FORECASTING CRIME:

NEW TOOLS, NEW RISKS, NEW ETHICS

Edited by
Szabolcs Mátyás

FORECASTING CRIME:
NEW TOOLS, NEW RISKS, NEW ETHICS

A Practical Introduction to Predictive Policing and Crime Prevention

Edited by

SZABOLCS MÁTYÁS

Forecasting crime: new tools, new risks, new ethics / dr. Szabolcs Mátyás - Oradea : Editura Universităţii din Oradea, 2025
Conţine bibliografie
ISBN 978-606-10-2445-2

'Who controls the past controls the future.
Who controls the present controls the past'
(George Orwell: *1984*)

FORECASTING CRIME:
NEW TOOLS, NEW RISKS, NEW ETHICS

A Practical Introduction to Predictive Policing and Crime Prevention

Edited by
Szabolcs Mátyás

Dear Readers,

The research presented in this paper focuses on various aspects of the application of artificial intelligence in predictive policing.

Since profiling is already used to identify perpetrators of crimes, the examples included in the paper, although mostly drawn from the Hungarian experience, demonstrate its usefulness in prevention, as well as the technical, forensic, legal, and ethical implications.

The considerations presented in various areas inspire the use of AI that conciliates crime prevention, fundamental rights and the rule of law.

Using AI to obtain a more precise profile in time and space, while maintaining the final interpretation by a human being, enables a better identification of risks and potential perpetrators, and consequently, protects both the security and freedom of citizens.

Yves Vandermeer
founder of the European Cybercrime
Training and Education Group

ORADEA 2025

The cover was created with the support of AI-assisted tools; the final editing was by Tamás Tímár.

Authors:

BÁCS, ZOLTÁN Ph.D. (assistant professor), BÜCKŐ ANITA (data-driven and predictive security analyst), CZENCZER, ORSOLYA Ph.D. (associate professor), CSABA, ZÁGON Ph.D. (head of department), FANTOLY, ZSANETT Ph.D. (full professor), GICZI, ISTVÁN (senior service development manager), KRASNOVA ALEXANDROVA KRISTINA Ph.D. (associate professor) MAJOR, RÓBERT Ph.D. (associate professor), MÁTYÁS, SZABOLCS Ph.D. (associate professor), NYITRAI, ENDRE Ph.D. (associate professor), PACKOSZ, NIKIFOROSZ (Ph.D. student), SIVADÓ, MÁTÉ Ph.D. (associate professor), SZABÓ, IMRE Ph.D. (prosecutor), TIHANYI, MIKLÓS Ph.D. (associate professor), TÓTH, LEVENTE Ph.D. (assistant professor), TRAUB, ZITA (university student), VAJDA, ENDRE (Ph.D. student), VÁRI, VINCE Ph.D. (associate professor)

Peer-reviewed by:

Dragana Čvorović Ph.D. associate professor

Proofreader:

Michael James Webb

Published by:

University of Oradea

e-mail: mszabolcs1975@gmail.com

Foreword

The writing of this book was partly necessitated by the rapid growth of artificial intelligence (AI) in recent years, which has radically changed not only policing but almost every aspect of life. We need to respond to the new challenges this brings, and our wish is that we all think together about the changes that can be anticipated in the field of policing.

In addition to presenting the general characteristics of predictive policing, this book also deals with four specific areas: traffic policing, terrorism, cybersecurity, and drug crime; each a key area with a significant impact on our everyday lives, so we deal with each of them in dedicated chapters.

This book does not present all the various software packages used in every country because there are hundreds of software products on the market. Moreover, software is often discontinued or replaced, which would quickly make the content in this book outdated. Only two software programs are presented in detail, Böbe and Sopianae, both of which are Hungarian developments.

This volume strongly focusses on presenting the ethical problems that have arisen in connection with predictive policing. After an initial flare of interest around the topic, a period of 'sobering up' followed in which people began increasingly realistically to see the place and role of predictive policing in the field of policing as a whole. It is clear that it does not offer a crystal ball that can foretell the precise time of a crime to the minute. In some countries (e.g., China), however, predictive software is being used increasingly widely. The authors feel that various predictive forecasts may play a significant role in the future, although it is essential to understand how to integrate new types of technology effectively.

It was not the intention of the authors to create a textbook, although it is likely that university students studying law enforcement will be the primary users.

This work can be successfully used by any theoretical and practicing law enforcement professional who wants to learn about the latest results in predictive policing, and of course, not just those working in the field of law enforcement but also lawyers, criminologists, IT specialists, and public administration professionals seeking to gain a comprehensive picture of the topic.

The authors sincerely hope that the book will not only educate but also initiate dialogue about the future of law enforcement, the responsible use of technology, and also what security in the 21st century truly means.

We extend our special thanks to retired Lieutenant Colonel Ferenc Traub and vice rector General László Kovács, and sincerely hope that you enjoy this book.

Debrecen, 8 September 2025

Szabolcs Mátyás
Editor

Chapter 1
Predictive Policing: the Term, the Concept, and Its Relationship to other Fields of Science[1]

Szabolcs Mátyás

1.1. The Term 'Predictive Policing' and the Concept behind It

Before examining the concept of predictive policing, it is worth taking a moment to consider the meanings of the two words that comprise the term: *predictive* and *policing*. According to the definition in *The Britannica Dictionary*, 'predictive' means 'making it possible to predict what will happen: useful in the prediction of something' (URL1). The long-established Oxford Advanced Learner's Dictionary defines 'policing' as 'the activity of keeping order in a place with police: community policing.' (Wehmeier, McIntosh & Turnbull, 2005, p. 1165.) In other words, police activity in any given place is community policing.

From these two definitions we can conclude that the term *predictive policing* is a combination of the meanings of the two English words, 'predictive' and 'policing' with the former referring to the ability to forecast events, and the latter referring to the law enforcement activities of the police. Predictive policing, therefore, is an approach to policing based on predictions, that is, police intervention that not only reacts to events that have already occurred but that can also be based on the anticipation of future events (Lippai, 2023).

The concept itself was first introduced in the book *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, in which Perry et al. (2013) offered the following definition:

[1] NB: This chapter is based on Chapter 1 of the book *Közrendészet* edited by Péter Ruzsonyi (2020).

> *Predictive policing is the application of analytical techniques – particularly quantitative techniques – to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions.* (Perry et al., 2013, pp. 1-2.)

Let's look at another definition, which can be found in the Hungarian Law Enforcement Lexicon, according to which predictive policing is

> *a mathematically based GIS application that predicts the expected location and time of crimes, as well as the possible range of victims and perpetrators, based on past crime data, with a certain percentage of error.* (Mátyás, 2019, p. 379.)

Over the past decade and a half, virtually all work on predictive policing has referenced Perry's definition and the Hungarian definition also 'grew out of' that. Both definitions were appropriate in their day; however, as we noted in the introduction to this book, significant changes have occurred in recent years that necessitate a revision of the concept (Pődör et al., 2024).

Developing Mátyás' definition further, the author gives the following definition of predictive policing:

> *A GIS application based on mathematical and statistical principles that – also enabling the application of artificial intelligence – predicts the expected location and time of crimes, as well as the possible range of victims and perpetrators, based on past crime data, with a certain percentage of error; predictive forecasting can also predict the expected location, time and type of traffic accidents.*

In the above definition, the possibility of using AI and the potential for predicting traffic accidents are included as additional information to the concept previously outlined. There are an increasing number of predictive policing software programs that utilise artificial intelligence, but there are also a large number that operate in the traditional way, without it.

Traffic accident prediction is another new element in the definition. The vast majority of software programs were created to predict crime, but in recent years there has also been an increase in the number of software programs that aim to predict the location, time, and type of traffic accidents.

1.2. The Relationship between Predictive Policing and other Scientific Fields and its Place within the Crime Sciences

Predictive policing has a relatively short history of about two decades, so its relationship with other scientific fields is still in the early stages of development (Lippai, 2024). It cannot be considered an independent scientific field or discipline, as its subject, conceptual system, methods, and scientific theoretical principles are based and depend on research in other scientific fields. In its current state, predictive policing is an area between police studies and criminology, which combines the results of several scientific fields. It is closely related to mathematics, statistics, geography, cartography, and GIS (See table 1 [Pődör, 2015]). Below you can see the contributions of each scientific field to predictive policing.

The scientific fields most closely related to predictive policing	
Theoretical foundations (methodology)	mathematics, statistics, criminology
Fields necessary for the practical implementation of the method	geography, cartography, geoinformatics
Fields of practical application of the method	criminalistics, criminology, criminal psychology, security policy
Related scientific field as a result of using the method	legal studies

Table 1: The relationship between predictive policing and other scientific fields

(Edited by the author)

- MATHEMATICS

The theoretical foundations of predictive policing are mainly based on mathematics (primarily mathematical statistics: regression, correlation, probability calculation, and standard deviation). The author does not consider it necessary to describe these in detail, partly because this publication will primarily be read by students of law enforcement in higher education and partly because in practice various software programs now perform these complex mathematical operations on behalf of their users. Regarding mathematical statistics, these can be considered a part of applied mathematics, they are relatively easy to learn, and are applicable in many areas of life (e.g., medicine, economics, and psychology) (Hajtman, 1991). Let us briefly review the most essential mathematical methods used by predictive policing software.

- CALCULATING CORRELTATIONS

During correlation calculations, we are interested in how two or more variables are related to each other (or whether they are related to each other at all) and what the strength of the relationship between the variables is (how close are they?). Below we look at the most important basic types of correlation. There may be no relationship between X and Y, meaning neither value affects the other. In such a case, the image of the function will be a horizontal line, so that we can talk about a lack of correlation (no correlation). One example is the relationship between hair length and robbery frequency. We can state (although we do not have any relevant research to draw on, but here assume it is so) that there is no correlation between the two factors. Those with longer hair do not commit a higher percentage of robberies. In other words, there is no correlation between hair length and the frequency of robberies (Figure 1, point e).

The opposite of *no correlation* is when a *correlation* exists between two values, that is, when two factors are functionally related to each other. Law enforcement

pays special attention to these factors, and thus tries to discover as many such connections between the individual factors as possible. Each X value has a Y value that fits the regression line in such cases. The correlation between the amount of alcohol consumed and the number of public nuisances can be cited as an example: if the amount of alcohol consumed increases, so do the number of public nuisance events.

If there is a relationship between two values, we must determine whether the correlation between the two values is *positive* or *negative*. The correlation is positive if the value of one factor increases as a result of the other (Figure 1, point a). If we want to examine the relationship between robbery and education, we can conclude that the frequency of robbery decreases with an increase in education. That is, there is a correlation between the two factors, and a negative correlation can be observed (Figure 1, point b). If, on the other hand, we examine the relationship between education and white-collar crime, we can establish a positive correlation since the higher someone's level of education, the greater the chance of their committing that type of crime. Suppose we want to represent the correlation on a scale from -1 to +1. In that case, the maximum value of the negative correlation will be -1, while the maximum value of the positive correlation will be +1. If there is no correlation, it takes the value 0 on the number line. Based on the strength of the relationship, the following degrees of correlation can be distinguished (Table 2).

The three most commonly used correlation coefficients are Pearson's, Spearman's, and Kendall's coefficients; here we highlight Pearson's, which is the best-known and most frequently used. The Moran I indicator is also worth a mention as a territorial autocorrelation analysis that was developed in 1995. 'Moran I is an indicator that shows how similar or different the value of the area under study is to its neighbour' (Tóth, 2003, p. 39), so a local indicator of spatial association (LISA) like Getis-Ord Gi*. This indicator allows us to examine

clustering, that is, whether the spatial pattern is the result of a random process or not – values are interpreted between -1 and +1 (Mátyás & Pődör, 2022).

Correlation Coefficient (r)	Description (Rough Guideline)
+1.0	Perfect positive + association
+0.8 to 1.0	Very strong + association
+0.6 to 0.8	Strong + association
+0.4 to 0.6	Moderate + association
+0.2 to 0.4	Weak + association
0.0 to +0.2	Very weak + or no association
0.0 to -0.2	Very weak – or no association
-0.2 to – 0.4	Weak – association
-0.4 to -0.6	Moderate – association
-0.6 to -0.8	Strong – association
-0.8 to -1.0	Very strong – association
-1.0	Perfect negative – association

Table 2. The strength of correlation coefficients (LaMorte, 2021)

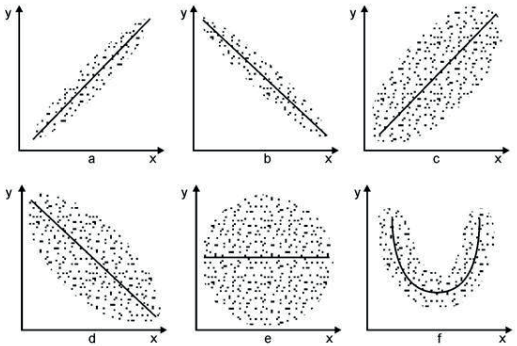


Figure 1. Degree of correlation

(a) Positive correlation/strong,(b) Negative correlation/strong, (c) Weak correlation/positive,(d) Weak correlation/negative, (e) Lack of correlation/no correlation,(f) Non-linear correlation (Fidy & Makara, 2005)

➢ REGRESSION CALCULATION (OR REGRESSION ANALYSIS)

When examining the correlation, we examined the relationship between the two factors (if there is one or not). However, even in the case of a correlation, we cannot predict one value from the other. During the regression calculation, however, we try to find a relationship between two or more variables that can be described by a mathematical function (Reiczigel, 2008). 'If two variables are linearly related, one can be used to predict the value of the other […] The closer the relationship between two variables, the smaller the forecast error.' (Balázs, n.d.) The opposite of *linear regression* is *non-linear regression*. We can talk about non-linear regression if the relationship between the dependent and independent variables cannot be described with a linear function. In this case, a curved line best fits the points (Fidy and Makara, 2005) (Figure 1).

Let us also look at a two-variable model that can be considered ordinary in relation to regression! We want to investigate an increase in the price of firewood and the number of illegal thefts of timber the forest. There is a clear connection between the two factors. An increase in the price of firewood can predict the amount timber theft is expected to increase. However, while it is clear that the two factors are related, many other factors also influence the development in the number of illegal acts: the weather, the rate of increase in wages or welfare benefit, etc. All of these must be taken into account in order for our forecast to be sufficiently accurate (Figure 2).

There are many spatial regression techniques, but the following three techniques are used most often in crime analysis:

1) *Spatial lag regression*: 'which considers the impact of the dependent variable in neighbouring areas in the model alongside the influence of other explanatory variables'
2) *Spatial error regression*: 'which gives an indication that the clustering observed in the dependent variable reflects the influence of unmeasured explanatory variables'

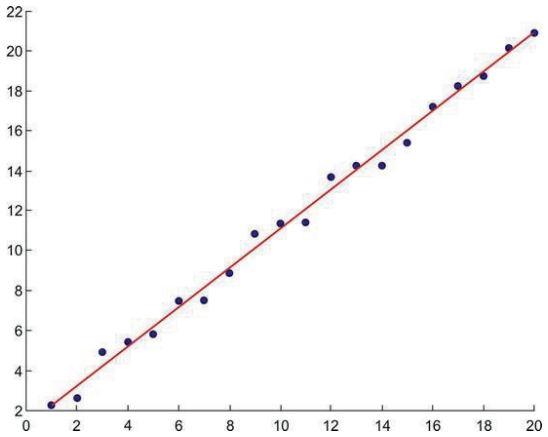


Figure 2. Linear regression (*URL 2*)

3) *Geographically weighted regression* (GWR): 'which performs local regression equations on each geographic unit in a study area' (Chainey, 2021).

* *Ordinary Least Squares* (OLS) are used to establish the basis for spatial analyses.

Ordinary least squares (OLS) regression *is an optimization strategy that helps you find a straight line as close as possible to your data points in a* linear regression *model. OLS is considered the most useful optimization strategy for linear regression models as it can help you find unbiased real value estimates for your alpha and beta.* (Alto, 2023)

➢ CALCULATING PROBABILITY

When calculating probability, we aim to determine the likelihood that a specific event will occur. To illustrate probability with an everyday example, consider the possibility of tossing a coin and determining the chance that it will land on either side (i.e., heads or tails). It is about 50-50%. But we cannot rule out the possibility that the coin will land on its side, although the probability of this is minimal. A case is well illustrated by the final scene of the film 'Odds and Evens' (1978) when the two lead characters in the film (Terence Hill and Bud Spencer) make a bet with each other. Their father tosses the coin, and a seagull flying by takes the

money, so neither heads nor tails come up. Neither of them won the bet, so an orphanage received $1 million (Figure 3).

Figure 3. Chance, as a possibility, must always be taken into account. Therefore, we cannot say with 100% certainty that a crime will occur
(Own editing based on the movie 'Odds and Evens')

In the case of a die, the probability of rolling an even or odd number is also 50%, but of course, it is also very rare for the die to land on its corner, but we will ignore this for the following example.

The above, when expressed in mathematical terms, appears as follows.

$$p = \text{probability}$$

$$p = \frac{\text{number of favorable cases}}{\text{total number of cases}}$$

If we want to roll a 6 (this will be the favourable case), the probability is 16.6%, since

$$p = \frac{1}{6} = 16.6$$

If we want to work out the probability of a crime being committed on a street in a city, the dice would need to have as many sides as there are streets in

the city, and the number of rolls of that dice would be given by the number of crimes committed on the streets.

Standard Deviation, Median, and Mode

The average itself is often misleading. The *median*, *mode*, and *standard deviation* are additional statistical measures that can help us better understand the structure of our data and better predict future trends or events (Harmati et al., 2025).

The standard deviation shows how much values deviate from the average. A simple example to illustrate this concept is a school setting. If a student received the following grades in school: 4, 2, 4, 2, 4, 2 then their average would be a 3. The average of a student who received the following grades: 5, 1, 5, 1, 5, 1 would also be a three, and the average of a student who received only threes (3, 3, 3, 3, 3) would also be a three.

The latter student has the smallest deviation from the average since they always got threes -- in their case, the standard deviation is zero. The other two students also have an average of three, but in their case, the standard deviation is larger because the grades deviate further from the average. This school example also illustrates that the average does not always provide a complete picture.

There are two other concepts that you need to know about with regard to standard deviation: the mode and the median. The mode is the most common value. For example, if someone has six grades in geography, of which 4 are 5s, and 2 are 2s, then the mode will be 5 because this is the most frequent grade. The median is the middle value, or more precisely, the middle element of the data set arranged in order (URL3). For example, if a student's grades are as follows: 1, 1, 2, 2, 3, 4, 4, 5, 5. The numbers are in ascending order and the middle grade is 3 (there are 4 grades before and after it). The median, in this case, is 3.

Let's apply the above mathematical theories to the practice of predictive policing.

- The STANDARD DEVIATION shows the stability of the data. If the standard deviation is high, it is more challenging to predict crimes. On the other hand, if the standard deviation is low, it means that the data is closer to the average, so the future is more predictable, and the police can plan to use their resources more effectively.
- The MODE helps identify the most common patterns, for example, it can show at what time of day the most traffic accidents occur, or the most common venue for the occurrence of a crime. This helps the police determine when and where it is worthwhile organising actions.
- The MEDIAN helps us get a realistic picture of the most typical crime rate without it being distorted by a few extreme cases. This allows for well-founded, proportional planning even in situations where outliers occur.

Crime Sciences

The methodological foundations of predictive policing largely come from criminology. In this regard, we can consider, among other things, research results that demonstrate the predictability of crime and victimisation. Predictive policing also widely utilises the research results of environmental criminology, which attempts to model the relationship between the location of a crime and the crime itself.

The relationship between predictive policing and forensics is also close. The basis of this relationship is that effective crime prevention can only be achieved through methods that can be used in practice (Hautzinger, 2019). From the perspectives of investigation and crime prevention, this can be considered a novel forensic method.

Earth Sciences

The relationship between predictive policing and geography can be seen in two areas. On the one hand, through the indicators used by the software, and on the other hand, through a map display of the forecast.

The geographical indicators used by the software can be primarily classified as social geography (e.g., population, age, infrastructure, and transport geography data) and, to a lesser extent, as physical geography (e.g., weather, climate). Of course, in addition to geographical factors, indicators belonging to other scientific fields are also present in predictive software.

Regarding map display, GIS (Geographical Information System) and cartography are the areas related to geography. Almost all software has a GIS system that makes the possible venues for crime visually apparent (Pődör and Dobos, 2014).

Law

Finally, let us take a glance at the relationship between predictive policing and the law. Predictive policing is not directly related to the operation of any software, nevertheless, the use of predictive software raises several legal problems the solution of which is currently still difficult to handle and may raise numerous legal concerns. The Anglo-Saxon legal system handles these problems in a 'more generous' way than the continental one, nevertheless; many legal and human rights problems still arise there today. The legal issues of predictive policing are discussed in detail in Chapter 8.

References

ALTO, V. (2023). Understanding Ordinary Least Squares (OLS) *Regression* (https://builtin.com/data-science/ols-regression)

BALÁZS, K. (n.d.). Lineáris regresszió. Statisztika I. 4. [Linear regression. Statistics I. 4.] (PowerPoint slides) (http://psycho.unideb.hu/munkatarsak/balazs_katalin/stat1/stat1ora4.pdf)

CHAINEY, S. (2021). Understanding Crime: Analyzing the Geography of Crime. Esri Press, California

FIDY, J. & MAKARA, G. (2005). Biostatisztika [Biostatistics]. InforMed 2002 Kft. (https://www.tankonyvtar.hu/hu/tartalom/tkt/biostatisztika1/ch10.html)

HAJTMAN, B. (1991). Matematikai statisztika [Mathematical statistics]. Tankönyvkiadó, Budapest

HARMATI, B., PŐDÖR, A. & TICK, A. (2025). Time's Effect on Crime Prediction Precision and Accuracy. *Acta Polytechnica Hungarica*, 22(8), pp. 157-177.

HAUTZINGER, Z. (2019). Gondolatok a kriminalisztika elméleti rendszeréről (Thoughts on the theoretical system of forensic science). *Jura*, 25(1), pp. 84-93. (https://szakcikkadatbazis.hu/doc/6885817)

LAMORTE, W. (2021). PH717 Module 9 – Correlation and regression (https://sphweb.bumc.bu.edu/otlt/MPH-Modules/PH717-QuantCore/PH717-Module9-Correlation-Regression/PH717-Module9-Correlation-Regression4.html)

LIPPAI, ZS. (2024): Újragondolt szerepek a biztonság megteremtésében [Rethinking Roles in Creating Security] (PhD thesis). LUPS, Budapest

LIPPAI, ZS. (2023) Magánbiztonságról határtalanul [Private security without borders]. *Belügyi Szemle*, 71 (6), pp. 971-1000. (https://doi.org/10.38146/BSZ.2023.6.3)

MÁTYÁS, SZ. (2019). Megelőző rendészet [Predictive policing]. BODA József (ed.). *Rendészettudományi Szaklexikon*. Dialog Campus, Budapest (https://real.mtak.hu/153920/1/743_Rendeszettudomyanyi_Szaklexikon_e_2020_04_28_.pdf)

MÁTYÁS, SZ. & PŐDÖR, A. (2022). Rendészeti térinformatika [Law enforcement GIS]. Ludovika Kiadó, Budapest

PERRY, L. W., MCINNIS, B., PRICE, C. C., SMITH C. S. & HOLLYWOOD, S. J. (eds.). (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation, Los Angeles (https://www.rand.org/pubs/research_reports/RR233.html)

PŐDÖR, A. (2015). Usability Study on Different Visualisation Methods of Crime Maps. *International Journal of Geoinformatics*, 11(4), pp. 15-22.

PŐDÖR, A & DOBOS, M. (2014). Official Crime Statistics versus Fear of Crime of the Citizens in a Hungarian Small Town. *GI_Forum: Journal for Geographic Information Science*, pp. 272-275.

PŐDÖR, A., OURANIA, K., MARIANA, V. & QILEI, H. (2024). Urban rehabilitation and the reflection of spatial reorganisation of crimes in citizens' crime perception. In: Szakál, A. (ed.). IEEE 24th International Symposium on Computational Intelligence and Informatics (CINTI 2024). Proceedings Danvers (MA), Institute of Electrical and Electronics Engineers (IEEE), 99-103.

REICZIGEL, J. (2008). Korreláció és regressziószámítás [Correlation and regression calculations] (PowerPoint slides)

TÓTH, G. (2003). Területi autokorrelációs vizsgálat a local Moran I módszerével [Spatial autocorrelation analysis using the local Moran I method]. *Tér és Társadalom*, 17(4), 39-49. (https://doi.org/10.17649/TET.17.4.914)

WEHMEIER, S., MCINTOSH, C. & TURNBULL J. (2005). *Oxford Advanced Learner's Dictionary*. Oxford University Press, Oxford

URL1: https://www.britannica.com/dictionary/predictive

URL2: https://tudasbazis.sulinet.hu

URL3: https://www.mateking.hu/valoszinusegszamitas/statisztikai-alapfogalmak/modusz-es-median#34

Chapter 2
Major Milestones in the History of Predictive Policing[2]

Szabolcs Mátyás and Csaba Zágon

The desire to know the future is not new; people have wanted to know what the future holds for thousands of years. In ancient Greece, numerous oracles existed that people could consult for a fee to learn about their future. The most famous Greek oracle was located at DELPHI, near the Gulf of Corinth, the ruins of which can still be seen today (Figure 1). The development of risk management science has been a fundamental prerequisite for the emergence of predictive policing. The concept of risk itself originated in Athens more than 2,400 years ago. Ancient thinkers concluded that it was important to review and evaluate the possible consequences of a decision and the likelihood of their occurrence in the future. These two factors together constitute the risk associated with an event and help in avoiding poor choices while minimising potential damage (Bernstein, 1996; Aven, 2016).

Law enforcement agencies manage the social risks of crime by looking ahead in time. They strive to understand what crime may look like in the future and make informed decisions about how to address it – whether by reducing or eliminating it – through the effective use of their resources, methods, and established procedures. A crucial component of this approach is predicting future crime trends. Although this prediction involves some uncertainty, it provides a valuable starting point for law enforcement strategies. Today's predictive policing goes beyond the observations of the ancient Greeks, incorporating not only

[2] The chapter is based on Chapter 2 of the book *Közrendészet* by Péter Ruzsonyi (ed.) (2020) – written by the author.

qualitative indicators, but also quantitative data supported by mathematics, such as probability theory, and other scientific disciplines.

Figure 1. The Athena temple complex, including the Delphic Tholos. With the Pleistos River Valley in the background (URL1)

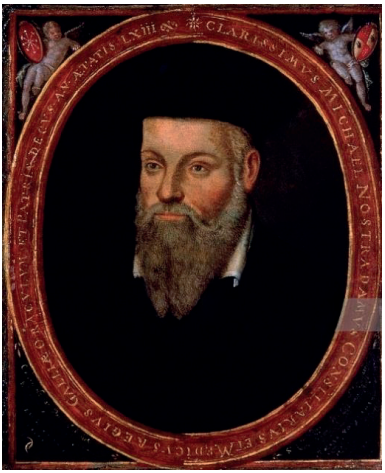


Figure 2. Nostradamus (URL 2)

Knowing about the future was also important to the Romans, who had a great tradition of bird divination. The augurs (bird seers) made predictions based on the sounds, flight, etc. of birds. People in the Middle Ages were no different from the people of antiquity. The most famous seer of the Middle Ages was the French doctor NOSTRADAMUS (1503-1566) (Figure 2), who wrote four-line poems about what would happen in the coming centuries.

Some say that Nostradamus predicted the French Revolution (1789), the First World War (1914-1918), the Second World War (1939-1945), the September 11 terrorist attacks (2001), and other events.

'The sky will burn at forty-five degrees.
Fire approaches the great new city.
By fire, he will destroy their city,
A cold and cruel heart, blood will pour.
Mercy to none.' (URL 3)

Some believe that the above poem predicted the September 11 terrorist attacks. In the case of nomadic peoples, soothsayers and shamans were 'tasked' with seeing into the future, and fell into trances by means of various intoxicating plants to do so.

People today are as interested in knowing the future as they were thousands of years ago. Today, however, we use scientific methods to examine past and present events, which – albeit with a certain margin of error – can help us to know the future.

2.1. The Roots of Predictive Forecasting

The idea of predicting crime has long preoccupied researchers, and over a hundred years ago, some attempted to identify potential criminals scientifically. Most notable among these was CESARE LOMBROSO (1835-1909), a Turin-based medical and criminal anthropologist, who believed that it was possible to determine whether a given individual was a 'born criminal' or not based on external physical and physiological characteristics. The doctor's findings were soon refuted by science, but the history of criminology still preserves his memory.

Among the predictive developments of the past few decades, it is necessary to mention first the various police models (philosophies).

- PROBLEM-ORIENTED POLICING (POP), developed by the American HERMAN GOLDSTEIN (1979), advocates the exploration of various threats that exist in society, which gives local police agencies a wide range of autonomy to deal with problems. The profession, expert work, and scientific analyses play prominent roles in the exploration and solution of problems. The theory was expanded by JOHN E. ECK and WILLIAM SPELMAN in 1987, placing greater emphasis on research, analysis, and crime prevention (Szikinger, 2016; Christián, 2022; Kozáry, 2007).
- EVIDENCE-BASED POLICING (EBP) was an important step on the path to predictive policing and drew attention to the importance of statistical analysis and empirical research. The development of the model can be attributed to the American criminologist LAWRENCE SHERMAN. EBP accepts traditional policing tools; but, it highlights attention to the importance of scientific analysis (URL4, Szikinger, 2016).
- Continuing the evolution of predictive policing, the next stop was the Compstat model. The term COMPSTAT is a portmanteau of the words 'computer statistics'. The New York City Police Department first used it under the leadership of Police Chief WILLIAM J. BRATTON (Figure 3).

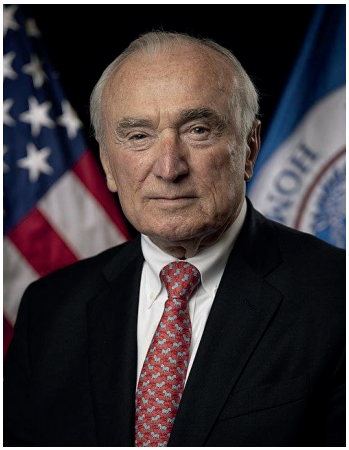


Figure 3. William J. Bratton (URL 5)

To analyse crime data, Bratton built a computer system that helped locate the most dangerous areas (hotspot mapping) and track crime trends.

The analyses were conducted on a monthly basis, and policing strategies were developed for each area.

One of the most impressive results was that the number of homicides in New York City fell by about half between 1995 and 2003, from 1,181 to 596. 'We didn't just react to crimes; we predicted them,' said William J. Bratton in an interview (Sárosi, 2008; Visnovitz, 2011). In other words, this model can already be considered the precursor of predictive policing.

- INTELLIGENCE-LED POLICING: In this model, the collection, systematic processing, and use of information for public safety and protection have become a fundamental and defining element of police work. The terrorist attack on the United States on September 11 2001 and the related law enforcement deficiencies drew attention to the need and urgency of developing intelligence-led policing. The police model is a collaborative performance task that combines the systematic collection and evaluation of data with the long-standing practice of community policing and problem-oriented policing. Data collection and processing must serve to address community problems.

  The data generated during the activity – and this also applies to the results of secret information collection – do not remain within the scope of law enforcement data management, surrounded by secrecy walls, but are used in the interests of law enforcement and crime prevention (Korinek, n.d.). The Hague Programme adopted in the European Union in 2004 also set the goal of implementing this model at the EU level (Boda, 2019, p. 279).

- HOTSPOT POLICING is one of the most important precursors of predictive policing, based on crime mapping. Hotspot policing is a policing strategy that developed after the recognition of crime hotspots and 'aims to proactively reduce the crime rate in the affected area. One of the key elements of the

strategy is to ensure an increased, demonstrative police presence' (Mátyás, 2019, p. 205).

- CRIMINAL PROFILING is possible using past criminal data. Profiling is a forensic method used to identify unknown perpetrators. It is based on the recognition that personality determines behaviour, and that behaviour can be used to infer personality (Petrétei, 2020).

> *The essence of profiling is to provide characteristics of the unknown perpetrator and his/her actions that can be used to select a suitable person from among those already in sight or to search for a suitable person in the victim's narrower or wider environment. The completed profile shows what type of person the perpetrator may be.* (Boda, 2019, p. 449)

During profiling, experts use behavioural science to try to predict the offender's next 'step' (e.g., victim and crime scene). In this case, the question we ask during the investigation is not 'who' we are looking for but 'what kind of' person we are looking for. In other words, profiling can also be considered a type of predictive technique, as it can also provide information about the future.

Profiling also involves identifying the common characteristics of offenders based on known cases over a specific period. This process helps in determining which individuals are likely to be perpetrators of a particular type of crime. It is crucial to note that while we cannot predict with certainty that specific individuals who fit a given profile will commit crimes, we can assert that individuals matching the profile – such as air passengers – are statistically more likely to be, for example, drug couriers than others. If our selection successfully identifies perpetrators based on their profile, it indicates that the profiling method is effective. However, if we consistently encounter false positives (wrongly identifying innocent individuals) or false negatives (failing to identify actual offenders), then we need to review or even discard the existing profile and apply new ones. The group of randomly selected passengers can be narrowed down by

the customs authorities who utilise such profiles. This process allows us to confidently state that the individuals remaining in the group are more likely to be couriers compared to any randomly selected set. Additionally, this narrowing process enables us to allocate law enforcement resources more effectively to manage the individuals identified (Zagon and Gecsei, 2021).

The German Federal Criminal Police Office (BKA) developed a similar investigative technique in the 1960s, referring to it as 'raster investigation'. Unlike traditional investigations, which focus on a known suspect, raster investigation aims to reduce the number of individuals to be checked in several stages. This is achieved by filtering certain groups from public and private databases, searching for characteristics unlikely to apply to the person being sought. Consequently, this procedure decreases the number of individuals that law enforcement agency needs to examine while increasing the proportion of potential targets within the sample (Schewe, 2006).

These profiling techniques may also be of interest to predictive policing, as they can reduce the uncertainty of our view of the future.

2.2. Civilian Antecedents of Predictive Policing

As is true of many methods and procedures used in the field of policing, the civilian sphere was where they were originally developed and then applied, and only later did the procedure seep into the field of policing. This was also the case for predictive policing. Noticing the effectiveness of preventive software used in the civilian sphere (commercially), police experts utilised preventive software to enhance crime detection and prevention.

In the United States, large commercial companies were first to start studying consumer behaviour and habits. They noticed that, in some cases, consumer habits changed significantly, so they collaborated with universities to

develop software that could predict future consumer behaviour with a certain percentage of accuracy.

Many American companies have begun to address this area, as predicting expected purchasing habits can lead to significant additional profits. On one hand storage costs can be reduced, and on the other hand, shortages of a given product can be prevented. In almost all cases, the literature on predictive policing highlights the American giant WALMART – a leader in predictive research – as a company that practically founded American predictive policing.

The experts at this American chain store noticed that meteorological (weather) conditions significantly influence both the desire to purchase and the range of products bought. Weather events can include, for example, a sudden shift in cold or warm air masses, a significant amount of precipitation, or strong winds. There is a clear link between weather and the range of products purchased in some cases. For example, we can consider the relationship between rainy weather and the number of Wellington boots or umbrellas sold, or snowfall and the number of snow shovels sold. However, there are products for which it is extremely difficult to find a link between weather and the given product type. Examples of such products – which Walmart employees also noticed – include STRAWBERRY POP-TARTS and duct tape, among others.

In these cases, it is evident that a more thorough analysis of shopping habits was required. The goal was to predict shopping habits using statistical methods, to prepare for expected increases in demand, and more precisely determine their future sales strategy (Figure 4) (Perry et al., 2013).

Figure 4. Strawberry Pop-Tarts (URL 6)

Finally, regarding civilian use, let us mention the large utility companies, which, long before law enforcement applications, also utilised statistical methods to predict where pipelines (e.g., water, oil, and gas pipelines) would fail and when consumption would be highest (e.g., electricity, water).

Nowadays, forecasts are widely used in business, so we find software that attempts to predict the exchange rate of individual currencies, the development of the global wheat market price, or the expected sales of various pastries in a given area. The method has worked effectively in commerce and is still working today, and its application is becoming more widespread. Upon learning of the method, American police experts drew an analogy between shopping habits and future crimes, so they began to use computer programmes to model the expected locations and times of crimes, as well as the groups of perpetrators and victims.

2.3. A Hungarian Innovation: the Public Police Service Support Program (BÖBE)

2.3.1. Factors Forcing the Development of the Software

The issue of crime prediction has also been a concern for law enforcement professionals in Hungary. Especially in the period following the change of regime (after 1989) when crime rates increased significantly over a few years, and the police were unable to respond successfully to the ever-increasing crime rate for a long period. To illustrate the gravity of the problem, the number of crimes

increased 2.7 times over a decade (Mátyás, 2017a). The drastic quantitative and qualitative change in crime affected the entire country, and the capital in particular where the crime rate was well above the national average even before the change of regime.

One of the acts that most severely damaged the population's subjective sense of security was vehicle theft. The capital was most affected by the crime. The territorial concentration of vehicle thefts and the severity of the problem are well illustrated by the fact that, during the period in question, more than 80% of vehicle thefts were committed in the city of Budapest and Pest County (Mátyás, 2011). Vehicle thefts affected different districts of the capital to varying degrees. The Budapest Police Headquarters (BRFK) District III Police Headquarters was among the most seriously affected districts, in which several vehicles were stolen daily.

2.3.2. The Birth of Böbe

To address the acute problem, Attila Markó, then head of the BRFK III District Police Headquarters, supported all possible new ideas that could be expected to reduce car thefts. In the 2000s, one of the deputy heads of the headquarters was Lieutenant Colonel FERENC TRAUB (Figure 5). He believed that a computer program could predict where and what type of crime would be committed in the future based on past crime data (Traub, 2005). The decision was followed by action, and after completing the office work, several months of endeavour followed.

Figure 5. Lieutenant Colonel Ferenc Traub (retired), 'father of predictive policing'

In his free time, and without any remuneration, Traub created the software known as 'the Public Police Service Support Program' in 2004 (in practice, the software became operational in April 2004).

At this point, it's worth pausing for a moment to consider the date: 2004. This is evidently the world's first predictive software, (Mátyás, 2017b), yet all the English-language sources published so far have cited the American PredPol software (or its predecessor) as the world's first predictive software. Clearly; this is a mistake, first place belongs to this Hungarian cop, Ferenc Traub.

Several people helped him in his work, including Lieutenant Colonel Attila Markó and Lieutenant Colonel Ferenc Rácz. The development work took place at Ferenc Traub's home, often through the night. Once the program was up and running, the developers had only one 'task' remaining, to name the predictive software: they came up with BÖBE (pronounced 'bø:bɛ).

So while the official name of the software is 'the Public Police Service Support Program', everyone called it Böbe. The reason for this was that Ferenc Traub's wife, Erzsébet, was nicknamed Böbe. The creators of the software were grateful to her, as she had prepared food and drink for them during the development. As a sign of their gratitude, Böbe became the unofficial name of the world's first predictive software (Mátyás, 2017b).

2.3.3. The Police Service Support Program in Practice[3]

This Hungarian software was employed operationally from 2004, although it underwent continual modification with Ferenc Traub incorporating user ideas and concepts into it. The software enabled the prediction of the following crime types, which significantly influence the subjective sense of security of the

[3] This chapter is based on the work and oral communication of Ferenc Traub (2004) entitled Documentation on the Public Police Service Support Program.

population: car break-ins, car theft, robbery, burglary, and fraudulent theft. Böbe assisted the police in the following areas:

- Organising daily public patrols
- Planning of operations and raids
- Preparing for district commissioner meetings
- Selecting the optimal location for surveillance cameras
- Planning the weekly service of the district commissioner and patrol staff

.The installation of the program requires several simple, logical steps: uploading the street names, district commissioner districts, area names, housing estate names, and other relevant information. The initial database demands approximately 30 days of crime data, and one important condition for use is that the uploaded data must be constantly updated because otherwise the forecast may be misleading. The data entry itself takes only a few seconds for each crime. In the case of an average-sized police station, only a few of the above crimes are committed each week, meaning that only a few minutes are spent daily on entering the data.

The program allows for various searches, including the location and timing of each type of crime. It is possible to determine the streets on which the most crimes have been committed, and the streets are sorted in descending order. It is also possible to examine the infection rate of each police station, and by predating the days of the week, you can see where crimes can be expected to be committed in the coming week for police stations.

Böbe ranks the percentage of each crime occurring on each day of the week. The practical benefit of this lies primarily in the fact that the commander

can foresee when it is possible to for leave to be taken when the fewest crimes are anticipated.

The operating principle of the software is based on probability calculation and standard deviation, with the number of crimes per day of the week in a special constellation. The probability of a crime occurring is calculated from all the data in the database. Similarly to 'dice theory' (where 1 to 6 rolls of the dice can be taken), instead of the six sides of the cube, the 640 streets of the 3rd district are substituted, so 'Böbe's dice' has 640 sides. In the case of this program, the rolls corresponding to the sides are replaced by the number of crimes committed on the streets.

The software asks how many patrol pairs are available on duty that day. Based on that, it specifies the streets where crime is most likely to occur. In optimal conditions, one patrol pair can cover approximately 8-10 streets, giving them a chance to catch the perpetrators of crime. One of the virtues of the program is that it compiled a ready-made action plan that stated who, when, and where to go. The action plan was automatically provided with a header and the names of the action leader. Regarding the program's effectiveness, it can be stated that at the time of its application, it predicted 30% of the five crime categories mentioned above.

The Óbuda Hajógyári Sziget (Óbuda Shipyard Island) is situated in the territory of Budapest's 3rd District Police Department, where Europe's largest open-air music event, the Sziget Festival, has been held since 1993, attracting hundreds of thousands of Hungarian and foreign tourists. The organisation of external security was the responsibility of the 3rd District Police Department until 2015. With the help of the Böbe software, it was possible to identify the streets where the most crimes had been committed during the festival in previous years. As a result, the number of crimes committed in the area around the festival has

decreased significantly since 2010. In fact, in some years, none of the crimes predicted by the software were committed.

Foreign delegations visiting the police station (e.g., from Austria, Germany, England, and the Netherlands) recognised the novelty and applicability of the Böbe software and took it back to their home countries. Neither the software developer nor the author has any relevant information about its use abroad (Molnár, 2016).

2.3.4. The Afterlife of the Böbe Software

The Böbe software was in operation from April 2004, and it was demonstrably years ahead of other software abroad operating on a similar principle, so it can be said that the police officers of the 3rd district were ahead of the Americans and the Italians in creating their program; and they did it alone, with neither professional nor financial assistance.

After Ferenc Traub's retirement, the software continued in use for years, thanks to Lieutenant Colonel Ferenc Rácz. However, when Rácz also left the police station, the new management did not invest any effort in entering new data, so it fell into disuse.

In summary, we can say that at the time of its creation (2004), the BÖBE software was a singular idea in the world, as this type of predictive program had not been used in the field of law enforcement anywhere else. Both the idea itself and its implementation were unique.

2.4. The Birth of American Predictive Software

Methods for predicting crime have been available for a long time; however, modern technology has only recently developed the mathematical algorithms necessary for this purpose. In connection with the creation of the predictive

policing model, we must also highlight the name of WILLIAM J. BRATTON, who served as the police chief of Los Angeles. In 2008, Bratton spoke extensively about the successes of the Los Angeles Police Department, also mentioning that they had developed a new method for predicting gang activity and tracking real-time crime. The research was initially conducted by the Los Angeles Police Department and UCLA, from which the software known as PredPol later grew (Perry et al., 2013). The second functional predictive software, which can be considered the forerunner to the PredPol software, was completed in 2006.

In testing and further developing the method, Bratton worked closely with JAMES H. BURCH II, Director of the Bureau of Justice Assistance, and KRISTINA ROSE, Director of the National Institute of Justice (NIJ), to study the new concept and draw conclusions for law enforcement agencies. During this time, two symposia were organised at NIJ. The first was in Los Angeles in November 2008, where Kristina Rose emphasised Bratton's role as a catalyst for the rise of predictive policing in her opening speech. She also mentioned that there was already a huge interest in learning about the new method across the United States. Among others, the heads of the police forces of Boston, Chicago, Los Angeles, the Metropolitan DC area, New York, and the Maryland State Police indicated that they would participate in predictive policing research and would be happy to serve as sample areas for experimental research. In addition to professional police organisations, the media, software manufacturers, and the executives of private security companies soon showed great interest (Perry et al., 2013).

The second symposium was held in Providence, Rhode Island (USA), where there was general agreement that predictive research needed to be continued and developed. Participants emphasised that further results could only be achieved if data sharing between police agencies was enhanced, regionalisation was strengthened, and strong analytical capacity was created (Perry et al., 2013).

In the two years following the second symposium, interest in predictive policing exploded. This was partly due to the media's exaggerated influence on predictive methods. A predictive software package called PredPol was reported (or at least alluded to) by several television networks and newspapers (e.g., CBS Evening News, *The New York Times*, and the NBC Nightly News) as predicting precisely where crimes would occur (Figure 6.)[4]


By BOB ORR / CBS NEWS / April 11, 2012, 8:40 PM

LAPD computer program prevents crime by predicting it

Share / Tweet / Reddit / Flipboard / Email

The L.A. police department's "Predictive Policing" computer program in Los Angeles, California. / CBS NEWS

(CBS News) LOS ANGELES - The Los Angeles Police Department has gone on an offensive to prevent crime.

Its latest weapon is a program that can actually predict where crimes will happen. CBS justice correspondent Bob Orr has a first look at the results.

In the Foothill Division, north of downtown Los Angeles, police are patrolling largely working class neighborhoods with specially-marked maps.

The small red squares are "hot spots" where computers project where property crimes are most likely.

