

Unified Criminalistic Information System for Investigation of Crimes and Violations of Law

Egle Kazemikaitiene, Rimantas Petrauskas

Lithuania Law University
Ateities 20, LT-2057, Vilnius, Lithuania
e-mail: egle@ltu.lt, rpetraus@ltu.lt

Abstract. The main objective in storing criminalistic records has always been to assist the smooth running of the criminal justice system. In other words the main objective of criminalistic databases and collections is provide with information the investigation of crimes and other violations of law. The research considers the use of criminalistic databases and other records within criminal justice system and analyses the Lithuanian criminalistic databases and other criminalistic records. The Lithuanian criminalistic databases are separate and uncoordinated. The research insists that a new unified national criminalistic information system should be created and held in computerised form on the police national information centre. The national unified criminalistic information system can ensure that investigators will be provided of reliable information as soon as possible. This new integrated system would combine all separate criminalistic databases, collections and records. The unified software and systematise electronic connection, progressive information recognition and research systems have to be used. The unified national criminalistic information system will be created by these factors: the entire information system should be held on a single computerised system with unified software and systematise electronic connection; the new classification criterions of facts; the new system should permit searching on characteristics other than name in order to exploit the investigative potential of the records; the main objective is investigation of crimes and others violations of law.

Key words: criminal justice system, criminalistic databases, criminalistic records and collections, investigation of crimes, unified criminalistic information system, crime analysis, forensic intelligence.

1.Introduction

Traditionally, each scene of crime is seen as an independent 'complete' set of data from which the intelligent investigator can find the signature of the offender. Links between cases are often inferred through police investigation; in a separate process, cases are also compared through the use of physical evidence collected at the scene of crime. The question of how to integrate the different pieces of data available into a coherent framework for intelligence purposes has become an important topic of

research. Increased mobility and new communication channels give criminals the capacity to better plan and organise their activities over large geographical areas. Patterns reflecting fraudulent activities are therefore always more difficult to reveal from the huge quantity of data scattered in files across independent police and legal structures.

A key part of law enforcement is to understand those activities, through the development and use of methods, models and tools for collecting and then interpreting the large volume of data available in real time. Consequently, intelligence programs have been developed, leading to the recognition of a field of activity called crime analysis, which has been described as 'the identification of and the provision of insight into the relationship between crime data and other potentially relevant data with a view to police and judicial practice'[6].

From an intelligence perspective, forensic science plays an important role in crime analysis, in that forensic science covers a broad range of methods and techniques aimed at revealing relationships between people, scenes of crimes and objects, as well as helping to develop working hypotheses. The great potential of physical evidence for linking crimes and bringing together other solid informative data has been shown, specifically through the use of multiple databases. Such developments have also greatly influenced crime scene management, because collection and treatment of data are highly interlinked.

The Lithuanian criminal justice system is a disparate entity consisting of different personnel and practitioners playing different roles and representing different individual and organisational interests. The main actors include the police, judiciary, lawyers, social workers and probation officers who collectively "process" a person from suspect through to arrestee, defendant and finally an acquittal or conviction and sentenced person, the case – from beginning to ending of investigation. The main objective in criminalistic databases and other records existence has always been to assist the investigators, to provide with trustworthy information the investigation of crimes and other violations of law rapidly.

The use of methods of collecting and exploiting large quantities of data for intelligence purposes is not new. At the beginning of the twentieth century, a number of authors described ways of recording data in filing systems; fingerprints are a well-known example, as is Bertillon's anthropometry. The proliferation of methods, as well as the development of a broad variety of incompatible classification systems, brought a response from Locard in 1906; he was already arguing for the creation of a uniform international method of recording data that could help identify people independently of borders [2].

During that same period, Reiss, in 1914, attending the congress of Monaco, and Locard not only recommended the harmonisation of methods but also emphasised the advantages of using the different types of data available [2]. These important works, pertaining to recording methods, have been reviewed, adapted and their efficiency increased through the use of computer technology. Simultaneously, the evolution of organised criminality highlighted the need to improve police information systems. Intelligence processes have been defined and crime analysis was recognised as a main component.

The research present the shot analyse of existing criminalistic information systems, discuss what problems occurred and compare these systems with Lithuanian

criminalistic information system, describe the future of criminalistic information system.

2.Crime Analysis

Developments in the field of information technology provide the police with a vast quantity of data, from different sources, reflecting criminal events and their relationships. Relevant patterns are not easy to extract from this huge quantity of noisy data. Moreover, the available data are often incomplete and uncertain; for instance, all criminal events are not reported to the police; the date and time of a particular event are generally not precisely known; and traces collected are often fragmentary. Dealing with imperfect data reflecting complex-evolving phenomena is very common to criminal investigation and crime analysis. Legal and organisational barriers, the proliferation of methods for collecting and interpreting data, and the consequent variety of incompatible recording systems make comparisons difficult, when performed. Poor analysis of similar offences crossing different police areas is recognised as one of the major weaknesses pertaining to police information systems.

Finally, the analysis of data is generally distributed between people with different knowledge, experience and culture. For instance, cooperation between the laboratory scientist, the crime investigator and the crime analyst is of increasing importance to provide the best use not solely of new techniques but also of scientific attitudes during the whole investigation.

As a consequence police have adapted information systems:

- new structures have been created to favour exchange of information across countries.
- new intelligence structures within the organisations have been created, with an important part dedicated to crime analysis.
- structured and normalised methods of analysing data have been developed.
- a broad variety of computerised tools have been introduced (geographic information systems, drawing programs, statistical packages, broad variety of databases, etc.).

Roughly, crime analysis aims at [1]:

- deciphering the knowledge used by experienced investigators to identify and formalise concepts and notions, and the methods used by them to marshal their information;
- conceiving new methods of treating data, and adapting existing ones, given that computer tools can improve the analysis process in a way that was not previously possible, and that criminality itself is evolving over time, and that weaknesses observed in the course of an analysis can necessitate upgrades;
- normalising language and symbols used in the course of the analysis in order to facilitate teamwork on complex problems, and to disseminate the results of the analysis in a way that is easy to interpret;
- using those methods to produce conclusions/ hypotheses that can help towards concrete actions.

A broad variety of analysis forms have been defined; for instance, crime pattern analysis, profile analysis, case analysis (course of events immediately before, during and after a serious offence), comparative case analysis, etc. Forensic science data are exploited in the most of these different forms of analysis.

3 Databases in Forensic Intelligence

Forensic intelligence is a process that starts from the collection of data, often at the scene of crime [5]. The exploitation of data relies entirely upon the quality and quantity of the collected data. It could therefore be said that inferences drawn, and action taken at the scene, are fundamental to forensic intelligence, as they will entirely determine what data will be collected and then exploited.

Computer systems in forensic intelligence can be classified into two groups. Locard, in 1920, noticed that investigative methods are essentially based on analogy [3]. Consequently, it is not surprising that most existing computer systems recognised as forensic intelligence systems can be viewed as an aid to performing this type of reasoning process. The second class of system pertains to collections that help classify evidence by the type of object that could have transferred a trace.

Similarities found between accessible information can lead to inferences on the profile of offenders, their mode of action and the means they have used. The identification of recidivists is the better-known form of this basic scheme. From a new situation or a new case, the purpose is to identify known offenders from their antecedents. The search for links between cases is another elementary activity that falls within the same framework; it allows groupings that delineate criminal events. Finally, when objects are found or perpetrators identified, all the cases in which there participation or presence can be supposed should be extracted. This process is traditionally incomplete because links may not systematically be searched *before* the offender has been arrested. It could be that identifying an offender for a crime is sufficient to put him or her behind bars, without being charged with other offences that could be difficult to prove. This is something that real-time crime analysis avoids. These steps have been partially reproduced in computer applications; the best-known illustrations are AFIS (automatic fingerprint identification systems) and DNA databases [4]. Thus, if a finger mark, even fragmentary, found at the scene of a crime is compared with the content of a database, a restricted number of similar fingerprints will be given to the experts who interpret them. Potentially, all the other marks transferred, or the information left by the offender (from clothing or accessories), could be analysed in a similar way.

The forensic intelligence process starts with the collection of data and ends with the integration of results into the analysis of crimes under investigation. If we assume that at least one database has been developed in this process, important intermediate steps may be described as follows (Fig. 1) [8]:

- the acquisition of new data in order to transform it into a digital or symbolic form suitable for searching for similar items in the database, and to memorise it in a way that will allow retrieval when needed;
- the search and matching process;

- the interpretation/verification of the returned result.

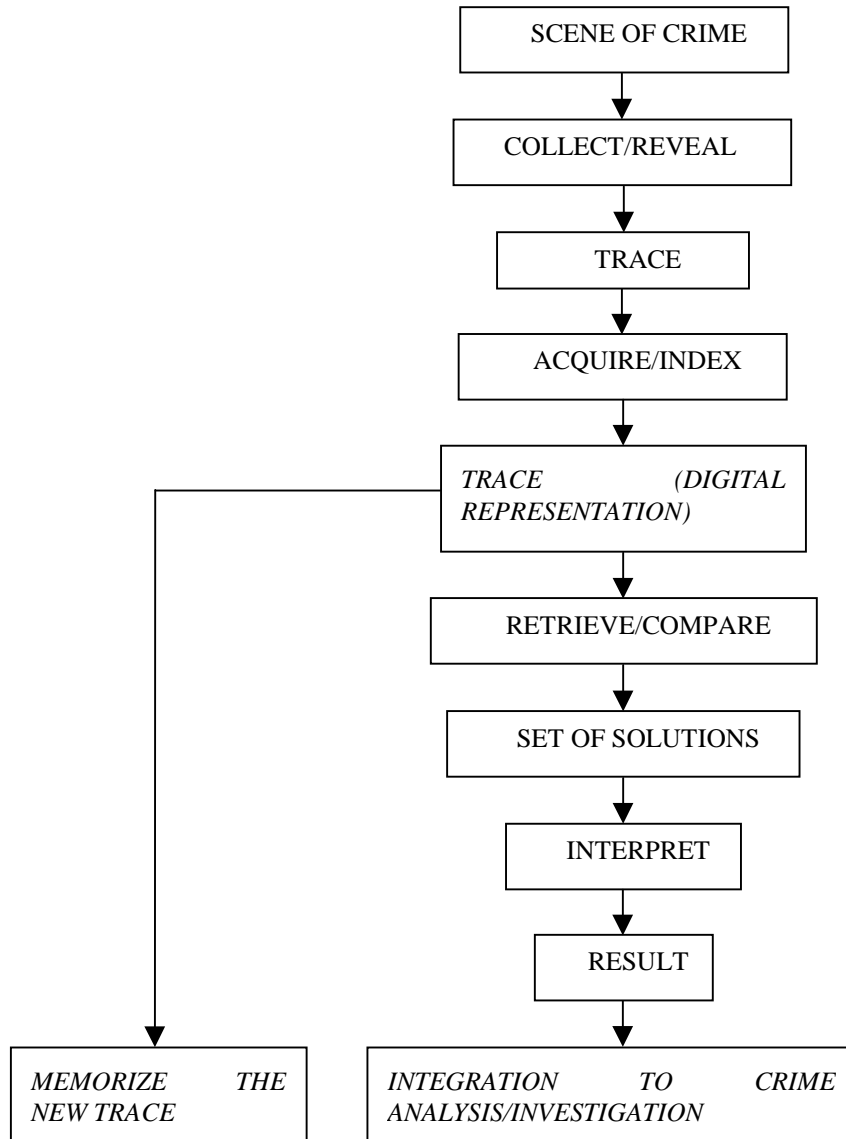


Figure 1. Forensic intelligence process, from the collection of data to the dissemination of results.

The people participating in this process for each database may range from the scene of crime officer to the expert responsible for the interpretation step. To ensure

that the process is reliable, and to diminish time and resources needed, three general rules may be applied [9]:

- check existing data, their coherence and their 'usefulness';
- write computer programs that implement part of the process, where possible;
- where it is not possible, define methods and control their application.

The specific difficulties pertaining to the nature of data have led to the separation of the implementation of the process for each type of information. Biological traces, finger marks, shoe marks, bullets, cartridges and tool marks are generally independently treated in separate databases. What follows is not an exhaustive inventory of existing systems and the way they function; it is only aimed at suggesting a framework for evaluating difficulties related to the computerisation of systems pertaining to specific types of trace.

3.1 The acquisition problem

The acquisition problem is the problem of transforming data (trace) into digital or symbolic form suitable for comparison with the content of the database, and then memorising it. This operation can be long and complex, and sometimes not fully controllable by machine. For instance, from a DNA point of view, it includes the application of the analytical techniques used to identify markers of a sample, together with encoding into the system the obtained values in the form of numbers.

Most information is gathered through a device that is interfaced with a computer, like a scanner or various types of camera. The image obtained is then treated to extract relevant features for encoding. This operation is computerised to different degrees, depending on the trace and its quality. Full automatic processing of good quality 10-print cards is sometimes possible, but computer workstations are generally designed with image enhancement processes, and interactive graphics editors mark minutiae and other features. Poor quality traces regularly require this manual operation.

Databases recording shoe marks provide an example that could be situated, in our framework, between DNA and fingerprints. Encoding by hand is difficult owing to the variety of, and changes in, sole patterns. Such systems give good results, but difficulties are encountered in maintaining the quality of data when there is more than one operator. Automatically extracting patterns from a fragmentary shoe mark, or when the mark is concealed under irrelevant data, is now a research topic but is computationally very complex, if not intractable for poor marks. The best practical solution is to capture the image through a device and to provide a graphic icon editor that helps a human operator to encode the mark.

3.2 Retrieval and matching

Collection of data at the scene of crime is always incomplete and imprecise, and collected marks are often fragmentary, even if the investigation is careful and thorough. An object that caused a trace can evolve, and marks or prints can be distorted. The match between recorded data and collected evidence (in its digital

form) is therefore generally only partial. A human operator must always interpret a limited set of possible solutions at the end of the chain.

A broad range of retrieval and matching algorithms using various techniques (statistical, neural net-worked-based or coming from artificial intelligence) are actually implemented to compare the data automatically. They must be designed so that the result of a search is a limited ranked list of possible matches; this avoids painful and time-consuming fruitless comparisons at the end of the process. Those algorithms are generally rarely published owing to economic interests, because they can be viewed as the heart of such databases.

From a practical point of view, DNA and fingerprints provide extreme examples; the problem of matching two DNA markers is very simple from a computing perspective, as the match is generally determined by an 'exact' comparison. (It is not claimed that the implementation of the whole process, from the collection of data to its storage in the system, is easy, but the 'retrieval and matching problems' themselves are not difficult.) A retrieval algorithm can be implemented directly with simple computer development tools. Common databases found on the marketplace are sufficient for this purpose. Comparing fingerprints is a far more complex task owing to the quantity of information to be treated and the imperfect nature of this type of collected data.

There are other fields where such matching processes are efficient, like shoe marks, bullets and cartridges; but yet other fields demonstrate difficulties in overcoming the imperfection and complexity behind the type of treated information. Tool marks, handwriting and voice recognition are three examples.

One other elementary criminal investigation question where forensic science plays a fundamental role is the determination of the type of object from a trace or evidence collected at the crime scene. For example, in hit-and-run car accidents, it is important to know quickly the make and model of a vehicle. This is possible with paint flakes found at scenes and the maintenance of a systematic database that helps determine correspondence. Knowledge of the type of printer that has been used to produce a document or a counterfeit banknote can constitute an essential element of investigation. Databases of toners can help in this determination. The difficulties encountered when using this type of scheme not only pertain to the nature of the data treated; market evolution, fashion, etc. render permanent upgrading essential to ensure that memorised classes are adequate and correspond to reality. This requires considerable effort because the field of interest can change rapidly: firearms, types of vehicle, printers, photocopying machines, types of shoe, types of fibres and cosmetics rapidly appear and disappear. Such efforts are generally distributed in collaboration between different forensic laboratories.

Faced with the increasing internationalisation of crime, national governments and their police have devoted much effort to developing co-operative counter-measures, and further evolution is under way through the machinery of conventions and arrangements. The international policy space for these departures is now additionally crowded by recent talk of more embracing systems of European policing, such as Europol, and also by both sectoral and bilateral arrangements. A central part in these initiatives is played by the attempt to develop adequate information system across national and jurisdictional borders. This extends, what we can call the "informatisation" of the police, to the inter-governmental level in all European

countries. Much of the development of “informatised” police work is nationally and internationally slow and piecemeal at the moment, but there are signs that the pace is quickening under various pressures from international agreements. The importance of rapidly communicated, secure, accessible and ample information to the goals of policing across borders is likely to stimulate further the harmonization or integration of information systems, and perhaps their eventual supranational centralization. The unified criminalistic information system has been created in such way that can be connections with international police information systems.

3.3 Training

The central information bureau has to provide training and other consultative services to criminal/justice public safety community on all criminalistic information system program areas. Areas of training include [6]: usage and controls of the system network, information reporting responsibilities of agencies set forth in state law, training in security controls for access to the system network or data derived therefore, reporting and use of crime statistics, and a host of other areas. The information centre professional staffs has to be responsible by law for the design, printing and state-wide distribution of a number of different blank forms used by law enforcement and other criminal justice agencies. Having the same blank forms available for use by all agencies has facilitated the development of standardised peace officer training programs statewide and the creation of a standardised records management system adopted for utilisation in both automated and non-automated criminal justice agencies and in state, county, and municipal law enforcement agencies.

4. Development of criminalistic information system in Lithuania

The principal mission of the Lithuanian criminalistic information system has been to assist all officials and agencies of the criminal justice system in the fulfillment of their varied responsibilities on a state-wide basis by providing round-the-clock access to needed information. Lithuanian criminalistic information system consists of separate databases, which are ruled of different departments. The main centered databases are “Population of Republic of Lithuania” (information about citizens – all data of identification card or passport), “Transport” (information about vehicles registration), “Firearms” (information about registered firearms and owners), “Wanted persons” (information about wanted criminals and missing persons), “Stolen vehicles” (information about stolen vehicles), “Stolen firearms” (information about stolen firearms), “Crimes and criminals” (information about committed crimes), “Police preventive record” (information about persons who is susceptible to violate), “Numbered objects” (information about registered numbered objects), “Administrative violations of law”, automated fingerprint identification system (AFIS) “PIRAT 2”, others criminalistic collections of traces, which were put from crime scene. Databases function in computers with UNIX operating system. The information loading, recognition, proofreading and searching programs accomplished

ORACLE SQL*Forms program measures, switched in user menu SQL*Menu. The loading of information could be fulfilled by regime SQL*Loader.

The Lithuanian criminalistic information system network operated by teleprocessing specialists provides direct terminal access to computerized databases maintained by Lithuania agencies. The Lithuanian criminalistic information system is the first state criminal records repository to have an automated fingerprint identification system (AFIS), which creates or updates criminal history records as a by-product of the fingerprint identification process. The current system supports electronic fingerprint submissions from the local agency and to the federal bureau. There are 6 senior agencies transmitting arrest fingerprint cards to central bureau. With the service these 6 agencies provide to other local agencies.

Conclusions

The all-existing separate criminalistic databases of Lithuania could be joined in unified national criminalistic information system, which have been ruled by the police department. The unified national criminalistic information system should be created and held in computerized form on the police national information centre. The unified national criminalistic information system has been created based on crime characteristic (corpus delicti), which include the object of attempt (victim), the crime subject (criminal), the crime situation and way of crime commitment. Investigator from beginning to the end will oversee every crime. The criminalistic information system has to provide the information about similar crimes, which were committed before, have to connect the new crime with already committed. The criminalistic database by crime characteristic parts:

1. information about the object of attempt (victim);
2. information about the crime subject (criminal);
3. information about the way of crime commitment;
4. information about the crime situation: crime motive, crime purpose, the type of situation (provocative, conflict, accidental)

The existing criminalistic databases and collections will be subordinated to this system. The future of the criminalistic information system is in computerization and more efficient storage. Data protection measures will be in constant tension with the accumulation and uses of police held information. System staff also has to take the lead in improvement of Lithuania criminal justice records. This effort includes creation of interfaces with local and state criminal justice systems and automated submission of data on arrests and dispositions to the center. Automation linkages are being installed that will allow for real-time inquiry of relevant identification and criminal history data from other states. The center's AFIS database also supports remote searching of fingerprints left by unknown suspects at the scene of crimes. The computer programmers and analysts will use their computers and databases to provide computerized investigative support to state and local law enforcement agencies. In a series of complex criminal investigations, the leads provided by criminalistic

information system center analysts have proven to be the keys to investigative and prosecutorial success.

Much work should be dedicated in the near future to the analysis of inferences used in solving the different problems of crime analysis, including forensic science data. There may be potential for computerisation artificial intelligence techniques (data mining techniques). Forensic scientists play an even more important role in the resolution of these problems, given that they can deal with the specific nature of the collected forensic science data. They provide the scientific attitude needed to approach such problems, with an extension of the role of forensic science, as well as a great potential for crime analysis.

References

1. Heberton Bill, Terry Thomas. Criminal records. Brookfield USA, 1993.
2. Crime Analysis Working Group (1997) *Crime Analysis Booklet*, 2nd edn. Lyon: Interpol.
3. Harrogate: Forensic Science Service. Locard E (1920) *L'Enquete Criminelle et les Me'thodes Scientifiques*. Paris: Flammarion
4. Henry C.Lee & Gaensslen R.E. *Advances in Fingerprint Technology*. New York: Elsevier, 1991.
5. Saferstein Richard. *Criminalistics: An Introduction to Forensic Science*. Fourth edition. USA: Prentice Hall Career & Technology Englewood Cliffs, New Jersey 07632, 1990.
6. Weston Paul B. and Wells Kenneth M. *Criminal Investigation: Basic Perspectives*, 2nd Ed. Englewood Cliffs, NJ: Prentice Hall, 1990.
7. 4. Kurapka E., Malevski H., Palskys E., Kuklianskis S. *Kriminalistikos technikos pagrindai*. V.: Eugrimas, 1998.
8. Колдин В.Я., Полевой. Н. С. *Информационные процессы и структуры в криминалистике*. МГУ: М., 1985.
9. *Криминалистика/ под ред. Белкина Р.С. М.: НОРМА-ИНФРА- М., 1999.*