

CSABA FENYVESI

Crime prevention function of criminalistics

The concept of criminalistics

If we review the work of the theoretical authors of the recent, approximately 120-170-year-old discipline, the set of criteria accepted and formulated also by me, making up the basis of the concept of criminology, has now its crystallized form. Namely, that in terms of its essence, criminology is mainly practical kind of – and to a lesser extent – theoretical criminal investigation, i.e. the branch of criminal sciences that explores, creates, organizes and applies the means and methods of detecting (preventing) and proving crimes within a normative legal framework. In addition to effective crime prevention appearing as a secondary function, its basic function is detection, as well as obtaining as much and as credible evidence as possible, establishing and ensuring criminal prosecution – ultimately by the court. In short, criminology is the science of effective and professional law enforcement,¹ which has no subfield that does not serve the fight against crime, i.e. exposing and bringing criminals to justice, either on the European continent being its birthplace, or beyond.

I would like emphasize that the methodology, collection of recommendations, and tools of forensics do not only help in establishing criminal facts, however, they can also be used by practitioners of other fields, such as of administrative law, criminal law, labour law (including disciplinary law), and civil law. There is a reason that János Zlinszky refers to the fact that the word “crimen” originally means “distinction” in Latin, that is, it is not the exclusive use of the criminal field, it can be applied to all kinds of situations.²

The place and role of the crime prevention function

At the same time, it is clear from the definition that its only secondary function is crime prevention, its primary and main

focus is detection, reactivity instead of proactivity. This can be observed in American PERCEPTIONS as well, for example, according to one of the most famous criminologists, Paul Kirk, forensics is nothing more than the science of individual identification: “Science of individualized identification”.³ In the case of continental thinkers, the presence of prevention is even more noticeable. Quoting the German Friedrich Geerds, “criminology is a factual or empirical science, by which we

mean the theory of direct, repressive and preventive law enforcement activities carried out in practice by law enforcement agencies and their assistants.”⁴ The Russian Rafail Samuilovich Belkin believes: “criminology is a science that deals with the legalities of criminal mechanisms, the places of occurrence of information about crimes and their perpetrators, the laws of collecting, collating, examining and using evidence, which, derived from these laws, is used to prevent crimes, it is based on knowledge of the tools and methods for its investigation and detection.”⁵ In the words of László Viski, who is deeply involved in the theory of forensics: “the theory of criminal investigation deals with the development of those methods and tools that facilitate the detection, prevention, interruption of crimes and the enforcement of criminal claims within the framework of substantive law”.⁶

There is also a continental, including a French one, view that characterizes forensics as “d’art de la deduction”, i.e. the art of deduction.⁷ In my opinion, we cannot really talk about art, however, I think the reference to deduction is appropriate, since cause-and-effect thinking occupies a central place in forensics. The harmful, criminal result (the crime) appears in front of the “trace reader” and he/she is rightfully curious about the cause-and-effect relationships. One has to go backwards, namely through the effect to the cause, that is, one has to use deduction to explore and learn about the past. This also

³ KIRK, P.: Crime Investigation. Interscience Publications, New York–London–Sydney, 1953; Also: CHAMPOD, C.: Overview and Meaning of ID. In: Siegel, J. A. – Saukko, P. J. – Knupfer, G. C. (eds.): *Encyclopedia of Forensic Sciences 1–2–3*, Academic Press, San Diego–San Francisco–New York–Boston–London–Sydney–Tokyo, 2000. Volume 3, 1077.

⁴ GEERDS, F.: A kriminalisztika helye a tudományok rendszerében. (Role of criminalistics in scientific system) In: Géza Katona (ed.): *A kriminalisztika aktuális kérdései. (Actual questions of criminalistics)* BM Kiadó, Budapest, 2001. 5.

⁵ BELKIN, R. S. cited in FILIPPOV, A. G.: The Russian Criminalistics – a Science and a Discipline. In: Csaba FENYVESI – Csongor HERKE – Bence MÉSZÁROS (eds.): *Bizonyítékok. (Evidence)* PTE ÁJK, Pécs, 2006. 154.

⁶ László Viski (ed.): *Kriminalisztika. (Criminalistics)* BM, Budapest, 1961. 13.

⁷ Loïc Chauveau: Les traces du crime. Survey sur la police scientifique – Calmann-Lévy, 1993. 24. In the past, some people classified forensics itself as an art. Their opinion is contradicted by the scientific (“scientific” or “forensic”) content in the name of the other form and in the title of one of their volumes. In our strongly science-oriented days, we no longer encounter this concept on a monographic level. See earlier Beveridge, W. I. B.: *The Art of Scientific Investigation*. Random House, New York, 1957; Fisher, J.: *The Art of Detection*. Carlton Press, New York, 1963.

¹ Zoltán HAUTZINGER: Gondolatok a kriminalisztika elméleti rendszeréről. (Thoughts of criminalistics’ theoretical system) *JURA*, 2019/1. 84–93.

² János ZLINSZKY: *Római büntetőjog. (Roman criminal law)* Textbook publisher, Budapest, 1990. 11.

shows that law enforcement activities are necessarily (and essentially) retrospective.

The good news regarding the prevention function of forensics is, in my opinion, that a certain kind of shift can be perceived in the world's forensics since the 2000s. Namely, in the direction of proactive measures, as opposed to a reactive, retrospective approach, neglecting prevention or thinking about it in a clichéd way. This is especially true since the American terrorist attack in 2001, which revived and intensified the process. Both secret services and law enforcement agencies specializing in law enforcement have realized that much more energy, specialists, and methods have to be deployed in order to effectively prevent crime.⁸ Because it is worth avoiding the trouble, the damage, the suffering, the irreversible horrors, the crimes, rather than suffering the (occasionally catastrophic) disadvantages and fighting for successful detection, learning about the past, and the inevitability of criminal prosecution.

In relation to the methods, I would like to point out the followings: it should not be forgotten that when interpreting the crime prevention function of forensics, a distinction is to be made between indirect and direct forms of proactivity.

Regarding the indirect function, I think that the basic goal and task of criminal sciences is to promote the fight against crime, and within that, in particular, to highlight the legal or non-legal means and methods of crime prevention. This is what criminal law does, for example, by emphasizing individual and general prevention. In criminalistics, the well-known scientific-experiential Beccaria theorem may and is to also be referred to, namely, that one of the most important components and the most effective guarantee for the prevention and reduction of crime is that all crimes and criminals are detected. In such cases, the potential deviant already considers the future perpetration too risky. As a consequence, criminology in general also indirectly fulfills a crime prevention function, when it increases and further develops the arsenal of tools and methodologies for detecting and proving crimes.

To its *direct crime prevention function*, I add as an interpretation that it has developed in very diverse forms, which are constantly changing even today, and of which I can only attempt to list examples in this study. These include:

- a) General and situational behavioral recommendations and tactical suggestions to avoid becoming a victim (damaged) (e.g. sexual immorality, bank card-bank account-related, property, including fraudulent, extortion, online and personal harassment, to prevent traffic crimes);
- b) the so-called technical and organizational recommendations related to "object protection";
- c) the promotion and placement of the use of safety equipment, including a number of devices that warn of light, noise, and movement and transmit signals to the authorities;
- d) encouraging the use of security (trace, object, chemical, technical (photo-film-video) traps);
- e) the tactics of timing coercive criminal proceedings;

- f) preventing the completion of the prepared or attempted crime and the commission of further crimes with open or widely used covert (secret) means, methods, and forces;
- g) conducting investigative actions in an educational manner, especially in the case of child or juvenile offenders.

The future of forensic crime prevention

Those listed so far can usually be found in previous forensic monographs, textbooks, and studies. However, let us turn our attention now to the new devices that are already partially used or in the initial stages. These will presumably play an important role in the criminalistics of the future. I will present some of them in a non-exhaustive manner:

1. Acquisition and analysis of electronic data;
2. Bayesian analysis;
3. Predictive application of the geographic method of crime;
4. Application of facial recognition programs;
5. The deployment of artificial intelligence.

Ad 1) Acquisition and analysis of electronic data

Before I indicate what areas of crime prevention can be covered with electronic data, I present the concept. It can be found in 2017. Tv. (a Be.). According to the definition of § 205 (1), "*Electronic data is the appearance of facts, information or concepts in any form that is suitable for processing by an information system, including the program that enables the execution of a function by the information system ensre*".

Choosing from several classifications, electronic data can be grouped "*according to their appearance*" as follows:⁹

- A) Electronic audio evidence:
 - a) audio recording in analog form;
 - b) digitized or digitally recorded audio material.
- B) Photo evidence:
 - a) still image information (face, iris, retina, etc.);
 - b) motion picture fixed directional source;
 - c) infrared camera (to detect dimly lit environments);
 - d) visual evidence obtained with a manual tracking system;
 - e) moving image tracking systems controlled by artificial intelligence.
- C) Imaging systems through which evidence can be obtained:
 - a) medical imaging systems (dRGTG, CT, MRI, fMRI, etc.);
 - b) personal body lighting systems for criminal purposes (THz frequency devices);
 - c) infrared camera for body heat mapping;
 - d) reduced energy package X-ray machines;

⁸ Géza FINSZTER: *Rendészettan*. (Police policy) Dialogue Campus, Budapest, 2018.

⁹ See more about this on the pages of this journal: Csaba FENYVESI – József ORBÁN: Az elektronikus adat mint a 7-5-1-es kriminalisztikai piramis modell építőköve. (Electronic data as stone of 7-5-1 criminalistical pyramid model) *Belügyi Szemle*, 2019/2. 45–55.

- e) underground imaging systems (such as ground-penetrating radar);
- f) ground surface imaging systems (vehicle screening system);
- g) atmospheric imaging systems (detection and tracking of devices moving in uncontrolled airspace for criminal purposes, drones).
- D) Electronically detected odor information;
- E) Radio Frequency Evidence:
 - a) radio frequency passive reconnaissance information;
 - b) radio frequency semi-active evidence (RFID);
 - c) radio frequency active evidence.
- F) Evidence existing in a circumstantial IT environment:
 - a) in IT data carriers and components (CD, DVD, USB key, hard drive, etc.);
 - b) in intelligent mobile communication and computing devices (smartphone, tablet, e-book, notebook, laptop, etc.);
 - c) in stand-alone IT systems;
 - d) in small networks including Wi-Fi;
 - e) in medium-sized firewall-protected IT systems;
 - f) by a large-scale firewall and VPN (virtual private network).
- G) Evidence that exists in cyberspace:
 - a) data found on the open internet (Facebook, LinkedIn, Twitter, Video, etc.);
 - b) data stored and transmitted on illegal networks.
- H) Evidence reconstructed with IT tools;
- I) Evidence of activity tracking and reconstruction systems;
- J) Evidence uncovered during electronic investigations that cannot be classified elsewhere.

Looking at the very long, but at the same time, almost constantly expanding list above, I can already describe some of the (incomplete) crime prevention possibilities inherent in them.

a) From the body heat map, the prevention authority can infer larger objects hidden under clothing, or elevated body temperature due to a state of excitement. (Think, for example, of a person about to explode in a stadium.)

b) The package inspection X-ray device, acting as an imaging system with low-energy X-ray radiation, artificially colours the objects inside the package based on the spectral properties. In this way, illegal and/or dangerous objects can be prevented from being transported, brought into objects, etc.

c) There are already access control systems where the examined person passes through a small lock chamber, the exhaust air of which is analyzed with sensors and the absence of drugs and explosives is detected.

d) The semi-active device absorbs energy when used in a suitable radio frequency environment. It emits its characteristic data using radio frequency radiation from the obtained energy. In some cases, for example, in the case of controlled animal species, the absence of a mandatory implantable device grounds the suspicion of a crime (forgery, smuggling, theft, etc.) and can be used to prevent further crimes.

e) RFID (*Radio Frequency Identification*) is a device built into a part, product or living being that contains information about the thing or living being's own characteristics or ownership. We can also consider goods protection devices or im-

planted chips used for animal identification as such, which make it pointless to commit certain crimes.

f) The data stored in the operative memory of the computer (and all microprocessor devices) can be saved even when the machines are in sleep mode, so the information before hibernation can be viewed, which can be useful to prevent planned illegal acts. (In the same way, virtual research and data from ethical hackers can be extremely useful.)

g) The NLJD (*Non-Linear Junction Detector*) equipment detects, for example, electronic devices designed for malicious use in the „hot spot” potential crime scene, regardless of whether they are on or off.

h) Open or covert scanning of cloud-based services, which are increasingly popular in cyberspace, can provide data that may indicate crimes in preparation. Data combing and data mining of mobile phones can have a similar result.

i) The grid-criterion-cluster automated data comparison can filter out potential criminal intent. (For example, the purchase of a large amount of fertilizer, when compared with other data, may indicate criminal planning or the preparation of an explosion.)

j) From the content of telephone conversations, e-mails, text messages, Internet (Wi-Fi)-based messages, the authority can infer future crimes.

k) Images from public area cameras (image analysis programs) may show the preparatory stages of crimes that have not yet been committed or completed.

l) Biometric scanning can reveal the means of committing a future crime. (Think of the illegal items you want to bring on board an airplane.)

Ad 2. The role of Bayesian analysis in crime prevention

In my opinion, Bayesian methods can be used not only in the detection of crimes and in the process of weighing evidence in courts in criminal cases, but also in the prevention of crimes. On what do I base my position -- not represented alone?¹⁰

The Bayes theorem and the related decision support methodology (e.g. the Bayes network) provide an opportunity for probability-based modelling of future actions. In other words, it can be used to (hypothetically) predict the occurrence of crimes in certain cities with a good chance. (The quotient of the probability of the event occurring and the non-occurrence, the likelihood ratio, can show the chance, location, and form of the future event.)

Ad 3. Predictive application of the geographic method of crime¹¹

The essence of Geographic Profiling is that a computer software can determine the most likely place of the next attack

¹⁰ See the work of József Orbán in this field, especially: Bayes-hálók a bűnügyekben. PhD thesis. PTE ÁJK, Pécs, 2018; We are talking here about a method already used in medicine, pharmacy, meteorology, and warfare. It is time for it to appear in forensics, including crime prevention.

¹¹ A separate monograph on predictive policing was also published. See: Szabolcs MÁTYÁS – Bence MÉSZÁROS – Imre SZABÓ: Prediktív rendészet. (Predictive policy) NKE, Budapest, 2020.

based on the related locations, as well as the place of residence of the potential (serial) attacker. Geographical profiling is a subtype of profiling, so it is also related to psychologically based behavioral profiling, which in turn falls within the scope of criminal ethics. What makes it classified as criminal technology is the fact that psychological profiling answers the “who” question, while geographic profiling answers the “where” question. Either before the crime (preventive) or after (criminal prosecution).

Ad 4. Introduction of facial and intent recognition programmes

Surveillance cameras, which are already widely used today, with special programs (e.g. so-called descriptive artificial intelligence) are capable (already today or will be) of observing faces, of stigmatizing possible tensions that have already appeared as a test in former criminals. On the basis of the tested signals, monitoring and follow-up movements can be carried out, which can provide an opportunity to prevent serious (even terrorist-type) crimes. Cameras with a special program can also take part in the depth border control in a preventive manner, recognizing unusual movement and possible illegal intent.

Ad 5. Deployment of artificial intelligence

I have left the most futuristic forensic prevention tool for the end, the previously mentioned artificial intelligence (MI=Artificial Intelligence). According to its concept, artificial intelligence-based systems are human-designed software that act in the physical or digital dimension to achieve certain complex goals and analyze their environment by collecting data, interpreting the collected organized or unorganized data, knowledge-based reasoning or information processing, and then they derive the best, most appropriate action, which is implemented from the data in order to achieve the specified goal (e.g. crime prevention).¹²

According to my prediction, the system will be able to make prognoses through the continuous knowledge and understanding of events, which will also be able to predict certain crimes or forms of criminal behavior.

The most sophisticated application method of artificial intelligence is currently Deep Learning.¹³ In this round: “In controlled (supervised) learning, the system filters the rules from the existing samples, and each new pair of problems and solutions gradually helps to find the correct connection. The teacher shows the data set and which of them meet the required conditions. Narrowing down the question to the security problem, the crowd is given, and which of these people are the ones who do not behave in accordance with the rules.”

“The indisputable advantages of deep learning can be utilized by crime prevention. The jointly identified recognition of several targets (e.g. vehicle, mobile phone) or target person (face, voice, movement), and the identification of the clus-

ter-forming force can also be an important factor in the recognition of risk and intent. In order to distinguish between coincidence, herd spirit, attention-grabbing flashmobs, and groupings with intent to cause harm, it is necessary to establish the group’s intent. Anticipating the possibility of a mass fight and directing law enforcement forces to possible foci – in addition to increasing the efficiency of the necessary human resources – improves the sense of security among those participating in mass events.”¹⁴

Finally, as the latest MI data, I mention an artificial intelligence-based nose developed by the specialists of the Hebrew University of Jerusalem and the University of Tel Aviv in 2021. Essentially, an infrared nose can detect odors and convert them into an image on a computer screen. Among other things, the development is also suitable for detecting airborne diseases, counterfeit alcoholic beverages, and spoiled or poisoned food. The development has so far identified dozens of odors with high accuracy, including those that the human nose cannot detect, such as the ingredients of alcoholic beverages. It is not excluded that it will also be able to recognize (components of) explosives, which would specifically serve the purpose of crime prevention.¹⁵

Final thoughts

In the light of all this, every citizen of common sense and integrity can rightly hope that in the future, the word “law enforcement” will not mean the “prosecutor” of the past, behind, or even later in time, but the preset “stepchild” of criminalistics, the prevention of crime that represents a preemptive strike.

The science of criminology should not stand at the scene of the crime with raised hands, but should extend its hand, not allow the visible scene to be created. Instead of an investigation following a trail, let us have a trail-free environment and life!

¹⁴ JÓZSEF ORBÁN: A Bayes-módszerek bünygyialkalmazásának alapjai. (Grounds of Bayes methods in criminal cases) In: Csaba FENYVESI – Csongor HERKE – Flórián TREMMEL (eds.): *Kriminalisztika*. (Criminalistics) Ludovika Egyetemi Kiadó, Budapest, 2022. 368.

¹⁵ WANG, Q. – LIU, Y. – CAMPILLO-BROCAL, J. C. – JIMÉNEZ-QUERO, A. – CRESPO, G. A. – CUARTERO, M.: Electrochemical Biosensor for Glycine Detection in Biological Fluids, *Biosensors and Bioelectronics*, <https://doi.org/10.1016/j.bios.2021.1131>; <https://www.sciencedirect.com/journal/biosensors-and-bioelectronics> (Accessed: January 21, 2024).

¹² See about this: Magyarország Mesterséges Intelligencia Stratégiája. (Strategy of AI in Hungary) 2020.

¹³ Goodfellow, I. – Bengio, J. – Courville, A.: *Deep Learning*. The MIT Press, Cambridge, London, 2016.