In one of its advertisements, IBM – although not seriously claiming this as a possibility – showed a police officer arriving at the scene of a crime before the perpetrators did thanks to data analysis (Perry et al., 2013).

Figure 6. A misleading article: Los Angeles Police Department computer program predicts crime (URL 7)

References

AVEN, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13. (https://doi.org/10.1016/J.EJOR.2015.12.023)

BERNSTEIN, P. L. (1996). *Against the Gods: The Remarkable Story of Risk*. Wiley.

[4] NB. The PredPol software was marketed under the name Geolitica from 2021, and its distribution was discontinued in 2023.

BODA, J. (ed.) (2019). *Rendészettudományi Szaklexikon* [Law Enforcement Lexicon]. Dialog Campus, Budapest (https://real.mtak.hu/153920/1/743_Rendeszettudomyanyi_Szaklexikon_e_2020_04_28_.pdf)

CHRISTIÁN, L. (2022). *Komplementer rendészet* [Complementary Policing]. Ludovika Kiadó, Budapest

KOZÁRY, A. (2007). *Rendészeti politológia II.* (Law enforcement political science II) Rendőrtiszti Főiskola, Budapest

MÁTYÁS, SZ. (2019). Forrópont [Hotspot]. Boda József (ed.). *Rendészettudományi Szaklexikon*. Dialog Campus, Budapest (https://real.mtak.hu/153920/1/743_Rendeszettudomyanyi_Szaklexikon_e_2020_04_28_.pdf)

MÁTYÁS, SZ. (2017a). Magyarország általános bűnözésföldrajzi helyzete [The general crime geography situation in Hungary]. *Hadtudományi Szemle*, 10(4), pp. 497-505. (https://epa.oszk.hu/02400/02463/00037/pdf/EPA02463_hadtudomanyi_szemle_2017_04_497-505.pdf)

MÁTYÁS, SZ. (2017b). A térinformatika a hazai rendvédelmi szervek gyakorlatában [Geoinformatics Practice in Hungarian law enforcement agencies]. In: Balázs Boglárka (ed.): Az elmélet és a gyakorlat találkozása térinformatikában VIII. Debreceni Egyetemi Kiadó, Debrecen, pp. 217-222.

MÁTYÁS, SZ. (2011). *A Debreceni Rendőrkapitányság kriminálgeográfiai elemzése* [Criminal geography analysis by the Debrecen Police Department]. Ph.D. dissertation, University of Debrecen

MOLNÁR, B. (2016). Térinformatika – Közterületi szolgálatot támogató program – BÖBE [Geoinformatics – Public Service Support Program – BÖBE].

PERRY, L. W., MCINNIS, B., PRICE, C. C., SMITH, C. S. & HOLLYWOOD, S. J. (eds.) (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation, Los Angeles (https://www.rand.org/pubs/research_reports/RR233.html)

PETRÉTEI, D. (2020). Elkövetői profilalkotás és a bűnügyi helyszín elemzése [Offender profiling and crime scene analysis]. *Rendőrségi tanulmányok*, 3(1), pp. 3-49. (http://epa.niif.hu/04000/04093/00009/pdf/EPA04093_rendorsegi_tanulmanyok_2020_1_003-049.pdf)

SÁROSI, P. (2008). 'Zéró tolerancia' [Zero tolerance]. *Beszélő* (http://beszelo.c3.hu/cikkek/%E2%80%9Ezerotolerancia%E2%80%9D)

SCHEWE, C. S. (2006). Rasterfahndung. In H.-J. Lange & M. Gasch (eds.), *Wörterbuch zur Inneren Sicherheit* (1st Ed., pp. 263–267). VS Verlag für Sozialwissenschaften, Wiesbaden.

SZIKINGER, I. (2016). Előrelátó rendőrség [Forward-thinking police]. In: FINSZTER G., KŐHALMI, L. & VÉGH ZS. (eds.): *Egy jobb világot hátrahagyni…* Pécsi Tudományegyetem Állam- és Jogtudományi Kar. Pécs, pp. 558-567.

TRAUB, F. (2004). Dokumentáció a közterületi rendőri szolgálatot támogató programról [Documentation on the program supporting public police services].

TRAUB, F. (2005). Újítási javaslat az ORFK 15/2005. (VIII.23.) utasítása alapján [Proposal for renewal based on ORFK instruction 15/2005. (VIII.23.)].

VISNOVITZ, P. (2011). A világ legjobb bandaszakértőjét importálja a sokkolt Anglia [Shocked England imports world's best gang expert]. (http://www.origo.hu/nagyvilag/20110815-william-j-bratton-a-britek-altal-segitsegul-hivott-amerikai-szuperzsaru.html)

ZAGON, C., & Gecsei, M. (2021). Kockázatelemzés a gyakorlatban: Cigaretta a repülőtéren. [Risk analysis in practice: Cigarettes at the airport] In V. Czene-Polgár, C. Zagon, A. Szabó, & Á. Zsámbokiné Ficskovszky (eds.), *Tradíció, tudomány, minőség: 30 éves a Vám-és Pénzügyőri Tanszék* [Tradition, science, quality: 30 Years of the Customs and Excise Education Department] (pp. 129–142). Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, Budapest. (https://doi.org/10.37372/mrttvpt.2021.2.7)

URL 1: https://en.wikipedia.org/wiki/Delphi#/media/File:Delphi,_Greece_-_panoramio.jpg

URL 2: https://hu.wikipedia.org/wiki/Nostradamus#/media/F%C3%A1jl:Nostradamus_by_Cesar.jpg

URL 3: https://www.standard.co.uk/lifestyle/nostradamus-predictions-come-true-hitler-world-trader-center-b1202038.html

URL 4: https://www.policinginstitute.org/wp-content/uploads/2015/06/Sherman-1998-Evidence-Based-Policing.pdf

URL5:https://commons.wikimedia.org/wiki/File:William_Bratton,_official_portrait,_Homeland_Security_Council.jpg

URL 6: https://www.poptarts.com/en_US/recipes/no-bake-strawberry-pop-tarts-cheesecake.html

URL 7: https://www.cbsnews.com

Chapter 3
The Concept of Big Data and its Role in the Predictive System[5]

Szabolcs Mátyás and Kristina A. Krasnova

Big Data based on information and communication technology is a defining phenomenon and method in the modern era that also plays a major role in the application of predictive policing techniques.

3.1. General Characteristics and Concept of Big Data

The reader of this book has probably noticed that when they search for something on the Internet, they soon receive similar advertisements and spam. The reason for this can be explained simply in two words: Big Data. Nowadays, this term is often heard but, unfortunately, the vast majority of people are not aware of its meaning. American professor DAN ARIELY has formulated the problem in an extremely clever way.

Big data is like teenage sex:
everyone talks about it,
nobody knows how to do it,
everyone thinks everyone else is doing it,
so everyone claims they are doing it.

People often discuss it, but they don't fully understand its precise meaning (at least, most people don't). There is no precise and universally accepted definition; however, an examination of scientific articles, books, and online

[5] The chapter is based on Chapter 4 of the book *Közrendészet* edited by Péter Ruzsonyi (2020) – written by the author.

sources on the subject reveals that most definitions share similar content. The Cambridge Dictionary gives the following definition of Big Data:

> *Very large sets of data that are produced by people using the internet, and that can only be stored, understood, and used with the help of special tools and methods.* (URL1)

This dictionary definition contains several essential content elements, one of which is that the use of the internet (e.g., Google, Facebook, Twitter, Instagram, LinkedIn, etc.) creates a large amount of data, which is precisely what is required to make the most accurate predictions. Of course, this does not only mean crime predictions but can also apply to purchasing habits, the expected world market price of grain, and the speed of spread of infectious diseases. Large amounts of data can only be stored in a specialised way (in the cloud). The amount of data generated globally is now measured in *zettabytes* (Figure 1).

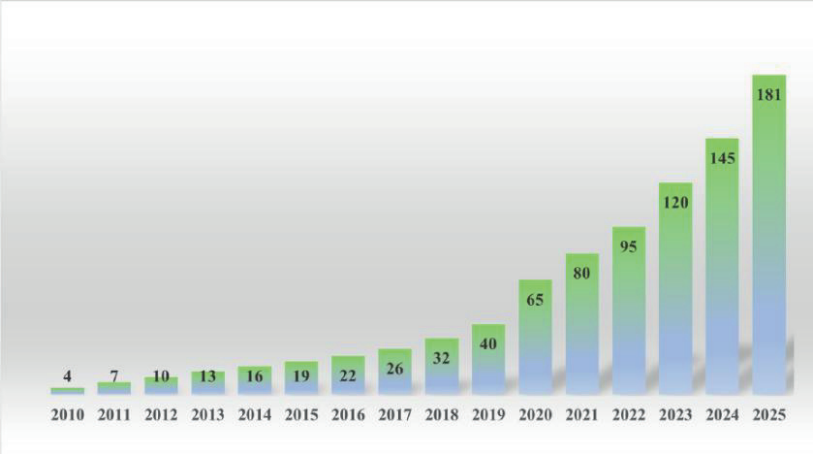


Figure 1. Global Internet data generated annually in zettabytes (Moghaddam, 2024, 7.)

Another important concept arises in connection with communication between machines, the 'Internet of Things', usually referred to by the acronym of this English term: 'IoT, which we understand in the following way:

> *The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. IoT devices – also known as 'smart objects' – can range from simple 'smart home' devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems. Technologists are even envisioning entire 'smart cities' predicated on IoT technologies. IoT enables these smart devices to communicate with each other and with other internet-enabled devices. Like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform various tasks autonomously.* (URL 2)

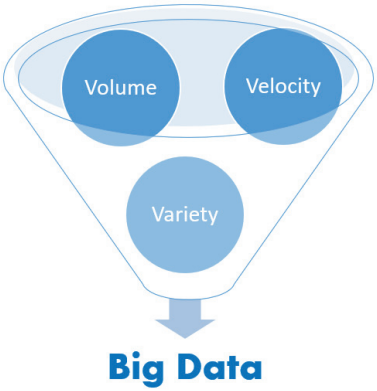
Communication between machines plays a significant role in the vast amount of data generated daily, which can also contribute to making various predictions. However, in addition, a huge amount of data is also generated by various sensors, smart devices, and the 'imprints' created during the use of social networks (e.g., tweets, hypertexts, geolocation information, audio and video files, clicks, transactions) (Giczi & Szőke, 2017).

3.2. The Three 'Vs'

The three 'Vs' are often mentioned in connection with Big Data. These are its most essential requirements, each starting with the letter 'V': volume, velocity, and variety.

- VOLUME: For forecasts to be accurate, data must be available in as large a quantity as possible. However, none of the definitions provide a precise statement on the amount of data required for an analyses or how large the

data must be before it can be considered Big Data. Thus one of the most important conditions for accurate forecasts is that the most significant possible amount of data is available.



- VELOCITY: This refers to rapid data processing, that is, how quickly the huge amount of data available can be processed. Increasingly powerful computers help with this (Figure 2).
- VARIETY: The third letter, 'V', refers to the diversity of the data. The more diverse the available data (to be analysed) the more reliable and accurate a forecast will be.

Figure 2. The three most important requirements for Big Data are: volume, velocity, and variety (Edited by the author)

Some predictive software is also criticised as flawed because the data used is too flat, which means that the forecast cannot be sufficiently accurate. The more varied the sources of data are the more accurate the forecast can be.

In addition to the three Vs, some people also consider other words starting with the letter V to be factors that contribute to the accuracy of the forecast. One such term, also beginning with the letter 'V' and related to Big Data, is VERACITY, which means the reliability of the data. If unreliable data is analysed, the forecast will not be reliable. Therefore, less data can sometimes be more effective, or in some cases, more accurate forecasts can be made with less data than with more data from unreliable sources. Reliability, in this case, should not necessarily be understood in the everyday sense, for example, where a forecast is

made from data obtained illegally, cheaply, or on the black market. There is no question that data from a reliable source can also be of poor quality. VARIABILITY refers to the constant change of data since the content of the data can also change. VISUALISATION refers to the presentation of data. It is not possible to present the relationships between data using traditional graphic methods, so alternative tools must be employed (such as tree-maps and parallel coordinates). VALUE is the potential value of data. All data has business value, and greater profits can be achieved if we better understand the customers of a given product or optimise a process. VALIDITY, by which we mean the correctness of the data. The forecast can be biased if the data is not up-to-date, particularly if there is a large amount of outdated data. Prior to analysis, therefore, it is advisable to get rid of data that might result in inaccurate forecasts (Devan, 2016; Giczi & Szőke, 2017). Of course, each 'v' can play a role and be significant, but the first 3Vs mentioned have the greatest impact on forecasts.

3.3. Classification of Big Data

Big Data can be classified into the following three large groups based on their origin (Giczi & Szőke, 2017).

1.) HUMAN-ORIGIN DATA: This includes previously created (now digitised) literary and artistic works, social media comments, likes, posts, blogs, vlogs, e-mail messages, text messages, etc.

2.) PROCESS-ORIGIN DATA: registry data (health, registry, banking) and transaction data (purchases, transfers, credit and debit card transactions, etc.) can be classified under this category.

3.) DATA GENERATED DURING COMMUNICATION between machines connected to the Internet (sensor data, log files), satellite images, webcams, geographical location trackers (GPS), etc. The amount of data classified in this category is growing at the fastest rate.

3.4. Big Data – Small Data

If big data exists, then, of course, *small data* must also exist. The term is typically used in contrast to big data, particularly when the amount of data is significantly smaller (a few terabytes), and the available dataset is less complex.

To determine what a given population thinks about an issue (e.g., the population of a country or city), it is possible to ask each individual. An example of this might be a referendum. Then, a portion of the people go to the ballot box and express their opinion. By aggregating the votes, the opinions of the voters can be determined, and predictions for the future can be made based on the results. Problems with referendums may arise if it is not possible to ask people about a new issue every week (and the majority would not vote anyway), it is time-consuming and expensive, and in most cases, only a small portion of the voters turn out to vote; furthermore, only the position of the population aged above 18 can be learnt from it, etc. To address the above problems, the questionnaire method is increasingly used in market research, from which it is also possible to draw conclusions about, for example, current and future purchasing habits.

However, several problems can arise in the use of questionnaires, including the issue of representativeness and the interviewer's influence. One of the main questions regarding the former is whether a sample of 1000, 2000, 5000 or more people can accurately represent the entire population of a country. Accurate sample selection is therefore one of the most critical aspects of questionnaire surveys, making the sample selection methodology a key area of focus. In questionnaire surveys, the issue of respondent honesty can also be a problem. How honestly will a respondent answer an interviewer? It is evident that in cases involving personal questions (such as those related to health or a person's sexual life) we cannot expect every respondent to answer honestly, meaning that any forecast based on this information will be neither reliable nor accurate. In addition, a problem may arise in that by the time the data is processed, the

acquired data may have become outdated and have lost its relevance (Giczi & Szőke, 2017).

If we want reliable answers, and not just a sample of a few thousand people, but the honest opinions of hundreds of thousands or even millions of people, then a different method must be used. The latest reliable method is big data. In this process, if we rely on data of appropriate quality and quantity, we can obtain the honest 'answers' (observed behaviour) of millions of people, which is already suitable for making reliable predictions, even with regard to the future development of crime (Mester, 2015).

3.5. Data Storage and Related Problems

The spread of various Big Data techniques was partly made possible by the emergence of ever faster and more powerful computers, which became widely available to companies and even to the general public. However, 'home' computers were no longer suitable for storing increasingly significant amounts of data, so nowadays, it has become natural that data storage (for large amounts of data) is not tied to the user's computer but to *the cloud* (virtual servers). Data storage in the cloud was greatly facilitated by the fact that the cost of this form of data storage has decreased significantly, making it practically accessible to anyone. In any case, it is a positive fact that the cost of storage has decreased significantly; however, this has generated several problems. The increasingly cheaper cost of data storage means that data owners no longer have to choose between incoming and existing data but rather save everything, resulting in a significant amount of unnecessary data among the existing data.

It is, therefore, necessary to filter the extant data and store only that which is needed for the forecast. The question may arise as to what problems can ensue from unnecessarily storing large amounts of data – apart from the fact that this is

a pointless waste of money on the part of the person storing the data since they still have to pay for the storage (Figure 3).

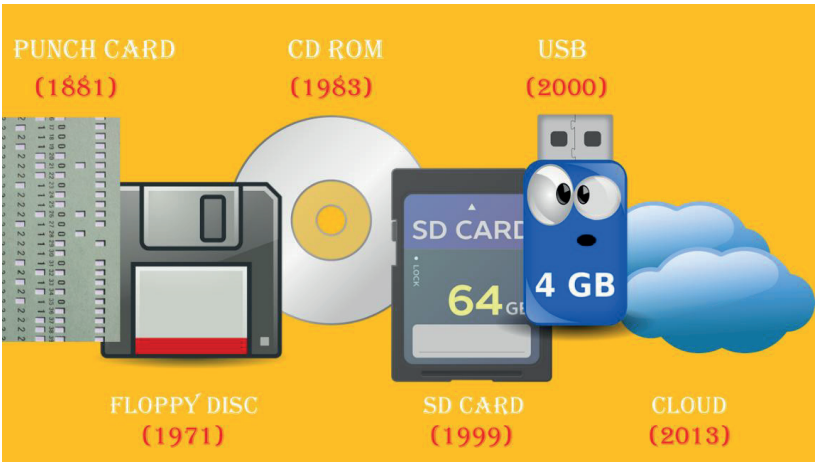


Figure 3. The evolution of data storage
(Based on URL 3, edited by the author using URLs 5 and 6)

As mentioned above, in addition to the 3Vs, other factors are also important in Big Data analysis. One of these is the validity of the data. Data devalues quickly, and not only is that not helpful, but it can also lead us astray when we are making a forecast. To illustrate the process of rapid data devaluation with an everyday example, let us take a look at a fashion-related problem: just because red clothes were in fashion one summer and red clothes were the most searched for on the Internet, it does not mean at all that red will be in fashion the following summer. Therefore, data related to red clothes can be considered redundant; if we attempt to develop a commercial strategy in this regard years from now, it will most likely lead us astray. However, if we consider more extended time frames, we can also think about changes in taste, fashion, mind-set, and shopping habits, among other things, caused by age, which can render some data sets worthless. Based on this, it is easy to see how, in many cases, even

a few months can bring significant change in the life of a community, which is why using data that is sometimes several years old can greatly impair the accuracy of a forecast.

Another problem may be the source of the data, that is, where the data comes from. An important research ethics issue in forecasts made using Big Data techniques is that the database and the type of data used are clear. Ethical issues of this kind are particularly important in the field of law enforcement since the forecasts may even lead to the implementation of measures that restrict personal freedom. The source of the data used and its reliability – especially in the case of crime forecasts – are, therefore, among the most important ethical issues.

3.6. Areas of Use for Big Data

The huge amount of data mentioned above has been utilised in various areas of life for years to assess the current state and predict anticipated future trends. The use is extremely wide-ranging, but this publication cannot and does not intend to present these areas in full detail. Still, it is worth getting to know some of the more important areas besides criminal use, which clearly illustrate the technical development that has taken place in the field of Big Data in recent years. It is no exaggeration to say that there is hardly any area today in which some form of Big Data technique is not used to make predictions.

Big Data is most widely used in commerce and the service sector. As mentioned in Chapter 2, predicting customer behaviour is one of the broadest areas of application for Big Data techniques. Proper market mapping can significantly improve the effectiveness of marketing and sales campaigns and also provides support for pricing and optimises logistics processes (URL 6).

In the field of commerce, American companies were among the first to attempt to maximise profits with the new method. Walmart stands out among

these; for example, the American giant uses Big Data software called Social Genome to reach as many customers as possible. The software connects information published on the Internet and social media with purchase data and contact information. Walmart also developed software called Shoppycat, which can recommend products to Facebook users based on the interests of their friends. In fact, it even provides the contact information of the nearest store (Szűts and Yoo, 2016).

We mentioned in previous chapters that large utility companies (water, gas, electricity, etc.) are also at the forefront of Big Data use. Employing Big Data techniques, predictive software is used to predict utility failures and anticipate consumption spikes.

> *The most exciting example, however, perhaps comes from New York. In 2012, the city's environmental protection department used Big Data to find restaurants responsible for clogging the sewer system. New Yorkers had been suffering from the environmentally damaging effects of drains clogged with cooking oil for years According to traditional methods, inspectors carried out spot checks. In the Big Data environment, the city's IT specialists linked the databases of private waste collection companies with the invoices and geographical data of the restaurants. Based on the results obtained, the detection rate increased to 95%* (Szűts and Yoo, 2016, p. 16).

Within the service sector, financial and credit institutions, as well as insurance companies, also prefer to utilise Big Data techniques. Financial institutions use large amounts of data in areas such as lending and financial investments.

One of the lesser-known applications of Big Data is in healthcare, although it is also increasingly utilising the predictive capabilities offered by Big Data these days. One of the most frequently used areas is the prediction of the spread of infectious diseases. Based on this, it is possible to give a relatively high

degree of certainty as to which area a pathogen causing a disease can be expected to be present at a given time.

One of the best-known pieces of research in this regard is associated with Paul Allen. A company called Vulcan, founded by the co-founder of Microsoft, is trying to predict the spread of the Ebola epidemic using artificial intelligence. The spread of the coronavirus pandemic, which began in late 2019 and caused mass illness, is also being predicted using data generated on the internet. Researchers at John Hopkins University in the United States use Twitter to obtain real-time information about certain diseases, and Google has been trying to identify the epicentres of influenza epidemics since 2008 based on the huge amount of data generated on the internet (Google Flu Trends) (Dodds and Zolfagharifard, 2020; Iot Zóna, 2020).[6] In the field of healthcare, many currently believe that the most effective method for predicting the spread of infectious diseases is the use of Big Data. Using much less data, but also classified as Big Data, are smart health devices that continuously monitor our health and provide doctors with 'real-time findings.' Such devices include the increasingly popular smartwatches and fitness bracelets (Szűts and Yoo, 2016).

Big Data techniques are also used in the labour market, primarily to predict which employees will be the most successful. According to many experts, the days when lines would form in front of a workplace after a job advertisement are over. Using the advantages of Big Data, only those candidates who have 'passed' Big Data analyses are invited for personal interviews so that the prospective employer only has to focus on a few candidates during the interview.

[6] In this regard, it is worth noting that the software had worked well for years, but in 2013, the predictions became inaccurate. This was due to news about influenza causing people who were not sick to search the Internet, which significantly worsened the accuracy of the prediction (Szűts & Yoo, 2016).

Finally, let us mention the potential applications of Big Data in the fields of law enforcement and justice. The field of law enforcement has only just begun to apply the potential of Big Data techniques, somewhat late.

Predictive policing based on the application of Big Data can be used in the implementation of many investigative actions, such as house searches, seizures and arrests. In the latter case, the software attempts to predict the defendant's expected behaviour (Szikinger, 2016).

Today, practically everyone has a digital footprint; every search, correspondence, share, comment, etc. on the internet is preserved, including of those who intend to commit illegal acts (Lippai et al., 2025). Big Data can, therefore, be used with great success in the fight against terrorism. Terrorists, even if they use pseudonyms, utilise the internet, their mobile phones, and social media in their everyday lives, leaving behind a digital footprint that can (and does) greatly assist investigative authorities in successful detection.

Big Data can also play a role in traffic policing. In the context of smart cities, the large amount of incoming data is of great importance, which helps, among other things, to optimise traffic and can also play a role in preventing accidents (Benedek and Molnár, 2013).

Within law enforcement agencies, Big Data and predictive software also have numerous potential applications in the field of corrections (see more: Chapter 3). Big Data analyses also play a significant role in the field of tax administration. Online cash registers record the location, time, amount, and other details of each purchase.

3.7. Advantages and Disadvantages of Big Data Analyses[7]

Like everything, Big Data has both advantages and disadvantages that should be considered when applying it. Among the most important advantages is that data is obtained in REAL-TIME, that is, it can be considered current, reflecting the state that we want to know about (i.e., it shows real behaviour, consumer habits, etc.). From the perspective of a survey, these can be considered key factors, as outdated data can often be misleading and fail to reflect the true situation accurately. Another great advantage is that there is NO INTERMEDIARY PERSON (interviewer), whose personality can greatly influence (both positively and negatively) the course of the questioning.

Traditional data collection techniques pay great attention to representativeness, that is, ensuring that each group is represented in the appropriate proportion based on area, gender, age, etc. However, this is not always ensured in Big Data. For example, we want to provide forecasts based on mobile phone traffic. In that case, it is uncertain that our survey will be representative, as the country is not completely covered, meaning that people living in some areas will not be included in the forecast. On the other hand, not only a lack of coverage but even a surplus of coverage may develop, which can also distort the forecast. Another problem with mobile phones is that different age groups use them to varying degrees, which also results in the survey not being representative of the population as a whole. The use of numerous technical devices is an example of the analogy with mobile phones, which shows that Big Data should only be used with due caution. Based on the above, it is evident that most BIG DATA SOURCES LACK REPRESENTATIVENESS.

Another problem may be that the acquired data is of INADEQUATE QUALITY. The Achilles' heel of applying Big Data techniques is DATA

[7] The chapter was compiled based on the 2017 study by Johanna Giczi and Katalin Szőke. (Giczi & Szőke, 2017)

PROTECTION, which is discussed in detail in Chapter 8. However, it is worth mentioning in this regard – especially from the perspective of law enforcement – that if the data sources are not reliable, the analysis methodology and the algorithms used are unclear, and the results become vulnerable to attack. The ACQUISITION OF DATA USUALLY HAS A COST, which in some cases exceeds the expected benefit. Of course, in such cases, it is necessary to consider whether it is worthwhile purchasing the data and using it at all. We mentioned at the beginning of the chapter that the application of Big Data techniques does not require the processing of data of a traditional magnitude. The analyses cannot be performed in the same manner and with the same operations as previously performed. A HUGE DATA SET CANNOT BE STORED ON A COMPUTER (or laptop), nor can it be put into a Word document or Excel file, but other analysis methods must be applied, which requires a type of expertise beyond that of an average computer user.

Another problem may be the difficulty of FILTERING OUT DUPLICATES. A large number of duplicates mislead a forecast, so an attempt should be made to delete them from the database.

As we have already mentioned earlier, social media posts often do not reflect genuine opinions, as they typically conform to the norm expected by a community (Pléh & Unoka, 2016); therefore, comments, likes, posts, etc., on social media cannot always be considered honest opinions. Another problem may be that SOURCES OF BIG DATA MAY CEASE TO EXIST (a website is closed, someone deletes their Facebook profile, etc.), which certainly makes comparability with later acquired data difficult.

Another disadvantage of Big Data is that we are interested in certain correlations but not in the correlation itself. As an example of this, consider the amusing case of credit card issuers discovering that of their customers, those who purchase chrome skulls are often late with their payments, while those who buy

anti-slip mats tend to be on time. However, financial institutions are no longer interested in cause and effect relationships, only in the fact that the probability of non-payment is higher for someone (Szűts & Yoo, 2016).

References

BENEDEK, A. & MOLNÁR, GY. (2013). ICT Related Tasks and Challenges In The New Model of Technical Teacher Training. In: TERZAKIS, J., PALEOLOGU, C. & GYIRES, T. (eds.) Eighth International Multi-Conference on Computing in the Global Information Technology. InfoWare, Nice, pp. 40-44.

DODDS, L. & ZOLFAGHARIFARD, E. (2020). How AI could combat the spread of China's deadly coronavirus. The Telegraph (https://www.telegraph.co.uk/technology/2020/01/21/ai-could-combat-spread-chinas-deadly-coronavirus/)

GICZI, J. & SZŐKE, K. (2017). Hivatalos statisztika és a Big Data [Official statistics and Big Data]. Statisztikai Szemle, 95(5), 461-490. (https://real.mtak.hu/54831/1/2017_05_461.pdf)

IOT ZÓNA (2020). Hogyan segíthet a mesterséges intelligencia a koronavírus legyőzésében? [How can artificial intelligence help defeat the coronavirus?] (https://iotzona.hu/big-data/hogyan-segithet-a-mesterseges-intelligencia-a-koronavirus-legyozeseben)

LIPPAI, ZS., ÁRPÁS, B. & KARDOS, P. (2025): Magánnyomozás Magyarországon [Private investigaton in Hungary]. *Belügyi Szemle* (special issue), 73(1), pp. 7-29. (https://doi.org/10.38146/bsz-ajia.2025.v73.i1SI.pp7-29)

MESTER, T. (2015). A nagy Big Data félreértés [The big Big Data misunderstanding). (http://adatlabor.hu/a-nagy-big-data-felreertes/)

MOGHADDAM, S. S. (2024). The Past, Present, and Future of the Internet: A Statistical, Technical, and Functional Comparison of Wired/Wireless Fixed/Mobile Internet. *Electronics*, (13), pp. 1-35. (https://doi.org/10.3390/electronics13101986)

PLÉH, CS. & UNOKA, ZS. (2016). Hány barátod is van? [How many friends do you have?] Oriold és társai Kft. Budapest (https://real.mtak.hu/71798/1/unoka_rec_1.pdf)

SZIKINGER, I. (2016). Előrelátó rendőrség [Forward-thinking police]. In: FINSZTER G., KŐHALMI L. & VÉGH ZS. (eds.) Egy jobb világot hátrahagyni... :Tanulmányok Korinek László professzor tiszteletére. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, pp. 558-567.

SZŰTS, Z. & YOO, J. (2016). Big Data, az információs társadalom új paradigmája [Big Data, the new paradigm of the information society]. Információs Társadalom, 16(1), pp. 8-28. (https://real.mtak.hu/43454/1/it_2016_01_1_szuts_yoo.pdf)

URL 1: https://dictionary.cambridge.org/dictionary/english/big-data

URL 2: https://www.ibm.com/think/topics/internet-of-things

URL 3: https://www.anycloud.dk/anycloud/data-management/data-storage-thoughout-history/ alapján

URL 4: https://pixabay.com/hu/vectors/search/pendrive/

URL 5: https://www.istockphoto.com/hu/search/2/image-film?family=creative&phrase=lyukk%C3%A1rty

URL 6: https://www.it-services.hu

Chapter 4
The Importance of Hotspot Policing in the Field of Predictive Policing[8]

Szabolcs Mátyás

The vast majority of predictive software is based on hotspot policing, utilising previously discovered criminological and policing models. To put it very simply, we can say that hotspot policing, which has been used for decades, has undergone a facelift, and predictive analytics, combined with today's modern technical achievements, has created predictive policing (it is not by chance that they jokingly say that predictive policing is actually 'old wine in a new bottle'). To understand the main principles of how the software works, knowledge of hotspot policing, which we will discuss in this chapter, is essential.

4.1. Analogue Maps

To gain a more thorough understanding of hotspot policing, we must go back to traditional cartography. Humans have long held the desire to depict their narrower or broader surroundings in a two-dimensional, compact manner. Thousands of years ago, proportionally reduced copies of the surface were depicted on rock, then on papyrus, and later on paper. The depiction of the surface, the possession of a map, was a factor of strategic importance even thousands of years ago, with significance for hunting, warfare, strategy, etc. These maps were two-dimensional, meaning they could depict latitude and longitude (Pődör, 2005). Earlier definitions of a map defined it as a two-dimensional, scaled-down version of the Earth's surface. However, with the advent of digital maps,

[8] The chapter is based on Chapter 5 of the book *Közrendészet* by Péter Ruzsonyi (ed.) (2020) – written by the author – and Szabolcs Mátyás *Crime Geography* (2024).

this has changed, and we can now talk about both two-dimensional and three-dimensional maps.

The spatial representation of crime has had nearly 200 years of history (see A.M. Guerry: *Essay on the Moral Statistics of France*, 1833). Following GUERRY, an increasing number of scholars have examined the relationship between space and crime, resulting in crime mapping playing an increasingly important role in crime prediction and trend identification.

4.2. Digital Maps

The advent of personal computers (PCs) brought about a qualitative leap in the field of mapping. Unlike traditional paper-based maps, digital maps provided a much broader range of analysis options. Since their advent (in the 1990s), it has been customary to divide maps into 'digital' and 'analogue' maps. However, it should be noted that if digital maps are printed, then they also become analogue (Pődör, 2007).

4.3. Grouping of Maps

Maps can be categorised according to several principles, one of which is grouping by content. On this basis, general and thematic maps can be distinguished. Thematic maps are used to depict crime.

> Thematic maps *'depict non-landscape elements and phenomena of the natural and social environment, their quantitative and qualitative characteristics. Simplified versions of general maps serve as the background image for thematic maps. Thematic maps include maps of the natural environment, social, economic life, science, public administration, politics, history, etc.* (Unger, 1994, p. 12)

Maps depicting the quantitative and/or qualitative characteristics of crime can, therefore, be classified as thematic maps. Thematic maps that depict crime

elements are called crime maps. In the application of hotspot policing and predictive policing, it is mainly digitally generated crime maps that are used.

> *A crime map is a type of thematic map that depicts one or more quantitative or qualitative characteristics of crime. Based on the type of crime map, it can be qualitative, quantitative, static, or dynamic. Additionally, based on the number and relationship of the topics depicted, it can be analytical, complex, or synthetic. Crime maps are now almost exclusively created with GIS programs.*(Mátyás, 2019a, p. 84)

4.4. The Hotspot

Research on hotspots dates back to a relatively short period. The American researchers SHERMAN, GARTIN, and BUERGER investigated crime hotspots in the city of Minneapolis. In doing so, they found that 50.4% of emergency calls come from 3.3% of the city (Sherman et al., 1989), meaning that the location of critical locations in the city is extremely concentrated. SHERMAN, L. W. and SPELMAN, W. (1995) later noticed that hotspots have temporal and spatial cycles, and their size can change periodically. Hotspots are not permanent formations, and they can even disappear over time.

There is no generally accepted definition of a hotspot in the literature. Most researchers agree that the area of a hotspot is relatively small, and its infection rate differs significantly from the environmental average, persisting for a longer period. However, there is no universally accepted position on the size (maximum and minimum) of a hotspot, or of how long the crime infection rate should be higher or lower than its surroundings, or how much the crime volume should exceed that of its surroundings. Until these relevant issues are clarified, we cannot talk about a uniform definition of a hotspot (Pődör, 2013).

According to SHERMAN, one of the most respected experts in research on hotspots, a time interval of at least one year should be examined in relation to the

hotspot and its surroundings, and his opinion, we can talk about a hotspot if the crime rate in an area is at least six times higher than in the surrounding areas (Spelman, 1995). Hotspots are usually marked in red (Figure 1).

Taking into account various definitions in the literature, Szabolcs Mátyás defined the concept of a hotspot as follows:

> *We understand it as a relatively small area (e.g., block, shopping center, street) whose crime rate is higher than the average for its environment for a longer period. There is no exact definition of the area of a hotspot, the duration of the above-average infection rate, and the extent of the difference from the environmental average. A hotspot is the opposite of a cold spot.* (Mátyás, 2019b, p. 206)

4.4.1. The Cold Spot

There are also areas where the crime rate is much lower than the environmental average. These areas are called cold spots. They are usually marked in blue. The same questions arise in the case of cold spots as in the case of hotspots (size, duration, intensity, etc.), but there is no unified position in the literature on these issues. Research into cold spots is relatively rare due to the fact that an area with a low crime rate promises less spectacular research results than a hotspot (Figure 1).

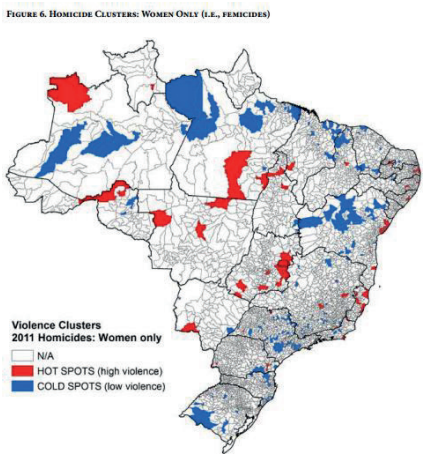


Figure 1. Homicide clusters in Brazil – Hotspots (red) and cold spots (blue) (Cawley, 2014)

4.5. Main Characteristics of Hotspot Policing

Human labour is increasingly valued, and the public increasingly expects law enforcement agencies to operate as efficiently as possible, that is, to ensure the protection of public order and public safety at an increasingly high level with as few people and as few resources as possible (Braga & Bond, 2008). This was the fundamental principle that gave rise to numerous policing strategies in the past few decades; which was no different in the case of hotspot policing.

The development of hotspot policing was facilitated by the technical advancements that occurred over the past three decades, as well as the growing interest in the field of criminology, which drew attention to the importance of 'place'. The development of computers and the emergence of analytical programmes enabled the conduct of much more detailed analyses than previously possible.

The development of hotspot policing was mainly influenced by 'place-based' policing strategies and criminological trends:

- Rational choice theory
- Routine activity theory
- Environmental criminology (National Institute of Justice n.d.) (see: Chapter 5)

The basic goal of hotspot policing is to make the most efficient use of limited resources and to determine patrol routes optimally. The policing strategy assumes that if the number of crimes in hotspots, the most affected areas, is reduced, then the volume of crime in a given settlement as a whole can also be reduced. Hotspot policing was first applied in the United States of America, where it is currently one of the most widely used policing strategies (National Institute of Justice, n.d.).

Hotspot policing, is defined by Szabolcs Mátyás as

> *a policing strategy developed after the recognition of hotspots, which aims to reduce the crime infection of the affected area proactively. One of the key elements of the strategy is to ensure an increased, demonstrative police presence.* (Mátyás, 2019c, p. 207)

4.6. The Problem of Covering a Hotspot

Hotspot policing is mainly based on the criminological principals that the distribution of crimes is uneven in space and time, but there are areas where the rate of crimes is well above average. One of the basic theses of hotspot policing is that crimes will only occur in above-average numbers where a criminal act has already been committed (Perry et al., 2013). The central issue is the delimitation of the hotspot area. If the hotspot is too small, areas that could be relevant may be left out of the analysis. If, on the other hand, it is too large, it will be difficult to cover the area effectively from a policing perspective (it is difficult to distribute the available forces and means with appropriate efficiency) (Lippai – Csatári, 2022). In the case of hotspot policing, one of the key issues is to define the area of hotspots as precisely as possible, for which there is currently a lot of software available.

Sources dealing with the subject usually mention the following four hotspot coverage techniques:

1) Grid mapping,
2) Covering ellipses,
3) Kernel density estimation,
4) Heuristic model.

1) During GRID MAPPING, the map is covered with square grids, which is technically relatively simple to solve, but the boundaries of the grids do not follow the boundaries of crime-infested areas in most cases.

> *A method for resolving an unequal area in which a standard-sized grid is used for analysis. The analyst begins by placing an artificial grid (generated by the GIS) on top of the area of interest and then uses graduated-color shading classifications to show different levels of crime.* (Santos, 2017, p. 610)

Grid mapping can be classified as one of the easiest hotspot covering techniques because the neuralgic areas are covered with square grids. On the other hand, the disadvantage is that the lines of the square grids usually do not follow the lines of the streets, so the covered area (hotspot) can be smaller or even larger than in reality.

2) The areas in question are covered with an elliptical flat shape, which is a relatively simple covering technique; however, as with grid mapping, the disadvantage of such COVERING ELLIPSES is that the covered areas do not always follow the hotspot area precisely.

3) KERNEL DENSITY ESTIMATION requires deeper GIS knowledge than the abovementioned techniques. Kernel density estimation is not only used in crime sciences but can also be used in many areas of life, for example, in economics for market analysis. In the case of crimes, they try to identify the places where the crime infestation (density) is the most intense, and then, moving away from this, we find decreasing values. Areas with decreasing infection values may still be part of the hotspot, as their infection levels may still be above the environmental average (Figure 2).

4) Among the hotspot coverage techniques, the most frequently employed is the so-called HEURISTIC MODEL. The word is of Greek origin and means 'I find, discover'. A police officer 'finds out' the area of a hotspot and 'leads themself' to where they need to take action. After a few years of service, they already have a good sense of how to identify the places where crimes are most likely to be committed. They know and are familiar with the temporal and spatial

characteristics of hotspots (for example, riots and assaults are likely on certain streets on Friday and Saturday nights, and robberies are typical on other streets). Based on this, the hotspots can be identified without any kind of geospatial analysis, although a software analysis allows a more thorough identification.

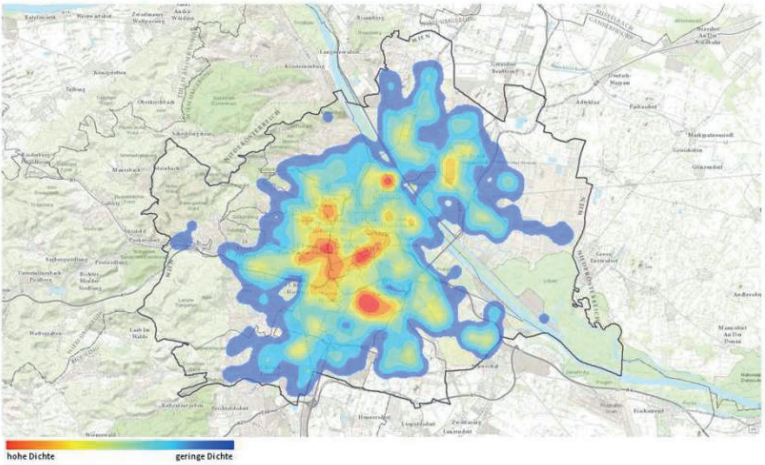


Figure 2. Heat map (Kernel Density Analysis) – Burglary in Vienna (Created by Austrian police crime mapping system)

4.7. Practical Aspects of Hotspot Policing

The common feature of the different policing strategies is that each of them – albeit in another way than the previous ones – wanted to achieve a crime reduction (Christián, 2015). Hotspot policing aims to reduce the number of crimes differently to previous policing strategies. Thanks to the spread of GIS software, the new kind of strategy has become a widely used method worldwide. Analysis programmes have enabled more thorough analysis than before, and hotspots can be delineated much more precisely. The prominence of place-based research has facilitated the success of hotspot policing. In this connection, two

policing strategies and one criminological part should be mentioned, which significantly impacted the novel theory: rational choice theory, routine activity theory (Cohen & Felson, 1979), and environmental criminology (Cornish & Clarke; 1986; National Institute of Justice, 2013).

There have been many experiments on the effectiveness of hotspot policing, most of them in the United States. These experiments sought to find the optimal patrol time that is sufficient to reduce the number of crimes (Braga & Bond, 2008). Among other things, experiments in this direction were carried out in Minneapolis (Koper, 1995) and Sacramento (Braga & Bond, 2008). It has been determined that a minimum of ten minutes of patrol time is required in a given hotspot area; the optimal patrol time was found to be between 11 and 15 minutes (Figure 3). The basic principle of hotspot policing is place-based, as opposed to previously used person-based policing techniques. In other words, they do not monitor specific persons, but patrollers have to stay in clearly visible places for 11-15 minutes and communicate with the residents. Patrolling should be repeated randomly, which increases the subjective sense of security of the population (since they regularly see the police) and deters criminals from committing crimes (since they know that patrols can appear in the area of a given hotspot at any time).

We should point out that hotspot policing is less popular in most other countries. Instead of hotspot policing (based on hotspot knowledge), many countries have used data-driven predictive policing since the early 21st century (Tompson, 2022).

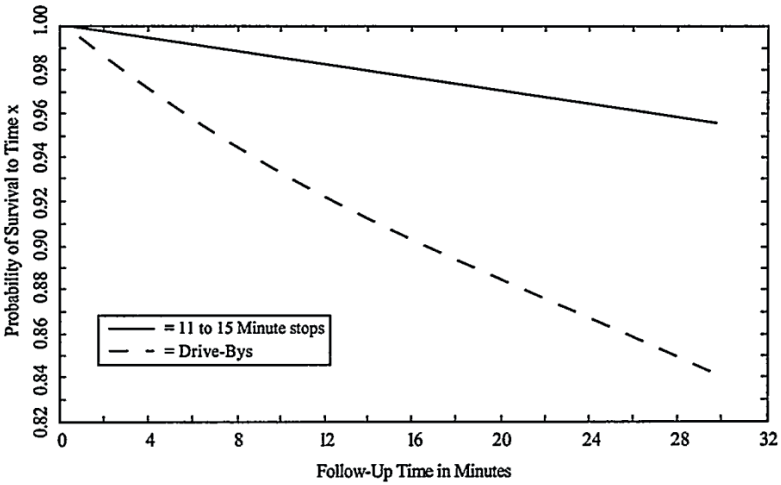


Figure 3. Log-Normal Survival Curves for Drive-Bys and 11- to 15-Minute Stops
(Coper, 1995, p. 666)

4.8. Classification of Hotspots

One of the primary tasks of hotspot policing is to provide an adequate response to various policing challenges. As mentioned above, hotspots are not uniform (they are different from each other); they change in time and space, meaning that law enforcement agencies must provide a variety of responses to illegal acts occurring in different types of hotspot.

There are several classifications of hotspots, one of the best known of which is the classification created by Jerry H. Ratcliffe, which categorises hotspots based on both spatial location (scattered, clustered, point-like) and temporal distribution (diffuse, focused, acute) (Table 1). Based on this, Ratcliffe distinguishes nine types of hotspot, each of which requires different police measures. One of the main merits of Ratcliffe's typology is that it examined not only the spatial extent but also the temporal dimension (Ratcliffe, 2004).

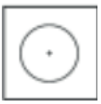
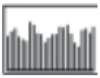
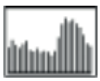
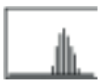
Policing Hotspot Matrix		Spatial: Dispersed 	Spatial: Clustered 	Spatial: Hotpoint 
Temporal	Diffused 	Uniform vehicle patrols, architectural changes, public education campaign	Random breath tests, foot patrols, architectural changes, publicity campaign	Roadblocks, plain clothes patrols, random breath tests, private security, CCTV
	Focused 	Uniform vehicle and foot patrols, improved lighting, public education campaign	Vehicle and foot patrols, random breath tests, private security, improved lighting	Surveillance units, plain clothes foot patrols, CCTV, surveillance of entry/exit points
	Acute 	Unmarked vehicle patrols, private security, improved lighting	Surveillance and plain clothes patrols, CCTV	Surveillance, arrest squads, CCTV, unmarked police units

Table 1: Ratcliffe's matrix of police measures

(Ratcliffe, 2004, p. 17)

References

BRAGA, A. A. & BOND, J. B. (2008). Policing crime and disorder hot spots: A randomized controlled trial. *Criminology*, 46(3), pp. 577-607. (https://cebcp.org/evidence-based-policing/what-works-in-policing/research-evidence-review/hot-spots-policing/)

CAWLEY, M. (2014). Mapping Brazil's Homicides at the Micro Level. *InSight Crime* (https://insightcrime.org/news/analysis/brazil-homicide-map-micro-level/)

CHRISTIÁN, L. (2015). Rendészeti politika [Law enforcement politics]. MTA Társadalomtudományi Kutatóközpont, Budapest

COHEN, L. E. & FELSON, M. (1979). Social Change and Crime Rate Trends – A Routine Activity Approach. *American Sociological Review*, (44), pp. 588-608.

CORNISH, D. & CLARKE, R. V. (1986). The Reasoning Criminal: Rational Choice Perspectives on Offending. Springer-Verlag, Hague

KOPER, C. S. (1995). Just enough police presence: reducing crime and disorderly68ravelledr by optimizing patrol time in crime hotspots. *Justice Quarterly*, 12(4)4, 649-672. (https://doi.org/10.1080/07418829500096231)

LIPPAI, ZS. & CSATÁRI, K. (2022): A budapesti Gozsdu-udvar rendezvényei biztosításának magán és közbiztonsági aspektusai [Private and Public Security Aspects of Event Management in Budapest's Gozsdu Courtyard]. In: Szabó, A. – Zsámbokiné Ficskovszky, Á. (eds.) Válsághelyzetek hatása a pénzügyi és rendvédelmi szektorra: tanulmánykötet Dr. Szendi Antal 60. születésnapjára. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, pp. 108-123. (https://doi.org/10.37372/mrttvpt.2022.1.8)

MÁTYÁS, SZ. (2019a). Bűnözési térkép [Crime map]. In: Boda J. (ed.). *Rendészettudományi Szaklexikon*. Ludovika Kiadó, Budapest (https://real.mtak.hu/153920/1/743_Rendeszettudomyanyi_Szaklexikon_e_2020_04_28_.pdf)

MÁTYÁS, SZ. (2019b). Forró pont [Hot spot]. In: Boda J. (ed.). *Rendészettudományi Szaklexikon*. Ludovika Kiadó, Budapest

MÁTYÁS, SZ. (2019c). Forró pontos rendészet [Hotspot policing]. In: Boda J. (ed.). *Rendészettudományi Szaklexikon*. Ludovika Kiadó, Budapest

MÁTYÁS, SZ. (2024). *Crime Geography*. University of Oradea, Oradea (https://real.mtak.hu/204407/1/Crime_Geography_MatyasSzabolcs.pdf)

NATIONAL INSTITUTE OF JUSTICE (n.d.). Practice Profile Hot Spots Policing (https://www.crimesolutions.gov/PracticeDetails.aspx?ID=8)

PERRY, L. W., MCINNIS, B., PRICE, C. C., SMITH, C. S. & HOLLYWOOD, S. J. (eds.) (2013). *Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation, Los Angeles

PŐDÖR, A. (2005). Térinformatikai alapú bűnözési térképek alkalmazása a helyi bűnmegelőzési stratégia kidolgozásában [Application of GIS-based crime maps in the development of local crime prevention strategies]. (XV. Országos Térinformatikai Konferencia előadása) (www.otk.hu/cd05/4szek/PdrAndrea.htm)

PŐDÖR, A. (2007). A térinformatika alkalmazásának elvi lehetőségei az önkormányzati bűnmegelőzési stratégia kialakításában [Theoretical possibilities of applying GIS in the development of local government crime prevention strategies]. In: MÁRKUS B. (ed.). *Földméréstől a geoinformatikáig: 45 éves a GEO*. Nyugat-magyarországi Egyetem Geoinformatika Kar, Székesfehérvár, 275-286.

PŐDÖR, A. (2013). Kartogramok alkalmazásának vizsgálata bűnügyi adatok példáján [Examining the application of cartograms using the example of criminal data]. In: LÓKI J. (ed.). Az elmélet és a gyakorlat találkozása a térinformatikában IV. Térinformatika Konferencia és Szakkiállítás. Debreceni Egyetemi Kiadó, Debrecen, 310-322.

RATCLIFFE, J. H. (2004). The Hotspot Matrix: A Framework for the Spation-Temporal Targeting of Crime Reduction. *Police Practice and Research*, 5(1), 5-23. (DOI: 10.1080/1561426042000191305)

SANTOS, R. B. (2017). Crime Analysis with Crime Mapping. Sage Publication

SHERMAN, W. L., GARTIN, R. P. & BUERGER, E. M. (1989). Hotspots of Predatory Crime: Routine Activities and the Criminology of Place. *Criminology*, 27(1), 27-55. (https://doi.org/10.1111/j.1745-9125.1989.tb00862.x)

SPELMAN, W. (1995). Criminal Careers of Public Places. In: ECK, John & WEISBURD, David (eds.). Crime and Place. Crime Prevention Studies 4. Monsey, Criminal Justice Press. 115-144.

TOMPSON, L. (2022). Crime Mapping and Policing. Criminology and Criminal Justica (https://doi.org/10.1093/acrefore/9780190264079.013.735)

UNGER, J. (1994). Bevezetés a térképészetbe (Introduction to cartography). JATE Press, Szeged

Chapter 5
Theoretical Pillars of Prediction: Criminological Foundations of Law Enforcement Practice

Vince Vári

5.1. Introduction

One of the most significant innovations in 21st century law enforcement thinking is the emergence of predictive models, which offer the potential for data-driven crime prevention and targeted police intervention. However, predictive policing did not emerge in a vacuum; it is based on criminological theories dating back several decades that recognised specific crime patterns and the spatial and temporal concentration of crimes long before the era of algorithms.

This chapter aims to explore the criminological theoretical foundations of predictive policing, with a particular focus on how classical and contemporary theories, such as rational choice theory (Cornish & Clarke, 1985), routine activities theory (Cohen & Felson, 1979), and environmental criminology (Brantingham & Brantingham, 1981), inform this approach. Empirical research shows that crime does not occur randomly, but rather in a concentrated manner, linked to space, time, and social environment, which predictive tools can accurately model. The emergence of near repeat theory further underlines how algorithmic models are anchored in the empirical reality of crime clustering, allowing preventive policing to anticipate not only generic hotspots but dynamic shifts in risk after recent incidents (Farrell & Pease, 2017).

By reviewing the theoretical foundations of predictive policing, this chapter contributes to the understanding of the scientific basis of policing strategy. At the same time, it highlights that modern criminology not only seeks to interpret the processes of crime but is also capable of supporting active,

preventive interventions through data-driven decision-making. The following section presents the theoretical frameworks in detail, without which predictive models would remain mere technological innovations, lacking real criminological depth and social sensitivity (Krasnova 2025).

It is essential to note that predictive policing is not an independent, technocratic innovation, but rather a continuously evolving and adaptive intervention system grounded in the multifaceted theoretical and empirical findings of the field of criminology (Braga et. al., 2019).

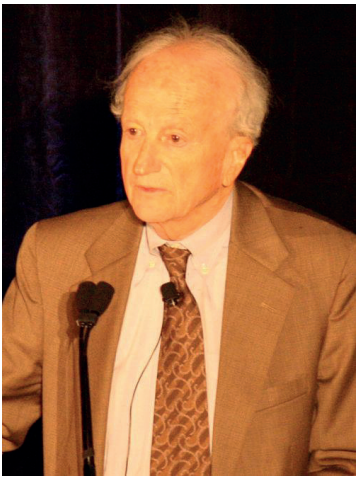
5.2. Criminological Theory Foundations of Predictive Policing

The theoretical basis of predictive policing integrates the results of several significant criminological trends. Below, we present the most important theories that define the scientific background of this strategy.

5.2.1. Rational Choice Theory

In 1992, GARY S. BECKER received the Nobel Prize for his work in developing theories that explain rational human behaviour (Becker, 1993). In it, he explains that humans always use their limited resources in the hope of achieving the most significant subjective benefit possible, which they can never fully attain, so they are constantly seeking alternative solutions (Lippai, 2023).

It is based on traditional economic decision theory and calculations of pleasure and pain. The aspect of criminal decision-making is the satisfaction of needs. The rational element is goal-oriented behaviour in crime, that is, the calculation of risks, efforts, benefits, and a cost-benefit analysis (decision-structuring factors) based on the number of targets, the possibility of profit, and



the risk of exposure. The 'criminal' acts just like everyone else does; this behaviour is essentially a criminal enterprise, where the entrepreneur takes on greater-than-average risk in the hope of relatively large profits. Before deciding to commit a crime, the same process takes place in a person as in an everyday routine situation, with the only difference being the goal to be achieved and the extent of the consequences.

Gary S. Becker (1930-2014) (URL1)

Proponents of rational choice theory, RONALD CLARKE and DEREK CORNISH, point out that there is a fundamental difference between committing a single crime and pursuing a life of crime, and that socialization and conditioned criminal patterns play a significant role, in which case the criminal model is chosen for the possibility of much smaller profits (Clarke & Cornish, 1985). Closely related to this theory is the theory of spatial and temporal displacement of crime, which can be observed as a function of better opportunities and risks.

Predictive policing is one of the most dynamically developing law enforcement approaches today, and it is closely based on rational choice theory. To understand this scientific connection, it is essential to examine the mechanisms of the two theories and their interaction.

According to rational choice theory, criminals do not commit crimes randomly; instead, they consciously weigh the potential benefits and risks. Individuals choose to commit crimes because the expected benefits outweigh the potential punishment or risk of being caught (Cornish & Clarke, 2014). Traditional crime prevention strategies, therefore, seek to increase the costs of

crime (e.g., increased surveillance, higher penalties), thereby reducing its appeal to offenders.

Predictive policing puts these principles into practice using advanced data mining, spatial, and temporal analysis technologies. The algorithms and statistical models used draw on historical crime data to identify patterns and predict where and when the risk of certain types of crime is likely to increase (Perry et al., 2013). This prediction enables police resources to be concentrated in areas where the risk of crime is highest. At the same time, it increases the risk of apprehension perceived by offenders in these temporal and spatial zones.

The essence of the scientific connection is that predictive policing systems are effective because they implicitly assume that crimes follow patterns that can be clearly defined in terms of time and space, which are shaped by the decisions of rational and calculating offenders. Suppose police presence is concentrated in locations and at times predicted to be risky. In that case, it increases the expected cost of committing crimes there, that is, it significantly influences the calculations of perpetrators. Thus, predictive policing is not only a technological innovation but also a practical application of criminological rationality (Brantingham & Brantingham, 1984; Townsley et al., 2016).

Empirical research supports this: where the concentration of police resources increases based on predictive analyses, there is a statistically verifiable decrease in the risk and frequency of crime (Mohler et al., 2015; Perry et al., 2013). Meanwhile, criminals adapt: if surveillance is increased in a given location, they choose another, less supervised location or time, according to rational choice theory. This is why it is essential to update predictive models and retrain patterns continuously.

Overall, the scientific basis of predictive policing is primarily provided by the strategies of rational choice theory. This relationship is key to the effectiveness

of crime prevention and law enforcement: a properly targeted, temporally and spatially optimised police presence can significantly reduce crime by increasing the risks for offenders. The success of the predictive system is therefore based on the assumption that crimes are calculable, as presupposed by rational choice theory.

5.2.2. Routine Activity Theory

According to the routine activity theory developed by LAWRENCE COHEN and MARCUS FELSON, a person motivated to commit a crime adapts to the opportunities that present themselves (Cohen & Felson, 1979). The triangle of crime consists of desire/need, ability, and opportunity, that is, the occasion. The goal is to keep the target and the perpetrator at a safe distance from each other.

Figure 1. Three conditions for crime (URL2)

Three minimum conditions must be met for a crime to occur. The first is the appropriate target, that is, something or someone who can become a victim or from whom something can be stolen, which can be one of three types: a person (victim or passive subject), an object (object of the crime), or a location (the scene of the crime or the scene of the offense). This has four characteristics: value, size, visibility, and accessibility. The second is the absence of suitable security/protection, that is, there should be no person present who can prevent or witness the crime. Protection can be formal

(e.g., security guards) or informal (e.g., neighbours). Examples of protection include police patrols, security guards, civil guards, doorkeepers, friends, neighbours, locks, fences, railings, lighting, security systems, or surveillance cameras. The third is the presence of a potential perpetrator who intends to commit the crime. The reasons for committing a crime may be need, poverty, or drug addiction. Factors that motivate the perpetrator include living in a social environment or culture where crime is accepted, significant peer pressure, a significant lack of education, unfavourable employment opportunities, or a disadvantaged family situation.

Examples of protection include police patrols, security guards, civil guards, doorkeepers, friends, neighbours, locks, fences, railings, lighting, security systems, and surveillance cameras. Third is the presence of a potential perpetrator who intends to commit the crime. The reasons for committing the crime may be need, poverty, or drug addiction. The perpetrator is motivated by living in a social environment or culture where crime is accepted, or where there is significant peer pressure, a significant lack of education, unfavourable employment opportunities, or a disadvantaged family situation. Becoming a perpetrator is also facilitated by perceptions or beliefs that certain crimes are permissible or acceptable, or by prejudice against minority/ethnic groups.

There is a deep conceptual and practical connection between predictive policing and Routine Activity Theory (RAT), which forms a foundational basis for contemporary crime prevention strategies. Routine Activity Theory was developed by Cohen and Felson (1979) with the fundamental premise that the occurrence of crime is not solely linked to the motivation of individuals, but also depends to a large extent on how everyday social life and collective activities are organised and repeated.

According to the theory, crime occurs when three critical components come together simultaneously: there is a motivated perpetrator, a suitable target,

and no suitable guard to prevent or hinder this encounter (Cohen & Felson, 1979). However, these components are not evenly distributed in space and time; instead, social routines, changes in location, events, and economic and social processes restructure the points of concentration of these factors. This creates recurring 'hubs' – such as routes to workplaces, transportation hubs, entertainment venues, or actual 'hotspots' – where the likelihood of crime increases dramatically (Oxford Research Encyclopaedia, 2021).

Predictive policing uses this theoretical basis when its algorithms analyse criminal, transportation, economic, and behavioural data to identify the times and locations where the three conditions are most likely to occur together. This methodology requires the routine analysis of past crime patterns, local socio-urban processes, and everyday movements, as these explain why crime is concentrated in a particular neighbourhood, period, and manner (Atlantis Press, 2018).

The practical benefit of predictive models is that they identify 'risk zones' in advance by analysing routine activities where the perpetrator, the target, and the absence of a guard coincide. By mapping these patterns, the police can allocate their resources (patrol pairs, camera systems, community watch) so that they are present in the places and at the times when the risk of crime is expected to be highest (Oxford Research Encyclopaedia, 2021; ABJournals, 2021). If the level of surveillance in a given space/time unit can be increased – for example, through the deployment of mobile patrols or targeted community prevention – the balance of the possible elements of an encounter is disrupted, thereby reducing the incidence of crime (Cohen & Felson, 1979).

Empirical research and case studies alike confirm that resource allocation based on predictive analysis has led to a significant reduction in crime in many cities, especially where law enforcement interventions have been tailored to the risk clusters generated by routine activities (Atlantis Press, 2018; ABJournals,

2021). Predictive policing is a modern, digital application of routine activity theory, seeking to prevent crime by systematically mapping repetitive movements, habits, and the use of social space in everyday life, thereby actively disrupting the simultaneous presence of structural conditions that are essential for crime.

The success and operational logic of predictive policing depend largely on knowledge of routine activity theory. The more complex the models are in revealing the fabric of social life – that is, the movement of actors, changes in space use, and the dynamic absence of surveillance – the more accurately they can predict and prevent crime waves (Oxford Research Encyclopaedia, 2021; Cohen & Felson, 1979; ABJournals, 2021).

5.2.3. Environmental Criminology

The development and theoretical background of predictive policing are closely related to the basic principles of environmental criminology. The central premise of environmental criminology is that crime does not occur randomly in space and time, but rather in a concentrated manner, influenced by environmental factors. The classic authors of the theory – mainly C. RAY JEFFERY and PAUL J. BRANTINGHAM and PATRICIA L. BRANTINGHAM – emphasise that understanding crime requires analysis of the physical, social, and infrastructural environment, its spatial structure, and its uses (Oxford Research Encyclopaedia, 2021).

The founders of environmental criminology and their main theories:

- As early as 1971, C. Ray Jeffery emphasised that the spatial and architectural environment of crime fundamentally influences the occurrence of crime. Jeffery coined the term 'environmental criminology,' emphasising that systematic analysis of the environment is essential for crime prevention (Jeffery, 1971, cited in Andresen, 2010).

- Paul J. Brantingham and Patricia L. Brantingham made outstanding contributions to the spread and deepening of environmental criminology. They are credited with the 'crime pattern theory,' which states that criminal events are determined by the 'routes' travelled daily by potential perpetrators, decision points, and the accessibility of targets (Brantingham & Brantingham, 1981).

- Modern predictive policing models apply the results of these classic theories in a digitised form based on data analysis. For example, the PredPol system, developed by Jeff Brantingham (son of Paul J. Brantingham), utilises machine learning to predict the likely locations and times of crimes based on past crime data and environmental characteristics. The RTM (Risk Terrain Modelling) theory is also based on the analysis of environmental factors and infrastructure, in line with the ideas of the Brantingham family.

- Environmental criminologists such as Gerben J. N. Bruinsma continue to play a leading role in expanding this field of literature, particularly in summarising international experiences in crime mapping, environmental risk analysis, and prevention (Figure 2).

The developers of RTM compare the space to be examined to a kaleidoscope, where the glass shards are the individual elements of the space. The dynamics of crime are not the same in different places (even for the same types of crime). The glass shards represent the characteristics of the space, the criminal attraction of individual elements.

Figure 2. A kaleidoscope of crime risk (URL3)

According to environmental criminology, certain local factors and elements of everyday routine, such as transport routes, public spaces, shops, parks, entertainment venues, and other places frequently visited by people, play a key role in the development of crime. Such environments, which favour the convergence of potential perpetrators, possible targets, and a lack of supervision (surveillance), form so-called 'criminogenic' fields. Environmental criminology explains the concept of hotspots from this structural perspective (Law Journal of St. Petersburg University, 2023). Predictive policing is linked to this theoretical framework in that it utilises advanced data collection and analysis techniques to identify environmental factors that contribute to crime.

Predictive policing is linked to this theoretical framework in that it utilises advanced data collection and analysis techniques to identify environmental conditions that lead to crime and their corresponding concentrations. Predictive algorithms analyse past crime, traffic, and social data to determine locations and times when crime rates are likely to spike. Modern models, such as Risk Terrain Modelling (RTM), integrate environmental risks, including poorly lit streets, deserted spaces, busy intersections, or high-value targets (Atlantis Press, 2018).

As a result, predictive policing can recommend preventive measures at the spatial (where), temporal (when), and environmental (under what conditions) levels. The principles of environmental criminology help the police to optimise their resources, for example, through targeted patrols, infrastructure development, or the use of surveillance techniques, not randomly, but in response to crime hotspots and dangerous periods.

Predictive policing, therefore, actively applies the perspective of environmental criminology, viewing crime as the result of the convergence of place, time, perpetrator, and target, which the conscious shaping and monitoring of the natural and built environments can significantly influence. International research emphasises that such methodological investments not only lead to a

short-term reduction in crime but also a longer-term reduction in risk if the criminogenic role of the given environmental conditions ceases or is significantly reduced (Oxford Research Encyclopaedia, 2021; Atlantis Press, 2018).

5.2.4. The Near Repeat Theory

Exploring the spatial and temporal patterns of crime is one of the fundamental methodological and theoretical challenges of criminology. Since the late 1990s, considerable emphasis has been placed on examining the fact that the distribution of crimes is not random in either space or time, but instead shows clustered, so-called 'hotspot' patterns (Johnson et al., 1997; Bowers & Johnson, 2004). These findings are closely related to the theories of repeat victimisation and near repeat. These findings are closely related to the theories of repeat victimisation and near repeat. While the former emphasises the risk of repeated victimization, the near repeat theory focuses on the greater likelihood of similar crimes being committed nearby in both time and space.

According to Bowers and Johnson's (2004, p. 63) classic summary:

> *Victimization at a given location increases the risk of further victimization at the same and nearby locations for a limited period following the initial offense.*

It follows that after a crime committed in a given area – mainly burglary, car theft, street robbery – a period of exceptionally high risk begins, during which the location and its immediate vicinity become vulnerable (Rasmusson, 2020). The theory explains why crime waves can spread rapidly between so-called micro-places and how this knowledge can be exploited for crime prevention.

The near-repeat phenomenon is primarily based on theories that examine the behaviour and decisions of criminals. After a successful crime, perpetrators often return to familiar areas, as their strategies have already proven effective there and they have gained valuable information about local conditions (Farrell &

Pease, 2017). Not only the property in question, but also neighbouring houses, become increasingly vulnerable, for example, because the perpetrators are already familiar with escape routes and the area's degree of vulnerability. This location-based, repetitive targeting process is a logical explanation for the spatial and temporal accumulation of crimes (Johnson et al., 1997).

Predictive policing systems, which leverage the tools of mathematical sociology, geographic information systems (GIS) (Mátyás, 2017), and Big Data-based analysis, hold the potential to identify future high-risk periods and areas based on past crime data (Hälterlein, 2021; Haberman & Ratcliffe, 2012). These predictive algorithms, primarily based on the near-repeat theory, offer a ray of hope as they can predict the highest probability of a subsequent crime at points closest to past incidents. The key advantage of predictive analysis is its flexibility and dynamism, unlike general, static hotspot identification. It focuses on the period following a 'fresh' crime, allowing for the more intelligent allocation of police resources, as emphasised by Bowers & Johnson (2004, p. 63).

In international practice, several innovative systems have been developed along these lines, such as PRECOBS in Germany and the PredPol and HunchLab algorithms in the United States. These software programmes display risk zones on maps that are updated daily or even hourly, automatically evaluating the location and time of reported crimes (Piza & Carter, 2021; National Policing Institute, 2018). The National Policing Institute (2018, p. 1) emphasises that*:*

> *Officers can be directed to at-risk areas, which can deter potential offenders and prevent subsequent crimes.*

The work of police patrols can thus be assuredly optimised in a data-driven manner: duty planning becomes more targeted, while preventive measures – such as patrolling, issuing warnings, and community counselling – can also be deployed where they are most effective.

However, incorporating the near repeat theory into predictive policing tools is not merely a technical or organisational issue, but also raises serious social and ethical considerations. Hälterlein (2021, p. 3) critically notes:

> *The predictive policing approach relies heavily on statistical patterns that may not always account for changing offender behavior or local context.*

The reliability of these methods is affected when offenders adapt or when past trends quickly become obsolete due to socio-economic changes (Tihanyi et al. 2024). It is also important to note that over-surveillance of a community can be a source of disproportionate intervention or even mistrust (About: Intel, n.d.). These potential negative implications underscore the need for careful implementation and monitoring of predictive policing tools.

It's important to note that predictive models often provide accurate estimates only over a relatively short time window; the near-repeat effect typically comes into play in the days or weeks following the crime (Rasmusson, 2020). This caution is necessary to ensure that the potential of predictive policing is not overestimated and that its limitations are fully understood and considered in its implementation. Based on experimental studies, it can be proven, particularly in the case of burglaries, that crime waves tend to develop during the first 3-7 days. Therefore, law enforcement agencies must respond quickly and in a targeted manner, using predictive analytics, if they wish to achieve meaningful prevention.

In addition to methodology, the quality of data, the transparency of predictive algorithms, and the integration of local knowledge (e.g., local knowledge, community relationships) into analytics are also subjects of debate (Hälterlein, 2021). The literature emphasises that predictive models can only be truly effective if they combine statistical and machine learning results with classical, experiential policing knowledge and knowledge of the local context (Farrell & Pease, 2017; National Policing Institute, 2018). Piza (2021) also

emphasises that only a combination of robust, up-to-date data, feedback from citizens, and flexible, situation-dependent responses can result in sustainable crime prevention.

In summary, the theoretical and empirical basis of the near-repeat theory is indispensable in today's predictive policing practice. Without data-driven, prediction-based decision support, crime prevention would remain largely reactive and random. At the same time, scientific research and practical experience suggest that the key to success lies in speed, social sensitivity, and a dynamic interpretation of the local context (Bowers & Johnson, 2004; Hälterlein, 2021; Farrell & Pease, 2017). As the literature states: 'Understanding near repeats allows for the more intelligent allocation of police resources' (Bowers & Johnson, 2004, p. 63), but only if the models are applied responsibly, critically, and based on local cooperation.

5.3. Summary

In this chapter, I have aimed to share the foundational theories surrounding predictive policing within the field of criminology, emphasising that this innovative model for crime prevention extends beyond mere technological advancements. It is deeply interconnected with both classical and contemporary criminological paradigms. I firmly believe that the rationale behind predictive tools, particularly algorithmic models, is rooted in established scientific frameworks such as rational decision theory, routine activity theory, and environmental criminology.

I have thoroughly explored how these theories provide vital insights into the spatial and temporal patterns of crime. Importantly, I have illustrated how they inform law enforcement practices, demonstrating that strategic police presence can indeed predict and help mitigate criminal activity. My arguments are fortified not only by theoretical perspectives but also by findings from

international empirical research. Studies showcase that the methodology of hotspot policing, especially when enhanced by community-oriented and problem-oriented policing strategies, effectively reduces crime rates. A significant takeaway from this research is the revelation that crime does not occur at random in urban environments; rather, it clusters in identifiable hotspots, presenting excellent opportunities for proactive police intervention.

A practical extension of these theoretical underpinnings is provided by the near repeat phenomenon, which highlights that, following a criminal incident, neighbouring places and periods display a temporarily heightened risk for similar events. This concept further supports the notion that crime patterns are not random but emerge based on recognizable spatial and temporal logic, offering a scientific basis for dynamic risk mapping and targeted responses within predictive policing frameworks.

Furthermore, international meta-analyses and case studies reveal that implementing hotspot policing strategies leads to statistically significant reductions in crime, particularly when community engagement and problem-solving approaches are integrated. This underscores the importance of acknowledging that crime is influenced not just by the perpetrator's intentions but also by a myriad of social, environmental, and regulatory factors.

The success of predictive models hinges on their ability to accurately interpret and operationalise the theoretical variables that underlie crime risk. These models make informed predictive decisions by considering elements of rational behaviour, typical movement patterns, environmental hotspots, and social dynamics. Moreover, the effectiveness of these systems is closely tied to the depth of collaboration among diverse disciplines.

A pivotal conclusion of this chapter is that the advancement and implementation of predictive models must occur through interdisciplinary

collaboration. Relying solely on IT expertise is inadequate; it is essential for criminologists, legal experts, sociologists, and practitioners in law enforcement to work hand in hand. It's also important to highlight that predictive technologies are designed to enhance, rather than replace, police discretion. Their fundamental goal is to strengthen human judgment through a scientifically sound approach that optimises intervention in both time and space.

Ultimately, predictive policing is deeply rooted in criminological theories, and its practical and sustainable application depends on skilfully merging algorithmic logic with social science insights and ethical considerations. By fostering this integration, we can pave the way for a more effective and considerate approach to crime prevention.

References

ABJOURNALS (2021). Predictive policing and risk mapping in urban environments. *African Business Journals* (https://www.abjournals.org)

ANDRESEN, M. A. (2010). *Environmental criminology: Evolution, Theory, and Application*. Routledge

ATLANTIS PRESS (2018). Application of predictive policing in crime prevention. Proceedings of the International Conference on Social Science and Humanities (https://doi.org/10.2991/icssh-18.2018.1)

BECKER, G. S. (1993). Nobel lecture: The economic way of looking at behavior. *Journal of Political Economy*, 101(3), pp. 385-409. (https://doi.org/10.1086/261880)

BOWERS, K. J. & JOHNSON, S. D. (2004). Who commits near repeats? British *Journal of Criminology*, 44(1), pp. 63–82. (https://doi.org/10.1093/bjc/44.1.63)

BRAGA, A. A., WEISBURD, D. & TURCHAN, B. (2019). Focused deterrence strategies and crime control: An updated systematic review and meta-analysis of the empirical evidence. *Criminology & Public Policy*, 17(1), pp. 205–250. (https://doi.org/10.1111/1745-9133.12353)

BRANTINGHAM, P. J. & BRANTINGHAM, P. L. (1981). *Environmental Criminology*. Waveland Press

BRANTINGHAM, P. J. & BRANTINGHAM, P. L. (1984). *Patterns in Crime*. Macmillan

CLARKE, R. V. & CORNISH, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry & N. Morris (eds.). *Crime and justice: An annual review of research*. (6), 147-185. University of Chicago Press, Chicago

CLARKE, R. V. & CORNISH, D. B. (2014). Rational choice theory. In: G. Bruinsma & D. Weisburd (eds.). *Encyclopedia of Criminology and Criminal Justice*. Springer, 4215-4222. (https://doi.org/10.1007/978-1-4614-5690-2_561)

COHEN, L. E. & FELSON, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), pp. 588–608. (https://doi.org/10.2307/2094589)

FARRELL, G. & PEASE, K. (2017). Preventing repeat and near repeat crime concentrations. In: S. G. Lab & C. Fisher (eds.). *Handbook on Crime Prevention and Community Safety*. Routledge (https://api.pageplace.de/preview/DT0400.9781317530824_A29696720/preview-9781317530824_A29696720.pdf)

HABERMAN, C. P. & RATCLIFFE, J. H. (2012). The Predictive Policing Challenges of Near Repeat Armed Street Robberies. *Policing: A Journal of Policy and Practice*, 6(2), pp. 151–167. (https://academic.oup.com/policing/article/6/2/151/1528334)

HÄLTERLEIN, J. (2021). Epistemologies of predictive policing: Mathematical social science and the politics of prediction. *Big Data & Society*, 8(1) (https://journals.sagepub.com/doi/abs/10.1177/20539517211003118)

JEFFERY, C. R. (1971). *Crime Prevention through Environmental Design*. Sage, Beverly Hills

JOHNSON, S. D., BOWERS, K. J. & HIRSCHFIELD, A. (1997). New Insights into the Spatial and Temporal Distribution of Repeat Victimisation. *British Journal of Criminology*, 37(2), pp. 224–241. (https://academic.oup.com/bjc/article/37/2/224/396423)

LAW JOURNAL OF ST. PETERSBURG UNIVERSITY (2023). Hotspot policing and environmental risk modeling. Law Journal of SPU, 39(1), 55-73.

KRASNOVA, A. K. (2025): Personal safety and criminal liability for murder in Russian and Hungarian legislation. Bulletin of Economics, Management and Law, 18(3), 40-45.

LIPPAI, ZS. (2023): A biztonság megteremtésének és fenntartásának állami és nem állami szereplőiről. Belügyi Szemle, 71(8), pp. 1391-1417. (https://doi.org/10.38146/BSZ.2023.8.4)

MÁTYÁS, SZ. (2017). A térinformatika rendészettudományi alkalmazásának lehetőségei [Possibilities of geographic information systems applications in law enforcement science]. In: Boda, J., Felkai, L., Patyi, A. (eds.) *Ünnepi kötet a 70 éves Janza Frigyes tiszteletére = Liber amicorum in honorem Friderici Janza septuagenarii*. Dialóg Campus Kiadó, Budapest, 371-377.

MOHLER, G. O., SHORT, M. B., MALINOWSKI, S., JOHNSON, M., TITA, G. E., BERTOZZI, A. L. & BRANTINGHAM, P. J. (2015). Randomized Controlled Field Trials of Predictive Policing. Journal of the American Statistical Association, 110(512), pp. 1399–1411. (https://doi.org/10.1080/01621459.2015.1077710)

NATIONAL POLICING INSTITUTE (2018). Tackling Near Repeat Crime. Strategy Brief (https://www.policinginstitute.org/wp-content/uploads/2018/07/REVISED-FINAL-Strategy-Brief_12.6.pdf)

OXFORD RESEARCH ENCYCLOPAEDIA (2021). Routine activity theory and spatial criminology (https://oxfordre.com/criminology/)

PERRY, W. L., MCINNIS, B., PRICE, C. C., SMITH, S. C. & HOLLYWOOD, J. S. (2013). Predictive policing: The role of crime forecasting in law enforcement operations. RAND Corporation (https://www.rand.org/pubs/research_reports/RR233.html)

PIZA, E. & CARTER J. (2021). An Analysis of Residential Burglary and Motor Vehicle Theft. *CrimeRxiv* (DOI:10.21428/cb6ab371.e1ec4277)

RASMUSSON, M. (2020). The Relationship between Near-Repeat Street Robbery Patterns and Opportunity Theory. ISPRS International Journal of Geo-Information, 9(4), 188. (https://www.mdpi.com/2220-9964/9/4/188)

TIHANYI, M., VÁRI, V. AND KRASNOVA, K.A. (2024). Ethics of Sin and Punishment. Kutafin Law Review. 11(4), 741–760, doi: 10.17803/2713-0533.2024.4.30.741-760

TOWNSLEY, M., JOHNSON, S. D., & RATCLIFFE, J. H. (2016). Space-time dynamics of crime. In: G. Bruinsma & D. Weisburd (eds.). *Encyclopedia of Criminology and Criminal Justice. Springer,* pp. 5156-5166. (https://doi.org/10.1007/978-1-4614-5690-2_105)

URL1: https://commons.wikimedia.org/wiki/File:GaryBecker-May24-2008.jpg

URL2: https://en.wikipedia.org/wiki/Routine_activity_theory

URL3: http://www.riskterrainmodeling.com/about.html

Chapter 6
Predictive Policing in the Age of Artificial Intelligence

Endre Nyitrai

6.1. The Structure and Central Areas of Artificial Intelligence

Data science and artificial intelligence (AI) are having a significant impact on forensics, and therefore on criminal investigations. Data science is a relatively new discipline. It analyses and interprets large data sets to examine the current situation, uncover anomalies, illuminate relationships, model complex systems, and make predictions about future events. (Pál & Iványi, 2024, p. 113) Furthermore, through the use of IoT devices and online activities, users generate a massive amount of data (Bzai et al., 2022).

Artificial intelligence can provide fast and efficient assistance in processing the large amount of data generated in this way. Artificial intelligence also plays a crucial role in the implementation of predictive policing systems that utilise pattern recognition to forecast the location and timing of crimes, while data mining combines information from diverse, complex sources.

The above data analysis procedures form the core of predictive policing, as the temporal and spatial distribution of crimes can be predicted based on the patterns revealed in this way.

6.1.1. The Concept and Interpretation of Artificial Intelligence

There are several different definitions of AI. According to Dobó and Gyaraki:

> *AI refers to the human-like capabilities of machines, such as reasoning, learning, planning, and creativity. AI enables technology to sense its environment, act on what it*

> *perceives, solve problems, and plan its actions to achieve a specific goal.* (Dobó & Gyaraki, 2021, p. 67)

According to the European Commission,

> *artificial intelligence refers to systems that display intelligent behaviour, analyse their environment and take action, with a certain degree of autonomy, to achieve specific goals.* (European Commission, 2018)

The Commission divides AI-based systems into two groups:

1.) exclusively software-based systems that operate in the virtual world (such as voice assistants, image analysis software, search engines, voice and facial recognition systems);
2.) AI that can also be embedded in hardware devices (such as advanced robots, autonomous vehicles, drones, and applications related to the Internet of Things). (European Commission, 2018)

6.1.2. Types of Machine Learning and the Role of Deep Learning

In his study, Sztanek highlights that machine learning is the primary driving force behind AI technology today, utilising statistical methods to develop intelligent systems. According to the survey, the essence of machine learning algorithms is that they learn from data without programming and can automatically build a knowledge base. They are also able to recognise patterns from available data and experience without receiving detailed instructions (Sztanek, 2024, pp. 213-214).

Figure 1 clearly illustrates the connection and relationship between machine learning and deep learning within the field of artificial intelligence.

The three main types of machine learning are supervised learning, unsupervised learning, and reinforcement learning, the latter of which is based on rewarding desired behaviours and punishing undesirable ones. (Hajdú et al, 2024, pp. 173-174) The goal of a supervised learning algorithm is to learn the mapping between inputs and outputs, enabling it to generalise to previously unseen data. In contrast, an unsupervised learning algorithm works solely with input data, lacking output labels (URL1). Within this, deep learning is a special subcategory of machine learning (Afsaneh et al., 2022).

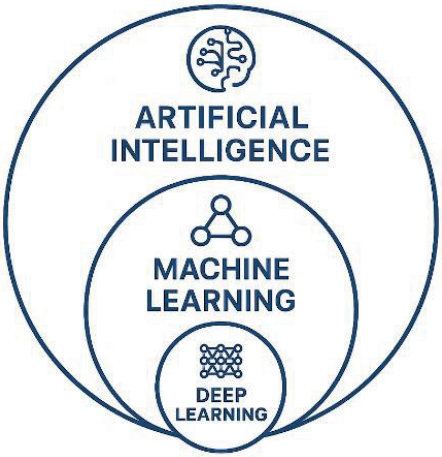


Figure 1. Artificial Intelligence, Machine Learning, and Deep Learning
(*Source: Generated collaboratively by Endre Nyitrai and OpenAI's DALL·E 3 via ChatGPT, on July 22, 2025*)

Crucial for predictive policing is the ability of deep learning to continuously improve prediction accuracy, adapting to changing crime patterns. The types of machine learning and the connection to deep learning are well illustrated in Figure 2 below.

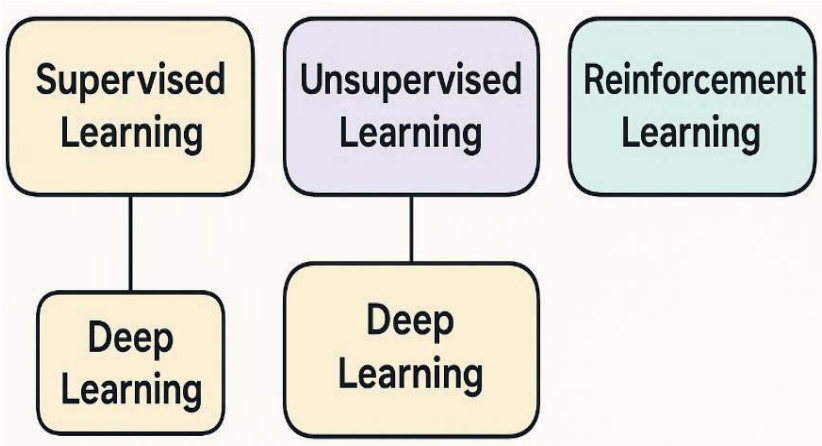


Figure 2. Types of machine learning and their relation to deep learning
(*Source: Generated collaboratively by Endre Nyitrai and OpenAI's DALL·E 3 via ChatGPT, on July 22, 2025*)

One of the defining branches of artificial neural networks is deep learning, also known as deep neural networks. (Németh & Virágh, 2022, p. 5) Deep learning enables us to interpret complex, unstructured data, which is achieved through the use of neural networks (Vargas et al., 2018). Neural networks model the functioning of the human brain, enabling computers to perform complex tasks such as language processing. (Pál & Iványi, 2024, p. 113)

6.2. Characteristics and Operation of Generative Artificial Intelligence

To develop generative AI, deep learning is used to extract multi-layered features from input data. The basic models trained in this way, when adapted to specific tasks, are then incorporated into products and services (URL2).

6.2.1. Main Application Areas of Generative Artificial Intelligence

The main types of generative artificial intelligence are the following, as illustrated in Figure 3 (URL2).

- Text Generation AI
- Image Generation AI
- Audio Generation AI
- Video Generation AI
- 3D Model Generation AI

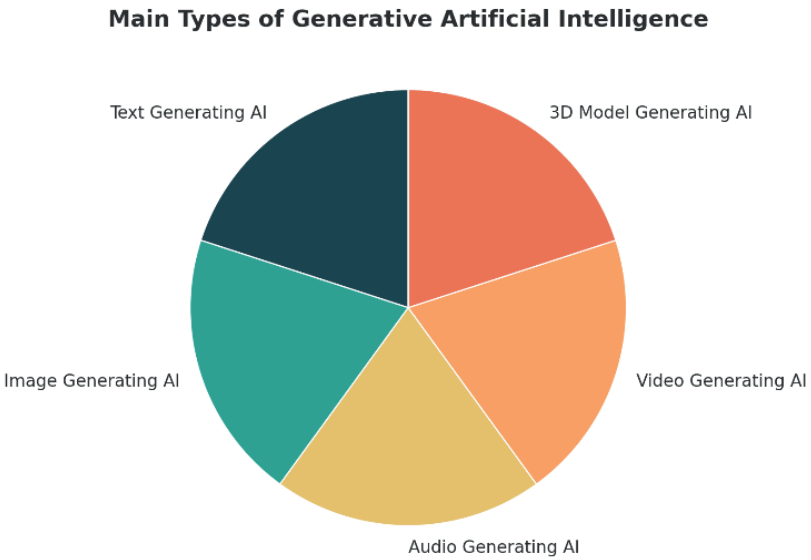


Figure 3. Main types of generative artificial intelligence (Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT, on July 22, 2025)

Generative AI is an AI model that creates new content, such as written text, audio, images, or video. (URL3) Generative AI uses deep learning to analyze large amounts of data and create innovative content (URL4).

6.2.2. Application of Generative Artificial Intelligence in Forensics

Texts generated by artificial intelligence support predictive policing by enabling rapid analysis through the automatic summarization of investigative data.

Documents and analyses created with generative artificial intelligence can assist in criminal investigations. The resulting forensic text content can contribute to the acquisition of evidence (e.g., witness statements, indictments, physical evidence, electronic data, etc.). It can also contribute to the implementation of evidentiary actions, such as inspections, on-site interrogations, evidence attempts, and identification (Nyitrai, 2025a), as shown in Figure 4.

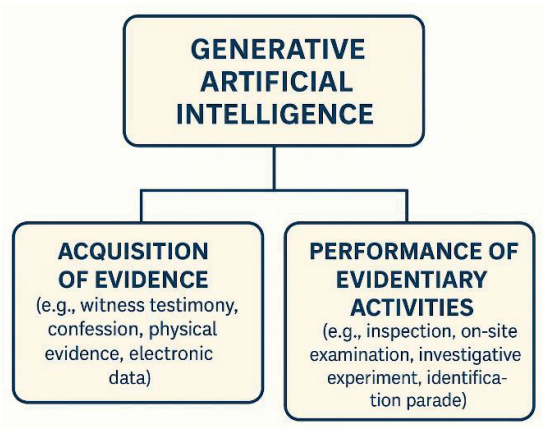


Figure 4. Generative artificial intelligence supporting evidence acquisition and evidentiary activities
(Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT, on July 22, 2025)

The use of generative artificial intelligence in forensics will revolutionise investigative methods, accelerate analysis, streamline electronic work, reduce the likelihood of human error, save investigators time, and produce high-quality content. Furthermore, they can also appear during the planning and organisation of the investigation, thereby enhancing the effectiveness of the investigation's outcome (Nyitrai, 2025a).

With the development of technology, artificial intelligence-supported technical tools appear, which, in addition to generative artificial intelligence, also play a significant role in the field of policing. The application of artificial intelligence requires a large amount of data, which in the case of the police can be provided by the Robot Cop system.

From the perspective of law enforcement, the relationship between national data assets, e-investigation, and artificial intelligence is illustrated in Figure 5, titled 'e-investigation ecosystem'.

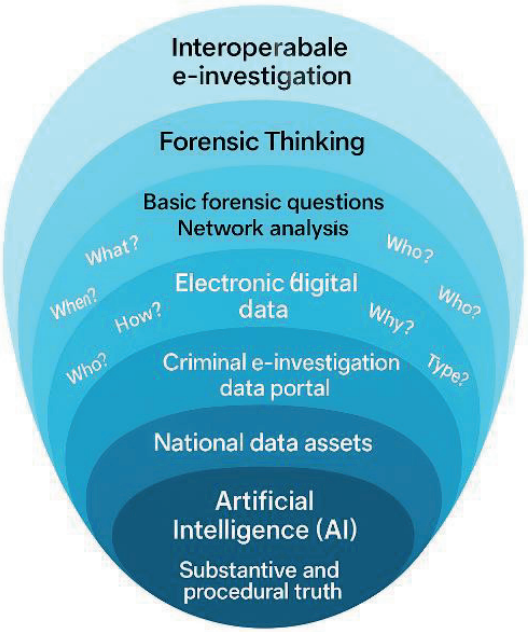


Figure 5. Generative artificial intelligence supporting evidence acquisition and evidentiary activities (*Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT, on July 22, 2025.*)

E-investigation refers to the process where the investigating authority requests information directly or indirectly from accessible databases to detect,

prove, and locate assets derived from the crime, while applying tactical recommendations to enhance the investigation's success (Nyitrai, 2020). The structured and unstructured data collected in e-investigation is essential for training machine learning models used in predictive policing. The data obtained during e-investigation can also serve as the basis for network research analyses, and the results obtained in this way can also contribute to the development of the digital crime ecosystem. Smart policing should also use the opportunities offered by artificial intelligence, as its application can increase efficiency. The use of predictive policing, combined with smart policing, enables law enforcement authorities to respond more effectively and quickly to criminal incidents, as illustrated in Figure 6.

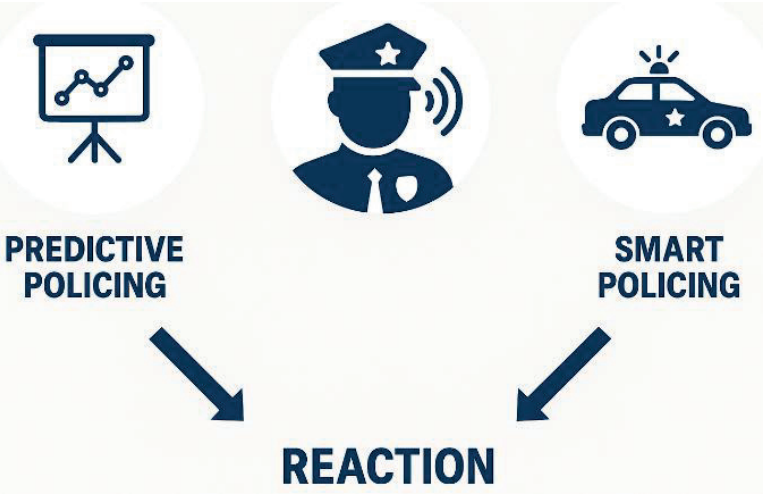


Figure 6. Integration of predictive and smart policing through technological reaction
(Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT with DALL·E, on July 23, 2025.)

Smart police are understood to be an organisation that uses modern and innovative information technologies in the performance of its tasks and can

exploit the opportunities offered by digitalization, artificial intelligence, and digital network research.

Figure 7. Smart policing – key conceptual components illustrated (Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT, on July 22, 2025)

The concept of smart policing also includes the operational implementation of predictive policing, which integrates AI tools into everyday police decision-making (see Figure 8).

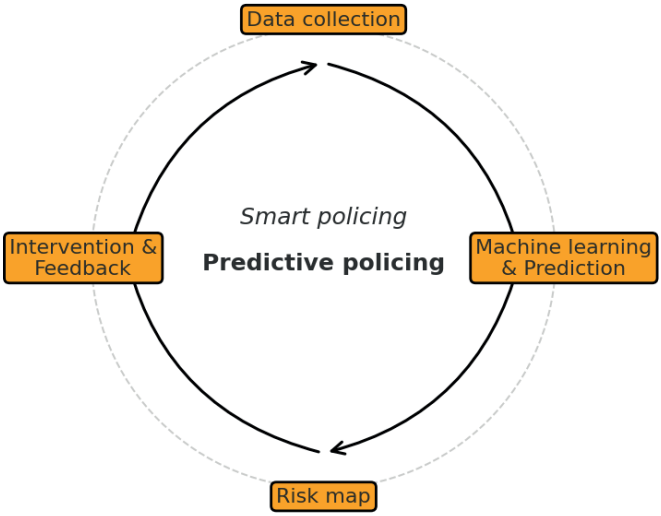


Figure 8. Predictive policing cycle – key conceptual components illustrated (Source: Generated collaboratively by Endre Nyitrai and OpenAI's ChatGPT, on July 23, 2025)

Artificial intelligence-powered tools and generative artificial intelligence are the pillars of the data explosion. The use of tools and programmes generates new data, which can trigger information flows and contribute to the execution of evidentiary actions (Nyitrai, 2025b).

References

AFSANEH E., SHARIFDINI A. & GHAZZAGHI H. (2022). Recent applications of machine learning and deep learning models in the prediction, diagnosis, and management of diabetes: a comprehensive review. *Diabetology & Metabolic Syndrome*, 14(1), p. 196. (doi:10.1186/s13098-022-00969-9)

BZAI, J., ALAM, F., DHAFER, A., BOJOVIĆ, M., ALTOWAIJRI, S.M., NIAZI, I.K. & MEHMOOD, R. (2022). Machine Learning-Enabled Internet of Things (IoT): Data, Applications, and Industry Perspective. *Electronics*, 11(17), p. 2676. (https://doi.org/10.3390/electronics11172676)

DOBÓ, J. & GYARAKI, R. (2021). A mesterséges intelligencia egyes felhasználási lehetőségei a rendvédelmi területeken [Some possible uses of artificial intelligence in law enforcement]. *Magyar Rendészet*, 21(4), pp. 67–81. (https://doi.org/10.32577/mr.2021.4.3)

HAJDÚ, N., SZÁSZI, B., ACZÉL, B. & NAGY, T. (2024). Felügyelt gépi tanulási módszerek alkalmazása a pszichológiai kutatásokban [Applying supervised machine learning methods in psychological research]. *Magyar Pszichológia Szemle*, 79(2), pp. 171-193.

NÉMETH, A. & VIRÁGH, K. (2022). Mesterséges intelligencia és haderő – A mesterséges intelligencia fejlődéstörténete II. rész [Artificial Intelligence and Military Power – The History of Artificial Intelligence Part II]. *Haditechnikai* 56(2), pp. 2-6.

NYITRAI, E. (2025a). Mesterséges intelligencia a kriminalisztikában: az AI Copywriting új dimenziói [Artificial Intelligence in Forensics: New Dimensions of AI Copywriting]. *Belügyi Szemle* (special issue), 73(1), pp. 127-138.

NYITRAI, E. (2025b). *A digitális adatok és a modern technikai eszközök jelentősége a kriminalisztikában: a deepfake és a fake news jelenségek* [The importance of digital data and modern technical tools in forensics: the deepfake and fake news phenomena]. Ludovika Egyetemi Kiadó, Budapest

NYITRAI, E. (2020). A bűncselekményből eredő vagyon visszaszerzése [Recovery of assets resulting from crime]. *Ügyészek Lapja*, 27(2-3), pp. 39–53.

OpenAI's ChatGPT (2025). *ChatGPT* [Large language model]. https://chat.openai.com/

PÁL, B. CS. & IVÁNYI, T. (2024). Gépi tanulás lehetőségei a marketingkutatásban [Machine learning opportunities in marketing research]. In: Szűcs, K., Putzer, P. & Törőcsik, M. (eds.). *A (marketing) világ megkettőződése. Egyesület a Marketing Oktatásért és Kutatásért XXX. Nemzetközi Konferenciájának Absztrakt- és Tanulmánykötete Pécs*, *Egyesület a Marketing Oktatásért és Kutatásért, Pécsi Tudományegyetem Közgazdaságtudományi Kar*, Pécs, pp. 112-118.

VARGAS, R., MOSAVI, A. & RUIZ, R. (2018), *Deep Learning: a Review*. pp. 1-10. (https://doi.org/10.20944/) preprints201810.0218.v1)

URL1: Mi az elsődleges különbség a felügyelt tanulás, a megerősítéses tanulás és a nem felügyelt tanulás között a képzés során adott visszajelzések típusát tekintve? [What is the primary difference between supervised learning, reinforcement learning, and unsupervised learning in terms of the type of feedback given during training?] (2024) Európai Információs Technológiai Hitelesítési Akadémia (https://hu.eitca.org/mesters%C3%A9ges-intelligencia/eitc-ai-adl-halad%C3%B3-m%C3%A9ly-tanul%C3%A1s/fel%C3%BCgyelet-n%C3%A9lk%C3%BCli-tanul%C3%A1s/fel%C3%BCgyelet-n%C3%A9lk%C3%BCli-reprezent%C3%A1ci%C3%B3s-tanul%C3%A1s/vizsga-%C3%A1ttekint%C3%A9se-fel%C3%BCgyelet-n%C3%A9lk%C3%BCli-reprezent%C3%A1ci%C3%B3-tanul%C3%A1s)

URL2: Mi az a generatív mesterséges intelligencia? Típusok, előnyök és felhasználási módok érthető magyarázat. [What is Generative Artificial Intelligence? Types, Benefits and Uses - An Easy-to-understand Explanation]. Monolith Law Office (https://monolith.law/hu/it/generativeai-types-benefits-applications?utm_source=chatgpt.com)

URL3: Mi a generatív mesterséges intelligencia? [What is generative artificial intelligence?] (www.sap.com/hungary/products/artificial-intelligence/what-is-generative-ai.html)

URL4: Mit jelent a generatív mesterséges intelligencia [What does Generative Artificial Intelligence mean?] (https://www.xlabs.hu/blog/mit-jelent-a-generativ-mesterseges-intelligencia-generative-ai)

Chapter 7

Practical Aspects of Predictive Policing

Szabolcs Mátyás, Zita Traub, Miklós Tihanyi and Róbert Major

7.1. The Sopianae Software

7.1.1. Accidents rather than Crime: A New Direction in Predictive Modelling

One of the basic conditions for the operation of predictive software is that there be a sufficient number of crimes or traffic accidents; otherwise, the prediction will not be as accurate as would be desired. Given that in Hungary – in line with the Western European trend – the number of crimes has decreased significantly in the past decade and a half, especially so-called street crime-type crimes (e.g., robbery, car break-ins, burglary, vehicle theft), it would not have been professionally justified to develop software that would have predicted crimes with sufficient accuracy. Almost parallel to this, a drastic reduction in fatal and personal injury accidents per member state became an EU expectation.

As a result of the above, the teachers at Ludovika University of Public Service felt the need to develop software that predicts traffic accidents rather than crime. The National Media and Information Communications Authority (in Hungarian: *Nemzeti Média és Hírközlési Hatóság*) provided the university with the necessary funds for the research.

The university's teachers provided the theoretical background for the project, identified the key indicators, and developed the testing criteria and principles of data collection. Ferenc Traub conceived the software, then developed its structure with Zita Traub, while Sándor Szaniszló was responsible for coding the software.

It is being tested at the Pécs Police Department (the test operation is still ongoing at the time of publication of this book).

The software was named Sopianae, which was the ancient Latin name for the city of Pécs (the location of the testing). The data has been uploaded, and the testing has been conducted by police Lieutenant Colonel Dr. Károly Böröcz, who is the head of the Traffic Police Department at the Pécs Police Department.

Szaniszló Sándor was responsible for coding the Sopianae software

7.1.2. Operation and Main Features of the Software

7.1.2.1. Indicators Used by the Software

To make the forecast as accurate as possible, the software utilises several indicators that help predict the location and timing of traffic accidents. The most important is the data regarding accidents that have occurred in the past, without which the forecast would not work. This is most important because it is the indicator that influences the accuracy of the forecast to the greatest extent. In the case of past accidents, not only the location and time are relevant data, but also several other factors. You can read about these in detail in Chapter 7.1.3.

From the perspective of accident occurrence, it is essential to understand the characteristics of a given road section and identify any abrupt elevation changes that may be present. The latter has been indicated as the cause of numerous accidents in the statistics in recent years. Weather can be classified as one of the factors that shows a clear cause-and-effect relationship with the number of accidents for the average person. The software examines the position

of the Moon when a given accident occurred. Many people mention that during a full moon (especially a supermoon), not only is the number of accidents higher, but many physiological processes also change (the body's water balance and circulation change, more people are born, and people's quality of sleep is worse). The precise reasons have not yet been scientifically discovered; however, the divergence from normal behaviour during these periods is significant enough to be taken into account (Roy et al., 2017).

7.1.3. Main Principles of Operation

The software consists of two main parts, a Microsoft Windows application and a database accessible on a Microsoft SQL server:

- The application is a client developed with Windows Form technology in the C# programming language,
- The database is a standalone server solution with its own tables and other SQL tools.

Considering cost-saving aspects, the software utilises the free Microsoft SQL Express server programme as its search engine. The software is based on statistical models and probability calculations, which rely on a wide range of risk factors.

According to the plans of the software developers, in the future, the central database will be available to multiple client applications in the event of network assistance, which will be a significant advantage during use. In its current phase, the software does not require access to other computers or data provider solutions, allowing this system to operate completely independently of other systems from a network perspective, both logically and physically. The software has eight menu items, which are as follows (Figure 1):

1. Accident registration (data entry)
2. Current forecast
3. Action plan
4. Statistics
5. Signalling guide
6. Backup function
7. Data editor
8. Escape.

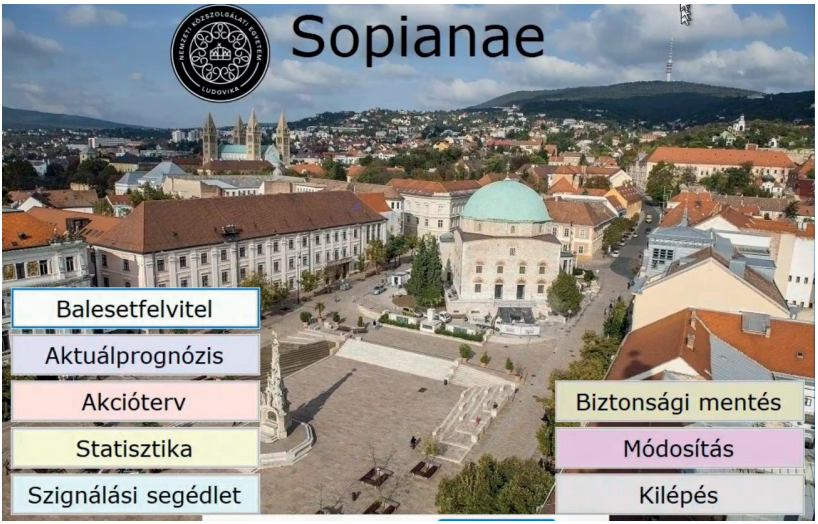


Figure 1. Opening image with menu items

ACCIDENT REGISTRATION: to ensure the forecast is as accurate as possible, the entered data must be up-to-date. Recording an accident takes 1-2 minutes. Entering the records of an accident consists of the following steps: Select the date. The software itself sets whether the given accident occurred on a workday or a holiday. When entering the time of the accident, the software also automatically performs the moon position calculation. It determines the moon phase for a given

day and displays the corresponding astronomical moon position and a visual effect for the time of the accident.

When recording an accident, you must select the street where the traffic accident occurs and specify the outcome of the accident. This can be injury, material damage, or other. The nature of the accident is also entered. The options are based on the Hungarian Central Statistical Office (HCSO) code dictionary. The cause of the accident is also aligned with the HCSO code dictionary. There are several options available. The accident could have occurred, for example, due to driver error, failure to yield the right of way, or for other reasons. After selecting the offending activity, the underlying cause must be entered. The cause is also specified from the HCSO code dictionary (e.g., inattention). The category of the vehicle causing the accident (e.g., car, truck) must then be selected.

Next come the risk factors. This is also based on the HCSO code dictionary. In the case of weather, we can enter the weather at the time of the accident, the visibility conditions, and whether the impact was frontal. Once we have recorded the necessary data, we can exit (Figure 2).

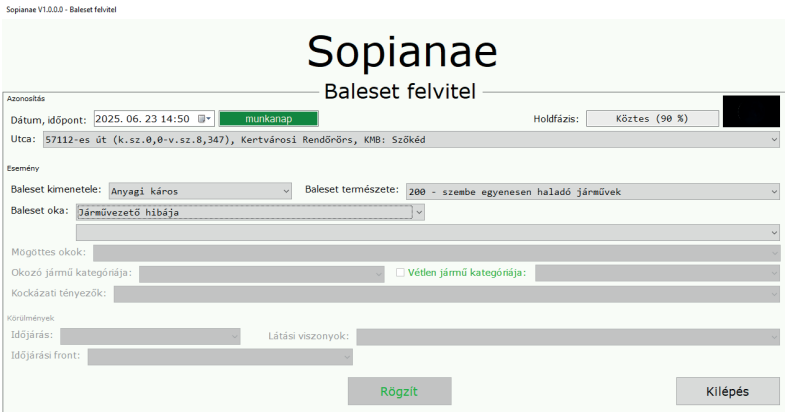


Figure 2. Accident registration from the Hungarian Central Statistical Office code dictionary

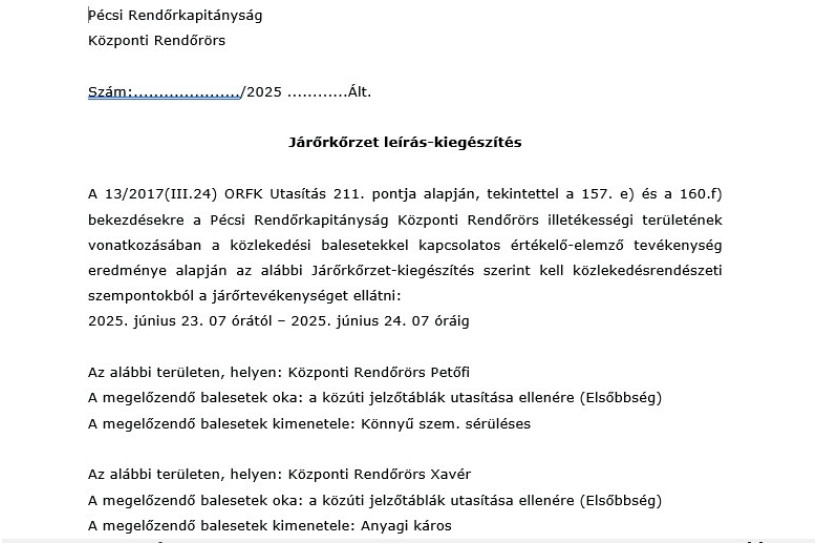
The following menu item is the current forecast. We use this menu item during daily duty and during briefings. Patrol officers receive a supplement from this menu item. This can be printed from the program, which we can also physically hand over to the patrol officers.

You must select which police station, for example, you want to print a patrol district supplement for. The date is given, but we can overwrite it. The commander can overwrite the plan offered by the software. The streets on which patrolling may be relevant, according to the forecast, are displayed. You can also view the expected outcome of the accident for the given streets, the police district to which they belong, the reasons for the accident, and the likelihood of the traffic accident occurring.

The commander has the option to remove the selection of the box next to the street name if he has information that the software does not have. Such appropriate knowledge could be, for example, if the commander is aware that a street accessible by the software has been closed due to ongoing road construction. In this case, the software will not take the given street into account in the planning when making the prognosis.

If we click on 'Create a Word document'; a text editor will start, in which we can write freely. It can be saved, edited, and printed. The commander can print this out, sign it, and hand it over to the patrols.

The ACTION PLAN helps in determining which day of the week is most suitable for organising a traffic action. The algorithm calculates on which day of the week accidents are most likely to occur, then fills in the action plan accordingly. This can be prepared for a specific police station or any police stations. If the action plan for the given police station is prepared, then by default the programme prepares the action plan with four cars, eight patrolmen and one commanding officer. If this is not proportionate, the number of available service vehicles or police officers can be increased or decreased (Figure 3).



Pécsi Rendőrkapitányság
Központi Rendőrörs

Szám:...../2025 .....Ált.

Járőrkőrzet leírás-kiegészítés

A 13/2017(III.24) ORFK Utasítás 211. pontja alapján, tekintettel a 157. e) és a 160.f) bekezdésekre a Pécsi Rendőrkapitányság Központi Rendőrörs illetékességi területének vonatkozásában a közlekedési balesetekkel kapcsolatos értékelő-elemző tevékenység eredménye alapján az alábbi Járőrkőrzet-kiegészítés szerint kell közlekedésrendészeti szempontokból a járőrtevékenységet ellátni:
2025. június 23. 07 órától – 2025. június 24. 07 óráig

Az alábbi területen, helyen: Központi Rendőrörs Petőfi
A megelőzendő balesetek oka: a közúti jelzőtáblák utasítása ellenére (Elsőbbség)
A megelőzendő balesetek kimenetele: Könnyű szem. sérüléses

Az alábbi területen, helyen: Központi Rendőrörs Xavér
A megelőzendő balesetek oka: a közúti jelzőtáblák utasítása ellenére (Elsőbbség)
A megelőzendő balesetek kimenetele: Anyagi káros

Figure 3. Action plan, generated by Sopianae (page 1)

When preparing the action plan, we can also exclude certain streets where, according to the commander, no relevant events are expected.

In Figure 4, we can see that most accidents occur on Tuesdays, so it is worth carrying out the traffic action on a Tuesday. We generate the Word document, and the programme suggests several Tuesdays as options among which we select March 18th. We then accept the offered document, and the software generates the action plan in a printable format. The editable action plan displays the names of the individuals who created, distributed, and approved it.

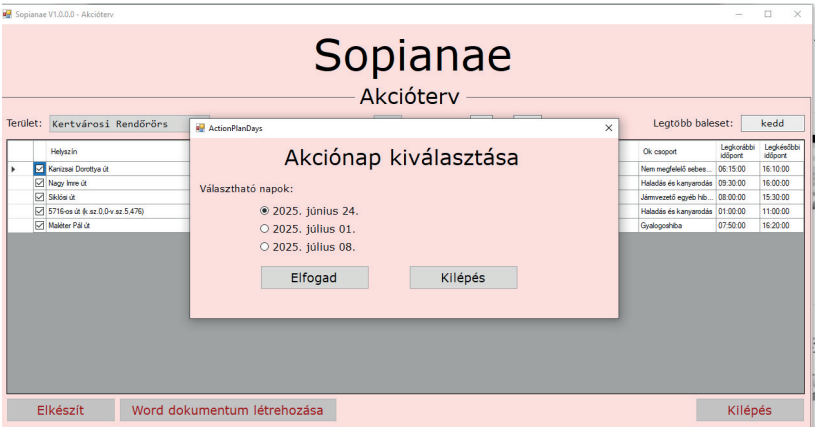


Figure 4. The software offers several possible days to create an action plan for

- STATISTICS allow for a wide range of analytical activities. With the ability to combine all recorded aspects, comparison and analysis of times, areas, and recorded data can be performed using the SQL engine embedded in the program.

We can set the time interval from which we want to retrieve data and also the police level (e.g., police department, police stations) we want to know about. In this case, we want to examine the statistical data of the *Központi* and *Gyárvárosi* [Central and Industrial Estate] Police Stations, and we obtain the graphs for a month.

The data for the Central Police Station is shown in yellow, and the data for the Industrial Estate Police Station are shown in orange in a monthly breakdown. If we want to determine which of the two police stations has more accidents, the software can also provide that information (Figure 5).

Figure 5. The software provides a diagram showing each police station area more traffic accidents have occurred.

- The next menu item is the SIGNALLING GUIDE. We can see this as a 'by-product' that does not help in forecasting but rather assists the people performing command duties. For example, if the commander does not know which police station a street belongs to, this information can be quickly obtained from the program. However, we can also identify which streets belong to a specific police district. This function is a great help in filing case files.
- The BACKUP function is used to save our database at certain intervals to prevent serious data loss. If the database becomes corrupted, we can restore the data that was previously recorded and saved.
- DATA EDITOR: The data stored in the database can be modified. It is possible to correct the recorded data (e.g., changing the content of the database to include streets, changing the street name, creating a new street, etc.) so that in the event of any possible change or expansion of a database

(accident causes, risk factors, etc.), the change can be updated in the programme as well.

- EXIT: This requires no further explanation.

In its current form, the Sopianae software is a prototype, which was created for the jurisdiction of the Pécs Police Department in order to predict traffic accidents. However, with modifications, the software could be used in other branches of service. Such areas could be, for example, by the border police or in criminal law. However, for this, the software must be modified taking into account the specificities of the new jurisdiction and organisational structure.

References

ROY, A., BISWAS, T. & ROY, A. K. (2017). A structured review of relation between full moon and different aspects of human health. SM J Biometrics Biostat, 2(1), 1007. (https://www.jsmcentral.org/assets/articles/fulltext_smjbb-v2-1007.pdf)

7.2. Predictive Software Applications in Drug-Related Crime Prevention: A Comprehensive Analysis

Máté Sivadó

7.2.1. Introduction

Drug-related crimes carry severe consequences not only for individuals but for society as a whole, affecting public health, economic stability, security, and social cohesion. Alongside traditional law enforcement methods, data-driven predictive software systems are playing an increasingly important role, enhancing the effectiveness of anti-drug efforts through forecasting capabilities and targeted analytical approaches.

Drug-related crime represents one of the most complex and destructive challenges facing modern societies. Its consequences are felt across all social strata, causing significant harm to public health systems, economic stability, and national security. Illegal drug trafficking fuels violence, overwhelms healthcare systems, and undermines the rule of law through corruption and the strengthening of transnational criminal organisations (Berk, 2021).

For decades, law enforcement agencies have relied on traditional investigative, surveillance, and reactive enforcement methods. While these approaches have achieved successes, they are often resource-intensive and struggle to keep pace with the dynamic, adaptive, and technologically sophisticated nature of modern drug trafficking networks. Globalization and the advancement of digital technologies have created new challenges that require a fundamental rethinking of law enforcement strategies (Berk, 2021).

In this context, the emergence of predictive software applications powered by artificial intelligence (AI) and Big Data analytics represent a potential paradigm shift in global efforts to prevent and combat drug-related crime (Berk,

2021). These systems are capable of processing vast and diverse datasets that far exceed the capacity of human analysts. Data sources include historical crime statistics, emergency call logs, arrest records, census data, social media activity, financial transactions, and even public health data on drug overdoses (Fitzpatrick et al., 2019).

The application of predictive policing to drug-related crime appears particularly promising, as this type of criminal activity often exhibits recurring patterns and spatial-temporal concentrations. The functioning of drug markets, consumer behaviours, and distribution networks are all elements that can be better understood and predicted through data analysis. This enables law enforcement agencies to act proactively, preventing the escalation of problems.

This chapter provides a comprehensive analysis of the role and impact of predictive software in combating drug-related crimes. It goes beyond simple cataloguing of technological capabilities to offer critical evaluation of their real-world applications, effectiveness, and the challenges they present. We examine the fundamental technologies and algorithms that enable these systems to predict criminal activity, from identifying emerging drug hotspots to mapping the complex structures of trafficking networks.

7.2.2. Theoretical Background and Conceptual Frameworks

7.2.2.1. Characteristics of Drug-Related Crime

Drug-related crime differs from other types of criminal activity in several important ways. First, it is often characterised as a 'victimless' crime, since direct participants (seller and buyer) generally participate voluntarily in the transaction. This complicates detection, as there is no complainant party, which fundamentally differs from the nature of traditional crimes (Marshall et al., 2024).

Second, drug markets are organised in complex network structures that encompass multiple levels: from international transportation to local distribution. These networks are extremely adaptive and respond quickly to law enforcement pressure, presenting special challenges for traditional investigative methods. Alongside hierarchical organisation, decentralised operation is often observed, where parts of the network operate relatively independently, increasing the system's resilience.

Third, drug-related crime is closely connected to other social problems, such as poverty, unemployment, mental health issues, and social exclusion. This means that effective intervention must apply a holistic approach that goes beyond purely criminal justice tools. Consideration of social determinants is crucial in developing long-term solutions (Marshall et al., 2024).

Fourth, the dynamic nature of drug-related crime requires continuous adaptation from law enforcement agencies. The emergence of new psychoactive substances, changes in distribution methods, and exploitation of technological developments are all factors that demand rapid response and flexible strategies (Rinaldi et al., 2020).

7.2.2.2. Data Sources and Integration

The effectiveness of predictive systems largely depends on the quality and diversity of data. The wide spectrum of data sources used in predicting drug-related crime includes the following:

- CRIMINAL JUSTICE DATA

Historical arrest records, crime reports, court judgments, and correctional data. These data form the backbone of most predictive models but raise critical questions regarding bias and feedback loops. The quality and completeness of criminal justice data significantly influence model accuracy.

- DEMOGRAPHIC AND SOCIO-ECONOMIC DATA

  Census information, unemployment rates, educational statistics, housing data, and income levels. These data help understand structural factors that may contribute to drug-related crime. Social-economic indicators are particularly important in predicting long-term trends.

- HEALTH DATA

  Overdose cases, emergency department visits, treatment admissions, and mortality statistics. These data are particularly valuable in early identification of new dangerous substances or regional problems. Health data provide real-time information about drug consumption trends.

- FINANCIAL DATA

  Suspicious transactions, money laundering reports, and unusual financial patterns. Financial tracking is crucial in detecting larger drug organisations. The growing use of blockchain technology and cryptocurrencies creates new challenges and opportunities in this area.

- DIGITAL FOOTPRINTS

  Social media activity, online communications, and dark web monitoring. These data sources are becoming increasingly important as drug trafficking shifts to online spaces. Analysis of digital traces enables mapping of virtual networks and tracking illegal activities in cyberspace.

- ENVIRONMENTAL AND INFRASTRUCTURE DATA

  Transportation data, building usage information, street lighting, and surveillance camera data. This information helps understand the role of physical environment in drug-related crime and identify potential hotspots.

7.2.3. Areas of Application

The theoretical power of predictive algorithms is realised through a wide spectrum of practical applications for preventing and detecting drug-related crime. These applications range from on-site operational support to high-level strategic planning, fundamentally changing how law enforcement agencies approach the multifaceted problem of drug-related crime.

7.2.3.1. Spatial and Temporal Analysis

- IDENTIFICATION OF INFESTED AREAS AND HOTSPOT PREDICTION

  One of the most established applications of predictive policing is the identification of geographical and temporal hotspots. By analysing historical data on drug-related incidents, arrests, and citizen complaints, algorithms can generate maps that highlight areas with a high probability of future criminal activity. This enables law enforcement to move beyond reactive patrolling and conduct targeted deployments, concentrating resources where they are most likely to be effective (Mohler et al., 2015).

- TEMPORAL PATTERNS AND SEASONALITY

  Predicting the timing of street drug sales based on temporal patterns enables forecasting when more active drug trafficking occurs – for example, on weekend nights, during festivals, or during school breaks. This is particularly valuable in optimal allocation of limited police resources. Consideration of seasonal variations helps in long-term planning and efficient resource distribution.

- VULNERABILITY MAPPING:

  The system can identify areas with the highest risk of new drug hotspots emerging. This includes protecting schools, youth centres, and other places frequented by young people, where drug consumption or distribution risks can

be predicted. Vulnerability maps help in targeted application of preventive measures.

- DIFFUSION MODELS

  Modelling the spread of drug use and trafficking helps understand how new hotspots form and how problems spread from one area to another. This is particularly important when new psychoactive substances emerge or existing markets change.

7.2.3.2. Network Analysis and Behavioural Patterns

- ANALYSIS OF COURIERS AND TRANSPORTATION ROUTES

  Based on previous arrests and field data, the system recognises movement patterns of drug couriers and helps identify possible routes. This extends to analysis of shipping and logistics routes, where suspicious shipments or transportation patterns can be identified for more effective action at borders and within countries.

- MAPPING CRIMINAL ORGANISATION CONNECTIONS

  Different data points can be used to identify criminal networks and understand their hierarchy. By analysing financial transactions, phone records, and social media connections, investigators can gain comprehensive understanding of a criminal enterprise, from its leadership to street-level dealers. Network analysis helps identify key players and the most critical connections.

- RECOGNITION OF TYPICAL OFFENDING PATTERNS

  The system can identify behavioural patterns and methods frequently associated with drug trafficking. This includes screening suspicious transactions based on financial, communication, or social media data. Pattern recognition helps in early identification of new offending methods.

- IDENTIFICATION OF REPEAT OFFENDERS

  Predictive software can recognise offenders who repeatedly come into contact with drug cases, even in different areas, enabling targeted intervention and monitoring. Predicting recidivism is an important tool in developing crime prevention strategies.

- COMMUNICATION PATTERN ANALYSIS

  A significant portion of modern drug trafficking occurs on digital platforms. Analysis of communication patterns helps identify encrypted messages, coded language, and the operational methods of trafficking networks.

7.2.3.3. Proactive Prevention and Social Intervention

- ANALYSIS OF SOCIAL-ECONOMIC FACTORS

  The programme considers environmental factors (unemployment, poverty, school dropout) that may facilitate the spread of drug-related crime. By correlating unemployment rates, poverty levels, school dropout rates, and access to social services with drug-related crime data, these systems can identify communities at high risk of developing drug-related problems.

- TARGETING DRUG PREVENTION PROGRAMMES

  This information is invaluable for targeting drug prevention programmes, such as school education and public awareness campaigns, where they are most needed. By analysing health data on overdoses and treatment admissions, the software can predict communities where addiction rates are likely to rise.

- PREDICTING DRUG ADDICTION RISK

  The system can identify community factors where there is higher probability of drug addiction development, indicating the need for increased mental health,

rehabilitation, and family support services. Early intervention is crucial in preventing escalation of problems.

- BUILDING COMMUNITY RESILIENCE

Predictive analyses help identify community resources and protective factors that can reduce drug-related crime risk. This includes assessing the role of social cohesion, educational opportunities, and economic development (Table 1).

Data sources and integration	Spatial and temporal analysis	Network analysis and behavioural patterns	Proactive prevention and social intervention	Operational and strategic decision support
- Criminal justice data	- Identification of infected areas and hotspot prediction	- Analysis of couriers and transportation routes	- Analysis of social-economic factors	- Targeted police presence and raids
- Demographic and socio-economic data	- Temporal patterns and seasonality	- Mapping criminal organization connections	- Targeting drug prevention programs	- Estimating illegal laboratory locations
- Health data	- Vulnerability mapping	- Recognition of typical offending patterns	- Predicting drug addiction risk	- Security for festivals and mass events
- Financial data	- Diffusion models	- Identification of repeat offenders	- Building community resilience	- Tracking online drug trafficking
- Digital footprints		- Communication pattern analysis		- Facilitating multi-agency data sharing
- Environmental and infrastructure data				- Recognizing corruption risk
				- Supporting international cooperation

Table 1. Summary table of the most likely predictive indicators for drug detection

Source: own editing

7.2.3.4. Operational and Strategic Decision Support

- TARGETED POLICE PRESENCE AND RAIDS

Predictions help concentrate police resources where drug use or trafficking is most likely. Through high-accuracy predictions, raids can be more effective, achieving greater results with fewer resources. Tactical planning can also consider expected resistance and security risks.

- ESTIMATING ILLEGAL LABORATORY LOCATIONS

  Based on seizures, odour detections, purchase of chemicals, and other traces, the location of illegal drug laboratories can be surmised, enabling proactive intervention. Environmental monitoring and tracking chemical shipments help identify production sites.

- SECURITY FOR FESTIVALS AND MASS EVENTS

  Such events are often associated with drug consumption; the system helps identify risky situations within the event area in advance, directing security and medical personnel. Mass events present special challenges requiring targeted strategies.

- TRACKING ONLINE DRUG TRAFFICKING

  By monitoring the dark web and social media, the system can filter illegal online sales, using natural language processing to analyse encrypted communication. Cyberspace monitoring is becoming increasingly important in combating modern drug trafficking.

- FACILITATING MULTI-AGENCY DATA SHARING

  The software coordinates police, customs, tax authorities, and social services databases, making cooperation more effective and enabling holistic approaches. Integrated data management is crucial in investigating complex crimes.

- RECOGNISING CORRUPTION RISK

  If unusually few drug seizures occur in certain areas while data indicates high risk, this may also suggest corruption, initiating internal investigations. Protecting system integrity is fundamental to effective operation.

- SUPPORTING INTERNATIONAL COOPERATION

  Based on data, conclusions can be drawn about the direction and sources of international drug movements, supporting international cooperation (Mátyás,

2007) and dismantling transnational criminal networks. A global perspective is essential in combating modern drug trafficking.

'This work was supported by AI-assisted tools, but all interpretations and conclusions are solely those of the author.'

References

BERK, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. Annual Review of Criminology 4(1), 209-237. (https://doi.org/10.1146/annurev-criminol-051520012342)

FITZPATRICK, D. J., GORR, W. L. & NEILL, D. B. (2020). Policing chronic and temporary hotspots of violent crime: A controlled field experiment. arXiv preprint arXiv:2011.06019. 30(20), 1-15. (https://arxiv.org/pdf/2011.06019)

MARSHALL, H., BACON, M. & SPICER, J. (2024). Emerging victims in contemporary drugs policing. The British Journal of Criminology, 64(6), 1292-1309.

MÁTYÁS, SZ. (2007): A határon átnyúló magyar-román rendvédelmi együttműködések bűnözésföldrajzi kérdései (Criminal Geographical Issues of Hungarian-Romanian Cross-Border Law Enforcement Cooperation). Kossuth Egyetemi Kiadó, Debrecen, pp. 317-322.

MOHLER, G., PORTER, M. & CARTER, J. & LAFREE, G. (2020). Learning to rank spatio-temporal event hotspots. Crime Science, 9(1), 2-12. (https://doi.org/10.1186/s40163-020-00112-x)

RINALDI, R., BERSANI, G., MARINELLI, E. & ZAAMI, S. (2020). The rise of new psychoactive substances and psychiatric implications: a wide-ranging, multifaceted challenge that needs far-reaching common legislative strategies. Human Psychopharmacology: Clinical and Experimental, 35(3) (https://doi.org/10.1002/hup.2727)

7.3. The Use of Predictive Techniques in Counter-Terrorism Strategies

Endre Edvard Vajda

7.3.1. Introduction

Efforts to establish and maintain security play a decisive role in the lives of the Member States of the European Union. Security is a fundamental prerequisite for the functioning of democratic states governed by the rule of law. It encompasses the interests and values of the state and society, as well as the freedom of the country's territory and population from danger and threats. It also includes administrative protection requirements and protocols, trained human resources, and the availability of defence technologies and equipment (Boda, 2019).

In our modern, globalised, and multicultural world, security challenges are becoming increasingly complex (Mátyás, 2016). The rise of the Islamic State in the Middle East has been accompanied by armed conflict, political and religious persecution, and economic instability. As a result, millions of people have left their homes and Europe had to face a migration crisis, notably in 2015. The decisions taken by the European Parliament and national governments on immigration have been accompanied by numerous political, economic and social debates. However, the crisis highlighted that significant differences between communities with different religious and cultural identities can lead to social tensions over time. Incidents posing a more moderate risk posed less of a threat to the security of European nations, but terrorist attacks with high numbers of casualties began to occur in Europe. Most terrorist organisations operate locally, meaning that their attacks are limited to a specific region. However, the areas threatened by international terrorism are less easy to define due to the presence of terrorist cells and lone perpetrators that are difficult to identify, inactive in terms of attacks, but capable of carrying out operations.

The attacks that took place between 2014 and 2023 forced Europe to rethink its security theories. The importance of this topic is confirmed by the fact that the fight against terrorism is one of the EU's top priorities. An essential part of developing strategies to combat terrorism is analysing and evaluating attacks that have already happened. The definition, ordering and implementation of targeted action plans and police operations are already the task of predictive policing. Predicting the likely location and time of attacks, as well as the perpetrators and victims, can provide significant support in preventing terrorism.

7.3.2. The Preventive Policing/Terrorism Nexus

Migration has significantly transformed the structure of the European population. The Muslim population has undergone dynamic growth over the past 70 years, in France increasing by 61% and in Belgium by 30%, meaning that the number of Muslims in France has increased thirtyfold and in Belgium nearly eightyfold. Similar trends can be observed in Germany, the United Kingdom, Italy, and Spain (Kettani, 2010). According to research findings on crime geography, the intensity of migration influences the age structure of a given settlement (Krasnova 2025). The largest percentage of immigrants are younger people, who are much more prone to crime, so it can be said that the crime rate increases with population growth (Mátyás, 2024).

The series of attacks that took place between 2014 and 2023, typically committed in the name of Islamic State, kept almost all of Europe in a state of fear. The level of terrorist threat is primarily determined by the intensity of the attacks and the extent of the damage caused. During the period under review, 94% of fatalities (421/397) were killed in Islamist terrorist attacks, which is why I focus on radical Islam in this paper (URL1).

Terrorist cells are closed, small groups and their activities and methods are characterised by conspiracy. The complexity of the fight against terrorism is

demonstrated by the fact that the organisation and execution of attacks require a network of contacts, tactical knowledge, and logistical and financial resources. The complexity of the challenge requires the involvement of all relevant fields of expertise and the use of new methods that are likely to yield results. The following table describes the system of predictive policing (Table 1).

Objective	Predictive analytics
Predicting crime	
Use of crime data.	Hot spot identification models, risk analysis.
Use of additional data.	Regression, classification and clustering models.
Risks of recent crime.	Near recurrence modelling.
Identifying areas and times at risk.	Spatio-temporal analysis methods.
Geographical aspects of crime risk.	Spatial risk analysis.
Prediction of offenders	
Risk assessment of violent offender groups.	Near-repetition modelling of violent offences.
Identifying potential offenders.	Regression and classification models (risk factors).
Predicting the identity of offenders	
Suspect identification using criminal data.	Computer queries and analysis (from police databases)
Serial crime identification.	Linking crimes to statistical models.
Finding the starting point of the offender.	Geographical profiling.
Locating suspects around the crime scene (GPS tracking, license plate number).	Computer queries and analysis (detection of vehicles, mobile phones).
Prediction of crime victims	
Identification of groups of victims of crime.	Hot spot identification models, risk analysis (territorial).
Identification of vulnerable places, persons.	Crime mapping.
Victimisation - identification of persons at risk.	Databases, regression and classification models.
Identifying the risk of domestic violence.	Computer query of several databases (local residents)

Table 1. Taxonomy of preventive policing methods

Source: Perry et al. 2013, own editing.

Predictive policing techniques aim to identify the places and times of greatest risk, as well as the possible circle of perpetrators and victims. However, in addition to making predictions, serious attention must be paid to the continuous collection and analysis of data on crimes and offenders, and to the implementation of police actions based on forecasts. The effectiveness of police measures must be continuously monitored and, where necessary, operations must be modified. The process is illustrated in the figure below.

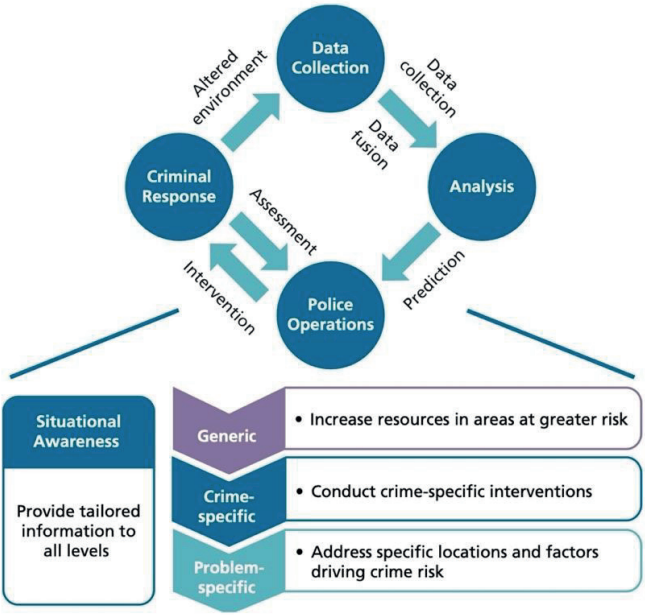


Figure 1. Process model for predictive procedures

Source: Perry at al., 2013, 3.

When designing predictive procedures, it is important to narrow down the focus areas so that police measures can be concentrated in smaller areas. During data collection, efforts should be made to ensure that relevant information of

sufficient quality and quantity is available for analysis and evaluation. Terrorism analysis methods are structured similarly to predictive procedures, so forecasts can also be applied and integrated into counter-terrorism strategies. However, knowledge of current terrorist trends and modes of attack is necessary to determine the most effective defence capabilities and optimal resources.

7.3.3. The Investigation of Terrorist Attacks from a Predictive Analytics Perspective

Preventive policing focuses on predicting crimes, perpetrators, and victims. In the following, I identify the highest-level threats and hotspots using statistical data analysis and crime maps. The empirical part of the study is based on data from Europol's Terrorism Situation and Trend Report 2015-2024. This document, published annually, identifies current and potential trends in counter-terrorism based on verified information (URL2).

Crime maps can be used in many areas of law enforcement to identify sectors that are criminally related. Hotspot policing can be used in urban areas where crime is most concentrated (Mátyás et al., 2020).

7.3.3.1 Predicting Terrorist Attacks

The mapping of crimes related to terrorism highlights differences between regions. Figure 2 shows that several European countries have been affected by at least one terrorist attack. Ninety-one per cent of the attacks took place in the United Kingdom, France, Italy, and Spain. After the countries listed, most attacks took place in Greece, Germany, and Belgium. It is worth noting that, with the exception of Greece, these are the European countries with the largest Muslim populations. The following map shows the distribution of terrorist attacks in Europe by country.

Radical Islam was most active in France, the United Kingdom, Germany, and Belgium. At least three Islamist attacks also took place in the Netherlands, Denmark, Spain, Italy, and Sweden. The attacks carried out by separatist, far-left and far-right movements did not result in fatalities or serious injuries in the vast majority of cases (URL1).

Based on their classification criteria, organisations that analyse terrorism register a wide range of violent criminal acts as terrorist attacks. However, a distinction must be made between arson attacks with Molotov cocktails, which cause injury or only material damage, and attacks carried out by groups or individuals resulting in fatalities (Figure 2).

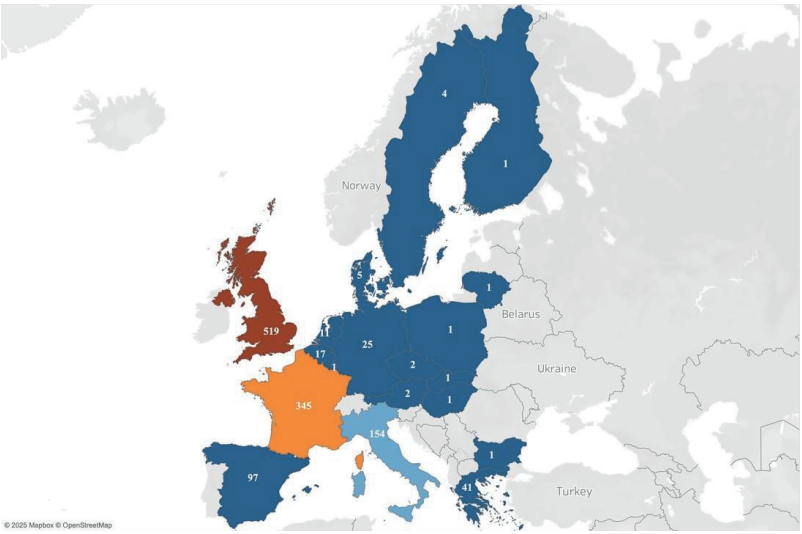


Figure 2. Terrorist attacks in Europe 2014-2023

Source: own editing based on URL1

The most serious attacks were carried out by terrorist groups in Paris and Nice, but there have also been terrorist attacks with fatalities in other French cities. The next largest circle is Brussels and the city of Liège, 98 km from the

Belgian capital (Figure 3). There were also attacks in Manchester, London, Barcelona, and Torre-Pacheco, in which victims lost their lives. In Germany, there were attacks causing significant damage in Berlin, Hanau, Ludwigshafen, Dresden, and Hamburg. In addition to the above, Stockholm, Utrecht, Vienna, Bratislava, Turku, and Copenhagen were also affected by similar attacks. The figure below shows the geographical concentration and number of terrorist attacks resulting in fatalities.

Figure 3. Number of victims of terrorist attacks 2014-2023[9]

Source: own editing based on URL1

Seventy per cent of terrorist attacks took place in large cities, but nearly a quarter of the attacks occurred in towns with a population of between 24,000 and 90,000. Although 7% is not a significant proportion, it is worth noting that

[9] The map shows 97% of terrorist attacks with fatalities, as the exact locations of the other 3% cannot be determined from TE-SAT reports.

terrorism has also appeared in small towns (Figure 4). In terms of the precise locations of the attacks, the terrorist trends of previous periods continued (Figure 5). Most of the attacks were carried out by terrorist cells or lone perpetrators in busy public areas (main streets, boulevards, famous bridges) and places where large numbers of people gather (train stations, concert halls, events, Christmas markets).

However, there were also attacks on means of transport (trains, subways, and trams), religious sites (Catholic churches, Jewish museums) and police buildings. There were also one or two attacks where the attackers chose the location for a specific reason (Paris, January 7, 2015, the editorial office of *Charlie Hebdo*). Figure 4 shows the distribution of the most serious terrorist attacks by type of settlement, while Figure 5 shows the proportion of attacks committed at specific locations.

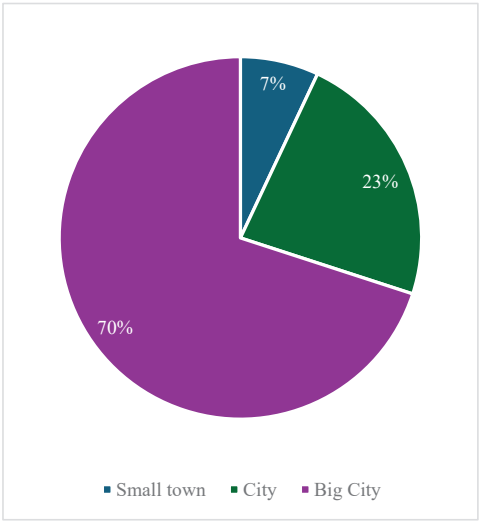


Figure 4. Types of municipalities involved in attacks[10]

Source: own editing based on URL1

[10] Small town: population < 20,000; City: population 20,000 - 100 000; Large city: population > 100,000.

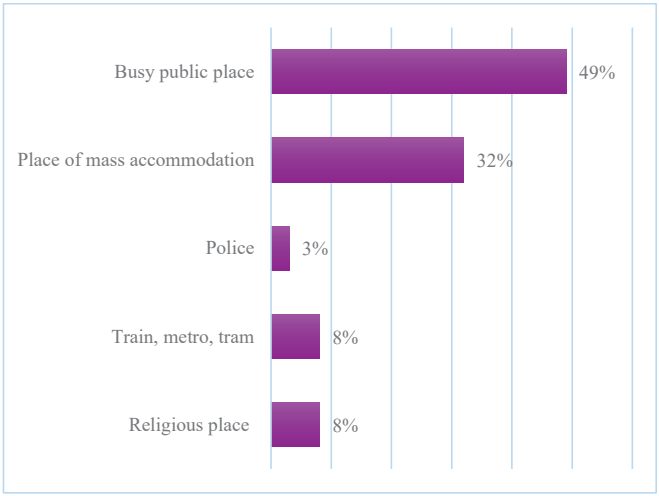


Figure 5. Locations where attacks were committed

Source: own editing based on URL1

The location of crime scenes is an extremely important factor in organising future police measures and security tasks. However, in order to carry out police operations safely, it is also necessary to be familiar with the most common methods of attack. In most attacks, perpetrators used knives (56%), vehicular attacks (18%) and firearms (15%), but there were also bombings (10%) and arson attacks (1%). It can therefore be stated that, in addition to traditional terrorist methods, stabbings and vehicular attacks carried out by lone perpetrators have emerged. These are high-risk methods of attack, as the perpetrators may become radicalised at an individual level and at a spontaneous moment. Until the moment the attack begins, the identity of the attacker and the preparations remain hidden from national security services and law enforcement agencies. No connection can be established between the attacks and the days of the week or the precise timing of the attacks. Terrorist acts are typically linked to specific events, occasions, or periods (e.g. Christmas), while some occur at completely unpredictable times, highlighting the difficulties of detecting terrorism.

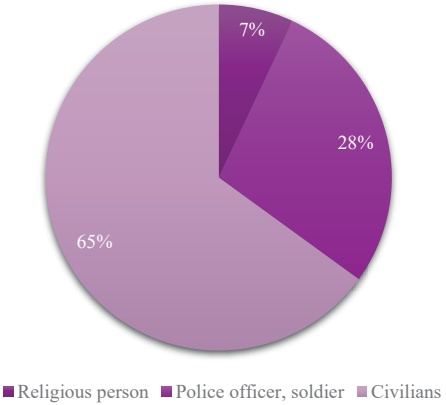
7.3.3.2. Predicting Perpetrators

Almost all of the attacks were committed by men. An analysis of the age groups shows that 12% of the perpetrators were young people between the ages of 15 and 18.79% were between the ages of 20 and 35, and 9% were men aged 35 and over. Ninety-four per cent of the attacks were carried out by individuals, with only four attacks linked to terrorist groups. According to reports, nearly 61% of the attackers came from North African countries (Morocco, Algeria, Libya, Tunisia, Sudan), and 39% came from Middle Eastern countries (Syria, Iraq) and neighbouring Afghanistan.

Sixty per cent of the perpetrators were French, British, or Belgian citizens born in Europe, and 40% arrived on the continent during the migration crisis. The vast majority of radicalised individuals come from Muslim families, but in some cases, the perpetrators had converted to Islam at some point in their lives. Islamic State claimed responsibility for most of the attacks that caused significant damage, indicating that the perpetrators held extreme religious views and most of them had a criminal record.

7.3.3.3. Predicting the Victims of Attacks

A common feature of the attacks was the unrestrained destruction of soft targets (defenceless civilians), but there were also a relatively high number of cases in which the attacks were directed at police officers (prison guards) or soldiers. It can be concluded that the terrorist trends of previous periods can be observed in terms of targets. In addition to civilians, police officers and soldiers have also become frequent targets for attacks.



The first category is a known terrorist tactic, but attacks against professional armed forces were not previously typical in Europe. Figure 6 shows the types of target.

Figure 6. Types of target
Source: own editing based on URL1

7.3.3.4. Summary of Forecasts

The results of the analyses suggest that Islamist terrorism poses the greatest threat to European countries with the largest Muslim populations. Busy public areas in large cities and places where large numbers of people gather require a greater police presence and more special operations. Stabbings and vehicle attacks can be expected to continue in the future, but traditional terrorist methods cannot be ruled out either. Terrorist attacks continue to pose the greatest threat to civilians, but tactical training for police and military personnel is also justified.

In the future, attacks will continue to be carried out by individuals who are prone to reactive violence, highly emotional, prone to strong stress responses, and have a criminal past (Haller et al., 2020). Frustration, retaliation as a goal, and provocative victims (also known as a bully victim) are also significant aspects in understanding the psychology of the perpetrator profile. For this reason, the possible self-defence reactions to attackers acting on religious beliefs must be carefully considered. Table 2 below summarises the complex prediction of Islamist terrorism.

	Forecast: regions, trends
Country	United Kingdom, France, Italy, Spain, Germany, Belgium
Type of settlement	Large cities >100 000 population
Location	Busy public spaces (landmarks, squares, bridges, boulevards), crowded places (event venues, railway stations, shopping centres, Christmas markets)
Types of target	Citizens, police officers
Mode of attack	Stabbing, vehicle-raming, firearm
Perpetrator profile	Male, 20-35 years old, single, religious fanatic, history of early offending, lack of empathy and fear, prone to reactive violence, European citizen with an immigrant background or migrant background, origin: North African or Middle Eastern country

Table 2. Projected trends in Islamist terrorism

Source: own editing based on URL1

7.3.4. Summary

Predictive policing is an important part of law enforcement strategies and police measures to prevent crime must be determined on the basis of forecasts. Effective police operations require management support, adequate resources, automated systems that provide the necessary information, and a workforce capable of responding effectively to crime challenges. Preventive police actions developed against this background offer a realistic chance of preventing predicted risks from becoming actual crimes. Predictive methods primarily support the detection of serial crimes, but terrorist attacks are of a different nature.

There are discernible patterns in terms of the type of location, the method of attack and the choice of target, but it is difficult to narrow down the circle of perpetrators due to the relatively large number of radical Muslims living across Europe. The particular risk of terrorist attacks lies precisely in the fact that they can occur almost anywhere on the continent at any time. Predictive procedures can be used to make forecasts, but in my opinion, due to the complexity of the background to the attacks, they will not provide accurate guidance for police operations. At the same time, the results of the analyses must be incorporated into law enforcement and counter-terrorism strategies and into the planning and implementation of tactical decisions.

References

BODA, J. (2019). *Rendészettudományi Szaklexikon* [Police Science Lexicon]. Dialog Campus, Budapest (https://real.mtak.hu/153920/1/743_Rendeszettudomyanyi_Szaklexikon_e_2020_04_28_.pdf)

HALLER, J., FOGARASI, M. & IVASKEVICS, K. (2020). Aggression and violent crimes. In: Haller, J. (ed.). *Criminal Psychology of Crime*. Ludovika Kiadó, Budapest

HOUSSAIN, K. (2010). Muslim Population in Europe: 1950–2020. *International Journal of Environmental Science and Development*, 1(2), pp. 157-160. (https://soerenkern.com/pdfs/islam/MuslimPopulationEurope1950-2020.pdf)

KRASNOVA, K.A. (2025). Public Safety: Reviewing Szabolcs Mátyás's Crime Geography. Kutafin Law Review. 12(2), 453-461. (doi: 10.17803/2713-0533.2025.2.32.453-461)

MÁTYÁS, SZ., MÉSZÁROS, B. & SZABÓ, I. (2020). Prediktív rendészet [Predictive policing]. Péter Ruzsonyi (ed.). *Közrendészet* [Public Safety]. Ludovika Kiadó, Budapest

MÁTYÁS, SZ. (2016). A külföldi bűnelkövetők területi és strukturális jellemzői Magyarországon [Territorial and structural characteristics of foreign offenders in Hungary]. In: Hautzinger, Z. (ed.) *A migráció bűnügyi hatásai*. Magyar Rendészettudományi Társaság, Budapest, pp. 75-87.

MÁTYÁS, SZ. (2024). *Crime Geography*. Oradea, Editura Universităţii din Oradea. (https://real.mtak.hu/204407/1/Crime_Geography_MatyasSzabolcs.pdf)

Perry, L. W., Mcinnis, B., Price, C. C., Smith, S. & Hollywood, S. J. (2013). 'Predictive Policing: Forecasting Crime for Law Enforcement'. Research Summary. Santa Monica, RAND.

URL1: https://www.europol.europa.eu/publications-events/main-reports/tesat-report

URL2: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_hu

7.4. Predictive Algorithms in Criminal Justice Decision-Making Procedures

Zsanett Fantoly

7.4.1. Introduction

The dynamic technological development of recent times has made a multitude of new tools available to the state and to authorities acting on criminal matters in both the United States and Europe to achieve more effective control of crime. Among these, the computer-based risk assessment algorithms grounded in probability calculation are worth highlighting, and the potential applications of which are very broad: from law enforcement and investigative duties (predictive policing tools) all the way to the imposition of sentences during court trials, and to the execution of sentencing (e.g., COMPAS risk and need assessment). They can be usefully employed in numerous fields.

This study deals with the opportunities and dangers inherent in the application of computer-based criminal risk assessment, by juxtaposing the social interest attached to establishing criminal liability with the individual interest of the accused in the right to a fair trial. In addition, it examines, from several perspectives (fundamental rights and criminal procedural law), the possible applications of computerised risk assessments in the future of Hungarian criminal procedure.

7.4.2. The Application Areas of Computerised Risk Assessment Algorithms in Criminal Justice

Algorithms used by the police in the course of crime prevention uncover previously unknown connections on the basis of which it becomes possible to predict which places are more likely become crime scenes, as well as those individuals with particular profiles who are more likely to commit crimes.

Surpassing traditional map-based predictions, the linking of various computerised databases also allows the identification of connections between people, places, and means of commission that were previously undetectable.

Risk assessment also appears as a predictive tool within the institutional system of corrections. With the help of algorithms, and based on pre-defined risk factors, convicted persons are classified into low-, medium-, or high-risk groups, to which, for example, the opportunity for parole eligibility is attached. Until now, decisions concerning reintegration of inmates into society, before they have served the full length of their sentences was mostly grounded in the subjective impression of the corrections judge; however, predictive analysis is capable of evaluating the circumstances that form the basis of the decision on objective grounds. Thus, society takes less of a risk in granting parole to convicts, since those who are not ready for it can be more easily filtered out by the algorithm. The final decision remains in the hands of the corrections judge, but the information provided by the software can provide significant assistance in making the decision (Fantoly & Lichtenstein, 2018).

In criminal justice, that is, in judgments, what is at stake is whether – by taking account of the defendant's profile – mathematical methods are used during proceedings to predict not only whether the accused is likely to appear at trial (and therefore, whether detention must be ordered for that reason), but also the form, degree, and length of sanction ideally suited to the accused (based on their prior record and the type of crime committed) that would also properly serve both general and special prevention. In reality, however, we are not envisaging a 'robot judge,' since determining criminal liability and the evaluation and weighing of the evidentiary tools separately and all together remain a human judge's task. The software is simply a support in the choice of the type and degree of the appropriate sanction.

7.4.3. Algorithmic Decision-Making in Criminal Justice and in Judgments

In delivering a judgment, it is the judge's task to select the appropriate, adequate sanction. The objective weight of the offense is examined but also – partially as a consequence of the requirement to individualise the sanction, during its selection – the judge examines the danger the offender personally poses to society, keeping an eye on the risk of repeated offending. In this activity, American judges are aided by data concerning the defendant's prior convictions, as indeed are their Hungarian counterparts. However, in the United States, pre-sentence investigation (PSI) reports, which serve as an information base for sentencing, have been used for decades. In recent years, this has been supplemented in several states with data from systems-based risk assessment, whereas here in Hungary this is still awaited (Fantoly & Lichtenstein, 2018). If society wishes to rely on algorithm-based risk assessments in a field as important as criminal justice, a particularly warranted critical examination of these methods is justified – a task assumed in the present study.

Artificial intelligence (AI) can play a role at several levels concerning judgment in criminal justice. Answering legal questions that require a single correct answer, for example, is 'child's play' for AI, and similarly, we receive useful results when we expect it to perform a unidimensional evaluation of numerical data or set it the task of applying unambiguous legal concepts (for example, what constitutes homicide and what penalty is weighed against it by the Criminal Code). However, correctly answering the qualification questions of more complex offenses requiring more intricate proof, as well as the comprehensive – even cross-jurisdictional – interpretation of legal norms, may pose a challenge even to AI. Selecting the proper temporal effect of (criminal) legal norms and maintaining a clear overview of the coherent system of closely related legal concepts are also more difficult tasks for algorithms.

Therefore, if we were to consider the hypothetical introduction of a 'robot judge', during criminal judicial decision-making the primary problem would be the examination of the aggregation of multiply qualified offenses, as AI knows neither the dogmatic principles of criminal law developed over centuries, nor the related, ever-evolving judicial practice. The dogmatic analysis of criminal culpability is likewise a critical issue, since distinguishing intent/negligence/blamelessness in connection with the subjective side of an offense (the so called *men's rea* or 'guilty mind') exceeds the level of machine learning. Further difficulties arise in making AI capable of correctly applying legal principles and constitutional norms developed over centuries during individual decisions, as well as of competently using the sociological background of criminal behaviours and the societal reactions to them, namely punishments.

Beyond the framework of precise legal concepts, navigating the complex and multifarious regulation of the legal system, and selecting and correctly interpreting the appropriate legal norm in any given case can thus represent challenges for an algorithm (Filatova, 2025). This situation is further nuanced by a constantly changing legal environment, meaning the frequent, sometimes almost untraceable changes in legislation, and the chaotic system of judicial decisions following contradictory jurisprudence (Ambrus, 2025). During sentencing, and in connection with the management of criminal records, however, AI may be a useful assistant for the human judge, and may even be entrusted with simple computational tasks such as calculating the precise amount of criminal costs.

7.4.4. Practical Examples of Decision-Making Algorithms Used in Criminal Justice

7.4.4.1. COMPAS: The World's Best-Known Criminal Justice Decision-Making Application

The globally best known decision-making application in the field of criminal justice is the U.S. COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) model, which has supported the work of judges grounded in the risk of recidivism (Szabó, 2024). The algorithm sorts convicted persons into three categories, depending on how likely the accused is to reoffend – such as, for example, the extent to which the convict's release back into society via parole poses a danger. The model has faced numerous criticisms, which has drawn attention to the dangers inherent in AI-based judicial decision-making. Critics most strenuously highlighted (race-based) discrimination, noting that the machine learning algorithm rated a much higher number of African-American defendants as high risk for parole, compared to convicted persons of other nationalities (Angwin et al., 2017). It must not be forgotten, however, that the machine learning algorithm makes its mathematically determined decisions based on the input data that is analysed (Miskolczi & Szathmáry, 2018); thus, in the case of COMPAS, the system could only access information from databases that were themselves grounded in pre-existing discriminatory social differences (Karsai, 2021). This problem only became apparent later, proving that from the outset, the operation of the system was neither clear nor unambiguous, either to actors practicing criminal justice (judges, prosecutors) or to defence attorneys (Zavrsnik, 2021). A lack of transparency is unacceptable in a criminal procedure governed by the rule of law because it undermines the guarantee system of the fundamental right to a fair trial; consequently, the operational order of the applied algorithm must be known to all participants in criminal justice – authorities and individuals alike (Lepri et al., 2017).

The best-known case associated with the COMPAS algorithmic decision-making procedure was that of Eric Loomis, who, based on several legal grounds, attacked the risk assessment software used in Wisconsin. According to Loomis, his right to a fair trial was infringed in the first instance when he was not able to contest the scientific validity of the underlying tests and the results of the 137-questionnaire, since neither he nor the judge presiding over his case possessed precise knowledge of the mathematical or statistical probabilities that were used in developing the software nor of the methodology on which its classification and evaluation was based. The company that developed the algorithm, Northpoint, did not make substantive data and information on the algorithm's operation public, citing business secrecy. Loomis also declared as a violation of his right to a fair trial the fact that his race and nationality were taken into account by the algorithm, with disadvantageous consequences for him (Angwin et al., 2017).

Despite the above criticisms, AI-based algorithmic systems have the undeniable advantage of being able to process large amounts of data quickly, thereby increasing and improving the efficiency of criminal justice, and promoting the handing down of judgments in criminal cases within a reasonable time frame. Among specific algorithmic application techniques, advanced analytics is capable of selecting documents for example by tone or topic, while a new achievement among process-mining algorithms is the filtering of risks. Another benefit of their use is that – provided they are supplied with data of adequate quality – they make decisions based on objective grounds rather than judicial subjectivity (Fantoly & Lichtenstein, 2018). Uniform judicial practice, which is an essential pillar of legal certainty, as part of a fair trial requires the judge to act impartially and without bias in exercising their judgment, that is, to make decisions exclusively in accordance with the law and their conscience. The spread of judicial subjectivity is impermissible and remains at the forefront of scholarly research to this day. For example, the 'hungry judge' theory is particularly notable on this topic; that

research found that after lunch, judges hand down more lenient judgments than before eating (Chatziathanasiou, 2022).

7.4.4.2. De lege ferenda Proposal for the Application of AI in Sentencing in Hungary

The research forming the basis for a *de lege ferenda* proposal on the use of AI in sentencing in Hungary analysed the sentencing practice in criminal proceedings for people-smuggling (Section 353 of the Criminal Code) brought before the Szeged District Court in a Hungarian city close to the Serbian border. Through processing the files (and judgments) of 514 human smuggling cases, the research examined the types and degrees of penalties imposed in actual cases. The criminal law researchers aggregated and evaluated this data and compared it with the sentencing principles of the Hungarian Criminal Code and related judicial practice (Fantoly et al., 2025). Subsequently, the group's statistician attempted to establish an algorithm that, based on the input data (e.g., the specific length of prison sentences imposed, the weighted aggravating and mitigating factors considered by judges allowing deviation from the so-called 'mid-range penalty'), would make it possible to determine values identical or very close to the actual length of prison terms imposed.

To create the algorithm, familiarity with the rules governing sentencing in Hungary was required. The Hungarian Criminal Code's sanction system contains absolute determinate penalties (for example, the 'three strikes' rule or mandatory exclusion from a profession under particular circumstances), as well as *de facto cogent* sanction rules (such as compulsory fines). The Criminal Code also regulates apparent cogent sanction rules – for example, deportation – and true cogent sanction rules -- for example, forfeiture (Gellér et al., 2019). The predominance of cogent rules may make the introduction of AI in determining the appropriate type and degree of sanction in a particular case seem simple; however, as

previously discussed, numerous other factors (e.g., non-uniform judicial practice) impede this application.

In examining sentencing practices in people-smuggling cases, the research group naturally set out from the Criminal Code's rules on sentencing. For prison sentences, the Hungarian Criminal Code generally defines a sentencing range with a particular minimum and maximum for each type of offense (for example, imprisonment from one to three years, from two to eight years, from five to fifteen years, etc.). When imposing a prison sentence within such a range, the judge must start from the so-called 'mid-range penalty,' which is half the sum of the lower and upper limits (e.g., five years in the case of a two to eight year range). Any deviation from that amount must be justified by the judge. In this the aggravating and mitigating circumstances applicable to the case are decisive, that is, circumstances related to the specific situation, such as the seriousness of the crime or the personal background of the offender. The list of aggravating and mitigating circumstances was laid down by the Supreme Court in Opinion No. 56 of the Criminal Collegium (mitigating circumstances include, for instance, a full, factual, and incriminating confession, remorse, or compensation for the harm caused; aggravating circumstances – to give a non-exhaustive list – include the national or local prevalence of the offense, the criminal record of the offender, repeated commission of offenses, etc.). In the algorithm built by the research group, each mitigating and aggravating factor featured with different weighting, depending on how relevant the human judges, presiding over the 514 human smuggling cases, considered those factors in determining sentence without AI, and how they had influenced the actual length of imprisonment imposed. For example, the number of persons transported was the most significant aggravating factor, while among mitigating circumstances, the defendant's cooperation with authorities – a confession – had the greatest effect on judicial decisions when the judge decided to depart from the mid-range penalty (Karsai et al., 2025).

7.4.5. Closing Remarks

In decision-making procedures within criminal justice – as in nearly every area of life – there remain numerous as-yet untapped possibilities in the application of artificial intelligence. However, the rendering of criminal judgments requires a complex legal mind-set, for which neither the development of legal terminology nor the analysis of supreme court case law by AI is, as yet, remotely sufficient to ensure proper decisions.

Nevertheless, there are many intermediate decisions (for example, the precise calculation of the amount of criminal costs, or the extraction of penalties previously imposed in similar factual scenarios for a given case) and administrative tasks (such as choosing the format of a resolution, transferring personal data from earlier judgments, or compiling a defendant's prior convictions from earlier cases) in which AI can assist a human judge. Even for these tasks, the elaboration of structured quality assurance regulations is indispensable.

References

AMBRUS, I. (2025). Using algorithms during criminal sanctioning – an Example of Hungary. Conference presentation*: 'Green and digital transition,' June 17–20*, Szeged, Hungary

ANGWIN, J., LARSON, J., MATTU, S., & KIRCHEN, L. (2017). Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased Against Blacks. ProPublica. (https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing)

CHATZIATHANASIOU, K. (2022). Beware the Lure of Narratives: 'Hungry Judges' Should Not Motivate the Use of 'Artificial Intelligence' in Law. *German Law Journal*, 23(4), pp. 452–464. (https://doi.org/10.1017/glj.2022.32)

FANTOLY, ZS., GÁL, A., & KELEMEN, B. (2025). Az embercsempészés bűntette miatt indult büntetőügyek büntetőeljárási sajátosságai a Szegedi Járásbíróság 2022–2023. évi joggyakorlatának tükrében [The criminal procedural characteristics of criminal cases initiated for the crime of human smuggling in light of the case law of the Szeged District Court in 2022–2023]. *Magyar Jog* (Forthcoming)

FANTOLY, ZS. & LICHTENSTEIN, A. (2018). Számítógépes kockázatelemzés és büntetőeljárás [Computerised risk assessment and criminal proceedings]. *Belügyi Szemle*, 66(10), pp. 5–22. (https://doi.org/10.38146/BSZ.2018.10.1)

FILATOVA, M. (2025). Generative AI for deciding the cases – limits and opportunities. Conference presentation: *'Green and digital transition,' June 17–20*, Szeged, Hungary.

GELLÉR, B., AMBRUS, I. & VASKÚTI, A. (2019). *A magyar büntetőjog általános tanai. II. Büntetéstan (A büntetőjogi jogkövetkezmények tana)*. [General doctrines of Hungarian criminal law. II. Criminal law (The doctrine of criminal legal consequences)] ELTE Eötvös Kiadó, Budapest

KARSAI, K. (2021). Algorithmic Decisions within the Criminal Justice Ecosystem and their Problem Matrix. In: G. Vermeulen, N. Peršak & N. Recchia (eds.). Artificial Intelligence, Big Data and Automated Decision-Making in *Criminal Justice*, 26–27, Maklu

KARSAI, K., FANTOLY, ZS., GÁL, A., KOVÁCS, P. & KELEMEN, B. (2025*). Judicial Discretion and Sentencing Disparities in Human Smuggling Cases: Empirical Evidence from Hungary* (unpublished manuscript).

LEPRI, B., OLIVER, N., LETOUZÉ, E., PENTLAND, A. & VINCK, P. (2017). Fair, Transparent and Accountable Algorithmic Decision-Making Processes: The premise, the Proposed Solution, and the Open Challenges. *Philosophy & Technology* 31, 4, pp. 611–627 (https://dspace.mit.edu/bitstream/handle/1721.1/122933/13347_2017_279_ReferencePDF.pdf)

MISKOLCZI, B. & SZATHMÁRY, Z. (2018). Büntetőjogi kérdések az információk korában [Criminal law issues in the information age] *HVG* Orac Lap-és Könyvkiadó Kft, Budapest, pp. 42-45.

SZABÓ, I. (2024). Automatizált döntéshozatal és a büntetőeljárás [Automated decision-making and criminal procedure]. *Ügyészek Lapja*, 2024(4-5)

ZAVRSNIK, A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*, 18(5), 623-642.

Laws and Precedent

Supreme Court (Kúria). 56. számú Büntető Kollégiumi vélemény [Opinion No. 56 of the Criminal Collegium of the Supreme Court]

Act C of 2012 on the Criminal Code (Btk.), Section 353 [on human smuggling], Section 80 (1)-(2) [on sentencing framework]

European Convention on Human Rights, Article 6.

State v. Loomis, 881 N.W.2d 749 (Wis. 2016). Wisconsin Supreme Court jurisprudence. Commentary: *Harvard Law Review*, Vol. 130, Issue 5.

7.5. Application of Predictive Systems in Private Security and Municipal Enforcement

Anita Bückő

7.5.1. A New Security Dimension: From Reactive to Proactive

Today's technological advances are having an impact on both public and private security thanks to the development of information technologies and artificial intelligence (AI). The increase in terrorist threats, crime, such as burglaries and other incidents against persons and property in recent years has prompted us to adopt a new approach to public and private security. While classic, post response-based approaches such as manual processing of crime data and post-incident assessment after on-site observation remain essential, we must keep pace with the dynamically changing threats and environment in urban transport, community, and private spaces to increase effectiveness (Mátyás et al., 2019).

A data-driven approach to safety provides an opportunity to transform a reactive approach into a proactive one.

Predictive analytics methods can help us make predictions by integrating historical crime, traffic, demographic and/or environmental data, as well as real-time sensor information into complex algorithmic models. Past events can help forecast future incidents, making the historical data approach a new way of working in the field of security (Ajay & Fussey, 2020).

Urbanisation has brought with it major social, infrastructural and security challenges around the world. Cities have become overcrowded, interaction between people has declined, and with it the likelihood of anonymity, indifference and, in many cases, crime.

The acceleration of urban life, the loss of personal control, and the possibility of hiding in the crowd have created an environment in which traditional law enforcement tools are often no longer sufficient.

In response to these threats, the data-driven approach to security is gaining ground. Municipal policing is gaining new opportunities in the design of security in urban spaces, while private security can use a data-driven approach to protect premises and to optimise the allocation of physical resources (Sankin & Mattu, 2023).

7.5.2. Data, Space and Behaviour: A New Approach to Urban Security

Keeping cities safe is no longer just a matter of physical presence, but increasingly of data usage. Classic CPTED (crime prevention through environmental design) seeks to reduce the number of incidents by shaping the physical environment. Both physical means (natural surveillance, area boundaries, access control, maintenance and preservation) and community involvement (education and training, information and awareness, land use, community functions) can help to create a more liveable and safer urban environment, but predictive analytics adds data-driven aspects to CPTED principles (Dallos, 2020).

Predictive technologies can be used to identify patterns in events in urban spaces, but this requires a lot of the data mentioned earlier. This type of approach is no longer based only on the physical presence of the people responsible for security, but also on the interpretation of the data, and let's face it, in a modern urbanised environment, the use of a data-driven approach is essential. Geospatial methods can be used to identify hotspots, provide answers to the question 'Where? What is there? What has changed since then?' or even 'What is the relationship between them?' (Bückő, 2025)

In order for the predictive method to be most accurate, we need to provide all the relevant additional information, whether it is about the object, the person or the environment. These can be of various types, but the following indicators may be relevant in the formulation of predictions:

- SPATIAL DATA

Under these, the GPS coordinates associated with past events, or location-specific information, form one of the fundamental pillars of predictive technology. They can be used to locate potential hotspots, thus allowing for a more targeted action. Spatial information is key to optimise camera systems, reposition live protection or determine patrol routes.

- TEMPORAL PATTERNS

When examining time-based data, information on time of day, time periods or seasonal effects can be used to identify time-based trends. Temporal patterns also help in capacity planning and the development of patrol structures. This could include focusing on street sections prone to clustering, street disturbances, and unlit, deserted areas during weekend evenings.

- BEHAVIOURAL PATTERNS

Different behavioural patterns, such as movement dynamics, grouping or body language, play a prominent role in predictive analysis. Intelligent surveillance systems can identify these patterns and detect them at the beginning of their development, thus preventing their evolution. They are particularly useful in the case of mass events and large crowds in confined areas, both for private security and law enforcement.

- ENVIRONMENTAL DATA

Environmental factors can have an impact on the development of security that you would never imagine. Lighting, noise, and weather all influence the

development of events (Eindhoven Design District, n.d.), from poorly lit street sections where limited visibility favours offenders to noisy areas where a call for help goes unnoticed. On a foggy, precipitous day, the number of people in public places is reduced, creating an environment that facilitates crime and increases the possibility of concealment.

- DEMOGRAPHIC DATA

Based on social composition, age, economic status and housing characteristics, the system can help identify which groups are more likely to commit crimes. This can be used to target programmes and develop prevention programmes aimed at disadvantaged or juvenile groups (Bückő, 2025).

7.5.3. Public and Private Security in Data-Driven Decision Making

DigitalTwin (DT) technology is a type of public and private security system method that provides a 3D model of the physical environment, updated in real time, which enables preventive interventions because the model allows not only for spatial mapping but also real-time data analysis. It reflects the current operation and condition of a city or object, and can use AI to predict security risks. It plays a key role for municipal law enforcement in the surveillance of public spaces and the timing of interventions. Think of the booming nightlife in cities, the clustering that goes with it, and the street sections that 'invite' vandalism. Pedestrian traffic and incident data can be used to plan patrol routes in advance which need to be reinforced in a district or at a given time and specific route.

The majority of municipalities have indoor and outdoor CCTV or IP cameras that provide and record data (Vári et al. 2025). Archived footage allows for post event analysis, but using predictive technology, the algorithm compares

the motion patterns from previous footage with the recent data and can generate real-time alerts.

In a related context, it is also necessary to mention the smart city concept, which is becoming increasingly widespread. These cities are equipped with a multitude of IoT systems such as sensors and cameras. Smart CCTV networks in themselves increase the security of the area and the protection of the built environment. The integration of IoT and AI is already next level in data analytics, as IoT digitally connects elements of the physical world and extracts information from them in real time. Together, they enable real-time data collection and analysis, helping to improve the responsiveness and effectiveness of security systems. Big Data can be processed and analysed in real time using AI, enabling the timely identification of potential threats, which in turn enables timely responses (Kisfonai, 2023).

Armed security guards in a special situation, bridging the gap between private security and law enforcement, are responsible for protecting critical infrastructure. In these places, real-time response to an unexpected event is key. However, early detection of dangerous situations can give you a head start in an environment that has a significant impact on the public (Bückő, 2025).

7.5.4. The Connection between Private Security and Data-Based Systems

In terms of private security, predictive analytics solutions offer the possibility of optimising protection resources – both technical and human – to time preventive measures and to proactively manage local risks. Information from enterprise security systems, such as access control and alarm systems, camera networks and live guarding all generate huge amounts of data. This can be used to identify patterns of entry and behaviour, which can also be used to detect anomalies and identify potential security risks (Harmati & Szabó, 2020).

Increasingly, private security providers are deploying AI-based systems that can indicate in real time which areas are likely to be affected by an incident, and can even suggest changes to patrol routes (Bückő, 2025).

The use of predictive technology can also help in asset protection maintenance strategies since data on the operating time, failure rate and environmental stress of a failed security element (e.g., camera, lock, motion sensor) can provide predictive information for the timing of replacements and services.

7.5.5. Municipal Security Tasks and the Predictive Approach

The municipal police have a key role in ensuring order in public spaces, promoting public safety and dealing with and investigating complaints from the public. Data-driven solutions in this environment also facilitate decision making based on real-time and historical data, making it more targeted and effective.

CCTV systems operated by municipalities, noise and traffic detectors, complaint reporting databases and, last but not least, feedback from the public can provide important information. By compiling these in a database and then processing the data predictively, it is possible to identify recurring incident locations, clustering areas or even zones with seasonal changes in load (e.g. summer events).

The combination of the above-mentioned spatial information tools and AI allows for optimal law enforcement interventions in space and time. Patrol routes or camera positions with fixed positions are no longer static, but can be dynamically modified and reorganised on the basis of forecasts.

Integrating community policing with predictive technology is a way of using information from the public to complement the patterns identified with

machine learning, thus promoting the acceptance of predictive technologies by the public.

7.5.6. Ethical, Technical and Social Challenges in the Use of Predictive Systems

AI-based systems are only as good as the data that feeds them. Models based on historical data often inherit the biases of the past. The usefulness, performance and reliability of the model depend on the data used. It must be accurate, up-to-date, complete, and representative. Statistics and data used may not necessarily reflect the real information, as they only include reported and therefore accessible cases. The high latency of crime statistics is well known, so the main distorting factor may be an unrepresentative data set (Suhajda, 2019).

Another problem is historical bias. That is, if some neighbourhoods have had a higher police presence in the past, they may have recorded more incidents, so the model may tend to classify these neighbourhoods as dangerous in the future. This is a perpetual feedback loop, which can become a self-fulfilling prediction of the model (Mátyás et al., 2020).

In the application of predictive technologies, be it in private security, municipal policing or law enforcement, the following principles should be given special attention:

- TECHNICAL STABILITY

  Continuous monitoring, updating and incident management of the system is essential. Decisions resulting from model failures should not lead to unpredictable risks in either the urban or private security environments.

- HUMAN OVERSIGHT

  Predictive systems cannot make decisions autonomously. Human control and human decision-making are required before implementation, which is of paramount importance in the field of security.

- DATA PROTECTION

  The system should process the data used only for the purpose and after prior verification. Sensitive data must be anonymised and the right of data subjects to access or delete the data must be guaranteed.

  The system may process the data used only for the purpose and after prior verification. Sensitive data must be anonymised and the data subject must have access to or the right to delete the data.

- TRANSPARENCY

  The operation of the system, the datasets used and the methodology should be documented and explained.

- ACCOUNTABILITY

  Version changes, data sources, parameterisation and interventions of the AI modules should be documented in a traceable manner. Actions should not be automatic, the person giving the instruction should be recorded.

- DISCRIMINATION

  Bias in historical data should not be a disadvantage, demographic data should not be a categorisation of anyone.

- SOCIETY

  The population should not be burdened by the use of a predictive model, it should help to increase their sense of security. It is important that the predictive system is not only transparent but also socially acceptable. The principles apply from model design through to operation and retraining.

7.5.7. Conclusion: The Usability of Predictive Systems in Private Security and Municipal Policing

In private security, predictive technology is based on data from access logs, camera images, alarm events and patrol logs. These enable the model to recognise patterns of entry and behaviour. Algorithms can be used to identify anomalies, predict anomalous activity, and provide contextual analysis of security incidents.

Municipal police can increase their efficiency in monitoring public spaces, responding to complaints from residents, and optimising patrol routes. Data from incoming IoT devices can help AI to identify hotspots, optimise interventions in a timely manner, and analyse public activity using geospatial tools. The predictive system can then propose, for example, changes to street lighting, patrols (both in terms of numbers and routes) or even urban planning.

The significance of the predictive analytical approach is thus the importance of AI-based forecasting, a new approach to security that has found its place in both private security and municipal policing.

'This work was supported by AI-assisted tools, but all interpretations and conclusions are solely those of the author.'

References

AJAY, S. & FUSSEY, P. (2020). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing and Society*, 31(1), pp. 66-81. (https://doi.org/10.1080/10439463.2020.1803315)

BÜCKŐ, A. (2025). *Prediktív analitika a közrend és magánbiztonság szolgálatában* [Predictive analytics in the service of public order and private security] (Thesis) NKE RTK, Budapest

DALLOS, E. (2020). Építészeti bűnmegelőzés gyakorlata I. [Architectural Crime Prevention Practice I.] (PowerPoint presentation)

EINDHOVEN DESIGN DISTRICT (n.d.). Intelligent Lighting System Eindhoven (https://www.eindhovendesigndistrict.com/en/projects/ilse)

HARMATI, B. & SZABÓ, I. (2020). A prediktív rendészet és az automatizált igazságszolgáltatás [Predictive policing and automated justice]. *Belügyi Szemle*, 68(5), 23-37. (DOI:10.38146/BSZ.2020.5.2)

KISFONAI, B. (2023). A bűnügyek jövőbeli megelőzése, avagy a prediktív rendészet új arca [Future crime prevention, or the new face of predictive policing]. *Rendőrségi Tanulmányok*, 6(3), pp. 58-73. (https://doi.org/10.53304/RT.2023.3.02)

MÁTYÁS, SZ., SALLAI, J., TIHANYI, M. & VÁRI, V. (2019): A rendőri elérhetőség és a bűnözés közötti összefüggések térbeli elemzése. *Területi Statisztika*, 59(2), pp. 152-163.

MÁTYÁS, SZ., MÉSZÁROS, B. & SZABÓ, I. (2020). Péter Ruzsonyi (ed.). *Közrendészet* [Public Safety]. Ludovika Kiadó, Budapest (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16197/TKP_Kozbiztonsag.pdf,jsessionid=42E9F8E7957BA203AE1EA1F79060F17C?sequence=1#page=1896)

SANKIN, A. & MATTU, S. (2023). Predictive policing software terrible at predicting crimes. *Wired Security* (https://www.wired.com/story/plainfield-geolitica-crime-predictions/

SUHAJDA, A. (2019). Néhány gondolat a prediktív rendészetről [Some thoughts on predictive policing]. Rendőrségi Tanulmányok, 2(3), 75-85. (https://real.mtak.hu/154754/1/suhajda.pdf)

VÁRI, V., MÁTYÁS, SZ., TIHANYI M.& KRASNOVA, K. A. (2025). CCTV and Crime Prevention Effectiveness: Experience of Hungary. BRICS Law Journal, 12(1), 40–55.

7.6. The Predictive Measurement Tool (PME) in the Hungarian Prison Service

Orsolya Czenczer

7.6.1. About the Risk Analysis and Assessment System in Hungary

The Hungarian Prison Service operates a Risk Analysis and Assessment system (hereinafter referred to by its Hungarian acronym: KEK system) for the purpose of assessing, evaluating and managing the risks of recidivism and the detention of convicted persons. The purpose of the KEK system is to increase the effectiveness of the penal system, to promote successful reintegration, identify, analyse and manage individual risks of recidivism and detention by motivating and maintaining the motivation of prisoners, and by reducing the number of reoffenders. The elements of the KEK system in Hungary are defined in Section 29(2) of Decree 16/2014. (XII.19.) IM (hereinafter: IM Decree) on the detailed rules for the enforcement of imprisonment, detention, pre-trial detention and detention in lieu of a fine.

The most important tool in the KEK system is the so-called predictive measurement tool (hereinafter referred to by its Hungarian acronym: PME), which conducts an assessment in order to facilitate the complex process of successful reintegration of convicted persons, the essence of which is to predict the probability of certain risks occurring using statistical and professional tools. In Hungary, in this process, assessment is followed by treatment, with targeted, standard programmes and the use of a so-called category system. So, the risk assessment tool known as the Predictive Measurement Tool is technically a software programme and, as such, provides a clear framework for collecting the data that forms the basis of the risk assessment and for displaying the risk levels based on the answers to the questions. Four different departments of the prison institutions are involved in the risk assessment, during which they independently

interview prisoners and enter the data into the PME system. Although the four departments enter the data into the same software, technically they ask four different sets of questions of the prisoners (Somogyvári, 2024).

The PME is thus a questionnaire used to predict the anticipated behaviour of prisoners using statistical tools, which also includes an admission (intake) interview. Its purpose is to obtain standard information that can assist professional work and provide a basis for predicting the expected behaviour of prisoners using statistical tools. Each questionnaire is put to the prisoners by a different professional field and the answers are recorded on a computer programme. When completing the questionnaire, it is important to keep the following rules in mind:

- The RELIABILITY OF THE DATA is of paramount importance. Accordingly, each answer must always be provided from the most reliable source available (e.g., court judgment, etc.).
- In the absence of reliable data, the INTERVIEWER'S SUBJECTIVE OPINION or doubts about the truthfulness of the answer CANNOT OVERRIDE THE PRISONER'S ANSWER. Therefore, it is not the interviewer's opinion of the correctness or truthfulness of the answer that should be recorded, but the prisoner's answer to the question. If the interviewer has doubts about the authenticity of individual answers, there is a space in the final section of the questionnaire for this, which asks about the interviewer's subjective impressions.
- The questions in the questionnaire should be interpreted, meaning that THEY SHOULD BE ADAPTED TO THE SITUATION, ASKED IN ACCORDANCE WITH THE PRISONER'S ABILITIES, and the answers given by the prisoner should be entered into the predefined answer options.
- The individual blocks of questions are intended to inquire about THE RISKS UNDER INVESTIGATION. At the same time, it should be noted that there may be

questions to which the inmates' answers may conceal quite different risks (e.g., in the case of professional qualifications, which, depending on the profession, may be a factor that either reduces or increases the likelihood of escape). There are examples and counterexamples for everything, but we cannot address these exceptions in a questionnaire that is used as a standard predictive measurement tool; accordingly, we will explore the generalities here.

- THE VALUE OBTAINED AFTER ASSESSING EACH RISK IS NOT EVIDENCE. Respondents in certain fields have the opportunity to correct the risk level, regardless of the values obtained, by evaluating the elements of the given situation and the personality of the prisoner as they perceive it, which we cannot ask about in a targeted manner in the questionnaire.
- A significant proportion of PRISONERS ARE UNLIKELY TO DISCLOSE INFORMATION THAT IS DETRIMENTAL TO THEM, but some are likely to do so; the questionnaire focuses on the latter group of prisoners.

The PME questionnaire targets the following risk groups:

- Self-harm, suicide
- Escape
- Aggression towards staff – aggression towards inmates
- Use of psychoactive substances
- Low or high status in the subculture

Some questions in the PME questionnaire should only be asked upon initial admission, while others will be asked again at certain intervals. Sections that ask for subjective, summary opinions are marked separately.

7.6.2. Implementation of the Predictive Measurement Tool (PME) in Everyday Prison Work

The uniform KEK system accompanies the convict from the beginning to the end of their imprisonment, providing information on the degree of risk of reoffending and the likelihood of law-abiding behaviour during the period of imprisonment. The essence of the analysis is that the identified risks provide an opportunity for intervention (treatment), which requires the provision of a targeted treatment programme. As a result of the interventions, a reduction in the level of detention risk and an increase in the effectiveness of reintegration can be expected (Figure 1).

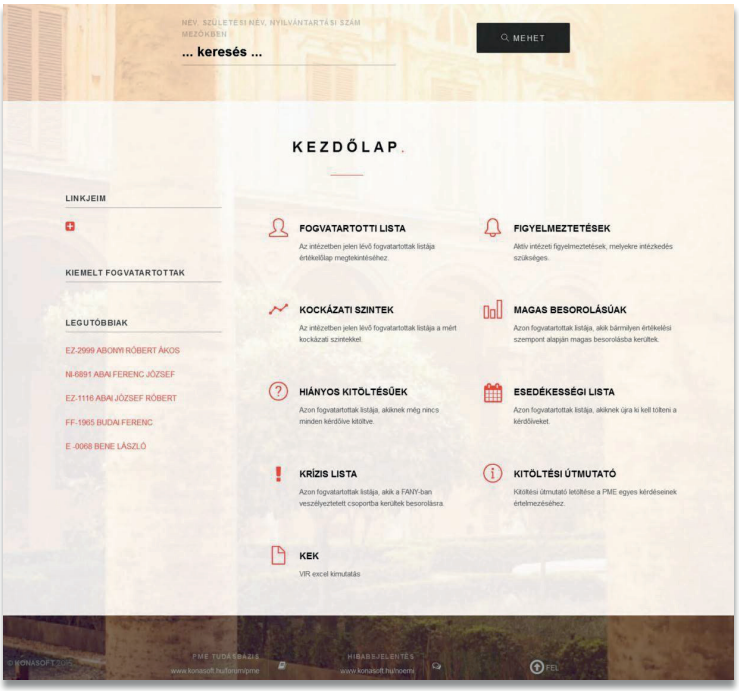


Figure 1: Risk Analysis and Assessment Module home page

For newly admitted prisoners, the PME questionnaire must be completed by the prison in which the prisoner will serve the prison sentence on which admission is based. Furthermore, if the PME has already been completed (from previous judgement and executions), its content only needs to be reviewed.

The prisoner is obliged to cooperate in the procedures for assessing the risks of recidivism and detention. The risk analysis is based on a general questionnaire covering four areas (registration, reintegration, health, and psychology) relating to prisoners, which records and stores in a database the information that is typically available and currently accessible at the time of admission.

The questionnaire is recorded in an internal electronic registration system (Főnix3 System) Risk Analysis and Assessment Module, which, in addition to recording and managing data, functions as a decision support IT system. The significance of the PME lies not only in the assessment and analysis of detention risks, but also in ensuring the flow of information between specialist areas by providing uniformly accessible data of the same scope (Bogotyán et al., 2024).

Using the answers to specific questions in the reintegration and registration sections, the PME creates an admission data sheet that collects the most important information revealed during the admission process. If a sentenced prisoner is transferred to another prison, it is not necessary to complete the PME questionnaires again, but the data collected at the previous prison must always be reviewed as part of the intake procedure.

A detailed presentation of the question groups for each of the four areas of expertise follows.

7.6.2.1. The Registration Department's Role in the PME Questionnaire

The Registration Department has the 'easiest' job with the PME, because most of the information the department is working with is from objective documents: court orders, conviction acts, police information, prosecutor documents, school certificates, etc. Thus, with regard to information on criminal history, the registration department's area of expertise is to collect objective data. As mentioned above, the official internal electronic system of the Hungarian Prison Service is the Főnix3 System, and the answers to most of the questions about a prisoner are taken from this register. As part of the admission procedure, the registration department must ask the convicted person questions that are not covered by the Főnix3 system. It is important to know, that the data for the PME must be recorded within 8 days of prisoner's arrival at the prison facility.

Information and data that are not available within the above deadline must be entered into the PME immediately after they become known.

7.6.2.2. The Reintegration Department and Officers' Role in the PME Questionnaire

The reintegration module of the questionnaire is designed to assess, among other things, the prisoner's demographic data, lifestyle, harmful addictions, social background, financial situation, personality traits, education, employment, and social contacts. These questions are asked by the prisoner's reintegration officer. Some questions may not be understandable to prisoners, in which case they should be explained to them. Some of the questions relate to the prisoner's own opinion, which should be recorded verbatim. In all such cases, we are interested also in the interviewer's subjective opinion, even if it contradicts what the prisoner has said previously. These opinions can be filled in a separate module at the end of the questionnaire. These opinions may be particularly important for the subsequent assessment and risk analysis.

The risk assessment of the convicted person (PME recording) must also be carried out during the admission procedure within 8 days of placement in the reception unit. Every prison has a 'reception or intake unit'. When a prisoner arrives at a prison they have not previously been held in, they must be placed in the reception or intake unit in order to learn the rules of the prison, and also for the prison to learn about the newcomer. This period can last up to 15 days.

The convicted person must be present in person to complete the reintegration part of the PME questionnaire. In the reintegration module, the following questions are used to gather information about the prisoner and assess their motivation:

- Life events, social relationships
- Upbringing, education
- Employment and financial situation
- Housing
- Criminality, antisocial values, adaptation
- Substance use and addictions
- Leisure time, interests, reintegration
- Law enforcement history and foreign connections

Here, for example, we highlight a few questions from the reintegration module:

Question: 'What is your marital status?'

The respondent may not understand the term 'marital status' or may not interpret its meaning correctly. Therefore, we recommend that the respondent consider the answer to the question and, if necessary, ask a clarifying question (suggestion: 'Are you married or just living together?').

Question: 'Where did you live before you were admitted?'

Here we are interested in the place of residence of the prisoner before they were admitted to the institution, i.e. the place where the prisoner habitually resided before their admission.

Question: 'Are you under guardianship or custody?'

This question aims to determine whether the prisoner was raised by their own parents or whether they were ever placed under guardianship or custody (for any length of time). The question may not be clear to the prisoner, but anyone who has been under guardianship will probably understand the meaning of the word, so if the respondent is not familiar with the concept, the answer 'no' should be selected based on the above assumption.

Question: 'Have you participated in competitive sports?'

The aim is to find out whether regular competitive sports activities were a feature of the prisoner's life, but it is possible that the prisoner is not familiar with the concept of 'competitive sports'. Competitive sport refers to athletes who are registered with a club, or compete regularly under the colours of an association.

Question: 'Do you smoke? Have you quit? If yes, how severe were the withdrawal symptoms?'

This question applies to prisoners who have tried to quit smoking. If the respondent has attempted to quit several times, it is necessary to assess how severe the withdrawal symptoms were during the most recent attempt.

Question: 'Have you been in prison in the last 5 years, and if so, were you employed?'

From a reintegration perspective, the work experience gained by prisoners in prison is essential, and this question is designed to measure this. The question asks the prisoner to answer for the 5 years prior to the time of completion, including their current sentence. We believe that data older than five years is not relevant to this question, which is why we have narrowed down the time frame.

However, if the prisoner does not remember the period five years ago accurately, we should simplify the question to the last few years from the time of recording.

Question: 'What is your opinion of prison work?'

The aim is to find out the prisoner's attitude towards prison work, that is, to what extent they consider it a compulsion or a good opportunity. The prisoner may mention wages as an advantage of prison work; we have not created a separate category for this, so this answer should be recorded in the 'good opportunity' category.

Question: 'Do you think complete alcohol withdrawal will be a problem for you?'

We would like to obtain information on how difficult it will be for the prisoner to abstain from alcohol in prison. The interviewer should consider the information provided and, if it is not sufficient to answer the question, ask further questions about the amount of alcohol consumed, the types of drinks consumed, and other characteristics of consumption. The purpose of the question is to find out how alcohol-dependent the respondent is and how much of a problem (security risk, possible involvement in extraordinary events, health consequences) alcohol withdrawal will be for them.

Question: 'If so, how has the frequency and amount of consumption changed?'

In the case of prisoners whose drug consumption has changed over the years, in terms of either quantity or frequency, it is important to know in which direction the change has occurred. If either factor, i.e. the frequency or quantity of drug consumption, has increased, the answer 'increased' should be marked.

Question: 'How much do you fear the following in prison?

Deterioration of physical condition, emotional abuse by fellow inmates, psychological terror; Lack of material goods and various services and

opportunities available in civilian life; loss of outside assets, business connections, job opportunities; being ordered around by prison staff.'

The purpose of this question is to find out how much the prisoner fears the occurrence of the events listed. How they view their situation in prison.

Question: 'Have you experienced any trauma, crisis, or loss in the past six months? Is there anything among these that you would like to resolve?'

This question applies to prisoners who have experienced a traumatic, crisis-inducing event in the preceding six months. The aim is to find out whether the respondent intends to resolve this difficulty or problem. The answer 'cannot be resolved' should only be recorded if the prisoner has indicated an event that is difficult or impossible to resolve (e.g., a death). However, if the answer 'cannot be resolved' only reflects the prisoner's current distress and pessimism, it is recommended to explore the question more thoroughly to find out whether they actually want to resolve the problem.

Question: 'How did you support yourself before you were incarcerated?' Alternative questions: 'Where did you get your money from? / What was your source of income?'

The interviewer should not automatically record the answer, as the prisoner may not be fully aware of the meaning of the terms listed, so it is necessary to clarify the nature of the employment relationship by asking leading questions (How regularly did you work? Who did you receive your money from and in what form? etc.).

Question: Would you take advantage of any of the following opportunities at the institution?

Craft clubs, art classes, other cultural activities, sports clubs – explain what activities take place at each of these. The aim of this question is to assess how the prisoner would spend their free time in prison.

With regard to reintegration, the form compiled by the PME contains the information that the reintegration officer needs to gather in order to get to know the prisoner. After assessing and evaluating the individual risks, the reintegration officer must work with the prisoner to draw up an individualised detention programme plan (in Hungarian an EFP) within five days, which also includes options for managing the identified risks.

When compiling the individualised detention programme plan (EFP), the prisoner's reintegration needs and social situation, as well as the risk factors that threaten the order and security of detention, must be taken into account in order to ensure the effectiveness of risk management. Risk management covers the entire period of imprisonment, and its individual elements may be modified depending on the performance and results of the prisoner (Bálint & Tóth, 2023).

7.6.2.3. Healthcare Questionnaire in the PME

The healthcare questionnaire is also based on objective data,[11] and assesses the health status of prisoners and the resulting risks. The health module of the PME therefore focuses on the prisoner's illnesses, disabilities, medication, and the other characteristics of their health status.

The questionnaire must be completed within 72 hours of admission, based on a physical examination and medical history taken by the admitting physician (Havasi, 2024). Prisoners with data indicating a potential health crisis are admitted to a healthcare unit on a priority basis.

Most of the questions are self-explanatory, but in some cases, the individual answer options or categories require further explanation and clarification to assist in completing the form. Based on the answers received, the

[11] With regard to the data recorded in the PME, the provisions of Act XLVII of 1997 on the processing and protection of health and related personal data: Act CLIV of 1997 on healthcare shall apply accordingly.

health module classifies the prisoner into one of the following categories answering two key issues: 'What is the prisoner's state of health? Do they have any known illnesses, and if so, what are they?'

The PME final categories:

a.) *Completely healthy*

No significant known illnesses.

b.) *Limb or sensory organ deficiency*:

Absence of a limb or sensory organ, or at least 50% functional impairment (this includes: persons with prosthetic limbs, limbs damaged or amputated proximally from the first major joint, visually impaired or hearing impaired patients; this does not include: the absence of 1-4 fingers or toes, or a functional impairment of the limbs or sensory organs not exceeding 50%).

c.) *Severe cardiovascular or pulmonary disease (at least 1 hospitalisation).*

Known severe cardiovascular or pulmonary disease requiring at least 1 hospitalisation in the past 2 years (including: myocardial infarction, moderate or severe COPD, hypertension that is difficult to control with medication, diabetes with cardiovascular complications, pacemaker, not including: drug-treated, stable hypertension, mitral valve prolapse, mild bronchial asthma or COPD).

d.) *Moderate or severe musculoskeletal or musculoskeletal disease:*

Known moderate or severe musculoskeletal or musculoskeletal disease (rheumatoid arthritis, Bechterew's disease).

e.) *Other, progressive, longer-term illness:*

Other progressive, difficult to treat and highly likely to be fatal, long-term diseases or conditions (nephrotic syndrome, multiple sclerosis, tumours, progressive autoimmune diseases, amyotrophic lateral sclerosis, degenerative nervous system diseases).

f.) *Major psychiatric disorders:*

Major psychiatric disorders (including schizophrenia, schizoaffective psychosis, bipolar disorder, paranoid disorders, severe personality disorders, unipolar depression; not including anxiety disorders, neuroses, adjustment disorders, conversion disorders).

g.) *Substance dependence:*

Substance dependence in the medical history (including: alcohol or drug dependence, pathological gambling; not including: smoking, occasional alcohol or drug use).

h.) Other chronic illness or physical disability:

Other chronic illness or physical disability (includes conditions and illnesses not listed above, as well as illnesses that fall under one of the above categories but do not meet the above criteria in terms of severity).

Here we highlight a few example questions from the health module:

Question: 'Is the prisoner taking any medication?'

Regular parenteral medication refers to, for example, insulin-dependent diabetics, COPD patients regularly using inhaled steroids, patients undergoing interferon treatment, etc.

Question: 'Are there any noticeable, visible, distinctive marks on their body (e.g., wounds, surgical or other scars, tattoos, noticeable moles, etc.)?' 'If so, what are they and where are they located?'

Distinctive marks may include tattoos, wounds, scars, moles, warts, or other marks. When determining the location, the following categories should be used: head, face, ear, forehead, eye area, neck, chest, abdomen, back, shoulder, waist, upper arm, forearm, hand, fingers, groin, buttocks, thigh, lower leg, foot, other. When describing a distinctive mark, the respondent should specify its exact location (right foot, left side, ring finger, etc.), size, and pattern.

7.6.2.4. Psychological Questionnaire in the PME

Every prison in Hungary has at least one psychologist, but the large prisons have an entire psychology department with a staff of 2-8 psychologists for the inmates and personnel.

The PME questions on psychological issues are intended to assess the risks of detention and recidivism as well as the state of mind and mood of the prisoner. These questions must be completed within eight days of admission. The convicted person must be present in person to answer these questions for each section of the psychological questionnaire. The question groups in the questionnaire are as follows:

- Life events, coping
- Psychiatric history
- Suicide, self-harm
- Psychoactive substance use
- Antisocial attitudes, aggression
- Goals, vision for the future
- Individual assessment

Prisoners with data indicating a potential crisis receive a consultation with a psychologist on an out-of-turn basis.

These are some examples of questions and explanations on these types of issues: *Question: 'Have you ever been under psychiatric or psychological treatment?' If yes: when, why, and how many times?*

Many lay people do not know the difference between a psychiatrist and a psychologist, which is why both are included in the question. The question is aimed at determining whether the respondent required regular treatment for psychological problems. If the prisoner visited a psychologist, it is worth clarifying what specific problem was behind this and whether it was indeed therapy.

Question: 'Were you under the care of a psychiatric ward?'

We probably already know the answer based on the above question, so we only need to clarify if any information is missing. That is, we need to ask: 'What was your relationship with the treatment staff like?' The purpose of the question is to find out whether the patient was able to adapt to the conditions of the closed ward or whether they were considered a problematic patient. In this case, 'problematic' means that with some cooperation, conflict with the staff could have been avoided. Cases resulting from a state of ecstasy or helplessness do not fall under this category. The question can also be phrased as follows: 'Did you get along well with the nurses and doctors?' 'Were you satisfied with the hospital care?' Some people start listing the reasons why they sued the hospital or why they turned to another attending physician, so conflicts may surface in the answer.

Question: 'How was your relationship with your fellow patients?'

This question helps us assess how well you were able to integrate into a forced community in the past.

Question: 'Were you placed in a healing-therapeutic ward?'

This question is only relevant for prisoners who have been in prison before. The name has changed, so those who are not familiar with it may know it as a 'healing-educational group.' Their integration can be well inferred from whether they were transferred from the healing-therapeutic ward. If not, and they remained in the group until their release, then it can be assumed that they were justified in being there and were able to behave appropriately. If they were transferred, this may indicate that they failed to integrate into the group or that there were repeated conflicts.

Question: 'Have you attempted suicide?' If yes, then: 'Where did it happen?' 'How many times in total?' 'When was the last suicide attempt?' 'What was the trigger?' 'How did it happen?' 'How serious was it?'

The question can also be phrased as 'Have you ever tried to kill yourself?' Generally, they do not object to the question. Be prepared for the possibility that the prisoner will answer yes, but later, when asked more detailed questions, it will become clear that they were referring to self-harm. In this case, it is necessary to clarify whether the act was intended to end their life, as this distinguishes attempted suicide from self-harm, regardless of severity.

Question: 'Are you currently having suicidal thoughts?' If yes: 'What is the reason for this?'

'Are you thinking about killing yourself these days?' 'Are you thinking about it right now?'

It's worth asking follow-up questions to get to the bottom of this, because manipulative inmates might say yes to get special treatment. The collective category of 'closed institutional conditions' includes everything related to prison life, such as admission itself, separation from family, uncertainty associated with pre-trial detention and charges, the sudden disruption of one's previous lifestyle, but it can also include serious conflicts with cellmates, abuse, and victimization. If they do not shut down, we can ask them about the details, and they may tell the psychologist something they have not dared to share with anyone else.

Question: 'Have you ever intentionally harmed yourself physically?' 'If so, where did it happen?'

Since self-harm is a completed act, it is not appropriate to talk about attempts. Instead, ask: 'Have you committed self-harm before?' 'Have you intentionally caused yourself injury?' We are interested in whether you have ever hurt yourself, not in an attempt to commit suicide, but to cause pain or attract attention. One can be more specific and say that one is are referring to cutting, blade swallowing, and the like, thus clarifying the question. If this question reveals that the cuts mentioned in the suicide attempt actually belong here, then the answers need to be corrected.

'If so, where did it happen, how many times, when, how, what was the trigger, and do you still think about it?'

The purpose of the question is to find out whether this behaviour is characteristic of the person in a closed institutional setting or in their life outside.

Question: 'Has anyone in your family committed (completed) suicide?'

If the answer is yes, ask whether the person died as a result of the attempt. Record any attempts that resulted in death.

Question: 'Do you consume alcohol?' 'If so, how often, what kind, what effect does it have on you, have you ever drunk it with medication? etc.'

If they do not know what we mean, provide examples. Some people do not know what 'alcohol' is, and only recognise terms such as beer, brandy, vodka, etc.

Question: 'Have you ever tried or used drugs?' If yes: when, what kind, for how long, alone or in company, etc.

It may be necessary to define 'drugs' because, for example, some may not consider marijuana to be a drug, or will not consider intoxicating substances that are not yet prohibited by law to be drugs.

Question: 'When you become tense or nervous, what do you do?'

If they do not understand the question, explain the situation using an example and then ask if they have experienced something similar.

Question: 'Have you ever been so upset that you couldn't control your emotions?'

The question is about aggression, so it does not count if, for example, they started crying because of a sad movie.

Question: 'Have you ever verbally or physically abused a member of the staff?' 'If so, how?' 'How did you resolve the situation?'

Suggested simplification: 'Have you ever been in a fight with guards?' 'Have you ever had a serious conflict with the supervisory staff?' Only cases where you acted

as the aggressor are relevant. Suggested explanatory question: 'Did you only verbally abuse the person, or did it escalate to physical violence?'

Question: 'Have you ever been a victim of abuse while serving your sentence?' 'If so, how?' 'Please briefly describe such a situation!', 'Has anyone ever hurt you in prison?'

If they are very hesitant, you can reassure them that they can talk about it without fear of harm or disadvantage. We ask about the nature of the abuse, which may be indicative of their integration.

One of the most important issues in the psychological module is the assessment of personal responsibility. The PME assesses this as follows:

Question: 'Please briefly explain why you are in prison now!'

The purpose of the question is to explore the following factors:

- Do they believe that what they did was indeed a crime;

- Do they feel remorse or shame about their actions;

- Are they related to the victim (this will be important later in maintaining contact);

- Do they blame the victim or someone else, or take responsibility for their crime.

Question: 'What do you think about being in prison now?'

The purpose of the question is to assess attitudes toward crime and, in part, to explore any negative feelings about prison, such as whether it matters to them how their friends and family will view them after this, etc. And on the other hand, whether they feel at home, have friends, or have a routine in prison. It can also be considered routine if a family member has been in prison and told them about it, because in this case they may feel that it does not come as a surprise. Those who have been conscripts (older men) usually mention that this situation is similar and can be endured.

For young people or those who are shy, you can ask the general question: 'What do you think about someone going to prison?' because they may be more honest in their answers about criminal attitudes if they do not have to talk about themselves.

Question: 'What is your opinion about your current sentence/pre-trial detention?'

The purpose of this question is to find out whether they consider the punishment/detention to be fair, justified, and acceptable. Those who cannot accept it may experience a psychological crisis as a result and may also develop a resistant attitude towards the institution.

Question: 'What are your current plans and goals?'

'What are your plans for your time in prison?' It is worth allowing time for them to come up with an answer for themselves. If, upon admission, they only list their plans for life after release, it is necessary to broaden their perspective to include prison and emphasise that it is important to have plans for the time spent in prison as well, because this will help them survive. During the follow-up interview, you can ask how well these goals have been achieved and what, if anything, has prevented them from achieving their goals.

Question: 'What are your plans and goals after your release?'

The lack of a realistic vision for the future is a sign of depression. Unrealistic ideas carry the risk of disappointment and failure to reintegrate.

7.6.3. Overall Assessment

The PME automatically performs calculations related to detention risks, but due to its nature, it cannot provide a complete overview of the attributes of the convicted person that are relevant from a penal enforcement perspective, so it is justified to use other individual analysis tools as well. With this information in

mind, the various fields of expertise may deviate from the detention risk values, i.e. they may modify the classification value given by the PME, either upwards or downwards. The convicted person must not be informed of the measured or modified detention risk values; the information provided should only cover which activities are recommended for him or her to participate in, in order to reduce the detention risk.

Based on the specialist assessments, the security risk analysis results in a classification that can be: HIGH, MEDIUM, or LOW, depending on the answers to the questions, the scores assigned to them, and the centrally determined score threshold.

The overall assessment is not based on the sum of the points awarded for the questions assessed by the specialist areas, but is aligned with the highest classification value of each specialist area.

After admission, no later than 15 days after placement in the receiving (intake) unit, the Admission and Detention Committee (in Hungarian, hereinafter: BFB) organise a hearing at which they talk to the convicted person. At this hearing the BFB decides on the prisoner's placement (in general or special unit), employment (prison work), involvement in a reintegration programme, education, training, and the level of detention risks based on the results of the PME (high, medium or low).

Furthermore, if necessary and based on the judgment and within the scope of its competence and jurisdiction, the BFB shall also decide on the initial category classification[12] of the convict.

[12] In Hungary there is a Category and Credit System: every convicted prisoner is placed in one of the five categories and receive extra contact time with relatives, extra benefits, more freedom depending on the category they are in. Of the five categories 1 is the easiest with the most freedom, 5 is the toughest with the strictest regime. Inmates can collect credits for almost everything they do right. They can move from one category to another based on credits.

The risk classification system offered by the PME is categorical, as it operates with mutually exclusive indicators along the lines of detention risks; for example, low and high status in the prisoner hierarchy are logically mutually exclusive. The risk of detention is absolute in the sense that it should not be determined on the basis of comparison with prisoners in a given prison institution, department, or category.

For example, a low-status prisoner remains high-risk in terms of this detention risk even if he or she is placed with similar prisoners, and the classification of a prisoner with a high risk of escape does not change simply because he or she is placed in a more secure prison.

The BFB must inform the convicted person of the overall assessment level of the classification based on the individual detention risks in order to recommend participation in a reintegration programme that reduces the risk of recidivism.

The situation assessed by the PME and the programmes provided by correctional institutions make it possible to treat prisoners arriving at correctional institutions earlier, based on the risks identified, before their detention and/or other problems become more serious.

The BFB is responsible for enrolling prisoners in the reintegration programme or terminating their enrolment, as well as for evaluating the effectiveness of their participation in the programme (awarding/withdrawing credit points).

The BFB is also responsible for providing appropriate information and guidance to at-risk prisoner populations (such as juveniles, drug users, drug addicts, prisoners with low socioeconomic status, etc.). These prisoners are be given appropriate information and guidance, and individual prisons place continuous emphasis on this when planning and implementing prisoner programs. In order to achieve reintegration goals, all interventions within the prison system aimed at preventing and treating aggression and drug problems within prison walls,

mitigating anger management problems after release, and laying the foundations for a drug-free life should receive special attention and support.

7.6.4. PME Based Programmes to Reduce the Risk of Recidivism

In Hungary, based on data recorded in the PME and professional classification, prisoners classified as high or medium risk in terms of substance use, aggressiveness, and high or low position in the subculture, are offered the opportunity to participate in reintegration programmes that reduce the risk of recidivism and incarceration after the admission procedure, upon placement from the reception unit. The individualised detention programme plan of the convict must specify which detention risk reduction activities are recommended for them based on identified risk.

Reintegration officers and social workers are trained by professionals on 12-session programmes aimed at reducing the risks of incarceration and recidivism. Examples of such programmes include: activities promoting self-assertion (assertiveness), group activities to reduce aggression (anger management), activities to help prevent drug use, and activities to help reduce alcohol consumption problems.

7.6.5. Electronic Display of the PME and Representation of the Process

In the Főnix3 Module, each prisoner has an individual data sheet, (as shown in the header in Hungarian – translated in English: Summary; Registration: Reintegration; Health; Psychologist; Other opinions). By opening the 'Other Opinions' panel, the system makes available the opinions recorded so far about the prisoner, that are relevant from the point of view of risk analysis and risk management (Figure 2).

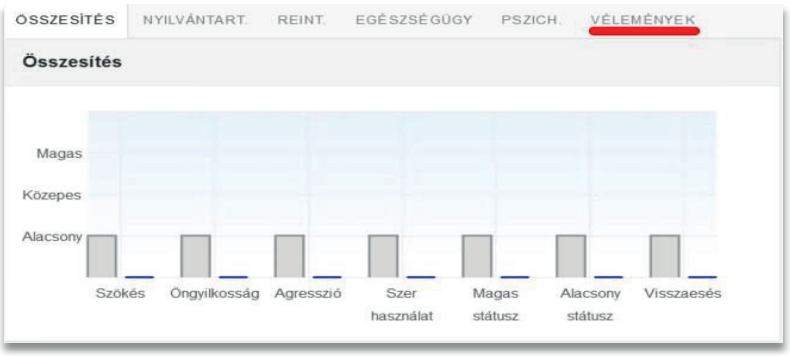


Figure 2: Opinions panel on the detainee's data sheet

Individual impressions during the PME recording can be recorded here, by every staff who got in contact with the prisoner during the PME process. To add further detail or opinion, the personnel only need to provide three additional pieces of information from a drop-down list: (see Figure 3.)

- The position/field of expertise of the person recording the opinion,
- The status of the opinion, which can be draft, not final, or closed,
- The type of opinion – only opinion types related to psychological and reintegration opinions are available here; other opinions and notes can still be recorded in Főnix3.

Text also can be entered into the 'Opinion text' field by typing or copying and pasting.

Figure 3: Form for recording a new opinion

7.6.6. Summary

The PME risk assessment tool used in Hungarian prisons is technically a software programme and, as such, provides a transparent framework for the collection of the data that forms the basis of risk assessment and for the display of risk levels. The methodological logic of the domestic risk assessment system is very similar to the operating principles of systems used in other European countries. The questionnaire is essentially based on the prisoners' self-reported answers, which are supplemented by specialist assessments. The system is therefore based on information known to the prisoner (e.g., crime data), or on the prisoner's self-reporting.

As is apparent in the above, four different departments within the prison system are involved in the risk assessment (PME) process. Prisoners are interviewed independently of each other and the data is entered into the Főnix3 system. The four areas of expertise therefore enter data into the same software, but technically they use four different questionnaires for the prisoners.

The REGISTRATION DEPARTMENT provides data on criminal background, previous and current terms of imprisonment (e.g., sentence data and information

on recidivism). It therefore primarily supports risk assessment with static data that can be extracted from the public registry and derives from the nature of the crimes and the criminal career of the prisoner in question.

The REINTEGRATION AREA records data on the prisoner's contacts, family background, education, employment and financial situation, housing conditions, and history of substance abuse and other addictions.

The HEALTH FIELD provides information on general health and the presence of diseases, medication use, and a history of suicide or substance abuse based on medical records.

The PSYCHOLOGY QUESTIONNAIRE is the longest, collecting and evaluating information on psychiatric history, suicide, self-harm, psychoactive substance use, and the prisoner's antisocial attitudes and aggressiveness.

In line with the four different questionnaires for the four fields, the software has a modular structure, and, given the sensitive nature of the data, its authorization system has been developed at a complex, hierarchical level. For example, health data can only be viewed by healthcare personnel and is not accessible to anyone else.

The risk assessment, i.e. the completion of the questionnaire according to the above modules, must be carried out for the first time when the prisoner is admitted, but in connection with certain events affecting detention (extraordinary incidents in prison, significant life events in the prisoner's life, etc.), the risk assessment must be carried out again. Based on the answers to the questions, a risk rating appears on the PME interface for each field of expertise, the value of which may be adjusted by the representatives of the respective fields based on professional decisions. The BFB decides on the level of the convict's risk categories by summarising the results of the individual fields of expertise, which becomes the PME'S FINAL RISK RATING.

References

BÁLINT, B. & TÓTH, V. (2023). Egy reintegrációs kiemelt projekt visszaesési hatásvizsgálata [Impact assessment of relapse in a priority reintegration project]. *Börtönügyi Szemle* 42(4), pp. 94-101. (https://bv.gov.hu/sites/default/files/bsz_2023-4_online.pdf)

BOGOTYÁN, R., SÓS, G. & SZAUTER, L. (2024.). Jövőbeli innovatív technológiák a büntetés-végrehajtásban [Future innovative technologies in the penal system]. *Börtönügyi Szemle* 43(2-3), pp. 9-27. (https://epa.oszk.hu/02700/02705/00137/pdf/EPA02705_bortonugyi_szemle_2024_2-3_009-025.pdf)

HAVASI, S. (2024). A fogvatartottak egészséghez való joga a digitalizáció korában [The right of prisoners to health in the age of digitalization]. *Börtönügyi Szemle*, 43(4), pp. 9-25. (https://bv.gov.hu/sites/default/files/bsz_2024-4_online.pdf)

SOMOGYVÁRI, M. (2024). Az elítéltek klasszifikációja, a kategória – és kreditrendszer működési elve a 2024-ben hatályba lépő törvény alapján [Classification of convicts, the operational principle of the category and credit system based on the law coming into effect in 2024]. *Börtönügyi Szemle*, 43(1), pp. 15-37. (https://bv.gov.hu/sites/default/files/bsz_2024-1_online.pdf)

7.7. Application of Dynamic Network-Based Risk Analysis and Evaluation in Preventive Policing

Zoltán György Bács

7.7.1. Introduction

Professor Géza Finszter often uses a phrase in his lectures, succinctly and with deep meaning, that encapsulates the purpose of prevention: 'the most acceptable crime for society is the one that does not even happen.' According to Section 5 (2) of the currently effective Criminal Code, 'an act, an activity or omission that violates or endangers the person or rights of others, or the social, economic, or state order declared by the Fundamental Law of Hungary is dangerous to society.' (Criminal Code 2012) Accordingly, Professor Finszter's expression can then be interpreted as the theoretical and practical-theoretical basis of prevention. Beside the laws and regulations concerning law enforcement activities that specify our tasks in general, the events, reasons and timing to prevent them can be deduced from Professor Finszter's words. The answer is simple: to make unlawful or contrary behaviour or action impossible before it occurs.

This seems a simple directive, but its implementation is a multi-faceted task. The first question – and it is of key importance – is whether detection is possible, which is *sine qua non* from the point of view of prevention. The next question is in essence what kind of criminal acts shall be prevented? Can we pick and choose the criminal acts to be prevented? The third question is rather more complex: How can repeated crimes, or socially highly dangerous crimes, be prevented, paying special attention to their multiplicity, repetitiveness, or their growing social threat? I must be clear here, all criminal acts are nothing more than the results of unique processes.

In this study, I will try to give an idea of a method that can provide positive answers to these questions.

7.7.2. The Basics

All activities and actions are complex phenomena, but – when examined statically – some general, individual or specific group characteristics exist. If a crime is a unique, one-off act, it will also have features characteristic of the perpetrator's personality, circumstances, individual personal qualities, abilities, and limitations. These have been dealt with by special disciplines for many years, and they have been processed from many perspectives. The large variety of general and specific characteristics have been catalogued in many ways from paper-based card systems, in drawings or boxes to digitalised, complex, online, queryable registration systems.

Examining this from the perpetrator's side, one can state that every perpetrator, or any person who is planning to commit any illegal act, or who commits one – with or without premeditation, under the influence of circumstances deemed favourable to them – will have unique characteristics indicating their individuality and personality. This is a subject for analysis in criminal psychology, and pre-eminently in the field of criminal profiling. It is obvious that the occasional perpetrator also has personality traits that can be inferred by the circumstances of the crime, which can and do provide clues during an investigation and evidence gathering process. The personality traits of a person who is planning and considering the possibility, method, means, time and other circumstances of a crime to be perpetrated are of particular importance.

The description of the unique characteristics of the instruments of any crime resembles a constantly expanding library. As crimes themselves change, the material contexts and the toolset that accompany them also change. It is obvious that the traces left by the tools used during a crime, as well as the micro-traces, have unique characteristics. All traces are revealed and evaluated first at the crime scene investigation and later in the forensic laboratories.

One of the greatest achievements of recent decades has been digitization, the process of expressing the properties of a subject in numerical form. While this was a huge step forward in many ways, it has been surpassed by modern requirements.

7.7.3. What is Needed Today?

7.7.3.1. A New Type of Information Theory

In order to make the previously statically examined phenomena known as *data* suitable for conducting a dynamic study, they must be distinguished from *information*. That means breaking with previous practice. The Data Protection Act does not define what data is (Act CXII of 2011). Consequently, it may even be correct to state that what is called data in today's understanding can actually be accepted as information according to the more modern understanding, since it has a conceptual basis. For example 'car' (which can be understood as an inactive element of information), and there is a qualifying part (active element) with which it can be connected to other information, for example: ' white coloured car'. The qualifying factor (active element) linked to the conceptual basis (inactive element) makes it possible to retrieve the information, i.e. the specific unit composed of inactive and active elements, the 'white car', that is to search it out in the registry during an investigation, the gathering of evidence or even a preventive or routine inspection. This unity of the inactive and active element[13] is the cornerstone of a new type of non-IT-based information theory (Bács, 2023a).

[13] Several active elements can be connected to one of the inactive elements, forming a network. Consequently, active elements connected to several separate inactive elements can also form a network with each other. Such a multiple or multi-part, multi-complex network also affects searchability. The more inactive elements there are, the more difficult it is to discover and connect the elements' own network with another network based on an inactive element. It is also true that the more active elements connected to an inactive element in the network, the more focused the search can be.

If we perceive actions as dynamic processes rather than static phenomena, then it will also be necessary to examine and evaluate information in terms of its dynamics. The prerequisite for this is to not simply state that information has a life cycle. Going beyond this, it is necessary to recognise that information can go through several value states during its life cycle, and that these value states can have different effects on the given examination (Bács, 2023b).

On the same line of thought, it follows that information has or can have a latent state, when the information already exists, but we do not yet know of it, and thus cannot take it into account. The existence of latent information can be indicated by the existence of two or more pieces of information that precede or follow the latent information and can be fitted into a logical (deterministic) sequence. In this case, the latent information can be deduced or made probable based on the deterministic relationship.

7.7.3.2. The Three 'C' Requirements

Let's take a look at the basis on which different pieces information can be connected to each other! The first 'C' is *compatibility*, that is, the part (active element) qualifying the conceptual basis of the information is supplemented by new information in some logical way – directly or indirectly – enriched by a new factor additional to the previous information. In other words, the new information is compatible with the old. The expression *new* in this case does not refer to the novelty of the information, but to the novelty of the *relationship* between two or more pieces of information. The second 'C' is *coherence*, meaning that the connection created by connecting multiple pieces of information fits into a logical sequence along a timeline. The third 'C' is the principle of *convergence*, which in this case means that information running on different threads should point in the same direction and be headed towards the same goal in terms of the ongoing investigation, investigative action, etc.

Unfortunately, the scope of this study does not allow for the elucidation of all the significant details of the 3 'Cs' principle. A doctoral dissertation in preparation will provide a suitable framework for this.

7.7.3.3. The Algorithmic Processing of Information (Algorithm Management)

Earlier in this paper, I referred to one of the great achievements of twentieth-century data processing: digitalisation. I have also mentioned that the current and foreseeable future expectations for crime prevention, combating crime, law enforcement, and within that preventive policing, require continuous, practically real-time reception and processing, systematization, filtering, control, analysis, and evaluation of ever larger and continuously expanding amounts of information. Alongside this, the continuous provision of information, so essential for preventive policing activities, the planning of necessary measures, and the execution of operational actions is also of vital importance. The most accessible method for this, but perhaps not the only one, is to transform information into algorithms and perform all other, additional operations on an algorithmic basis. Algorithmic processing allows each and every individual information phenomenon, down to the very smallest, to be recorded, examined, and broken down into its elements before being compared and recombined with other elements. The authenticity and correctness of information appearing in algorithmic form is also easier to verify; it only needs to be compared with similar information obtained from other sources.

7.7.3.4. Forming Networks

Since the antecedents of actions do not follow each other in a linear, deterministic relationship, they are created and implemented as a result of the convergence of several previous events through which it is clear that they were already connected

and interacting with each other. It is also evident that the effect they had on each other when the connection was established could have had some influence on the further progress of the action. The fact that every further change in the flow of events, in the action, is created as the result of an earlier effect coming from several possible directions, gives rise to two new conclusions:

1) They form networks of events/actions that interact and influence each other, which can form new networks. The condition for networking is necessarily the existence of the previously mentioned '3 Cs'.
2) The timing of the occurrence of the events/actions that make up the network, both within the network itself and in relation to other networks, can be separated in time – even at the quantum level – so they are process-like (that is, not static, but dynamic). The dynamic nature of the process requires that the nature of prevention also becomes dynamic.

If we examine this latter conclusion based on the information value theory, it becomes clear that the impact of events interacting with each other does not necessarily appear immediately in terms of consequences, it may only increase in value or change in effect after some other, later event(s) have taken place. This leads to the straightforward, logical conclusion that one of the fundamental characteristics of effective preventive policing is that it must be dynamic.

7.7.4. Practical Conditions for Dynamic Preventive Policing

The basis of all activities in which decisions have to be made is the satisfaction of news needs, for which the means are the collection, acquisition, processing, analysis, evaluation of the necessary information and the formulation of decision alternatives and their dissemination to decision-makers. Everyone knows and applies this information or news cycle. At the same time, when formulating news needs, currently known valid information can be relied on, but which may significantly lose its validity and become obsolete over time. If an assessment is

compiled based on this information, it is practically nothing more than a 'snapshot of the past' and is not necessarily suitable for bridging the gap between the presented situation and the real-time situation that has changed over time. Another negative factor affecting the period of validity is the time required for decision-making. Imagine that while traveling on a tram, you see an acquaintance walking alongside the tram with whom you would like to meet, so you get off at the next stop and head back in the direction where we saw them. You get there, but they are nowhere to be seen, and because you do not know whether they have continued in the direction they were previously travelling, have turned back, or crossed the road, or perhaps gone into a shop, or have just taken a taxi and left the scene. In other words, you were hoping to find your acquaintance at a scene from the past based on a 'photo'.

The solution is to implement a planned qualitative leap, the steps for which are as follows:

1) Higher-level information gathering and information acquisition methods that meet the expected needs of both the present and the future must be developed, including the expansion and networking of the range of accessible data and information bases. General, regular, individual-focused, targeted, and one-off information research needs to be continuous.

2) In accordance with the previously described theories, the analytical and evaluative activity must be transformed, the 'photographic' evaluations tied to the previous news demand and its repetition must be made continuous, dynamic, 'film-like', reducing the 'turnover time' of the news cycle, increasing the speed of rotation, reducing the time for decision preparation and decision-making. The decisions themselves must also be made in such a way that they can be modified as quickly and operationally as possible depending on the changes affecting the process under study (Deitel & Deitel, 1986).

3) The necessary technical background is provided by an IT system supported by artificial intelligence (AI), the functions of which are as follows:

1.) Development of the following algorithms:

a) Scanning, analysing and breaking down data and information bases into algorithms;
b) Screening, in accordance with the direction and purpose of the research;
c) Selection of mutually compatible algorithms (a 3C requirement);
d) Synthesising and recombining algorithms that meet 3C requirements;
e) Real-time (dynamic) evaluation based on retrospective process and trend analysis;
f) Continuous monitoring and debugging (continuous validation of information).

2.) Running the application:

a) Continuous collection of information and support for information acquisition (scanning of data and information bases);
b) Filtering, analysing, evaluating, comparing information, organising elements serving prevention and treating them as of utmost importance, prioritising any necessary decision alternatives, taking into account possible consequences;
c) Continuous re-running of the application and forwarding dynamically changing prevention alternatives and measures to managers (Bács, 2025).

7.7.5. Possible Fields for Application of the System in Preventive Policing

What can we prevent? This is perhaps the most important question for professionals, contractors and volunteers working in law enforcement, policing, public safety and other fields. The following areas serve only as examples, they can be 'deployed' in other areas as well (Bács, 2023c).

1.) The system is suitable for predicting the areas of development of criminogenic processes, their increase in intensity, their sources and possible directions of spread, creating the opportunity to plan preventive measures and to change action plans continuously depending on the information received from the area (Bács & Rusu, 2025).

2.) The system is also suitable for preventing acts of violence within families, at schools, and in the community, as well as for preventing suicide attempts involving specific individuals (Bács & Rusu, 2025).

3.) The system is suitable for dynamic prediction of the development of traffic anomalies, modelling the solutions for critical situations, and determining the necessary technical and human resources for those. The system is capable of preliminary screening of groups with dangerous, anti-social behaviour accompanying particular sports events, determining the location, time, and necessary technical and human resources for preventive measures, and dynamically supporting operational management (Bács & Tóth, 2023).

4.) The system is suitable for planning possible disturbances arising as result of tensions and changes in society, as well as measures to prevent them, with the parameters previously described (Bács, 2023c).

5.) The system is also suitable for supporting the analytical and evaluation activities necessary for decision-making, even under operational circumstances, during the interruption or liquidation of crimes showing an organised pattern of commission, serving to detect and prevent them (Bács, 2022).

The five points above only mention a small section of the possible application areas. But how can such different areas be 'under one roof'? The explanation is in the previous chapters. The basis for everything is algorithm management, new-aspect evaluation, networking and the modernised, dynamic development of long-known prediction calculations.

What does the system work on? The answer is surprisingly simple; it works on:

- Information bases that have any impact on the given field at any time and in the broadest sense;
- From all previously conducted investigations, expert reports, complex legal documents;
- The entire range of knowledge of related sciences, from all previously documented sources;
- The vast amount of information and communication channels available on the World Wide Web. Finding these sources is relatively easy task. The challenge lies in the algorithmisation and processing of this mass of information in several stages, in accordance with the general and specific goals of preventive policing.

7.7.6. Instead of a Closing Statement

We are in a situation where we have in our hands all the elements of the most modern locking system, with all the possible combinations and spare keys. It is up to us when and what to do with it, but do we understand what it supports and can we use it? This system, by its very existence, encourages us to face our profession and ourselves to take a new look at the policing of the future and, within that, preventive policing.

References

BÁCS, Z. GY. (2022). Új, innovatív módszer megalapozása az elemző-értékelő munkában: A dinamikus mátrix alapú módszer [Establishing a new, innovative method in analytical and evaluation work]. *Magyar Rendészet*, 22(3), pp. 83-89 (https://doi.org/10.32577/mr.2022.3.5)

BÁCS, Z. GY. (2023a). Gondolatok az információ szerepéről – más, egyéni szemszögből [Thoughts on the role of information – from a different, individual perspective]. *Nemzetbiztonsági Szemle*, 11(3), pp. 83-92. (DOI: 10.32561/nsz.2023.3.6)

BÁCS, Z. GY. (2023b). Az elemzés és értékelés új módszerének szerepe a megelőzésben, felderítésben és nyomozásban [The role of the new method of analysis and evaluation in prevention, detection and investigation]. In: Gaál, Gy. & Hautzinger, Z. (eds.). *A biztonság védelme a rendészetben: Jubileumi kötet Zámbó Péter ny. rendőr ezredes 70. születésnapjára*. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, pp. 103-109. (https://pecshor.hu/periodika/XXV/Bacs_Zoltan_Gyorgy.pdf)

BÁCS, Z. GY. (2023c). Új tényezők a radikalizáció folyamatában [New factors in the process of radicalization] *Rendvédelem tudományos Folyóirat*, 12(1), 43-52. (DOI: https:// doi.org/10.53793/rv.2023.1.3)

BÁCS, Z. GY. & TÓTH, N. Á. (2023). A sportrendészeti kutatások biztonsági vonatkozásai [Security aspects of sports policing research]. *Rendőrségi Tanulmányok*, 6(3), pp. 74-95. (https://doi.org/10.53304/RT.2023.3.03)

BÁCS, Z. GY. (2025). *Network-researched Based Dynamic Method in Crime Prevention and Investigation*. Ludovika University of Public Service, Ludovika University Press, Budapest. (ISBN: 9789634986812)

BÁCS, Z. GY. & RUSU, D.O. (2025). *Community Policing as an Early Warning Opportunity of Domestic Violence. The Dutch Practice*. Ludovika University of Public Service, Ludovika University Press, Budapest

DEITEL, H. M. & DEITEL, B. (1986). *An Introduction to Information Processing*. Academic Press College Division (ISBN: 0122090055, 9780122090059

Laws

Act C of 2012 on the Criminal Code

Act CXII of 2011 on the right to informational self-determination and freedom of information

7.8. Predictive Maintenance of Security Technology Systems

István Giczi and Levente Tóth

7.8.1. Introduction

Physical security systems – particularly video surveillance, intrusion detection, fire alarm, and access control systems – are indispensable components of modern infrastructure, typically operating on a continuous 24/7 basis. The reliable functioning of these systems has a direct impact on both personal and asset security. In consequence, ensuring that their maintenance is carried out to a high-level is essential, not merely from a repair standpoint, but also in terms of preventive care.

Traditional maintenance strategies – such as reactive maintenance (repairs in case of failure) and preventive maintenance (periodic inspections and scheduled component replacements) – often prove insufficient in preventing unexpected, costly, and high-risk system failures (URL1).

In contrast, predictive maintenance (PdM) leverages advanced technological tools – including IoT, sensor-based monitoring, big data analytics, and artificial intelligence (AI) – to forecast potential malfunctions, thereby enabling timely and targeted interventions.

Industry trends indicate that the PdM approach not only contributes to the optimization of operational costs but also markedly improves system reliability and risk mitigation (URL2). PdM is no longer considered an exceptional initiative but is increasingly seen as a fundamental requirement for the operation of complex, integrated security technology environments.

According to a report by Grand View Research, Inc., the physical security market was valued at approximately USD 127 billion in 2022, with sustained growth anticipated in the coming years. Forecasts suggest that by 2030, the

market size will reach or exceed USD 216 billion, with a compound annual growth rate (CAGR) of around 6.5% (URL3).

This chapter aims to present a systematic and academically rigorous overview of the role and benefits of PdM in the context of security technology systems. By combining up-to-date scholarly references with relevant real-world case studies, particular emphasis is placed on cost-efficiency, uninterrupted system availability, and enhanced levels of operational safety.

7.8.2. Comparison of Maintenance Strategies

Among the following three maintenance strategies, the predictive approach currently offers the highest added value in the context of security technology systems (Ledmaoui et al., 2025).

7.8.2.1. Reactive Maintenance

In the case of reactive maintenance, technical intervention occurs only after a failure has already taken place. This approach can be particularly risky in safety-critical environments because temporary system outages may lead to security incidents. For instance, a service disruption caused by a malfunctioning camera could compromise the safety of a specific area.

7.8.2.2. Preventive Maintenance

The preventive model relies on time-based maintenance, which does not consider the actual condition of the individual devices. While it reduces the likelihood of more serious failures, it often results in excessive expenditures or suboptimal timing, as component replacements are not necessarily scheduled based on real wear or degradation.

7.8.2.3. Predictive Maintenance

The most advanced approach is PdM, which builds upon continuous sensor data collection and the analysis of this data using machine learning and analytical tools. The goal is not merely to predict failures, but to prevent them through timely and optimised interventions. This method is not only more efficient but also potentially more economical, as it reduces the number of unnecessary maintenance actions and minimises unplanned downtime. It is based on real-time monitoring of the actual system condition and data-driven decision-making; interventions are performed only when indicated by the data, thereby avoiding imminent failures. This approach combines reliability with cost-efficiency by ensuring that interventions occur neither too early nor too late.

7.8.3. The Technological Foundations of Predictive Maintenance

PdM represents a complex, multidisciplinary framework that integrates a range of advanced technologies to continuously monitor the status of technical equipment and anticipate potential failures. In the following, we present the key technological and organisational components that form the scientific foundation of this system.

7.8.3.1. Sensors and IoT Devices

The core components of PdM are sensors that provide real-time data on the operational status and performance parameters of equipment. In modern industrial environments, these may include temperature, vibration, current, or voltage sensors monitoring the primary structural and functional variables of machinery. Built-in sensors and self-diagnostic capabilities are becoming increasingly common in security systems as well. For instance, internal sensors in surveillance cameras can monitor image quality or detect changes in camera positioning, while intrusion detection systems may use sensors to report battery charge levels, communication quality, or even physical tampering. IoT-based

device integration enables the continuous, secure, and scalable network transmission of sensor data to central data acquisition and analytics platforms.

7.8.3.2. Data Collection and Big Data Analysis with Pre-processing

The effectiveness of modern PdM systems greatly depends on the quantity and quality of the collected data. The high-volume and often heterogeneous data streams – such as temperature, vibration, voltage levels, network packet loss, or image quality indicators – are stored and processed via cloud-based or edge computing infrastructures.

Big Data technologies enable the efficient management of both structured and unstructured datasets. During pre-processing, operations such as noise filtering, normalization, handling of missing data, and extraction of relevant features are performed. These steps optimise the accuracy and efficiency of analytical and AI-based processing tasks.

7.8.3.3. Artificial Intelligence and Machine Learning

The 'intelligent' aspect of PdM is represented by advanced AI and machine learning models. These models analyse large volumes of continuously incoming sensor data in real time to detect potential anomalies (URL4). They are capable of identifying patterns that deviate from the norm (anomaly detection), modelling equipment conditions through time-series analysis, recognising degradation trends and critical thresholds, and forecasting the likely time of failure – thereby supporting targeted and optimally timed interventions.

Such models can filter out abnormal behaviours that may indicate an impending failure. For example, the gradual blurring or flickering of a camera image may indicate that the lens has become contaminated or that the device mounting has loosened. In the case of an intrusion detection sensor, an abnormal

battery voltage curve may signal imminent depletion. AI can predict when a failure is likely to occur if current trends continue, allowing for pre-emptive intervention. The advantage of artificial intelligence is its ability to continuously learn and provide increasingly accurate forecasts, thereby dynamically adapting to new operating and environmental conditions.

7.8.3.4. Maintenance Management and System-Level Integration

Alerts or work order suggestions generated by PdM algorithms can be directed specifically to maintenance specialists. These notifications may be integrated into enterprise-grade maintenance management systems (e.g., CMMS – Computerised Maintenance Management System) or comprehensive physical security management platforms, enabling fast, transparent, and well-documented interventions.

Modern security systems often support remote access and control, which allows for automated corrective actions – for example, restarting a camera via software in the event of a network anomaly.

The cybersecurity implications of PdM must also be addressed, as numerous IoT sensors and networked devices are involved. It is essential to ensure data encryption and device protection so that the system does not introduce new vulnerabilities exploitable by unauthorised parties. Accordingly, modern physical security platforms mandate encrypted communication and robust access control to ensure that the collection of maintenance-related data does not endanger overall system integrity.

The technical foundation of PdM is therefore a connected system of smart devices that provides real-time 'health monitoring' of security equipment. Such a configuration is capable of continuously tracking the status of cameras, sensors,

and intrusion detection devices and providing immediate alerts when anomalies are detected that may signal an impending failure.

The following sections will examine how these principles are applied in practice across various domains of security technology, and why their implementation is increasingly vital.

7.8.4. Predictive Maintenance in Security Technology Devices: Fields of Application and Examples

7.8.4.1. Video Surveillance Systems

The reliable operation of video surveillance systems is vital in modern security infrastructure, particularly in larger facilities where hundreds or even thousands of cameras may be operating simultaneously. Failure of any component within these systems can pose a critical security risk, as offline cameras may create blind spots, thereby reducing area protection. In traditional operations, a camera malfunction often only becomes apparent when reviewing footage of a particular incident, and there is no recorded image of the event. However, with PdM, the condition of camera systems can be continuously monitored and faults predicted in advance (URL5).

An analysis of a British railway video surveillance network revealed that the camera system on board trains was among the weakest performing technical systems. Between 2020 and 2024, 33 video surveillance system faults were reported. There were a total of 51 surveillance camera failures, 33 monitors, 2 systems, and 2 recording device failures, causing significant operational disruptions, including delays and cancellations. In response, experts applied advanced machine learning algorithms such as Random Forest, XGBoost, Gradient Boosting, and Decision Tree regressors to analyse 1214 event records. The predictive models were successful in forecasting the likely timing of failure

events, thus improving system reliability, operational continuity, and ultimately passenger safety (Rahman et al., 2024).

AI-based camera management solutions are now available that monitor the video feed and operational status of surveillance cameras in real time. The Sentry AI security technology platform, for example, offers a 'health check' function. By continuously analysing reference images and sensor data, the system can automatically detect if a camera's field of view has changed (e.g., due to rotation or displacement), if the lens has become blurred, or if it has been deliberately covered. In such cases, operators receive immediate alerts to enable rapid intervention (URL2).

This functionality significantly reduces downtime: for instance, if a camera becomes inoperable due to vandalism, the system's instant notification enables corrective measures – such as cleaning or replacement – to begin within a matter of minutes. In contrast, with traditional methods, such outages might only be discovered after several days.

Operational experience with Sentry AI and similar platforms indicates that employing intelligent diagnostic and PdM functions can result in significant savings in both maintenance and operational costs, while continuously optimising system performance and enhancing return on investment.

According to some studies, approximately 20% of cameras in large-scale video surveillance networks are malfunctioning or under-parameterised at any given moment; as a result, the entire security system operates at reduced effectiveness or is 'partially blind' during such periods (URL6). The concrete example of the iOmniscient IQ-HealthCheck system aptly demonstrates the practical implications of this technological paradigm shift. This platform provides simultaneous status monitoring for thousands of cameras, enabling real-time performance analysis and automatic detection of deviations. The system can

identify various anomalies such as signal loss, image quality degradation, or camera displacement – issues often caused by physical impacts (e.g., vibration, vandalism) or environmental factors (e.g., heavy contamination, insects on the lens). Following anomaly detection, the system automatically generates a fault report that includes a probabilistic assessment of the underlying cause, as estimated by predictive algorithms. Additionally, the software applies spatially based alert grouping for technicians, thereby optimising inspection and maintenance routes.

The effectiveness of this method has been validated in the field: during a practical test, predictive notifications and optimised location-based maintenance scheduling increased the operational efficiency of the maintenance team by nearly 40%, primarily by reducing travel times and minimising unnecessary dispatches (URL6). As a result, the camera network can maintain high-level coverage continuously, minimising security risks caused by offline devices.

It is important to emphasise that PdM extends beyond physical camera malfunctions to the broader optimization of operations. The latest AI-based security cameras – commonly used in smart city surveillance or high-security facilities – now routinely incorporate built-in PdM modules.

The CC1005G model, a high-performance security camera developed by Horizon Powered, is explicitly equipped with PdM functionality that continuously monitors the device's operational status and identifies potential issues before they lead to system failure (URL7).

Such advanced devices significantly reduce downtime and ensure uninterrupted surveillance, even in highly critical environments such as ports, airports, and industrial facilities.

It is evident that the integration of PdM architectures into large-scale video surveillance networks represents not only a technological advancement but

also a substantial improvement from operational, economic, and security perspectives.

The available software and hardware solutions now enable the incorporation of intelligent, prediction-based maintenance into everyday operations – establishing it as a cornerstone of future-oriented physical security systems.

7.8.4.2. Intrusion Detection Systems

The primary function of intrusion detection systems is to immediately detect unauthorised entry and relay alerts to the appropriate responding personnel or organisation. Given that the operation of such systems is directly linked to the protection of both individuals and property, it is of paramount importance that all components remain in a continuously operational and fault-free condition.

Failures in individual system elements – such as battery depletion in a wireless sensor or a malfunctioning outdoor siren – can substantially impair overall system effectiveness, potentially leading to the failure of protection when it is most needed. Under traditional maintenance strategies, such faults are often only detected retrospectively – that is, following an actual incident – posing an unacceptable risk from a security operations perspective.

In this context, predictive maintenance refers to the continuous monitoring of system components and the early detection of potential faults when certain operational parameters approach predefined limits.

Modern intrusion detection systems already feature control panels capable of collecting diagnostic data from zones and sensors – such as signal strength, power supply voltage or battery charge, and internal temperature in the case of motion detectors. If one or more of these parameters presents a faulty value or a

declining trend based on previously trained predictive models, the system automatically generates a service alert – pre-empting full equipment failure.

This enables maintenance personnel to proactively schedule component replacement or sensor cleaning as part of the next scheduled inspection, thereby avoiding unexpected outages or loss of alarm functionality.

A well-structured PdM programme can substantially reduce the incidence of unexpected failures in intrusion detection systems. For instance, if a particular zone displays an unusually high frequency of false alarms compared to its historical average, the algorithm may identify the cause as a sensitivity anomaly, sensor degradation, or environmental change (e.g., drafts, smoke). By responding proactively to such patterns, it is possible to prevent customer dissatisfaction and avoid a scenario where security personnel become desensitised or 'alert-skeptical' due to repeated false alarms. Furthermore, in IP-based intrusion detection systems, PdM can also extend to network infrastructure components (e.g., routers, switches). For example, instability in a switch port may forecast failure in a network module, which – if addressed in time – can prevent the communication failure of the intrusion detection control unit.

Of course, regular testing remains essential for intrusion systems. However, PdM supplements this by providing a continuous self-monitoring capability to the system. As highlighted by relevant industry recommendations, critical security devices should be checked more frequently, and AI-powered maintenance systems can greatly support this via automated fault detection and alerting (URL9).

This ensures that security system operators can be confident that the intrusion detection system is always ready to function, and not discover – too late – that a sensor had failed during an actual break-in.

In this way, PdM serves both to enhance the reliability of intrusion detection systems and to reduce false alarms, since devices approaching failure often produce spurious alerts. By identifying and remediating such issues in time, the system can continue to operate reliably and continuously.

7.8.4.3. Access Control Systems

The PdM of access control components – such as card readers, electric locks, turnstiles, and other entry management devices – can be significantly enhanced by analysing usage data. For instance, if the mechanical movement of a barrier or turnstile begins to stiffen (resulting in increased current consumption), or if an RFID reader starts to show signs of unreliable performance, the system can issue a warning before the access point becomes entirely dysfunctional. This allows operators to prevent incidents in which, for example, employees are unable to enter the facility during shift start due to the unexpected failure of a critical entry mechanism.

The predictive approach thus supports not only security operations but also contributes to uninterrupted business continuity.

7.8.4.4. Fire Alarm and Emergency Communication Systems

In fire detection systems, reliability is of particular critical importance, and maintenance is strictly regulated by law. Predictive maintenance offers a viable solution for monitoring sensitivity drift in smoke and heat detectors – since, over time, detectors can become contaminated, which may lead to decreased or increased sensitivity. For example, if the system detects that a smoke detector is taking progressively longer to respond to standard test signals, it can be proactively cleaned or replaced before it reaches the point of malfunction.

In this way, PdM not only preserves the core safety functions of the system but also helps maintain compliance with regulatory safety standards – by

ensuring the system remains within required performance thresholds at all times (URL8).

7.8.4.5. Integrated Systems

Nowadays, many cities and organisations use integrated security management platforms that allow for centralised supervision of video surveillance, intrusion detection, access control, and fire alarm systems through a single software interface. These platforms handle vast amounts of data in real time.

In such environments, predictive analytics makes it possible to interpret system states in a contextualised and interconnected manner. For instance, during complex events (such as a simultaneous fire and intrusion scenario), the system can distinguish genuine alarms from potentially faulty sensor signals. AI technologies can jointly evaluate diagnostic data from all connected security devices, enabling the system to prioritise maintenance actions – for example, identifying which faults are critical and which are less urgent.

This allows for the optimal allocation of maintenance resources. Holistic PdM therefore shifts the focus from individual devices to the readiness of the entire security infrastructure. In practical terms, this translates into enhanced safety, reduced false alarms, and more efficient system operation.

7.8.5. Benefits and Outcomes: Why the Predictive Approach Is Essential

As the above discussion already suggests, the growing prominence of industrial digitalization and data-driven decision-making has positioned PdM as an increasingly vital element in modern operational management. Scientific research and industry assessments consistently confirm that the integration of predictive technologies exerts a significant positive impact on equipment reliability, resource utilization, and organisational risk management.

In the following section, we present a structured overview of the proven benefits of the predictive approach, with particular emphasis on its application within physical security systems.

7.8.5.1. Reduced Downtime and Maximised Availability

At the heart of PdM lies condition monitoring and real-time data collection, which together enable the early detection of operational anomalies in equipment. This approach ensures continuous system functionality by significantly reducing the likelihood of unexpected failures.

Empirical studies – including an international report published by PricewaterhouseCoopers (PwC) – indicate that implementing PdM increases equipment availability by an average of 9%, proportionally reducing the number of unplanned outages (URL9).

This advantage is particularly critical in the context of key physical security infrastructure – such as surveillance cameras, intrusion detection systems, and access control solutions – where uninterrupted operability directly impacts the security of protected areas and minimises the emergence of 'protection blind spots.'

7.8.5.2. Cost Savings and Maintenance Efficiency

The core principle of PdM is that maintenance interventions are not carried out on a pre-defined schedule, but rather as the result of continuously updated condition assessments and risk-based decision-making. According to an analysis by PwC, this strategy can reduce direct maintenance costs by an average of 12% (URL9).

This can be attributed to the dual benefits of avoiding acute, high-cost failure-related repairs while simultaneously optimising the allocation of servicing

resources. Unnecessary interventions are avoided where the actual condition of the equipment does not warrant action, allowing both human and material resources to be allocated specifically to resolving genuinely anticipated issues.

Case studies indicate that well-planned, predictively driven maintenance logistics can lead to up to 40% increases in workflow efficiency. As a result, the organisation's overall cost level is reduced, while the return on investment (ROI) of deployed systems improves significantly.

7.8.5.3. Extension of Equipment Lifespan

PdM procedures make it possible to intervene before equipment reaches a critical point in its degradation process. In consequence, devices can avoid damage caused by excessive operational stress, allowing for a significant extension of both their designed service life and their economically useful lifespan. According to measurements by PwC, systems maintained under a proper PdM regimen can, on average, operate fault-free for 20% longer than without such interventions (URL9) (Sobiyi et al., 2025).

This benefit is particularly significant for physical security equipment, which often involves high-cost, long-term capital investments – such as urban surveillance networks or complex building security systems. Devices need to be replaced less frequently, and asset depreciation is deferred. For example, while a standard outdoor PTZ camera typically operates reliably for five years under normal conditions, with PdM it may function flawlessly for six or even seven years – thanks to timely interventions such as fan replacement or mechanical cleaning, undertaken before the occurrence of serious malfunctions.

7.8.5.4. Minimization of Safety Hazards and Accidents

Although it is discussed less frequently, the benefits of PdM extend beyond economic considerations to include substantial improvements in occupational safety and operational risk mitigation. Malfunctioning security technology components – such as short-circuited control units or faulty automated doors – have the potential to cause personal injury or significant material damage.

According to PwC statistics, the application of PdM can reduce accident-related, environmental, quality-related, and health risks by up to 14%.

When systems operate reliably on a continuous basis, the likelihood of endangering human lives or property due to equipment failure is significantly reduced – for example, in cases involving tampered fire alarms or inoperable emergency exits. Moreover, continuous condition monitoring can serve as a deterrent against potential criminal activity and improves incident detection times, thereby enhancing the overall level of protection provided by the system.

7.8.5.5. Regulatory Compliance and Auditability

In numerous industries and operational domains – such as banking and critical infrastructure – regulations explicitly govern the maintenance and documentation of security systems. PdM solutions typically generate detailed logs and reports on device status and maintenance activities. This is not merely a matter of efficiency, but also one of legal compliance: such documentation can be readily retrieved for audits to demonstrate when and which device (e.g., a malfunctioning camera) reported an error, and when that issue was resolved. Moreover, because predictive approaches reduce the frequency of unexpected failures, the likelihood of non-compliance with mandatory operational requirements (e.g., the continuous functionality of authorised access gates) is also diminished. When integrated with quality management systems, PdM contributes to the fulfilment of service-level

agreements (SLAs), which often mandate specific levels of system availability for physical security operations.

Overall, the implementation of a predictive maintenance strategy in the operation of security systems represents more than just the modernization of maintenance practices – it constitutes a paradigm shift in comprehensive security management. Proactive, data-driven systems not only enhance the level of security, but also yield substantial reductions in operational costs, improve asset utilization, extend the life cycle of installed equipment, and reduce systemic risks.

Aligned with the broader objectives of Industry 4.0, this approach plays a central role in the development of future intelligent, self-sustaining security solutions, and is expected to become a fundamental requirement in the management of physical security environments – commonly referred to as Security 4.0[14]. As such, PdM should not be viewed merely as a technological innovation, but as a scientifically supported, system-level paradigm shift for more sustainable and cost-effective security management.

7.8.6. Challenges and Implementation Considerations in the Adoption of Predictive Maintenance

While the implementation of PdM promises numerous strategic benefits and significant improvements in organisational efficiency, it is essential to emphasise that its design and operation entail complex, multidisciplinary challenges. These obstacles arise at the intersection of technological, data engineering, organisational, and cybersecurity domains, and they directly influence the success of the investment as well as the realization of the expected return on investment.

[14] The term Security 4.0 refers to a modern paradigm in physical security technologies that mirrors the principles of the Fourth Industrial Revolution (Industry 4.0), emphasising digitalization, automation, data-driven decision-making, and artificial intelligence.

7.8.6.1. Initial Investment Requirements and Technological Integration

The implementation of predictive maintenance systems entails substantial infrastructure and technological investments. The deployment of sensor networks, data collection devices, intelligent software solutions, and robust networking infrastructure is an essential prerequisite for high-level, data-driven maintenance operations.

While these investments significantly contribute to long-term operational efficiency, they also represent considerable short-term cost factors that organisations must evaluate through comprehensive cost–benefit analyses.

An additional challenge arises from the need to integrate PdM solutions into existing, often heterogeneous security technology environments. Legacy systems with lower levels of intelligence – such as analogue cameras or traditional intrusion alarm systems – can only be adapted for predictive functionality by retrofitting IoT sensors or, in some cases, complete replacement of devices.

To mitigate these issues, an increasing number of plug-and-play, modular predictive solutions are emerging in industrial practice. However, the successful implementation of such systems depends heavily on precise planning and strong project management capabilities (URL10).

7.8.6.2. Data Quality, Algorithmic Reliability, and Modelling Challenges

A critical prerequisite for effective PdM is the continuous generation, storage, and processing of relevant, consistent, and high-volume datasets. Deficiencies in data integrity – caused by sensor malfunctions, network failures, or improperly configured data collection – can significantly undermine the accuracy of predictive models, leading to false forecasts and incorrect alerts.

The development of predictive algorithms based on machine learning and artificial intelligence relies heavily on robust model training, systematic testing,

and ongoing refinement. During initial deployment phases, a high incidence of false positive alerts may occur; these can be mitigated through iterative annotation and the active involvement of AI specialists.

The most effective PdM implementations are typically founded on close collaboration between data scientists and physical security experts. In this context, domain knowledge plays a pivotal role in ensuring both the interpretability of the models and their practical utility under real operating conditions.

7.8.6.3. Organisational Adaptation and Human Factors

The introduction of PdM signifies not only a technological shift, but also a paradigm change in human resource management. For maintenance and operations personnel, traditional, time-based routine checks are replaced by dynamically evolving, data-driven tasks. This transition brings about a substantial transformation in workplace culture and may initially trigger resistance among staff.

To support a successful transformation, regular and targeted training, as well as the strengthening of internal communication, are of critical importance. Ongoing development of personnel competencies – including the interpretation of digital dashboards, proper assessment of predictive alerts, and the management of data-driven interventions – is essential for user acceptance and for building long-term organisational commitment.

Research has shown that involving end-users – particularly maintenance personnel – in the design and testing of PdM systems significantly increases trust in the technology and contributes to greater levels of acceptance and adoption (URL11).

7.8.6.4. Cybersecurity and Data Protection

The digitised, IoT-based nature of predictive maintenance systems expands the potential cyber threat surface. The networked integration of sensors, endpoint devices, and central control units introduces new risk factors – particularly when data communication or remote access is insufficiently protected. Therefore, the PdM architecture must inherently incorporate modern cybersecurity protocols (such as TLS encryption, VPN tunnelling, and multi-factor authentication), the application of the zero-trust model, and network segmentation for security-related devices.

Beyond technical safeguards, the proper handling of personal data and compliance with data protection regulations – such as the General Data Protection Regulation (GDPR) – are also critical requirements, especially in cases where personal information may be inferred from sensor data, log files, or video streams. While many industrial PdM platforms now provide built-in privacy protection mechanisms by default, ultimate responsibility lies with the organisation that deploys and operates the system.

Despite these concerns, both scientific studies and industrial practice indicate that the benefits of predictive maintenance clearly outweigh its initial implementation challenges, particularly within the domain of physical security systems. The portfolio of hardware and software solutions offering predictive functionality continues to grow, and as a result of ongoing innovation in the field, system transition is becoming increasingly seamless.

In parallel, the convergence of artificial intelligence and the Internet of Things is introducing new standards for physical security systems – where proactive, data-driven operation is evolving from a competitive edge into a fundamental aspect of service-level expectations.

7.8.7. Summary

PdM represents a key developmental direction in modern operations and physical security, elevating equipment reliability and operational efficiency through the integration of digitalization, the Industry 4.0 paradigm, the Internet of Things (IoT), big data analytics, and artificial intelligence (AI). Predictive methodologies enable continuous and dynamic condition monitoring and maintenance forecasting for security systems. When implemented effectively, these methods can substantially increase system availability while simultaneously reducing maintenance-related expenditures.

This strategy not only prevents major system failures but also extends the service life of devices and ensures more stable and reliable performance – especially in the realm of security technology, where uninterrupted operation is critical to maintaining seamless protection.

In the field of physical security, equipment failure was previously regarded as an unavoidable risk, compromising system integrity and resilience. PdM now offers the ability to pre-empt many of these issues, ensuring that security systems remain operational even under high-stakes conditions, such as during an attempted intrusion or criminal event. As a result, the number of prevented incidents increases and response times decrease, since the systems continuously self-monitor and notify operators of impending faults – mitigating the need for manual diagnostics and thereby raising the overall level of security.

PdM, therefore, should not be viewed as an isolated technical innovation but as an essential component of wider trends in digitalization and Industry 4.0 / smart city development. It replaces traditional reactive operational models with proactive, data-driven system management.

Predictive Maintenance represents a strategically significant approach in the operation of security technologies. Beyond its quantifiable benefits, it aligns

closely with contemporary digital trends and the concept of Security 4.0. This paradigm is not merely a technological innovation, but a scientifically grounded transformation in security management – one that fosters the development of an active, intelligent defence ecosystem aimed at more effectively protecting human life, assets, and critical infrastructure in an increasingly complex risk environment.

References

LEDMAOUI, Y., EL MAGHRAOUI, A., EL AROUSSI, M. & SAADANE, R. (2025). Review of Recent Advances in Predictive Maintenance and Cybersecurity for Solar Plants. *Sensors*, 25(1), pp. 1-23. (https://doi.org/10.3390/s25010206)

RAHMAN, M. M., ALKALI, B., JAIN, A. K., PARRILLA GUTIERREZ, J. M., MCNEIL, C. & NELSON, J. (2024). *Predictive Maintenance Optimisation for CCTV Systems in Electric Multiple Unit Trains Using Machine Learning Techniques.* pp. 1–11. (https://doi.org/10.4203/ccc.7.8.11)

SOBIYI, T. O., EGBUNA, C. C., KAREEM, S. R., & LAWAL, R. O. (2025). AI-driven predictive maintenance systems for loss prevention and asset protection in subsea operations. *World Journal of Advanced Research and Reviews*, 25(2), pp. 923–933. (https://doi.org/10.30574/wjarr.2025.25.2.0460)

URL1: https://spd.tech/machine-learning/predictive-maintenance/

URL2: https://smartsentryai.com/2025/01/25/ai-based-predictive-maintenance-takes-center-stage/

URL3: https://www.grandviewresearch.com/industry-analysis/physical-security-market

URL4: https://promwad.com/news/top-predictive-maintenance-iot-trends

URL5: https://aimlprogramming.com/download/pdf/predictive-maintenance-for-cctv-cameras-1709448902.pdf

URL6: https://iomni.ai/autonomous-predictive-maintenance-to-increase-productivity/

URL7: https://horizonpowered.com/boosting-port-security-with-ai-powered-cameras/

URL8: https://commandhubsolutions.com/maintenance-scheduling-security-firms/

URL9: https://www.pwc.de/de/industrielle-produktion/pwc-predictive-maintenance-4-0.pdf

URL10: https://www.xyte.io/blog/iot-predictive-maintenance

URL11: https://www.diva-portal.org/smash/get/diva2:1940811/FULLTEXT01.pdf

7.9. To Pay or Not to Pay? Predictive Policing in the Context of Crimes Related to Online Payment

Nikiforosz Packosz

7.9.1. Introductory Thoughts

7.9.1.1. Positioning Predictive Policing

In the framework of the classical law enforcement model,[15] predictive policing can be viewed as the zero level, that is, an action that precedes and supports prevention. Predicting or forecasting danger is not prophecy but (strong) probability, which primarily supports more effective crime prevention. The visions of predictive policing and crime prevention coincide in that their subjects are abstract, that is, the 'crime not yet committed.' The difference lies in the self-contained specification of predictive policing: it supports the abstract risk of occurrence based on behaviour and risk factors, which may refer to locations or groups of people.

Personally, I consider predictive policing to be a well-defined, autonomous discipline, which, at the same time, is interpretable only within the conceptual framework of crime prevention. In other words, crime prevention is a defining attribute of predictive policing.

7.9.1.2. The Online Dimensions of Predictive Policing

Predictive policing can gain significant ground and realise its full potential with regard to crimes committed or planned for commission in cyberspace. With the use of modern technologies, especially artificial intelligence, not only past but also real-time data can be processed. This allows for more accurate predictions and

[15] Crime prevention, detection, investigation, examination.

earlier interventions, while at the same time we meet the unique challenges of cyberspace: anonymity, speed, and borderlessness.

One key difference from predictive policing in the physical realm is that spatiality (the place of commission) must be interpreted in an entirely different way. The online (cyberspace) dimension of predictive policing means that the preventive mind-set and predictive toolset can now be applied not only in physical spaces but also in virtual environments. In this different realm, the 'scene of the crime' is not a clearly defined geographic location but rather an IP address, an email account, software infrastructure, or a financial transaction pattern. In other words, the goal of online prediction is not to identify specific perpetrators or acts but to detect risk patterns and behavioural anomalies that may indicate future abuse or crime. Predictive systems of this type are typically used by financial institutions, where AI-analysed data makes it possible to detect in real time when a client's behaviour deviates from the usual (e.g., based on transaction time or recurrence), or where the location of a transaction is incompatible with the client's known geographic position (e.g., a card purchase at an offline vendor on another continent).

Thus, predictive policing in cyberspace not only involves introducing new technologies but also implies a new way of thinking. Here, the focus is not on spatial or temporal determination but rather on intention, motivation, behaviour (e.g., browsing habits), and their associated digital footprints. Therefore, online prediction is more of a behaviour-based security forecast, the effectiveness of which is inseparable from the technological capacities of the private sector and its cooperation with the law enforcement sector.

7.9.2. Focusing on Crimes Related to Online Payments

7.9.2.1. Intriguing Interests and Challenges

Trust in state-recognised, internationally accepted payment forms and systems (and maintaining that trust) is a cornerstone of national and global economic operations, so any breach in it violates a key interest. Although a significant part of the financial sector is privately owned – and thus primarily driven by private interests – public and private interests overlap in this area, as the stability of financial systems serves not only the profit of individual market players but also the economic security of society as a whole.

Within this context, it is clear that crimes related to online payments occur in increasingly diverse forms. Perpetrators adapt quickly in terms of both method and target to enhance their efficiency. In response to new security measures and defence technologies implemented by financial service providers (e.g., stricter client identification and transaction authorization protocols), fraudsters increasingly target the human factor – the customer – as the weakest link in the transaction chain. This trend is reflected, for example, in the FBI IC3[16] 2024 report, which shows that PHISHING[17] ranks first in the number of reports, while BUSINESS EMAIL COMPROMISE[18] ranks second in terms of damage caused. Both types of offense are forms of SOCIAL ENGINEERING,[19] that is, psychological manipulation that targets the human element.

[16] Federal Bureau of Investigation – Internet Crime Complaint Center: An official platform operated by the FBI where individuals and businesses can report internet fraud and other online crimes.
[17] A fraud method in which perpetrators pretend to be a legitimate organization or authority and deceive the customer into obtaining confidential data (passwords, bank card details, etc.)
[18] A special fraud method in which perpetrators send deceptive emails to companies in order to trick them into making an unintended financial transaction (transfer).
[19] Social engineering fraud is a broad category of fraud in which criminals manipulate a person's trust to directly obtain money or confidential information, often with the intention of facilitating further criminal activity. While social media is the preferred channel, perpetrators may also make contact by phone or even in person (Interpol, n.d.).

Additionally, various *modus operandi* have evolved, based on deception, fear (of consequences suggested by the perpetrator), greed, ignorance, and gullibility – or any combination of the above. The most effective defence against these lies on the human side, that is, through raising user awareness within the framework of crime prevention.

At the same time, it should not be overlooked that artificial intelligence (including generative AI[20] and deepfake technology[21]) is also available to perpetrators, meaning the degree of risk exposure is certainly increasing.

7.9.2.2. Limitations, Possibilities, and Opportunities

The applicability of predictive policing has legal, ethical, and institutional limitations, especially when it comes to transactions based on civil law and contractual relationships. In the case of online financial transactions, the relationship is typically based on a contractual legal relationship between two or more parties (typically the financial service provider and the customer), into which law enforcement bodies are generally not entitled to intervene. Official intervention within the scope of public criminal proceedings can only be based on legal authorization (suspicion of a crime).

Therefore, in the world of online payments, predictive and probability-based preventive measures primarily fall within the interest, duty, and responsibility of the financial service sector. Financial institutions possess the technical and operational tools to reduce the likelihood of crimes (such as fraud, phishing, or unauthorised transactions) within their contractual relationship with clients, using predictive analytics in the interest of both parties. Consequently,

[20] Generative artificial intelligence is capable of creating new, creative content.
[21] A *deepfake* refers to media content in which a person's features are artificially altered using artificial intelligence to make them appear to be someone else. The term is a combination of 'deep learning' and 'fake'. The creator's intent is to deliberately deceive the viewer, typically by using machine learning and AI technologies (Magony, 2023).

financial service providers are continuously developing algorithms, machine learning-based models, and real-time monitoring systems capable of early detection and prediction of suspicious activities, allowing them to intervene in time.

By contrast, the role of law enforcement agencies in this environment is reactive: they intervene when a certain act reaches at least the attempt stage, or when a crime is reasonably suspected. In such cases, close cooperation with financial providers is essential to minimise damage and bring offenders to justice.

Still, what role can law enforcement play in predicting crimes related to online payments? The answer begins with the fact that it is in the fundamental interest of law enforcement that fraud prevention mechanisms in the financial sector (based on technological or other methods) are as effective as possible. This will reduce the number of crimes reaching the attempt or completion stage, thus sparing law enforcement capacity.

At the same time, it must be acknowledged that the financial sector is often unable to validate or assess all data or information within its own system. Law enforcement can provide feedback to payment providers through data from other agencies, service providers, and their own records, thus creating an operational level of predictive and preventive cooperation. Naturally, these data exchanges and information flows must be backed by legal (data protection and usage) and contractual (between financial providers and clients) guarantees. As such, the large volume of data generated by predictive crime prevention technologies ('Big Data') can be shared with law enforcement under appropriate legal and data protection conditions. This enables law enforcement to respond more rapidly and effectively when concrete suspicion of a crime arises. Using data collected, organised, and pre-analysed by financial service providers, law enforcement can obtain a more accurate picture of specific fraud techniques, trends, and perpetrator groups. Based on this information, they can supplement,

expand, or update their investigative protocols. This type of mutual data sharing between the service sector and law enforcement promotes the development of a complementary law enforcement model operating in the online space. This means the parties can jointly establish a crime prevention and investigative practice that significantly enhances security in the world of online financial transactions. Numerous established examples of this can be found worldwide:

- The UK's National Crime Agency (NCA) operates a joint fraud prevention system with commercial banks (Barclays, HSBC, Lloyds), based on real-time transaction analysis. The cooperation aims, among other things, to prevent phishing and social engineering-based fraud.
- The Singapore Police has signed cooperation agreements with local e-commerce platforms, which automatically report suspicious sellers and purchases via direct data connections to the police.
- The FBI's IC3 collaborates with major internet companies (Microsoft, Meta, Google) to rapidly identify suspicious email addresses, IP addresses, and financial transactions, while Europol's European Cybercrime Centre cooperates with banks, fintech firms, and crypto exchanges in similar data sharing initiatives.
-

7.9.2.3. Ethics in Another Space

To prevent crimes related to online payments, predictive policing conducted in cyberspace – especially since it is typically carried out by the private sector in practice – raises specific ethical questions. The (financial) service provider may gain knowledge of a broad spectrum of user behaviours, which may indirectly or often directly reveal sensitive personal data (e.g., political views, religious affiliation, or sexual orientation).

Consider that when someone attends a religious service or ceremony in a physical space, they implicitly and automatically accept that others may see and identify them as belonging to that religious community. The same applies if someone visits a so-called sex shop and purchases products there: there is a chance that another customer or third party may notice or find out.

In contrast, in online financial transactions, the key difference is that the client is often unaware of how deeply their data is analysed and profiled for predictive purposes. Even if this is done in the client's interest, the lack of detailed information and explicit consent raises fundamental data protection concerns. The boundaries of the private sphere become blurred, and the balance between security and autonomy (self-determination) becomes questionable.

Since predictive analyses are conducted using private-sector tools and decision-making mechanisms, state oversight is often absent. This is especially evident when private-sector actors, for instance, transfer data to law enforcement agencies or impose restrictive measures (e.g., blocking a transaction) based on their own decisions.

In my opinion, all of this implies that in conflicts between security and other fundamental rights (e.g., data protection), private sector actors must define transparent priorities. These declarations should be subject to review by the state legal system, thereby allowing for the creation of an organically built, effective, and reliable system in which anomalies still occur but are investigated and managed according to clear protocols.

7.9.3. From Synergy to Sustainability

Predictive policing is not merely a technological innovation but also a change in mind-set regarding crime prevention and law enforcement operations. Crimes related to online payments clearly show that the classical, reactive law

enforcement model is outdated. Instead, law enforcement agencies must become partners capable of sharing data and resources within an integrated system alongside service sector actors and be willing to play a complementary (reinforcing, verifying) role in the prediction process. In most cases, law enforcement lacks the financial resources to procure the internal human resources to operate, update, and supervise online predictive technologies. Meanwhile, the private sector does not (and ideally should not) hold the monopoly on (state) force.[22]

The future of the predictive approach lies in this ecosystem – where the state and civil spheres jointly and complementarily ensure safety, prevent crimes, and maintain trust in online payments.

The next stage of the synergy described above is sustainable security, the criteria of which are technological, sociological, and institutional in nature.

Predictive systems must adapt to new types of threats (e.g., generative AI, deepfake) and ensure interoperability among interconnected systems. The technological dimension of sustainability is therefore embodied in updatability and interoperability.

Secondly, security measures implemented through technological tools can only be effective if society accepts and trusts them. Social trust is especially sensitive in the case of predictive technologies, where results may lead to 'labelling.' Sustainable security cannot exist without democratic social legitimacy.

Long-term, functioning security systems must be supported by a structured institutional network based on clear role distribution. This requires formal and informal norms that guarantee legal and ethical compliance in information flow, data management, and decision-making.

[22] For example: the use of coercive measures, such as house searches or seizures.

References

MAGONY, G. (2023). *In Too Deep(fake) – Suggestions on How to Avoid Harmful Social Influences of Deepfakes*. Constitutional Discourse. (https://constitutionaldiscourse.com/gellert-magony-in-too-deepfake-suggestions-on-how-to-avoid-harmful-social-influences-of-deepfakes/)

INTERPOL [n.d.] *Social engineering scams*. Interpol.int (https://www.interpol.int/Crimes/Financial-crime/Social-engineering-scams)

Chapter 8
Legal Aspects of Predictive Policing[23]

Imre Szabó

As previously mentioned, the application of predictive policing necessitates a legal analysis. In this chapter, we will examine the most important legal areas involved.

8.1. The Increasing Value of Data

The societal, economic, and technological changes brought about by the increased volume of data are referred to as the Big Data phenomenon. We are living in an era in which the rapid growth in the quantity of data means the primary interest of law enforcement is to acquire and utilise data as widely as possible to guarantee a higher degree of security for citizens. A result of this development is also the processing of data with the help of automated decision-making systems, including various forms of profiling and the application of different artificial intelligence systems to support law enforcement tasks.

The comparison and processing of data for law enforcement purposes have always been part of the law enforcement toolkit. However, supporting these tasks with IT systems enables the rapid and accurate comparison and processing of ever-increasing amounts of data, and the discovery of hidden correlations within that data, which greatly supports effective law enforcement.

Citizens, while being open to law enforcement solutions necessary to guarantee their security, are simultaneously sensitive to the state extending its

[23] The chapter is based on Chapter 3 of the book *Közrendészet* by Péter Ruzsonyi (ed.) (2020) – written by the author.

authority to areas that restrict an individual's personal freedom in order to enhance its effectiveness.

In connection with the latter, in cases where in order to effectively perform its tasks – for example, to increase security – the state restricts spheres for private individuals that enjoy protection against state interventions, the suspicion inevitably arises against the state that it is striving to develop an Orwellian system through such interventions. This suspicion has an unfavourable impact on the relationship between the state and the individual, and thereby on social cohesion and the democratic social order.

Utilising the potential inherent in data is an important tool in the performance of law enforcement tasks, as it undoubtedly contributes to increased work efficiency. Finding a favourable balance, however, is also in the interest of society as a whole. Generally speaking, equilibrium is found when the state achieves the greatest security with the least restriction of individual liberties.

The courts of the United States and the United Kingdom (United States Court of Appeals for the Second Circuit: Case 14-42, privacyinternational.org 2015) have clearly defined in their decisions the boundary line at which the state crossing endangers this equilibrium. According to these decisions, the state can only intervene in the private sphere as long as people do not begin to fear that their daily activities are being monitored by the state. On the state's side of the boundary line, a further distinction must be made as to which data law enforcement authorities can freely access, and which require the permission of state bodies supervising investigative authorities (such as courts and prosecutors' offices). The role of these organisations, independent of the investigative authority according to the separation of powers, is to ensure that investigative authorities carry out their institutions enabling intrusion into the private sphere only within the framework of the laws authorising them to do so. In the

interpretation of the courts, only in this system can a society living under a developing, secure democratic rule of law be maintained.

The definition and adherence to this boundary line are possible through the creation and enforcement of laws ensuring the protection of the private sphere, and within that, the protection of personal data.

In the following are presented – through the relationship between law enforcement and profiling – the most important points to consider during the law enforcement use of personal data, in order to ensure that decisions based on personal data and subsequent law enforcement measures comply with legal requirements, and in light of the purpose and meaning of these laws, meet the demands of a developing democratic society.

8.2. General Concept, Characteristics, and New Directions in Profiling

Profiling is already applied in many areas of life. Thus, it is present in marketing activities (for example, when an online bookseller's website offers additional books for purchase based on what other books previous buyers of the viewed book have looked at or purchased), in the insurance market (when an individual's credit rating is determined based on their payment ability during a loan application), and it is also already present in the field of law enforcement.

Several attempts have been made to define the concept of profiling. According to Hildebrandt, profiling is a new form of knowledge that makes visible patterns that are invisible to the human eye. Marx and Raichmann – from a law enforcement perspective – characterised profiling as a method of systematic data research that allows an investigator to evaluate, through the correlation of several independent data points, how characteristic a predefined trait or the violation of a rule is for a person or an event (Ferraris et al., 2013, p. 6). Highlighting the dark side of profiling, Roger Clark (1993) stated that profiling is

nothing more than a surveillance technique in which a profile is created and applied.

The concept defined in the joint study by De Hert and Lammerant summarises the essence of profiling well: profiling is a technique where the characteristics of a certain group of people are inferred from past experiences, and data sets containing such characteristics are then used to find individuals who match these characteristics (De Hert–Lammerant, 2016, p. 145).

According to the latest research, profiling is the categorization of citizens based on their personal traits and characteristics. These characteristics can be constant (such as age, etc.) or variable (clothing, habits, etc.). The central element of profiling is the profile, which consists of characteristics, features, and attributes that distinguish one person or group from another. During profiling, we infer – within a certain margin of error – unobservable characteristics based on observable characteristics (FRA, 2018, p. 15).

8.2.1. The Impact of Big Data on Profiling

The use of profiling for law enforcement purposes is not a new phenomenon. Currently, traditional profiling characteristics dominate law enforcement, which primarily attempts to find correlations between the characteristics of the commission of the same type of crimes and to identify the potential perpetrator. In the new directions of law enforcement profiling, however, profiling techniques related not only to crime detection but also to crime prevention are applied by various law enforcement actors, and all this with the help of artificial intelligence.

A characteristic of traditional profiling is that it first establishes a hypothesis (assumption) based on experience and known and recognised correlations, and then this assumption is checked and verified with data. Traditional profiling uses statistics to determine and measure the truth and credibility of the hypothesis; in

the new approach, statistics transform into a discovery method (De Hert and Lammerant, 2016, p. 145).

New profiling techniques developed through Big Data, such as data mining, use data not only to verify or refute assumptions but also to search for and identify new, previously undiscovered or unknown correlations. A specific method of this type used in data mining is 'knowledge discovery in databases,' the goal of which is to find usable correlations and patterns among data from different sources, that is, to generate knowledge by researching databases.

The field of profiling is multifaceted and can provide assistance in a wide range of law enforcement tasks. Imagine a situation in which, to find a person, it would be sufficient to provide that person's mobile phone number, and a programme would, in real-time, by automated comparison of location data managed by telecommunication providers and, for example, data recorded by fixed speed cameras, and by providing photographs, display the vehicle in which the sought person or their phone is travelling. Continuing the thought: let's say, at the same time, all legally managed data of the vehicle would automatically appear, including the owner's data, and a facial recognition programme would identify the persons travelling in the vehicle. This would undoubtedly be a useful tool in the hands of the investigative authority, and although the development of such supporting systems is almost limitless, their practical implementation and widespread adoption in everyday law enforcement – although there are already initiatives related to this, such as the '*Szitakötő*' [Dragonfly] system in Hungary – are difficult to predict.

The 'Szitakötő' system was developed to make public area cameras located in different systems centrally accessible in one system. The system was developed within the framework of the 'Integrated Traffic Organisation and Regulation System public safety, traffic safety, law enforcement IT development program.' (IKSZR, n.d.)

The knowledge generated by data mining methods and supported by artificial intelligence in the field of crime prevention now offers opportunities for, among other things, identifying suspicious transactions executed on bank accounts provided by credit institutions, as well as potential perpetrators and their victims.

8.2.2. Classification of Profiles

Based on the subjects of profiling, we can distinguish between personal and group profiles. A personal profile refers to a specific individual (for example, a fingerprint as a profile belongs to one person, but this category also includes all other biometric profiles, such as data managed by facial recognition software). The essence of individual profiling is to identify a person within a group, or to determine a person's habits, behaviour, preferences, knowledge, or the risk inherent in their person from the perspective of committing a crime.

A group profile contains the common characteristics of several people. It can be used to determine the common characteristics of several people, a community (e.g., common characteristics of members of the Catholic religion), and to identify individuals and thereby form them into a group who share common characteristics, for example, women with red hair and green eyes (Hildebrandt, 2008, p. 6).

Within a group profile, we can distinguish between distributed and non-distributed group profiles. If every member of the group shares the profile characteristics, then the group is characterised by a distributed profile. A non-distributed profile can be spoken of when only a statistical relationship can be demonstrated between the characteristics of the persons belonging to the group profile, or when the members of the group do not carry all of the characteristics typical of the group. An example of the former is a club fan group, where a common characteristic of every member is that they support the same team, while

the latter could be, for example, smokers as a group, whose profile includes the possibility of developing smoking-related diseases.

Once the profile is created, it can be applied. The essence of applying a profile is that the profile characteristic must be taken as given for persons identified based on the profile (distributed profile), or its possibility must be considered (non-distributed profile).

Here, Hare's psychopathy list can be mentioned, which is a non-distributed group profile. Hare's profile has 20 characteristics (e.g., lack of guilt, superficial charm, pathological lying, and poor impulse control), which must be checked on a three-point scale (0 – false, 1 – partly true, 2 – true) in relation to the examined person. A person whose personal profile scores 30 or more points can be classified into the group of psychopaths (Edens, 2001, p. 1084).

A common characteristic of this group's members is that there is a high probability that they will commit violent crimes. Thus, the examined person's belonging to the group can justify the application of compulsory medical treatment against that person.

Further distinctions can be made in profiling based on the extent to which the creation and application of the profile are electronic, automatic, or based on human behaviour. In this relation, a distinction can be made between non-automated, automated, and autonomous profiling. The essence of non-automated profiling is that computer technology plays a minor role in it; the creation and application of a profile, and any decisions based on it are directly under human influence. Automated profiling can be spoken of when IT systems assist in the creation and application of the profile. However, at several points in this process, especially when determining further law enforcement measures based on the decision resulting from the application of profiling, human intervention occurs. In contrast, during autonomous profiling, there is no human intervention in the

creation and application of a profile, or the decisions based on it; the procedure is carried out by IT systems. In this case, at most, the human factor appears retrospectively, for example, when judging an appeal lodged against a legal violation implemented by an autonomous system. Currently, few such autonomous decision-making systems operate. However, their application is expected to spread in the future.

8.2.3. Automated Profiling

The essence of automated profiling is that profiles are managed and assigned to individuals or groups by algorithms (programs) for the purpose of enabling the investigative authority to initiate measures based on them.

An algorithm is understood to be a method, instruction, sequence of instructions, or detailed guide consisting of permissible steps, suitable for solving a given problem. For example, a procedure or algorithm can be given for assembling a table (or other furniture), or preparing a certain food, but also for finding the way from Deák Square to the Chain Bridge, or even for calculating the greatest common divisor of two integers. Computer programs generally contain algorithms, which instruct the machine to perform the given task.

The method of creating most profiles operated by algorithms is practically identical to the 'behavioural analysis' method, which associates specific characteristics with behavioural patterns. For example, from data on how much alcohol a defined group of people drinks and data on the lifespan of the same group, the algorithm (even in the absence of human behaviour following the writing of the program) can determine how a certain amount of alcohol consumption affects life expectancy.

Spam filters, whose task it is to identify unsolicited emails and prevent their delivery or collect them separately, work similarly. This is generally based on

the fact that several people have previously classified the given email as unsolicited, so subsequently, emails from the same source that match the spam profile are treated as spam. These systems operate with high efficiency nowadays, but unsolicited emails can still end up in an inbox. This is referred to in the literature as a *false negative result*. Another possibility is that the system places an electronic email among the spam, which is referred to as a *false positive result*.

Algorithms used in profiling can also lead to false positive and false negative results. The result of profiling is called a false positive result when it indicates the need for further law enforcement action in relation to a person who was mistakenly classified into a risk category that generates an obligation to act, and a false negative result occurs when it fails to highlight a person who actually poses a risk. These inherent error possibilities in the system require that the results of profiling applied in law enforcement activities be subject to further verification. For this reason, the widespread adoption of autonomous profiling systems in law enforcement activities seems less advisable, given the inaccuracies inherent in the profiling process and the severe legal restrictions that can be caused by them. Therefore, profiling applied in law enforcement activities should always be followed by a law enforcement measure that verifies the result of the profiling and either confirms or refutes it.

8.2.4. New Directions in Profiling

Among the new directions in profiling, two are of particular importance for law enforcement, both areas that can provide effective assistance in performing law enforcement tasks in the future: *behavioural profiling* and *location-based profiling* (Ferraris et al., 2013, p. 12).

Behavioural profiling refers to the creation of profiles based on behavioural patterns and the identification of similar behaviours based on the

profiles thus created. It has two main directions: one is profiling related to the behaviour of online users, and the other is biometric behavioural profiling.

The primary purpose of profiling the behaviour of online users is to send the advertisements most relevant to a user's interests based on their internet browsing habits.

The more behavioural characteristics and traits that can be linked to a given user, the more accurate a picture can be obtained of their habits and values. However, there is a risk that the information obtained from such linked profiles will allow data mining techniques to know the person better than the person knows themselves. This can lead not only to influencing the person's preferences but also to subtly controlling their decisions.

In the field of law enforcement, this type of profiling primarily enables a more thorough understanding of perpetrators, for example, biometric behavioural profiling examines human characteristics in relation to conscious and unconscious human behaviours (Consultative Committee of Convention 108 T-PD, 2005). A biometric sample obtained during profiling can be applied to the biometric data of specific individuals (for example, a person's gender can be inferred from their voice). It also provides an opportunity to determine the person's preferences and mood. In the future, technology – especially with the spread of cameras and various sensors – will enable the recognition of moods, emotions, gestures, and the identification of a person based on the dynamics of their human gait, voice, and mouse movements.

This profiling technique, through camera surveillance of mass events such as music festivals, allows for effective law enforcement intervention, for example, by recognising fights before they are even reported, enabling the organisation of necessary law enforcement intervention to resolve them.

Profiling based on location data – given the widespread recording of such data – offers further opportunities. Such data is recorded by smartphone GPS

data and other location data, but also includes GPS data found in photographs taken with phones.

With the help of location data, taking into account the timestamps associated with that data, the profiles listed in the table below can be identified (Table 1).

Location data can help to determine, among other things, where a given person was at a given time, or which persons were in a given area at a given time. The preference system and habits of a specific person, can also be extracted from it. Furthermore, if an area is examined within a time interval, the characteristics of the people present in that area can be learnt (for example, typical routes of fans leaving a football match, movement habits of people socialising in the 'party district,' e.g., where people typically go after a club closes, etc.) (Ferraris et al., 2013, p. 14.).

		SPATIAL DIMENSION	
		At a single point	Within a given area
TEMPORAL DIMENSION	At a single point in time	For example, the time and location of a hospital visit.	It does not apply to individuals: an individual can only be in one place at a time. In the case of groups: it can help identify cooperation, networks, and connections.
	Over a time interval	Can show the person's work, home, social environment, and personal preferences (e.g., what restaurants they frequent, what regular habits they have, etc.).	Shows shopping habits, average road traffic speed, etc.

Table 1. Location-Based Profiles

Similarly useful information can be obtained from a person's bank card usage data. This data also reveals where the person was at what time, where, what,

and how much they purchased. Based on all this, detailed insights can be gained into the person's habits and preferences, which are part of their personal profile.

8.3. The Relationship between Predictive Policing and Profiling

Profiling and predictive policing show connections at several points, which are discussed below.

8.3.1. Profiling in Law Enforcement Tasks

Profiling as a law enforcement technique was also used in earlier periods, typically providing assistance in identifying unknown perpetrators. Its renewed prominence and increasing significance came about because the analysis and processing of ever-increasing amounts of data, which are also available to investigative authorities, injected new energy into the field of profiling, proffering the possibility of more efficient and cost-effective performance of law enforcement tasks.

The areas of application of law enforcement profiling are defined in Hungarian legal literature by the *Rendészettudományi Szaklexikon* (Law Enforcement Science Lexicon) as follows:

> *Profiling is the process during which, based on information available about a given crime or crime scene, a psychological-sociological portrait of the unknown perpetrator of a crime can be created. It is the creation of a side-view, cross-sectional outline of someone or something, or the description of its operational area and comprehensive characteristics. In criminal activity, profiling – by processing characteristic data of perpetrators of unlawful acts – creates a kind of image of the data that characterizes the perpetrator and/or object of individual crimes and misdemeanours. Current profiling is an activity that, in a given situation, determines and reveals the changes in someone or something caused by influencing effects and stimuli, and the characteristics and essential features*

developed as a result of these changes. Its purpose is to define an individual criminal profile, i.e., a probable set of characteristics related to a specific crime. The essence of profiling is to provide characteristics of an unknown perpetrator and their act, based on which individuals already within the scope can be selected, or the corresponding person can be searched for in the narrower or wider environment of the victim. The completed profile shows what type of person might have committed the crime. There are several methods and approaches to profiling. These include the following:

The FBI school assesses the personality traits and behavioural characteristics of offenders based on clues. It categorizes offenders into types (organized, disorganized), assesses the procedural peculiarities of the crime (e.g., technical skills), the appearance of psychological needs independent of the crime (e.g., sexual aspects, criminal 'signature'), and then creates a criminal profile that includes demographic, family, educational, and military background information. It may also include suggestions for applicable interrogation techniques.

Geographic profiling delimits the perpetrator's residence from investigative data. It works based on several hypotheses, e.g., the principle of least effort, rational choice, routine activity. It is found effective in serial crime cases.

Psychiatric profiling searches for elements indicating mental disorder in the investigative material, then narrows the circle of suspects based on these, while also prognosticating the perpetrator's future behaviour.

The concept of statistical profiling is that similar crimes are committed by people with similar characteristics. By processing a database of crime cases, it compiles the perpetrator profile most characteristic of the given crime. Behavioural profiling creates the criminal profile by analysing criminal behavioural patterns. It categorizes behavioural patterns into dimensions (e.g., hostility: hits the victim, tears off clothes, etc.; need for control: ties up the victim, threatens, etc.), assigns numerical values to each dimension and behavioural pattern, and then lists those who are closest to the perpetrator

based on their behaviour, and those cases where similar behavioural patterns occurred. (Boda, 2020, pp. 451–452.)

The first area of law enforcement profiling is profiling in the classical sense, the main goal of which is to identify the perpetrators. In this, the profile is fundamentally based on existing evidence, based on which the characteristics that the perpetrator of a crime is likely to possess are determined.

Another, new area of profiling is the general identification of persons and geographical areas relevant to the performance of the investigative authority's tasks, in order to prevent a crime. The foundations of profiling in this area are empirical knowledge and assumptions based on data analysis. The profile produced during this process includes not only characteristics related to specific behaviour but also all other characteristics that can be linked to the goal of profiling.

While classical profiling belongs to the field of intelligence-led policing, the latter belongs to predictive policing. The essential difference between the two types of profiling is that while the former is reactive, meaning it is applied after a crime has already been committed, the latter is proactive, meaning it is applied before a crime is committed in order to prevent it from being realised.

The goal of the former is to identify and apprehend the perpetrator, while the goal of the latter is to predict when and where a crime is likely to occur, and who are the persons who could potentially be perpetrators or, in certain cases, victims (FRA, 2018, p. 18.).

The significance of the two law enforcement profiling methods mentioned above is that regarding the persons affected by profiling, or in certain cases, geographical areas and time periods – on the basis that the given profile fits a person or geographical area – it is possible to initiate law enforcement measures (identity checks, entry into a defined area, etc.), which essentially creates the basis

for police action. In law enforcement profiling, the suspicion arising in connection with human behaviour – as the basis for law enforcement intervention – is replaced by suspicion arising from the characteristics of the given person, the effects of this shift will be discussed later.

8.3.2. Profiling in Predictive Policing

The essence of predictive profiling is to recognise new correlations by utilising and automatically processing digital traces, thereby facilitating the more efficient performance of law enforcement tasks.

A profile, which we derive from past behaviours, known cases, or the characteristics of individuals, can be used to infer current or future behaviours and events. However, it must not be forgotten that the profiling process inherently carries the possibility of error, meaning that the results presented by algorithms should be treated with caution. A profile is always merely a probabilistic model, the reason being that humans and human behaviours are constantly changing. The correlations identified in profiling represent a relationship between data, but they do not prove causality. The pattern is merely an indication of the underlying causal process, which in some cases may be completely irrelevant.

The findings of profiling are merely general correlations and relationships, and therefore are not applicable to every individual. It may happen that the person to whom they are applied is precisely an exception to the rule, or it may happen that inaccurate correlations are produced.

The assumption that women live longer than men is factually proven. Nevertheless, it happens that some men live longer than some women. Therefore, any decision concerning a woman based on this assumption may be inaccurate, as this is only a generally true statement.

It often happens that private individuals lend their cars to other people, which can, therefore, lead to inaccuracies if the characteristics in a driver's profile derived from information about a vehicle's movement in traffic is simultaneously treated as being characteristic of the vehicle's owner (FRA, 2018, p. 17.).

In other words, profiles do not provide evidence; they merely suggest where to look, where law enforcement activity is most likely to be needed.

The essence of law enforcement profiling, therefore, is to uncover relevant correlations in the data of an undesirable but previously occurring sequence of actions or events, and thereby prevent another similar event or action. If an undesirable event is known, a profile can be created from its antecedent data, that is, from the data that led to the occurrence of the action. The profile thus created helps in recognising a situation that previously led to an undesirable outcome. Based on such similarity, it is possible to take law enforcement action with the aim of preventing the occurrence of the situation that caused the undesirable outcome. The similarity of the two life situations, that is, the agreement of the two profiles, helps in selecting the appropriate special procedure or measure, which must then be carried out with traditional law enforcement tools.

According to Custers', profiling can be successfully applied in law enforcement in four areas. Firstly, as a *selection tool*, which helps in deciding which individuals or groups require greater law enforcement attention. Secondly, as a *decision-making tool*, which makes decisions automatically or through human control based on a profile. Thirdly, it can be applied as a *detection tool*, which helps in uncovering rule violations from data. Finally, fourthly, it can also be an evaluation tool for the practice of law enforcement activities and the performance of law enforcement interventions (De Hert–Lammerant, 2016, p. 145).

The legal presentation of predictive policing and profiling will now focus on two fundamental selection tools according to Custers' classification of predictive policing: pseudonymised or anonymised predictive mapping (pseudonymised maps) and predictive risk profiling.

Mapped profiling deals with the prediction of crimes, helping to identify places and times where the risk of committing crimes increases.

Risk profiling is applied in three areas. These include (1) forecasting perpetrators, that is, identifying individuals who are likely to commit crimes in the future; or (2) the perpetrators of crimes that have been committed; and (3) identifying the potential victims of crimes (Perry et al., 2013, p.8).

Both types of profiling involve the creation of profiles by analysing existing data to generate probability-based forecasts that assist in the efficient performance of law enforcement tasks in the future.

In predictive law enforcement mapping, such a profile could be, for example, the finding based on criminological research, primarily attributed to Jeffrey Brantingham, that criminals tend to operate within their comfort zones (Perry et al., 2013, p. 8.). This means they tend to commit the same crime at generally the same time and place where they have been successful in the past. This forms the basic thesis of the CAS mapping profiling system used by the Dutch police, which states that where a burglary has occurred, another burglary is expected within two weeks near that location. Based on this profile, if we know the location of a burglary, we have a higher chance of preventing another burglary by directing patrols to its defined catchment area than if the organisation of patrol routes were based solely on experience. This also includes the following case: if we identify geographical features associated with, for example, a robbery (e.g., date of family allowance pay out, a nearby tobacco shop, lack of a surveillance

camera), then based on the profile, we can identify locations where a similar act is more likely to occur than at any other location.

In the case of risk profiling, we most often find foreign examples of profiles created to prevent recidivism, the essence of which is that if a group profile of juvenile recidivist perpetrators of violent crimes is created (for example, most perpetrators were characterised by divorced, alcoholic parents, a desire to drive luxury cars, etc.), then a certain level of risk of recidivism can be predicted for first-time offenders who fit the group profile. Knowing this, targeted programmes or the application of more severe sanctions can be used to prevent recidivism. This is especially true if the group profile also includes data on which programmes and sanctions were effective for this group in reducing recidivism.

However, risk profiling is increasingly appearing in the field of law enforcement, first and foremost in border policing. The essence of these techniques is that profiles are used to select individuals who could be potential perpetrators, meaning those who are more likely to commit crimes. For individuals identified in this way, stricter, personalised checks are required to authorise their crossing at a border.

The importance of classifying profiling in this way is that a significant difference can be made between the two models from a legal perspective. While the former primarily determines the likely location and time of a crime's occurrence based on statistical data (i.e., data not attributable to individuals) the latter involves the processing of personal data linked to specific individuals, which places the latter under a stricter regulatory regime from a data protection perspective.

8.3.3. Specific Applications of Profiling in Predictive Policing

In the actual application of predictive policing, the United States leads the way, but more and more EU member states are also using profiling to support law enforcement work.

The Federal Bureau of Investigation (FBI) in the United States is at the forefront of profiling methods used for identifying individuals. The FBI previously had a biometric fingerprint database (IAFIS), which was used to identify perpetrators. As an extension of this, the NGI system (Next Generation Identification System) was introduced, which, in addition to previously managed data, includes iris patterns, palm prints, movement and voice recordings, fingerprints, scars, and tattoos. This data is used with the support of photo search and facial recognition software to identify unknown participants in criminal proceedings (Ganeva, 2012).

Another useful area of profiling in the field of personal identification is OSINT (open source intelligence). The essence of this is that the data required for profiles is obtained by systems operated by law enforcement actors from publicly available information, and the data thus collected is then processed and analysed by those systems (Haves, 2010).

Profiling is also used to aid in the detection of crimes. To detect money laundering and similar crimes, the SAR system (Suspicious Activity Report) was introduced in the United States, where economic actors must notify investigative authorities if they suspect money laundering. Detection is performed by an automated monitoring system, which attempts to filter suspicious behaviours from transaction databases purely with the help of algorithms (Ferraris et al., 2013). In the European Union, similar tasks are performed by the Financial Intelligence Units established through the directive on money laundering (Directive 2015/849 EU of the European Parliament and of the Council). By

analysing financial processes, connections between criminal organisations can also be uncovered.

Another important area of profiling used for detection is financial crimes, primarily understanding the detection of budget fraud and fraud. An example in this area is the German SCHUFA system, created by the German national bank in cooperation with other financial service providers. Data collection by the system occurs voluntarily by bank customers, based on the provision of data on activities related to bank accounts and financial behaviour. The SCHUFA system creates behavioural profiles of reference groups based on the incoming data. The goal of profiling is to uncover correlations that result in a risk classification for a person based on their banking habits and financial activities. The profiles thus created – with particular attention to profiles containing risks of fraudulent behaviour – are subsequently used by individual banks during their credit assessments. This data also carries useful information for investigative authorities.

Another profiling system for preventing and detecting budget fraud is, for example, the Redditometro system used in Italy, which analyses the client's financial situation and spending habits, attempting to identify (unusual) operations that are similar to financial transactions used in other budget fraud cases.

Predictive law enforcement mapped profiling is used by several member states. Typically the task of these programmes is to determine, based on past and, ideally, real-time data, where and when a crime is most likely to occur (for example: the CAS system in the Netherlands, and the Precobs system in Germany and Switzerland).

The application of predictive mapped profiling does not have a past from which far-reaching conclusions can be drawn from these evaluations; however, it

is undeniable that the energy and legislative will invested in the technology point towards the application of these systems.

The European Union also operates several databases containing significant amounts of law enforcement data (SIS II, VIS, EURODAC, EES, PNR, API, ETIAS, ECRIS-TCN). The essence of these databases is to identify individuals based on alphanumeric or biometric (currently fingerprint) data.

Among the above databases, the algorithms operated by the ETIAS and PNR systems serve not only as a basis for creating the profile of a known, identified person, but are also capable of designating individuals possibly connected to the commission of crimes.

The ETIAS system[24] (European Travel Information and Authorisation System) pre-screens whether individuals arriving from visa-exempt third countries pose a risk regarding immigration, security, or health. The system automatically compares the data in applications submitted by travellers with other EU and international databases, as well as with pre-prepared profiles containing risk indicators. Specifically, the algorithm developed by Frontex compares the traveller's individual profile (which includes, among other things, the traveller's age, gender, nationality, place of residence, education, etc.) with risk indicators and signals when a traveller's profile fits a risk profile that requires the traveller to undergo not only automated but also manual examination of their application for adjudication.

[24] Regulation 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulation (EU) No 1077/2011, Regulation (EU) No 515/2014, Regulation (EU) 2016/399, Regulation (EU) 2016/1624 and Regulation (EU) 2017/2226 (hereinafter referred to as Regulation 2018/1240 of the European Parliament and of the Council)

Another already operational system that uses an automated decision-making procedure is the PNR system,[25] which operates using Passenger Name Record data.

The PNR primarily records data of passengers involved in air travel, including especially travel times and details, payment and contact information, baggage information, and also data on the person's eating habits, health data (information on hearing, sight, and mobility impairment), and, in the case of child passengers, data on the kinship relationship with their legal representative. There is no central database for this data, but the PNR Directive requires providers to provide data to the national PIU (Passenger Information Unit). This data is analysed and used by the information units for the purpose of preventing serious crimes and terrorist acts, based on which – with the help of specific risk indicators – individuals with higher risk are identified. The information units can continuously update the profiles containing the indicators from a central database.

The purpose of using PNR data, according to the directive, is to identify persons and objects subject to a warrant, and to prevent, detect, investigate, and prosecute terrorist offenses and serious crimes. The data can also be used to enhance internal security, gather evidence, and, where appropriate, detect accomplices and dismantle criminal networks (Recital 6 of PNR Directive). By evaluating PNR data, individuals who may be involved in serious crimes can be identified. If such involvement arises for an individual, the authorities must conduct further investigations regarding that person.

[25] Directive 2006/24/EC of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (hereinafter referred to as the PNR Directive, Regulation 2006/24/EC of the European Parliament and of the Council)

8.4. The Inherent Dangers of Law Enforcement Profiling

The most important advantage of profiling is that its application can increase the efficiency of law enforcement, which can be observed partly in the prevention of crimes and partly in the identification of perpetrators. It is also important to emphasise that law enforcement supported by IT systems can also show economic advantages; for example, its security function can be organised more efficiently with its help.

However, it is undeniable that law enforcement profiling, despite its numerous advantages, can also entail potentially harmful consequences for society. As previously presented, by systematically classifying personal data, detailed information about a person's behaviour and preferences can be obtained, and to this extent, these methods can undoubtedly also be used to monitor citizens.

Following the rise of information technology, the social impacts of new types of state intervention techniques affecting citizens' rights and freedoms are dealt with by surveillance studies. One sub-area of surveillance studies examines whether democratic, rule-of-law-compliant surveillance can exist. According to the current state of science, this is possible if the restriction of fundamental rights and interests during surveillance occurs for a legitimate purpose, in compliance with the requirements of the necessity-proportionality test, and in a transparent and accountable manner (Székely, 2014, p. 11).

For a profiling technique to meet this requirement, it is necessary to observe the boundaries defined by law. Exceeding or violating these boundaries brings to the forefront all the negative effects that the application of profiling techniques entails.

The negative effects of improperly applied profiling can primarily stem from non-transparent decision-making systems, interference with privacy,

including interference with the right to data protection and violation of the right to informational self-determination, and discrimination (De Hert–Lammerant, 2016).

8.4.1. Non-Transparent Automated Decision-Making

The danger of non-transparent decision-making can arise at several phases of the decision-making process. Firstly, during the creation of the profile, and secondly, during the decision-making based on its result, that is, the application of the profile.

It is important that the creation of the profile takes place in a transparent manner, meaning the collection and selection of data during profile creation. Intentional and unintentional errors can occur in the process of profile creation. These can originate from the personality of the human task performer associated with profiling, as well as from organisational culture. It is also possible that incorrect data in the algorithm led to an incorrect result, or that a malfunction of the algorithm resulted in an incorrect decision.

If it is not clear on what data the algorithm based its selection of a person, and which of these were most important in the selection, then in the event of accountability for a possibly incorrect decision, it cannot be clarified at which phase of the profiling a omission occurred, meaning that accountability issues cannot be satisfactorily clarified.

The Beware software used in the United States searches for correlations in police databases and other accessible data (arrest data, existing asset data, commercial databases, deep web research, social media posts). During an official investigation into the programme's operation, doubts arose regarding its application because its decision module and algorithms – which constituted trade secrets – were confidential, and thus, in the event of a possible incorrect decision,

the cause and responsible party for the error could not be determined (FRA, 2018). To overcome this, for example, the Dutch CAS software now works on open source code, thereby ensuring the transparency of the algorithm. Another solution could be if the investigative authority itself develops such programs, provided it has the appropriate professional capacities.

A further adverse consequence is that stigmatising effects may arise in connection with individuals selected due to false positive results from profiling systems and errors inherent in the program. A false positive result increases the risk that certain individuals and groups will be systematically, regularly, and disproportionately identified as persons requiring law enforcement intervention, and thus stigmatised individuals who – as stigmatization and labelling theories have pointed out – begin to exhibit criminal behaviour regardless of whether they had previously exhibited such behaviour. This process has a detrimental effect on social cohesion, so it is important to avoid it (van Brakel, 2016). Although it is undeniable that predictive law enforcement forecasts primarily justify further investigative actions, and decisions involving more severe legal restrictions truly depend on the outcome of these further measures, the harmful consequences caused by stigmatization should not be trivialised.

8.4.2. Violation of Privacy

Surveillance, and profiling as part of that, constitutes an interference with privacy. Technical possibilities encourage the availability and use of increasing numbers of data sources, as they can enhance the efficiency of law enforcement work. At the same time, the opacity of these systems carries the risk of informational asymmetry. The essence of informational asymmetry is that while a person knows that others have information about them, they do not have the same amount of information about others. This feeling undermines people's trust in state institutions.

Interception is justified in itself if it occurs for the purpose of detecting a serious crime. In other words, in this case, the necessity of uncovering a serious crime justifies informational asymmetry. At the same time, for example, general data collection does not reach a level that would permit it. If informational asymmetry occurs somewhere and there is no sufficient reason for it, then it constitutes an interference with privacy (Székely, 2014). This risk arising in connection with profiling affects all people whose data was used to create the profile, and also those people to whom the profile is applied.

8.4.3. Violation of the Prohibition of Discrimination

The essence of profiling is that a group profile's characteristic should be considered as a characteristic of the person fitting the profile. It is important, however, to always keep in mind that this carries a certain degree of inaccuracy in the assumption.

The greatest danger that can occur in this area is that the use of a profile, that is, the categorization of a person into a group, can lead to discrimination. This discrimination can manifest in persons falling under the profile being more frequently subjected to stricter control, or discrimination can also arise in a hidden way if the algorithm used data to create a profile that was not discrimination-free at the outset. For example, if during traditionally conducted police identity checks, individuals belonging to a certain ethnic group are disproportionately overrepresented without justification because, in the opinion of the police officer conducting the check, individuals belonging to that ethnic group are more likely to commit crimes than individuals belonging to other ethnic groups, then a profile based on data from these checks could more easily lead to individuals of similar ethnicity being selected as subjects of the next law enforcement measure based on this. This, in turn, will again result in individuals belonging to the same ethnic group being overrepresented in the group of persons affected by measures carried

out as a result of the application of the given profile. This can then lead to false self-justification for the law enforcement officer already performing selection in a discriminatory manner.

In the algorithms developed and used for profiling, the above errors can occur at any step of the process. To avoid that, every person involved in the creation of the program, and the investigator collecting and interpreting the data, and ordering the measure, must be aware of the requirements of profiling in accordance with the law (FRA, 2018).

Therefore, to avoid the above negative effects, law enforcement profiling, as a state intervention into citizens' rights, has to pay particular attention to three main areas regulated by law. These are the *protection of privacy*, the *protection of personal data*, and the *prohibition of discrimination*. Adherence to the legal requirements, in addition to serving to avoid violations of the law, also serves to protect other social interests and values enshrined in law (including the interests of law enforcement). One of the most important consequences of non-compliance with the law is that unlawful profiling – as these characteristics can also be treated as consequences of several other unlawful law enforcement interventions – adversely affects relationships between law enforcement agencies and the communities they serve. Unlawful measures provoke resentment in the affected communities and reduce trust in law enforcement activities. This process undermines the effectiveness of community-based law enforcement methods (FRA, 2018).

8.5. Lawful Law Enforcement Profiling

For law enforcement profiling to avoid negatively impacting societal development, its application must meet legal expectations. These rules aim to define the boundaries within which the indirect harmful effects of profiling do not occur. Therefore, the regulations must be respected throughout the entire

profiling process. There are two distinguishable levels of legal expectations: firstly, specific law enforcement profiling must be based on national laws, including, where applicable, regulations within the European Union where they apply directly; secondly, these national laws must comply with the rules set out in relevant European Union legal sources and applicable international treaties, as well as the judicial practice of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

The protection of privacy, personal data, and the prohibition of discrimination are also enshrined in international legal sources, such as the European Convention on Human Rights (ECHR) (URL1) and the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights, 2009). National and EU rules on profiling must respect all of these, and their interpretation must take into account international court practice regarding the restriction of fundamental rights.

Given that profiling itself is not fully developed, , and the related Hungarian and international legal practice even less so, it is necessary to present the existing jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union on the subject.

8.5.1. Rights Affected by Profiling

Below, we will present those rights which may be violated by the improper application of profiling.

- PRIVACY AND PERSONAL DATA

In its 1976 judgment on X v. Iceland, the ECtHR, characterised the right to respect for private life under Article 8 of the ECHR as identical to the protection of privacy, meaning the right to live as we wish and to be protected from public view. However, respect for private life does not end there; it includes the right to

develop relationships with other persons without interference, especially for the purpose of developing one's own personality.

Many see the necessity of privacy protection within it as a prerequisite for democratic social institutions and as a building block of democratic society (Simitis 1987, p. 3.). Privacy is part of society's commitment to individual freedom, as it promotes the moral independence of citizens, a central feature of democracy, and thus its assurance is also a foundation of democratic government (Gavison, 1980).

However, the reduction of privacy limits social relationships among private individuals, who only disclose certain information to certain people and not to others; a reduction in the scope of their privacy also reduces the possibility of social relationships developing, as people will have fewer opportunities to cultivate their social connections (Roessler & Mokrosinska, 2013).

The right to self-realization, which is part of private life, has extended in the information society to the opportunities for communication and other social behaviours provided by information systems – activities carried out on social media sites – and to the personal data generated during these activities. Therefore, it is necessary to ensure the realization of fundamental rights free from unjustified state interference in these contexts as well.

Data protection, as a legal protection for the privacy of natural persons, emerged in Europe in the 1970s as a response to the dangers of increasing automated data processing due to the information revolution. The right to informational self-determination, which protects the individual rather than data by allowing the individual to dispose of their personal data, emerged and spread in the 1980s (Infojegyzet, 2018) and, as such, constitutes the active side of personal data protection.

Informational self-determination, on one hand, allows for freedom of decision, including actions based on such decisions (Sári & Somody, 2008). On the other hand, it allows for development and flourishing based on self-determination (Roßnagel & Richter, 2016). The general image of an individual's personality is determined by their actions and communication as manifested in a variety of social roles. The development of personality requires that a person be able to represent these roles and that they be reflected in their communication with others. The success of an individual's development and flourishing can depend on their being able to control the disclosure and publication of their personality. If an individual cannot keep track of when and under what circumstances their data was published, their ability to plan and decide on matters of self-determination is limited (BVerfGE 65, 1 [43]). Part of the self-determination decision is also what information the individual shares with others in their various social roles. This autonomous decision-making is the protected subject of informational self-determination, which is violated when someone possesses or acquires a person's data against their wishes, or perhaps without their knowledge (BVerfGE 84, 192 [195]).

It is also important to state that informational self-determination is not merely a personal right of a data subject. It is also the basis for free and democratic communication. A social and legal order in which citizens do not know who knows what about them in any given situation is incompatible with the right to informational self-determination. It not only hinders personal development but also harms the public interest because self-determination is a fundamental element of a free, democratic community, and only in such a community are members capable of independent action, which is an essential element of community development (BVerfGE 65, 1 [43]; BVerfGE 2006, p. 979). For this reason, the right to informational self-determination limits all state measures that, after their implementation, leave citizens in an uncertain situation, precisely

because they do not know exactly who knows what about them. These state interventions must be placed within appropriate limits because this uncertain state, and the fear of it, limits the actions of community members (BVerfGE 2006, p. 979).

From all of this, it follows that the rules of profiling must respect all personal data that individuals use for their communication and behaviour carried out over the internet. This means, for example, in the case of data found on public websites during the application of OSINT, as well as in profiles based on an individual's criminal data.

- PROHIBITION OF DISCRIMINATION

The emergence of the prohibition of discrimination can be linked to the demand for equality during the civil revolutions. These demands aimed to ensure that the same legal order applied to everyone, and that the state would not differentiate between people either in their relationship with the state (exercise of political rights) or in their private legal status (acquisition of property, inheritance). In this understanding, the essence of this right is that members of society should not be granted special entitlements or burdened with special obligations. To ensure equality, the requirement of equal treatment emerged, one element of which is the prohibition of adverse discrimination (Sári & Somody, 2008). The purpose of enforcing these principles is to ensure the development of democratic and tolerant societies that enable the participation of all people (Recital 12 of Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin). For all these reasons, the avoidance of discrimination must also be ensured during profiling.

Discrimination is prohibited by Article 14 of the ECHR and its Protocol No. 12. According to this, the enjoyment of the rights and freedoms set out in the Convention shall be secured without discrimination on any grounds such as

sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. The Charter of Fundamental Rights of the European Union contains a rule of similar content.

According to Article 21(1) and (2) of the Charter of Fundamental Rights, any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. Furthermore, any discrimination on grounds of nationality shall be prohibited.

An important role in the body of law concerning discrimination is played by Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (hereinafter: Equal Treatment Directive, Council Directive 2000/43/EC), which concerns the application of the principle of equal treatment. According to this legal source, the principle of equal treatment means that – during state measures – there shall be no direct or indirect discrimination based on racial or ethnic origin.

Literature classifies discrimination in several ways. During profiling, direct discrimination and indirect discrimination play a decisive role, so these two forms of discrimination will be discussed below.

We can talk about direct discrimination when on grounds of race or ethnic origin one person is treated less favourably than another is, has been, or would be treated in a comparable situation, or if a person is subject to less favourable treatment wholly or partly because of a characteristic affecting a protected area.

For example, in response to the threat of terrorism, police officers have the possibility of checking people's identities because they suspect that those

people are involved in the commission of a terrorist act. If the terrorist threat originates from a terrorist organisation operating in a specific area of the world, then direct discrimination occurs if police officers check someone's identity merely on the assumption that the person probably comes from the same geographical area as the terrorist group posing the threat (FRA, 2018).

Indirect discrimination occurs when an apparently neutral provision, criterion, or practice would put persons of a particular racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion, or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary.

The following case provides an example of indirect discrimination. Members of the investigative authority in City X – due to a routine check – stopped every tenth vehicle between nine in the evening and one in the morning. During this period in City X, 60% of the drivers were of Afro-Caribbean origin, although their proportion in the total population did not reach 30%. Therefore, it can be concluded that the measure indirectly disadvantaged this group of the population. It should be taken into account that if the reason for the action was that the number of traffic accidents was higher during this period than in other periods, then when assessing the necessity of police measures carried out to prevent this, further aspects would have to be considered to establish discrimination.

However, discrimination can occur due to several protected characteristics simultaneously. If a police officer checks the identity of a young African-American person, and does not check all young people and not all people of African descent under the same circumstances, then the person checked is subjected to adverse discrimination due to two protected characteristics (FRA, 2018).

- LEGAL SOURCES OF FUNDAMENTAL RIGHTS CONCERNING THE PROTECTION OF PRIVACY, PERSONAL DATA, AND THE PROHIBITION OF DISCRIMINATION

A common characteristic of these fundamental rights is that they appear as rights of citizens that the state must respect. However, such rights are not unlimited, meaning the state can enact laws that restrict them. However, for the state to enact such a restriction, adequate reasons would be necessary.

The ECHR, in Article 8(2) concerning the respect for private life, states that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

At the time the ECHR was drafted, the rise of data protection law was not yet evident, so the Convention does not specifically regulate this fundamental right. However, it is important to state that the ECtHR's jurisprudence interprets questions arising in connection with the protection of personal data within the framework of the right to respect for private life, and thus the restriction of the right to protection of personal data can only take place by taking into account the rules on the restriction of the right to private life.

According to Article 52(1) of the Charter of Fundamental Rights, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be applied if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The relationship between the Charter of Fundamental Rights and the ECHR is regulated by Article 52(3) of the Charter of Fundamental Rights. According to this, insofar as this Charter contains rights which correspond to the rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, their meaning and scope shall be the same as those laid down by the Convention. This provision does not prevent Union law from providing more extensive protection.

According to Article I(3) of the Fundamental Law, the rules relating to fundamental rights and obligations shall be laid down by law. A fundamental right may be restricted for the purpose of enforcing another fundamental right or protecting some constitutional value, to the extent strictly necessary, proportionately to the aim to be achieved, while respecting the essential content of the fundamental right.

- PROTECTION OF PRIVACY

The protection of privacy also appears among the provisions of the ECHR and the Charter of Fundamental Rights.

According to Article 8(1) of the ECHR, everyone has the right to respect for his private and family life, his home and his correspondence. According to Article 7 of the Charter of Fundamental Rights, everyone has the right to respect for his or her private and family life, home and communications.

- PROTECTION OF PERSONAL DATA

Article 8(1) of the Charter of Fundamental Rights assures, everyone of the right to the protection of their personal data, and according to paragraph (2), such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access the data collected about them and the right to have it rectified.

8.5.2 Summary of Data Protection Rules Affecting Profiling

Below, we review the data protection rules that apply to or affect profiling.

- RELATIONSHIP OF DATA PROTECTION RULES AFFECTING PROFILING

The Stockholm Programme of the European Council aimed to integrate a proactive and intelligence-led approach into the EU's internal security strategy, as well as to increase information exchange and the application of preventive measures (point 3.5.2 of the chapter on criminal law in the Stockholm Programme entitled 'An open and secure Europe serving and protecting citizens,' reinforcing the Union's international presence in the field of justice).

As a consequence of this, European Union legislation has re-regulated the framework for the use of personal data for criminal purposes with the Law Enforcement Directive[26] and the GDPR[27] coming into force. Automated profiling, as a basis for preventive measures, has been included in the EU's set of rules on personal data protection. The main purpose of establishing the new legal norms was to facilitate the European Union's exploitation of the benefits of managing increasing amounts of data, and thus its economic development, while not restricting the development of EU citizens, which is the basis for the economic, cultural, and innovative development of democratic societies.

One novelty of the data protection regulation is that the GDPR rules have become directly applicable in the legal systems of all Member States. The GDPR – with the exception of certain areas requiring specific regulation, such as those

[26] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter: Law Enforcement Directive; Directive (EU) 2016/680 of the European Parliament and of the Council).

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: General Data Protection Regulation, GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council).

falling under the scope of the Law Enforcement Directive – applies to all activities involving the processing of personal data that fall within the European Union's regulatory competence.

The regulatory subject and purpose of the Law Enforcement Directive, which should also be treated as the purpose of data processing, is that competent authorities process personal data for the prevention, investigation, detection, and prosecution of criminal offenses, or for the execution of criminal sanctions – including protection against and prevention of threats to public security – in order to protect natural persons. The legal act was created with the aim of ensuring a high level of data protection in the areas of police cooperation and judicial cooperation in criminal matters, and also to strengthen mutual trust and facilitate the free flow of data between the police and judicial authorities of the Member States.

According to the rule detailed in Article 2 of the Law Enforcement Directive, the directive applies to the processing of personal data wholly or partly by automated means, and to the processing by non-automated means of personal data which form part of a filing system or are intended to form part of a filing system.

In summary, the Law Enforcement Directive applies exclusively to the data processing relationships of organisations carrying out certain public order and security, crime prevention and detection, law enforcement, criminal procedure, and correctional activities – including activities related to misdemeanours – and thus national legal provisions implementing its requirements may also be limited to this scope (Recital 35 of the Law Enforcement Directive).

➢ LEGAL CATEGORIES OF DATA AFFECTED BY PROFILING

Identifiability concerns the possibility of directly or indirectly recognising natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Among personal data, special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

➢ BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

Personal data may be processed exclusively for a clearly defined, lawful purpose, for the exercise of a right and for the fulfilment of an obligation. Data processing must comply with the purpose of data processing at all stages, and the collection and processing of data must be fair and lawful. These principles encompass the requirements of lawfulness and fair processing.

Further important requirements are the principles of purpose limitation and data minimization. Only personal data that are essential for the fulfilment of the data processing purpose and which are suitable for achieving that purpose, and only to the extent and for the duration necessary for the fulfilment of that purpose. The essence of the purpose limitation requirement is that data collection should only take place for a specified and clear purpose, and the processing of data should not be carried out in any manner incompatible with such purposes.

The essence of the principle of data minimization is that the collected data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, meaning only those data can be processed that are required to achieve the data processing purpose specified in the law.

Personal data retains this quality during processing as long as its connection to the data subject can be re-established. The connection can be re-established with the data subject if the data controller has the technical conditions necessary for restoration.

During data processing, the accuracy, completeness, and – if necessary for the purpose of processing – the up-to-dateness of the data must be ensured, as well as that the data subject can only be identified for the time necessary for the purpose of data processing. The essence of the principle of accuracy is that processed data must be accurate and, where necessary, kept up to date; and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Personal data must be stored in a form that allows identification of data subjects only for the period necessary for the purposes for which the personal data are processed (storage limitation requirement).

During data processing, with regard to the requirements for data integrity and confidentiality, it is important to emphasise that data processing must be carried out in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (integrity and confidentiality principle).

➢ LEGAL BASIS FOR LAW ENFORCEMENT PROCESSING OF PERSONAL DATA

In general, personal data can only be processed if it is ordered by law and the scope of data that can be processed is defined by law. Data processing is also possible if the data subject has explicitly consented to it, or if the data subject has explicitly made the personal data public. Special data may also be processed if it is ordered by law for national security, for the prevention, detection, or prosecution of crimes, or for national defence purposes.

It is important that in cases where investigative authorities obtain data through a data request – since this was mandatory data provision and only voluntary to the extent that non-compliance would otherwise be sanctioned – we cannot talk about voluntary consent. In the case of such data, Member State laws may provide that the data subject may consent to the performance of DNA analysis within the framework of criminal investigations, or to monitoring the whereabouts of the data subject using electronic identification during the execution of criminal sanctions (Recital 37 of the Law Enforcement Directive).

Personal data processing includes any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction.

➢ PROCESSING OF PERSONAL DATA DURING AUTOMATED DECISION-MAKING AND PROFILING

The concept of profiling is treated identically by the GDPR and the Law Enforcement Directive. According to these legal acts, *profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work,

economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

It follows from this definition that the concept of profiling in the examined legal environment is limited exclusively to the automated processing of personal data. The above legal acts regulate profiling as a case of automated decision-making. It is also important that the additional requirements prescribed during automated decision-making procedures apply only to data processing based on automated decision-making procedures, and their consideration is not necessary in the case of other data processed within the scope of non-automated decision-making.

According to the Law Enforcement Directive, a decision based solely on automated processing – including profiling – which produces legal effects concerning the data subject or similarly significantly affects him or her, is prohibited, unless it is authorised by the European Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including at least the right to obtain human intervention on the part of the controller.

Data processing carried out during automated decisions is lawful if it does not violate the requirement of equal treatment. From this, it follows that such decisions cannot be based on special categories of personal data. These personal data are by their nature particularly sensitive in relation to fundamental rights and freedoms and deserve specific protection, as their processing circumstances may entail significant risks for fundamental rights and freedoms.

The processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic and biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex

life or sexual orientation, is only permitted – with appropriate safeguards for the data subjects' rights and freedoms – if it is strictly necessary.

A further condition for this is that it is permitted by European Union or Member State law, and serves to protect the vital interests of the data subject or of another natural person; or relates to data that the data subject has manifestly made public. For all these reasons, it is of paramount importance that a measure is not based solely on data relating to a protected characteristic; its lawful execution also requires evidence based on additional data.

The following requirements are considered appropriate safeguards for the rights and freedoms of data subjects: the data in question may be collected only in connection with other data relating to the said natural person, stricter rules are laid down for access to the data by the competent authority's staff, or the transmission of the data is prohibited. The processing of these data may also be permitted by law if the data subject has explicitly consented to processing that is particularly intrusive for them. However, the data subject's consent alone cannot serve as a legal basis for the processing of such special personal data by competent authorities (Recital 38 of Law Enforcement Directive).

A decision based on automated data processing, the purpose of which is to evaluate certain personal characteristics relating to the data subject, and which would have an adverse legal effect on or significantly affect him or her, may only be applied if appropriate safeguards are in place. Such safeguards include ensuring specific information to the data subject and their right to obtain and receive human intervention, in particular to express their point of view, their right to obtain an explanation of the decision made based on such an evaluation, and to challenge the decision. