effects of technological systems, without taking into account the side effects that are created by a new class of antitheses. In such circumstances, technological implementations create unintended uses, violations, misuses and unpredictable behaviour.[6]

Hence, the handling of information through technology-based systems gives rise to a domain that is becoming more and more central to the development of coordinated action in tackling criminal activity at both national and international levels: the domain of Information Systems (IS), in particular, the role they occupy across various subsystems that focus on tackling criminal behaviour.

IS are considered tools that can be harnessed for both preventing and detecting criminal activity; and, indeed, they have found a number of applications at national and international levels. IS are generally recognized as important catalysts for progress and transformation and there may be good reasons why IS are seen as critical in the fight against crime: they organize data in structured ways, while the character of automation embodied in these technologies is perceived as an enabler that allows for rapid data processing and swift communication between stakeholders. It is believed that this combination of automation/communication can prove critical in tackling criminal activity across national borders.

In addition to the communication possibilities opened up by modern technology, advances in data storage have led, and continue to lead, to long-term storage of large datasets.[7] This creates vastly different dynamics in the way data can be manipulated from small-scale technological installations as data sharing magnifies the phenomenon. The mass of data available can be used to infer characteristics for certain types of behavioural patterns, from which general profiles can be created that encapsulate an abstraction of criminal behaviour. By abstracting such behaviour and subsequently applying its characteristics to future data, one is – in theory – able to estimate the probability of an individual

[6] I. Angell, *The New Barbarian Manifesto: How to Survive the Information Age* (London: Kogan Page, 2000); I. Angell, 'As I See It: Enclosing Identity', (2008) 1 *Identity in the Information Society* 23.

[7] C. Apte, B. Liu, E. Pednault and P. Smyth, 'Business Applications of Data Mining', (2002) 45 *Communications of the ACM* 49.

committing a crime. It is worth pointing out that the digital traces of individuals unrelated to particular criminal activity are also parties to this process. Their contribution lies in simply providing more and more data that can be used to infer how 'normal behaviour' can be categorized and clustered according to different age groups and various other demographics. Against the backdrop of this supposed normality, suspicious behaviour can be flagged and then further analysed, as will subsequently be explored with the use of illustrations regarding money laundering. The effectiveness of this process remains to be examined in more detail. At this stage, it is worth pointing out that the role of IS is not only enabling, by supporting solutions for the problem of criminality and augmenting traditional efforts by automating processes or providing further intelligence, but also constraining in ways that are often subtle and interfere with regulatory intentions. Technology creates bottom-up effects that sometimes counteract top-down impositions.[8] Unintended consequences come into play, despite the strict logical paths upon which technological operations are executed.

On the basis of the context briefly discussed above, this chapter investigates how IS exert influence in preventing and detecting criminal activity. *First*, the phenomenon of data growth is analysed, as it is central to the problems that are created when there is an effort to profile suspicious behaviour. Through a series of properties, data require processing, manipulation, categorization and analysis. *Second*, two key concepts are presented that are very important in pondering the greater role of IS. They are at the core of manipulating large datasets, namely *profiling* and *data mining*. These are examined from a non-technical perspective in order to highlight how they are being used as techniques for spotting suspicious behaviour and how data are being used to profile, algorithmically manipulate and distil actionable information for preventing criminal behaviour. *Third*, the majority of the chapter focuses on the domain of money laundering for highlighting the interaction between technology and the detection and prevention of criminal activity. Reference to the anti-*money laundering* (AML) domain is helpful in considering both how technology is being used as an early warning mechanism in order to flag suspicious activity, and how the development of group/individual profiles that simulate money laundering behaviour have important side effects.

[8] D. Demetis, *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach* (Cheltenham: Edward Elgar, 2010).

By extrapolating from the issues identified above, a theoretical framework is presented at the end of this chapter that addresses the influence of technology on tackling criminal activity and considers the information dimensions for monitoring criminality. Peripheral, yet important, issues are factored into the considerations of this framework and include how criminal activity can be balanced with civil liberties, as well as the potential for using Privacy Enhancing Technologies (PETs) for (partly-) anonymous data sharing between stakeholders at an international level.

Data growth, databases and the algorithmic construction of criminal behaviour

Current criminal activity is unfolding (in both its cyber and real-world dimensions) and characterizes our information age. Governments, intelligence agencies, police authorities and other organizations or stakeholders have at their disposal an unprecedented amount of data to prevent or detect criminal activity. Making sense of this data is the challenge at hand; and it is no easy task.

Every year we produce a staggering volume of data, equivalent to about 37,000 libraries the size of the US Library of Congress.[9] Most of these data are unstructured from a computational perspective, meaning they are not tied to a specific coherent database structure. We create text-based data in word processing, presentations, numerical data in spreadsheets, communicate by exchanging emails, publish tweets, produce (or become subjects of) audio recordings, digital pictures and full motion video, while at the same time participating in social networks on the Internet and other forms of web-based communication. In equal measure the various industrial actors produce or store their own sets of data, thus giving rise to different industry-specific data categories participating in the growing pool of data. For example, the medical industry creates medical data such as MRI, or the financial sector stores raw transaction datasets created by individual financial transactions, thereby recording the movement of money. More and more data are being created year on year. These data are stored on paper, film, magnetic or optical storage and flow through broadcasts, telephony and the Internet.

Massive as the volume of data may be, they constitute the raw material that is being monitored, used, analysed, categorized and filtered for

[9] P. Lyman and H. Varian, 'How Much Information 2003?' (2003), available at www2.sims.berkeley.edu/research/projects/how-much-info-2003/.

various reasons. To an extreme level, the volume of data becomes the subject of indiscriminate massive monitoring by intelligence agencies (national security agencies). The approach that has been suggested by the US National Security Agency (NSA) director, General Keith B. Alexander, is to 'collect the whole haystack rather than look for a single needle in the haystack; collect it all, tag it, store it . . . and whatever it is you want, you go searching for it'.[10]

Crime detection and prevention are key concerns that have always made use of various forms of data. Therefore, while there could be an obvious information value in this pool of data for crime detection and prevention, it is the set of consequences that emerge from utilizing data that is fascinating to explore. These consequences create severe side effects, not only on data subjects that may be under investigation, but also on 'future suspects' that will be filtered through the exploitation of data. At an ontological level, a much deeper effect percolates, as the dimensions of criminality are being constructed through technology. Legislation may be regulating the top-down imposition by defining the nature of behavioural activities that can be categorized as criminal (and the penalties for engaging in such activities), but technology maintains the infrastructure through which suspicious cases are advanced and given priority over others. Moreover, the sheer complexity of the operations involved at a computational level implies that the full extent of these processes cannot always become visible.

Technology acts in a bottom-up fashion and often in contradistinction to the function of legislation that sets the norms through which criminality is interpreted. By automating complex processes, technology also carves a different space in establishing a systemic role. In turn, these elements mutate into new social forms. They are transformed into new conditions which take the form of an infrastructural reorganization in the shape of electronic information.[11]

Algorithms create the logical platform through which suspicious behaviour is deconstructed and encapsulated. *Machines* provide the technical infrastructure upon which automated operations are undertaken and communicated. And *humans* are called upon to validate or discard the *technologically constructed suspicious behaviour*. The last

[10] E. Nakashima and J. Warrick, 'For NSA Chief, Terrorist Threat Drives Passion to "Collect It All," Observers Say', (2013), available at www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49–11e2-a301-ea5a8116d211_story.html.

[11] J. Kallinikos, *The Consequences of Information: Institutional Implications of Technological Change* (Cheltenham: Edward Elgar 2006).

stage in this process (i.e., human intervention) maintains the illusion that human judgement intervenes to establish a control mechanism for what is being automatically generated. However, this ignores a complex stratum of technical interconnections that yield unpredictable results. Technology acquires a systemic role that functions in an unpredictable manner, not because at the micro-level the results of specific operations cannot be predicted with accuracy, but because at the macro-level the system of technology acquires such a degree of complexity that it is impossible to monitor all the interactions that take place at the level of the system.[12] At the same time, it is impossible to predict how the interactions between different algorithms will affect the platforms that support them, or how their interactions will play out over time.

An illustration, among many others, can be found in the financial markets. In what is known as 'the crash of 2:45', the Dow Jones Industrial Average recorded the biggest one-day point decline in its history (998.5 points) due to automatic computerized traders on the stock market engaging in 'algorithmic trading', where the automated execution of orders without human intervention led to an unpredictable level of withdrawing from the stock market, thereby creating liquidity problems.[13] This incident was meant to illustrate the unpredictable systemic nature of large-scale automated operations, thereby indicating that technology is not subordinate in the causal sense. It gains an autonomous character that goes against social and legal norms, as the processes that support technology feed off each other in unpredictable ways. Such processes tend to create 'positive feedback loops' that have a tendency to destabilize the system from what an observer would consider as a predictable state.[14] Moreover, in the context of dealing with criminality, the embodiment of human working practices into technologically supported processes means that the nature of work in the fight against transnational (and other forms of) criminality has changed drastically, particularly when international collaboration is demanded.

While the communicative role of technology has established a faster and better way to support the communication between authorities in

[12] N. Luhmann, *Social Systems, Writing Science* (Stanford: Stanford University Press, 1995) at iii, 627; N. Luhmann, *Law as a Social System* (Oxford, New York: Oxford University Press, 2004) at viii, 498.

[13] T. Hendershott, C. Jones and A. Menkveld, 'Does Algorithmic Trading Improve Liquidity?'(2001) 11 *Journal of Finance* 1.

[14] N. Glass, 'Chaos, Non-Linear Systems and Day-to-Day Management', (1996) 14 *European Management Journal* 98.

different countries, there is yet another role that technology acquires. This is primarily concerned with the development of techniques for understanding the nature of criminality with a view to developing mechanisms that facilitate the profiling of criminal behaviour. This is usually based upon a series of techniques, such as statistical analyses of datasets with crime-related information, geographic mapping of hotspots where criminal activity takes place, economic or other indicators which may suggest that a rise in criminality is about to occur, and so on. This exercise in figuring out how criminal behaviour presents itself in different contexts is an important one, but the role of technology therein is largely underestimated. Technology is not only applied to delineate certain patterns of criminal activity/behaviour by shifting large volumes of data. Once that process is over, it is assumed that the results achieved have a near-causal developmental link to the processes that gave rise to them. Put simply, it is assumed that this is 'what criminality looks like'. The next step seems to follow almost naturally, but the leap is significant. Once we have what we believe to be the fundamental building blocks of a criminal phenomenon (in how/when it occurs, what we should be looking for to observe as early signs for future criminal behaviour, etc.) then we can apply this 'pattern' (or series thereof) to new data that are either real-time or near real-time data (or within a certain timeframe) and reduce this new volume of data to a few suspicious cases that could be examined more closely.

This process has nothing to do with the search for a unique suspect who has committed a crime (either at a national level or through international cooperation) or a network of criminals. It is not a process through which criminals are uniquely identified, but it becomes a process where *potential* criminals are singled out for further investigation because they fit a set of abstract characteristics. These characteristics have been deduced, not only by analysing previous criminal cases, but also by using various other data sources. The process of discovering patterns in large datasets is the overall goal of data mining.[15]

The fact that this constitutes some type of 'pre-emptive strike' against criminality is one element to the process: the one that allows us to simulate and prevent. But the much deeper effect is usually side-lined and not considered at all. This is what, in this author's contention, can be described as the *technological construction of criminality*. In a sense, and

[15] S.-O. Tergan and T. Keller, *Knowledge and Information Visualization: Searching for Synergies, Lecture Notes in Computer Science* (Berlin, New York: Springer, 2005).

in the 'eyes of algorithms' where pattern is king, the results of the applications of filters for criminal activity, yield outputs that are already considered as highly possible criminal cases. This algorithmic prejudice inflicted upon the subsequent human evaluation must be taken into serious consideration. As we shall see in the paradigm devoted to AML technology, this has had serious side effects that hinder both national and international efforts in combating the phenomenon.

Reliance on technology for supporting processes that tackle criminality is not only to be found in the communicative role of IS. Technology assumes a more important function as it becomes extensively used to conduct profiling at a pre-criminal level, on the basis of data that are stored from previous criminal cases. The institutionalization of these processes creates an iron cage that treats possibility as suspicion.[16] Through a series of self-referential processes more data leads to more profiling and more suspects, but also to an elevated risk of being completely overwhelmed by the white noise that permeates these processes to begin with. In turn, conducting manual checks becomes a painstaking process; ultimately the checks become more costly and counterproductive, staff may become demoralized and prosecution rates remain low. International cooperation is hindered at the national level as technology places increasing demands on cooperation by simplifying communication. Requests on information for suspects need to be prioritized and the technological modes of operation need to transcend the national in support of the international cases that exhibit a greater degree of complexity. But how has the technology shaped the international dimension of cooperation against crime?

The role of information and technology-based systems in the internationalization of policing

From a historical perspective, advances in technology were deemed to be 'instrumental in facilitating the internationalization of policing in a form that is independent of law and politics'.[17] The evolution of technology

[16] P. J. Dimaggio and W. W. Powell, 'The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organization Fields', in W. W. Powell and P. J. Dimaggio (eds.), *The New Institutionalism in Organizational Analysis* (Chicago, IL: University of Chicago Press, 1991).

[17] M. Deflem, 'Technology and the Internationalization of Policing: A Comparative-Historical Perspective', (2002) 19 *Justice Quarterly* 453.

has led towards cross-border cooperation because barriers to communication between institutions were rendered obsolete. Structural conditions that had to be satisfied for the control of international crime were met, for example, by establishing interoperability between systems, or by agreeing on common standards such as methodologies for fingerprint measurements. IS pre-dating the information exchanges that were supported by computers (e.g., telegraphic code, radio communications, printed publications) facilitated the early forms of data exchange. However, the evolution in communication, exchange and storage has been phenomenal; and it is all down to the invention of the microchip, which gave rise to what we can nowadays call a 'computer'. This dynamic has also been completely altered by the invention of the Internet, which removes the locale of information and has a substantial impact on data storage and availability.[18]

Of course, another issue that changes the scope of what data becomes available through the Internet, remains the fact that users are willing to put personal information online, including their locations, photographs, personal preferences, education, age, work experience, activities, and a lot more. This information is available immediately through the Internet and constitutes an ever-growing platform of exploration for intelligence purposes, exploration of social networks and extraction of statistics for developing various models that can assist in understanding demographics, socio-economics, political implications and trends that may be considered as proxies to criminality. While it may not be immediately evident how such data can be used to deal with criminality when they are provided wittingly by non-offenders (in most cases), it needs to be made clear that criminals are perceived as 'anomalies' within the broader system. At least from an IS perspective, they may be viewed as exceptions to the normality that non-offenders may exhibit in their digital traces. It is in the distinction and the difference between criminal/non-criminal that data manipulation rests, while both sides to a distinction[19] are necessary in order to examine the phenomenon and gain a deeper understanding of how the 'anomalies' can be algorithmically traced or how technology can assist in collaborative work between nations for this purpose. Needless to say, privacy implications are very important also, even though not the subject matter of this chapter; the potential misuse

[18] J. Kim, 'Phenomenology of Digital-Being', (2001) 24 *Human Studies* 87.
[19] N. Luhmann, *Theories of Distinction: Redescribing the Descriptions of Modernity* (Stanford, CA: Stanford University Press, 2002).

of data[20] can create negative effects and cast serious doubt upon the aggregated operations of both governments and companies, who are bound to suffer from security breaches as no system can be considered fully secure.[21]

Through automation, and propelled by it, data become the irresistible source that must be harnessed in order to lead to action; data become a source of pre-action. The question then becomes slightly different in the context of tackling criminality. How can we 'derive benefits from this increased data availability'?[22] How can the *anti-criminal value of information* be considered, both in light of the technological developments and in the context of the internationalization of policing?

Forensic technologies are also considered under this prism: for example, fingerprints. While the collection of such biometrics constitutes a physical process to begin with, the internationalization of their use in policing has been facilitated by the deconstruction of a specific set of information characteristics that describe the physical biometric. Interoperability in the methodology for measuring fingerprints (i.e., agreement on the unique measurements that will be taken) is necessary in order to develop an infrastructure that will communicate the measurements, or store the metrics in databases so that they can be shared or searched more effectively. For example, in the case of fingerprints, it is not the image itself that is searched, rather the deduced mathematical structure and numerical pattern that has been extracted from the image.[23] From an information science perspective, this becomes an informational subset that needs to be manipulated. Information then acquires another set of properties that become fundamental and absolutely critical in characterizing the information age. The demands that are placed by the increasing volume of information place further strain on the functionality that needs to be powered by technology in order to improve international cooperation. This requires more thorough forms of international cooperation. For example, there needs to be an

[20] C. Arndt, 'The Loss of Privacy and Identity in the 21st Century: Causes and Possible Solutions', (June 2006) *Biometric Technology Today* 3.

[21] G. Dhillon and J. Backhouse, 'Information System Security Management in the New Millennium', (2000) 43 *Communications of the ACM* 125.

[22] A. Gotlieb, C. Dalfen and K. Katz, 'The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles', (1974) 68 *American Journal of International Law* 227.

[23] U. Uludag, and A. K. Jain, 'Attacks on Biometric Systems: A Case Study in Fingerprints', in *Proc. SPIE-EI 2004* (San Jose, CA: 2004).

agreement on information management, such as an agreement on the categories that should be used in the semantic tagging of crimes throughout different countries; otherwise, comparisons become meaningless and inferences regarding the characteristics of crime are rendered unfounded.

Table 7.1 summarizes some of the key communication technologies and developments that have been used in policing and tackling crime; these have further transcended national borders to achieve some degree of cooperation between nations.

By looking at Table 7.1 one can observe a main strand of development: the communications/technological strand that allows for the establishment of communication between different countries, much like the first telegraphic messages exchanged between the UK and the USA, leading to the Internet, which allows for global communications nowadays. But there is another strand with complimentary characteristics that refer mostly to the storage and processing of data, such as the invention of the microchip, leading to the development of both hardware and software: the constituent components of the modern computer. Nowadays, we have even got the application of anti-crime specific software, or tools for supporting the collaborative work between countries aiming to prevent or detect criminal activity.

In Table 7.1, the Internet is considered as the latest major development as a medium for the communication of criminal cases, suspects, etc., between authorities. Moreover, the Internet is used as a communication facilitator for data across national law enforcement agencies (LEAs) that feed data into specific IS with structured databases.

Table 7.1: *Evolution of communication systems in tackling crime*

Time horizon	Information and communication technologies (ICTs) development
1850	Telegraph
1876	Telephone
1900s	Radio communications
1924	Fingerprint measurements
1932	FBI inaugurates forensic laboratory
1940	Radar used in policing
1964	Facsimile
1970s	Modern computers
1980s	The Internet used as a medium for networking/communication and replacing a lot of pre-existing functionality from other ICTs.

When considering the internationalization of policing and the collaboration through which crime can be prevented and detected, the role of the Internet cannot be stressed enough. Even though important security concerns may be raised in the context of providing multiple cross-national user access to crime-related data,[24] particularly when suspect-related data can be modified, the utility from deploying web-based resources for tackling international crime remains extremely important.

The IS of Europol

Looking at how IS are being used at cross-border level it is pertinent to describe briefly the three core IS being used by Europol in order to facilitate the exchange of information: the Europol Information System (EIS), the Secure Information Exchange Network Application (SIENA), as well as the Europol Platform for Experts (EPE).

The first information system, the EIS, constitutes the 'reference system for offences, individuals involved and other related data to support member states, Europol and its cooperation partners in their fight against organized crime, terrorism, and other forms of serious crime'.[25] Europol not only allows LEAs to transmit data into its systems, but also validates and feeds data from third parties into the system, the majority of which is inserted by means of automated data loading systems. As of December 2012, more than 185,000 data objects reside in its database, including 48,000 suspected or convicted criminals, a rise of 17 per cent compared to 2011. About 34 per cent of the data objects relate to drug trafficking, while the major crime areas that are also identified include forgery of money, robbery, illegal immigration and fraud. Member states transmit data on entities that can be cross-matched, such as persons, cars, telephone numbers and firearms. National LEAs both share and compare data with the EIS. The EIS is being used when conducting investigations, thereby acquiring a detection character, but it is also used as a reference tool from which statistics, characteristics and inferences can be drawn, thereby developing profiling tactics through which criminality can be dissected into categories.

The SIENA system supports secure exchange of both operational and strategic information related to crimes and it is an important information

[24] Basel Committee, 'Sharing of Financial Records between Jurisdictions in Connection with the Fight against Terrorist Financing', (Basel Committee on Banking Supervision, 2002).

[25] Europol, 'Information Exchanges', (2013) available at www.europol.europa.eu/content/page/information-exchange-1848.

exchange network in the context of tackling criminality at an international level. This becomes evident when one examines the initiation of criminal cases; only 8 per cent are actually initiated by Europol itself.[26] The majority are initiated by Member States (82 per cent) while the remaining 10 per cent are undertaken by third parties that have cooperation agreements in place with Europol, thus establishing a means of international communication and cooperation in criminal cases. More than 400,000 operational messages were exchanged through the SIENA system between Member States, with more than 15,000 new cases initiated. The majority of information exchanges between states involved cases related to drugs (almost 30 per cent of all new cases), followed by fraud (15 per cent), robbery (11 per cent), money laundering (9 per cent), and illegal immigration (8 per cent).[27] A number of different countries collaborate in the SIENA system and of the total of sixty parties participating, twenty-seven are Member States.

Finally, exploiting the possibilities opened by collaborative tools in the web sphere, Europol has developed a secure environment, the EPE. This is meant to facilitate knowledge sharing between experts from different jurisdictions in a secure platform where similarities, differences and common practices can be discussed and improved. In this information system no personal data are being used; the aim is to enable sharing of suspect data between users on a variety of topics such as kidnapping, child sexual exploitation, counter terrorism, corruption, environmental crime, financial crime, fraud, etc. More than 2,000 users have joined the different expert online communities in the EPE.

The work undertaken by Europol illustrates that the use of technology to facilitate information exchange between different jurisdictions is multi-dimensional. Technology is used for a variety of purposes and establishes links that assist both in preventing and detecting criminal activity. Technology also allows the parties to gain distributed access to the same digital entities: the digital objects that variously characterize suspects for criminal activities. Distributed access through the Internet allows for the internationalization of tackling criminality,[28] while the aggregation of different digital objects into single platforms allows for the emergence of collaboration as a critical factor. While all

[26] Ibid.
[27] Available at www.europol.europa.eu/content/page/europol-information-system-eis-1850.
[28] G. Papanicolaou, *Transnational Policing and Sex Trafficking in Southeast Europe: Policing the Imperialist Chain* (Basingstoke: Palgrave Macmillan, 2011).

these aspects appear to be positive in advancing the internationalization of policing and the fight against transnational crime, there is a dark side to technological implementation. In addition, there are restrictions on how far automation can be allowed to intrude into human decision-making processes, even when these boundaries are constantly pushed forward (and usually making more room for technology along the way).

Profiling data

Demands to cut down on the complexity generated by increased data availability have led to a number of techniques that attempt to reach a subset of these data, so that their manipulation can become more meaningful in a specific context. This seems to come almost naturally, as it is impossible to consume all the data that we have at our disposal in any given situation. As human beings, this restricts us in a most fundamental way. Let us take Google as an example. Behind a highly efficient infrastructure that swiftly ranks search results by using complex algorithms, lies a peculiar form of profiling that becomes dependent on the search engine itself; human profiling, namely profiling by human beings. The top thirty results from a search receive over 90 per cent (!) of search traffic.[29] The capacity and complexity of computational processing in such scenarios becomes vastly undermined while the output of an algorithm is fiercely cut down by what computer scientists may view as a necessary evil: human processing. Therefore, computer profiling and human profiling become structurally coupled and co-dependent. Advanced computations are irrelevant if they are decontextualized and human decision-making restrictions are not considered, unless of course, computers are allowed in the future to *become decision makers* instead of constructing part of the reality for decision makers. But isn't this technological interference already developing influential preconditions upon which humans are called to exercise their judgement?

In *profiling*, the goals are to extrapolate and formulate a set of characteristics (e.g., behavioural) about an individual, a collective entity, or even a general phenomenon (e.g., money laundering); thereafter, this set of characteristics (i.e., the profile) is applied to other entities that are being treated in light of these same characteristics.[30] While in the field of

[29] B. Jansen and A. Spink, 'An Analysis of Web Documents Retrieved and Viewed', in The Fourth International Conference on Internet Computing (Las Vegas, NV: 2003) at 65–9.

[30] H. Hirsh, C. Basu and B. Davison, 'Learning to Personalize', (2000) 43 *Communications of the ACM*, 102.

information science *profiling* is considered a process with a number of distinct stages, it needs to be acknowledged that the profiling process has two key components which must be distinguished and which are central to the extraction of 'anti-criminal value from information'. The first concerns *profile generation*, which is the process of inferring a profile, and involves analysing personal data in search of patterns, sequences and relationships in order to arrive at a set of assumptions, while the second relates to *profile application*, which treats entities in light of this profile. The latter assists in decision making and more specifically in limiting the number of results (or suspects in the context of criminality) so that the remaining subset becomes meaningful to manipulate.

Hence, the need for profiling emerges from the need to cut down on this complexity (or even just volume).

But what implications does this have for individuals? Firstly, the 'use of extensive data profiles by public or private institutions deprives the individual of the capacity to influence decision making',[31] with decisions being made on the basis of individual 'data shadows'. Secondly, excessive reliance on technological infrastructures or sophisticated software for monitoring criminal behaviour may lead to human decision makers abdicating their responsibilities. But the real issue here is to define the essential characteristics of a decision taken by computer software. According to Bygrave: '. . .a negative answer would say that software cannot actually make a decision because mental action is required . . . an affirmative answer would say that the *logical processes of computer software would seem to parallel sufficiently the processes of the human mind to justify treating the former as analogous to the latter*'.[32] The affirmative answer also implies that human activity is always involved, even if he/she is not part of the process as he/she is responsible for programming the software.

The major flaw in the affirmative position is that the collective actions embedded within the technology cannot be monitored due to an emergent complexity. It must be understood that to attribute a singular intentionality to particular artefacts or technologies:

> simplifies the complex texture of technologically embodied functionalities (because the intentions of many groups are mingled in the design and

[31] L. Bygrave, 'Automated Profiling; Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling', (2001) 17 *Computer Law & Security Report* 17.

[32] Ibid. (emphasis added).

> development process) ... and that technology influences human agency not by imposing a single and mechanical functionality but by *inviting specific courses of action, courses of action that are engraved by the distinctive way by which each technology frames its reference domain*.[33]

In the context of tackling criminality there has been a tremendous increase in the frequency and intensity of profiling practices.[34] An emergent industry has grown out of this, building upon a number of techniques such as data warehousing and data mining. Software that is specifically designed to assist in investigations comes in various forms, with many different companies offering 'solutions' that can be used by both the private and the public sector in order to prevent and detect several types of criminal activity. In most cases the software is custom-made to detect specific activity (such as software for spotting money laundering). In other cases, particularly useful for large-scale criminal operations, software is being used to determine the structure (and hierarchy) of criminal organizations and to create a platform where different individuals can collaborate in this process, contributing with different data objects, allowing for an online distributed collaborative effort. Software has even been used to screen inmates in prison and their interactions with visitors, attempting to prevent further criminality by monitoring and deconstructing the 'support criminal network' of inmates on the outside in order to infer further suspects.

While simple surveillance can be found in police databases throughout the world, where image/voice recognition and real-time video monitoring is taking place in order to locate suspects, a notable shift is taking place in attempting to monitor the social context in which criminals operate. The more open habitat of information availability lends itself as an excuse to such projects. Monitoring includes close business associates and family members, recognizing that there is a network of support through which serious criminality operates and that the very monitoring of such a network could provide new opportunities for preventing further criminal activities. The social networking dimension of preventing and detecting criminal activity is yet another testament of the need to capture the mobility of criminals and their networks and to consider action plans through international efforts. The chapter now turns to the key example

[33] J. Kallinikos, 'Reopening the Black Box of Technology: Artifacts and Human Agency', in Twenty-Third International Conference on Information Systems (2002).

[34] M. Hildebrandt and S. Gutwirth, *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Berlin: Springer, 2008).

of AML in order to discuss these issues, before presenting a theoretical framework for considering the different information dimensions that interact in the operation of technology against criminality.

IS in tackling money laundering and implications for countering the financing of terrorism

The integration of technology in the fight against money laundering is one of the finest examples where data growth, profiling, the technological construction of criminality, and national/international implications can be brought together. The volume of transacting data that needs to be monitored, coupled with the requirements of profiling such a complex behaviour, creates interesting dynamics.

First of all, financial institutions have to cope with a staggering volume of data. For instance, one large financial institution in the UK deals with about 15–20 million transactions per day. Checking those transactions for money laundering-related behaviour over a period of time (typically for a three-month timeframe) becomes a difficult profiling exercise. The vast mass of data creates a unique challenge: the development of profiling queries (i.e., a series of conditional statements) that will be applied to the totality of these data with the aim of identifying suspects for money laundering. In this process there is an attempt to exploit possible relationships between the data and to uncover transacting anomalies or patterns of transacting that would have a high probability of being the traces of launderers. One problem that arises here lies in the construction of the profiling queries themselves: are the relationships uncovered by profiling meaningful? Or is it simply that the relationships are imposed by the profiling queries in the first place?

Regulators generally ignored these issues. Technology was introduced hastily. Financial regulators around the world wanted banks to deploy transaction-monitoring systems so that they could identify potential money launderers and report them to the authorities (e.g., DP22 in the UK[35]). With money laundering tied to serious primary criminal offences

[35] With Discussion Paper 22 (also known as DP22), the Financial Services Authority (now disbanded and organized otherwise) in the UK, kick-started the suggestion that regulated entities should incorporate 'automated monitoring systems' according to the complexity of their business, number of branches, functionality required, IT infrastructure, etc. See more at FSA, 'Reducing Money Laundering Risk – Know Your Customer and Anti-Money Laundering Monitoring', (2004) available at www.fsa.gov.uk/pubs/discussion/dp22.pdf, at 18–21.

(such as drug and human trafficking), the potential that technology could deliver seemed enormous. Hence, financial institutions globally were forced into a swift adoption of AML software. The software industry around AML, profiling, fraud, AML training, compliance, and so on, boomed in the 1990s. However, the unintended consequences were many and diverse, both in the application of the software and their side effects at the domestic level.

An example from a real bank in the European Union area will help clarify the issue at hand. The financial institution under consideration bought an off-the-shelf software platform. Following the installation of the software and after months of customization efforts, the software produced about 2,000 Suspicious Activity Reports (SARs) per day. But while the SARs were coming in the thousands, manual analysis of the reports by money laundering analysts was limited to roughly one hundred SARs per day. The rest were considered white noise, an obstacle to the method of producing real suspicious reports. After the software had supposedly done its job in producing suspects for money laundering, human decision making took over. Money laundering analysts were called to decide which of those technology-generated cases were truly suspicious. The result was a numerical percentage that is known as the True Positive Rate (TPR). Such a number characterizes the effectiveness of every profiling technique. This rate indicates what percentage of the software-generated suspicious reports were considered as actually suspicious following the manual examination of the reports by analysts. For instance, if the software generates 100 suspects for money laundering, following which due diligence and manual analysis of the suspects finds that only one out of 100 is considered to be truly suspicious (based on human judgement), then the TPR would be 1 per cent. In financial institution under examination this number was approximately 0.02 per cent. Of course, while this percentage of the TPR is extremely disappointing, it is far from unusual. In fact, most financial institutions start off with TPRs at this range and gradually manage to increase them (to about 15–25 per cent) after years of optimizing the queries that simulate how a money laundering suspect would transact. Even so, this means that technology is generating 75 per cent false suspects for money laundering, at a best-case scenario. These cases that are mistakenly considered as suspect cases are known as *false positives*.

Despite all the computational expertise that is on parade and the evolution in constructing supposedly sophisticated algorithms for tracing suspicious transactions for money laundering, the unintended consequences escalate to cause problems at both national and international

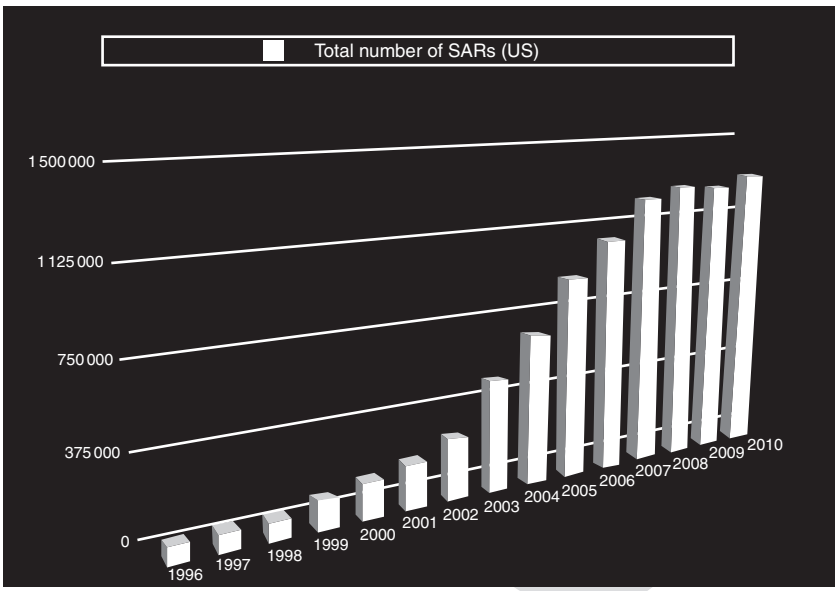
levels. The fear of financial fines for non-compliance (a recent example is HSBC, which was fined $1.9 billion for non-compliance with money laundering regulations[36]) has led to a reckless use of such technology. Even with some financial institutions increasing the number of their staff members six-fold to cope with the analysis of the technology-generated suspects, the volume of alerts was much greater. This has resulted in a 'hot-potato syndrome': financial institutions would pass on technology-generated suspects to the national authorities (the Financial Intelligence Units (FIU)) and these in turn will often request assistance from other jurisdictions where financial activities are linked to criminality in other countries. Hence, the volume of data and the reckless use of technology have led to an increasing number of computer-generated suspects, passed on to FIU, which were swamped with white noise instead of useful information. This phenomenon has been behind the considerable increase in the number of SARs collected at a national level. Examples of this increase for the UK and the USA can be viewed in Figures 7.1 and 7.2.

The increased volume of SARs available to the authorities resulted in the quality of information being jeopardized,[37] accompanied by very low prosecution rates. Similarly, the results in asset recovery have been horrendously poor. In the UK, this led in the past to the dismantling of the Asset Recovery Agency (ARA) after it became known that the cost of investigation for confiscating £40 million (out of an estimated £1.5 billion laundered annually)[38] was £400 million. While at the macro-level the

[36] A. Viswanatha and B. Wolf, 'HSBC to Pay $1.9 Billion U.S. Fine in Money-Laundering Case', Reuters (2012), available at www.reuters.com/article/2012/12/11/us-hsbc-probe-idUSBRE8BA05M20121211.

[37] A severe and direct consequence was experienced as a result of the above practices, mostly referring here to the issue of *over-reporting*. The databases of Financial Intelligence Units (i.e., the organizations responsible for collecting the SARs for money laundering) were filled with white-noise. Instead of useful information that could initiate an investigation and even a prosecution of money laundering, the FIUs ended up receiving useless information. In all these processes, technology has played an important role because it gave the tool to the financial institutions to report excessively. It was specifically this problem that led – much later – to the introduction of the risk-based approach in the Third Directive of the European Union. That introduction alone is meant to reduce the compliance-fear experienced by the majority of financial institutions (accompanied with a series of financial fines for non-compliance) and indirectly to maximize the potential for useful submissions of SARs. Nevertheless, despite the intentions, this approach has led to considerable confusion because of the ambiguities intrinsic in the concept of risk itself.

[38] BBC, 'Assets Recovery Failing', (2006) available at http://news.bbc.co.uk/2/hi/uk_news/politics/5077846.stm.



Figures 7.1: Suspicious Activity Reports (SARs) in the USA, 1996–2010

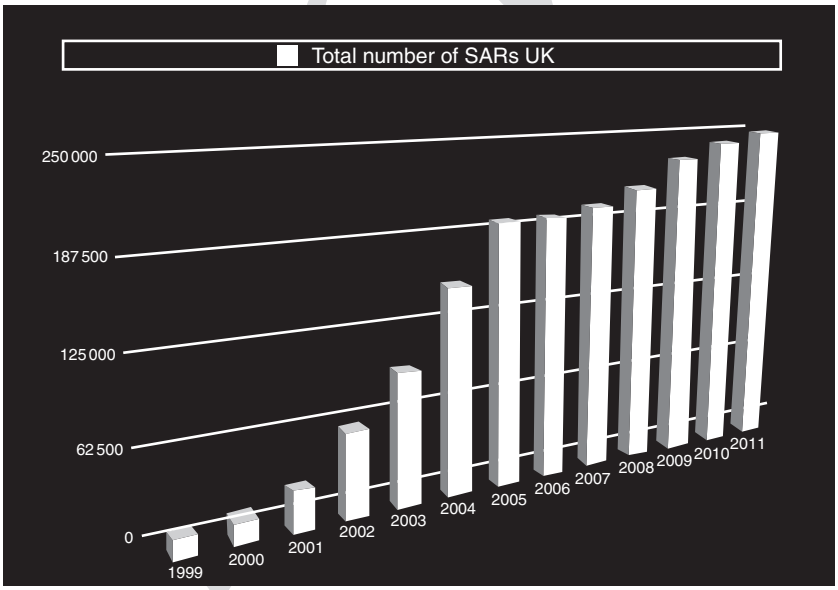


Figure 7.2: Suspicious Activity Reports (SARs) in the UK, 1999–2011

system has become ineffective, at the micro-level the question is why it is so difficult to model money laundering. Why is technology causing so many problems across a wide number of stakeholders in AML (and not just financial institutions)? Furthermore, how should IS be considered in light of an increasing demand to establish international cooperation for tackling criminality while taking security, privacy and civil liberties into consideration?

With IS, data are stored in the databases of financial institutions and other stakeholders. The difficulties in monitoring can be attributed to a number of factors. Firstly, databases degrade and their information value deteriorates due to human error and non-updated information. Secondly, the complexity of the phenomenon cannot be easily encapsulated in a computer model; financial information is a proxy to other types of behaviours (e.g., lifestyle that involves singularities) that are also important but which are not susceptible to a mathematical representation. Thirdly, financial institutions have access to a fragmented view of transacting behaviour, given that customers/suspects may engage in a much broader spectrum of financial transacting through other institutions (and quite often, in other jurisdictions).

Therefore, when a financial institution reports a SAR for money laundering or terrorist financing it identifies a potential suspect (or group of suspects) and sends the identity information to the national authority (i.e., the FIU) along with a record of transactions. The FIU has several options. It can either request additional information from the initial reporting entity (e.g., all transaction data from the account opening), or seek additional information from all other financial institutions for the individual(s) involved. Then it has to wait until it receives a response from the reporting entities and examine whether the collected information constitutes a real money laundering case that can be forwarded for prosecution.

In the totality of a national AML system, the above information workflow can be viewed as both time-consuming and random. Suspicion emerges as an outcome even with only a shadow of the totality of information being available (at national level). Decentralized databases that are scattered in various financial institutions are pieces of the puzzle for identifying suspects for money laundering. A logical next step would seek national access to financial data, with regulators and mostly FIUs demanding some sort of access. This is the situation in Italy where the Italian FIU receives all the raw financial transaction data from all financial institutions in the country. This is done after the transactions are

anonymized and the original identity information is kept at the reporting institution. What is sent to the FIU is a proxy-identifier (say an ID number that has been modified). Still, it gives the opportunity to the FIU to store the data in a single database, known as the *Archivio Unico Informatico* and connect with the same identifiers transactions from individuals throughout the country and in different institutions.

Needless to say, an advanced information exchange structure that would support the international effort against money laundering does not exist in this sense. IS that are currently available for the exchange of information between different countries are in use (e.g., through the Egmont Group, Interpol, etc.), but these involve cases on specific suspects. By doing so, they lack in one major aspect: *they do not allow the collective information that is spread out in different countries to be used for the emergence of suspicion itself*. This is where the serious cases of criminality can be found and where organized crime distributes its own information-footprint to avoid detection. In the closing section of this chapter we will see how such a framework can be considered for the exchange of information at an international level for tackling criminality. This constitutes a theoretical contribution that applies to different types of criminal activity, and even though privacy considerations are not examined in detail they are taken into account by introducing layers of civil rights protection mechanisms.

While the use of technology in centralized environments inhibits security risks, it also needs to be pointed out that the transition from more data to both more and useful information is not straightforward. Complexity always finds a way around any system, and as a property of any system, complexity is a transcendental property. It may change form and shape or even philosophical underpinnings, but hardly ever loses its characteristics as complexity. In this manner and when considering technology as an assistant in the tackling of criminality at the international level, we need to recognize that a series of transitions occur. For instance, when there is an effort to monitor money laundering behaviour logical complexity transforms into mathematical complexity, then into algorithmic complexity, followed by profiling complexity and even into visual complexity while data visualization is employed to examine large datasets. From a systems theoretical approach no system can escape the intrinsic complexity of the elements that constitute it.[39]

[39] N. Luhmann, 'Deconstruction as Second-Order Observing', in W. Rasch (ed.), *Theories of Distinction: Redescribing the Descriptions of Modernity* (Stanford, CA: Stanford University Press, 2002) at 94–112.

The aforementioned remarks point towards an important distinction that remains central to the role of technology in all efforts against international and transnational crime. Technology is often viewed outside of its organizational implications and the consequences that are created when an automated function (like that of technology) re-arranges the already-present bureaucracy of organizations. This is only part of the problem. Technology is also viewed as a solution that – when imposed onto the problem domain – will somehow ameliorate the difficulties of spotting criminal behaviour. Such a belief is flawed because it does not consider the contextual use of technology. The integration of technology within an organizational setting has implications that stretch beyond the best of intentions/expectations of computer programmers.

When it comes to any type of technology being embedded within an organizational setting these contingencies give rise to an emergent information system. This interacts with the pre-established basis of other IS and at the same time it constructs part of the organizational reality through which modern institutions attempt to combat criminal activity.

A theoretical framework for the use of IS in tackling criminality

In the development of the theoretical framework that follows there are a number of dimensions that need to be considered before the role of IS can be more specifically laid down. These are presented as distinct dimensions below and reflections on their synthesis are provided at the end of this chapter following the presentation of Figure 7.3. Money laundering is occasionally being used here as an example, without this jeopardizing the generality of the framework.

The goal for outlining this framework is to develop an overview of considerations regarding technology-supported information exchanges for tackling criminality. A number of distinctions and categories are used in order to highlight the different monitoring possibilities. These start with data-specific processes and move onto semantic issues, classifications, as well as possibilities for the exchange of information. Reflections are provided in each dimension in relation to the context in which they are being discussed.

Dimension 1*: types of data*

The type of data being monitored is possibly one of the most interesting starting viewpoints for the purposes of profiling. Generally, five data types can be distinguished: text, number, audio, image and video. Video can be

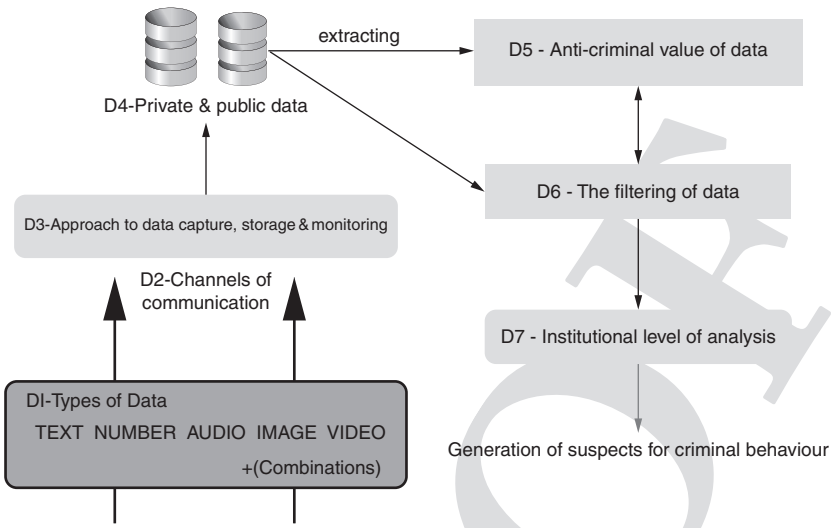


Figure 7.3: A framework for the technological construction of criminality and the generation of suspicion

considered in tandem with the image data-type as it constitutes a consecutive time-sequence of images. In the dimension that we can call 'types of data' there are also possibilities for combinations. For instance, data can include both text and audio. Different combinations yield a different information value, while data manipulation, recognition and analysis become harder as the data represent more media-rich objects (like video).

Dimension 2*: channels of communication*

Supported by cable, satellite or terrestrial technologies, data are communicated between individuals, or between individuals and institutions in all different data types. Basic channels of communication, such as radio, the telephone or the Internet are routinely used to allow for the types of data to be exchanged between users. Depending on the technology used and the medium of exchange (e.g., use of the Internet for exchanging emails) data are stored in different ways or may not be stored at all.

Dimension 3*: approach to data capture, storage and monitoring*

Unless actively monitored for crime prevention purposes, there are data types in certain communication channels that may not be captured or stored at all (e.g., telephone calls). In this scenario their information value

is lost immediately. But the transition from analogue to digital, as well as the economies of scale that have made data storage cheap, now means that data are increasingly being captured and stored for longer periods of time. The actual depth and storage of data are difficult to dissect, but recent revelations in the USA about the activities of the National Security Agency point to very ambitious programs whose aim is to collect data indiscriminately. If we exclude the intelligence community that focuses on national security rather than the full spectrum of criminal activity, then data are captured by two distinct approaches that influence the dynamics of profiling in relation to the approach for data monitoring. The first one is a 'collect all' approach that can be considered as more invasive from a privacy perspective. In this case the strategy for the monitoring of data is decided *a posteriori* from its collection. Both public and private data may be collected. The second approach to data collection and monitoring is a 'pre-filter' approach. What data are actually collected is decided on the basis of what is explicitly required in order for particular monitoring processes to be accomplished. For example, if terrorist activity is being monitored on a particular telecommunication channel (e.g., telephone) then keywords that may raise suspicion (e.g., bomb) can isolate certain communications for further analysis. Finally, there are hybrid approaches between the two, of which a good example is Echelon (the international electronic eavesdropping network run by the intelligence communities of the USA, UK, Canada, Australia and New Zealand). While it is not considered to be a real-time tapping network, it captures traffic and then filters it for specific keywords that are semantically considered to be associated with suspicious behaviour. Interceptions are considered to take place through terrestrial radio antennae that intercept satellite transmissions.

Dimension 4: *private or public data*

Data that can be used during a profiling process may include both private and public data. Private data reside in databases that have restricted access to a select number of users. For instance, the raw transaction data stored in the databases of financial institutions are proprietary. Only personnel that are designated to have access to bank transaction data can gain access (excluding security breaches, of course), as well as authorities that demand access in the course of specific investigations. Aggregate collection of such private data by authorities is considered to be more invasive but there are ways to alleviate some concerns.

Anonymization and PETs can be used at that level so that individual identity data become stripped off the data that will be manipulated.[40]

In addition, there exist public data that can be (and usually are) used in profiling. Public data are considered to be available in a format that is accessible to all and is most recently propelled by the use of the Internet and a number of social media in which people participate. But what is surprising about this is that people will willingly share a great deal of information about themselves in order to participate in an online platform. If we take Facebook as an example, then users usually upload information about their hobbies, age, current location, activities, marital status, personal interests and preferences (what they like), what they read, what they share and who they are connected to. While all of this information may not necessarily be in the public domain automatically (depending on the privacy settings of the user) it does demonstrate how users react to having their personal information online.

The value of that public social networking information for countering criminality is notable. In a number of cases, the police have already used such data for monitoring individuals during ongoing investigations. In this way, social networking information has 'anti-criminal value'.[41]

Dimension 5*: the anti-criminal value of data*

Regardless of whether data are stored on known criminals, simple suspects, or non-criminals, data are known to possess an anti-criminal value or dimension. As discussed in relation to Europol IS, there are different ways in which technology can be used. In the case of known criminals, their personal data are stored and shared so that they can be arrested. In the case of suspects, data are shared, corroborated and

[40] See V. Senicar, B. Jerman-Blazic and T. Klobucar, 'Privacy-Enhancing Technologies – Approaches and Development', (2003) 25 *Computer Standards & Interfaces* 147. Privacy mechanisms like PETs include: encryption and steganography (hiding signals inside other signals), blind digital signature, trust centres (TTPs, certification services, etc.), identity protectors (these generate pseudo-identities as needed, convert pseudo-identities into actual identities desired, and combat fraud and misuse of the system), cookie management software, anonymizers, re-mailers, a system called Crowds, Crypto-Heaven, etc. Projects researching and developing PETs are P3P (by W3C), Privacy Incorporated Software Agent (PISA), Roadmap for Advanced Research in Privacy and Identity Management (RAPID), and the EU GUIDES project.

[41] K. Knibbs, 'In the Online Hunt for Criminals, Social Media Is the Ultimate Snitch', (2013) available at www.digitaltrends.com/social-media/the-new-inside-source-for-police-forces-social-networks/.

additional data objects are required to establish criminal acts. But as already discussed in the previous sections there is also an anti-criminal value in the data traces of non-criminals, if only to establish a distinction between criminal/non-criminal for statistical/demographic/socio-economic purposes. It is on the basis of such distinctions that criminal behaviour is supposedly understood: as an anomaly within an otherwise predictable system of norms. Then it is believed that there is some sort of structure in the anomaly itself, a series of behavioural patterns that can be absorbed into algorithmic queries, and that in this process non-criminal data can establish a firmer ground upon which the antithesis can be considered.

Dimension 6*: the filtering of data*

The filtering of data takes place through a 'filter' that constitutes a series of queries that attempt to encapsulate suspicious behaviour. The purpose of the filter is to raise an alarm for specific transactions in respect of a particular crime. The filter contains the algorithmic expressions that attempt to capture suspicious behaviour for different criminal activity (e.g., money laundering, terrorist financing, fraud, identity theft, etc.) and, as it is applied to the data, it also reduces the original population of the data to a supposedly manageable subset. For example, in the context of AML, a financial institution can apply a filter to raw transaction data; the filter describes in algorithmic terms how the potential money launderer would transact and would deliver suspects for further manual analysis. Alternatively, if the analysis were to take place at a national authority (an FIU) that aggregates transactions from all financial institutions, other profiles can be used. The function of the filter is to model (in algorithmic queries) the basic characteristics that can trace a criminal phenomenon by exploring the data. Hence, different filters are required to model different phenomena: money laundering, terrorist financing, imminent terrorist attacks, etc., by exploring both public and private data, different channels of communication, types of data, storage and semantic tagging techniques, etc. Enhancing these profiles for capturing criminal behaviour in more accurate terms is the most critical challenge that institutions face. Of course, this is inhibited by the complexity of the phenomena being studied and their underground activity, as well as the volume of data that is at the heart of the problem (but also the scope for opportunity).

Dimension 7: *the institutional level of analysis*

There are three institutional levels of analysis where technology can participate in order to extract anti-criminal value from data: the local level where institutions have proprietary databases (e.g., banks), the national level (e.g., FIUs) where institutions can demand access (or data) from the local level, and the international level where national institutions typically collaborate by exchanging data on specific cases and advancing shared intelligence (as in the cases of Europol and Interpol). However, the profiling element at the international level is considerably more restricted due to data restrictions and privacy concerns. While this is both understandable and desirable there are ways to include both anonymization and PETs in order to elevate profiling practices towards an international scope. These would target criminal activity that has a truly international dimension and where the silos of nation states restrict a timely response to targeting criminality.

Dimension 8: *time*

While not included in Figure 7.3, time plays a central role throughout any modelling problem. Even though time can be considered as one of the most elusive dimensions, in the context of using technology for combating criminal activities there are some important time-classifications that are relevant. Three different time-horizons can be distinguished: real-time profiling, near-real-time, and batch processing of data. Real-time monitoring is critical in the cases of known criminals that still escape arrest or are monitored for other purposes. For example, the process of embedding terrorist suspects in lists such as the one published by the US Treasury's Office of Foreign Assets Control requires an immediate response if said individuals attempt to carry out any transactions. Financial institutions are required to block their transactions immediately. In respect of decisions that can be delayed enough for human intervention one can move into the category of near-real-time monitoring. Finally, the time horizon can be explored in a more relaxed manner in the context of batch processing. In this scenario, data is examined for its anti-criminal information value in certain timeframes where profiles and filters are applied to the data. For instance, in AML transaction-monitoring software this timeframe is typically a three-month window. As some criminal activity like money laundering is spread out over time in particular typologies (e.g., smurfing – or breaking

up large amounts of money to be laundered into smaller sums and depositing them just under the reporting thresholds) the time horizon for engaging in profiling is critical. Obviously, the bigger the timeframe to be used the greater the challenge in data manipulation.

Conclusions

Technology occupies an important role in the fight against transnational criminality and there is little doubt that it will continue in an enabling role in communicating data and applying profiling practices. A number of IS influences have been discussed in the context of this chapter and it is important to stress that more theoretical work is necessary in order to delineate part of the complex nexus of effects that technology imposes in the fight against criminal activity. The continuous challenges that are faced in the fight against transnational criminality will require novel considerations and governmental action to apply PETs for curbing the invasive character of data manipulation that proposes a 'collect all' approach.

Similarly, researchers that find themselves at the boundary between technology and the law will need to investigate further the legal implications arising from those technological implementations whose bottom-up approach counteracts existing law. This involves the realization that technology does not always function as a subordinate tool with strictly defined conditions but assumes a systemic role. By doing so it maintains categorical assumptions and distinctions between criminal/non-criminal relations and these are propelled by automation to acquire a more synthetic role. The *technological construction of criminality* (or of criminal reality) as laid down in this chapter denotes precisely this conditioning.

Of course, the challenges that remain in the international dimension of tackling criminality are manifold and will continue to evolve. In this regard, it is important to emphasize again that the technological role of data sharing and collaborative work remains central and needs to be enhanced. But at the same time the emergence of suspicion by profiling through international collaborations constitutes an important step to be explored. The several dimensions discussed above, each entailing a number of other elements, illustrate that the role of technology is critical. While technology allows for the distributed communication of data, the processes that participate in extracting anti-criminal value from said data are more subtle; and it is in this context that fascinating new developments may occur and must be pursued.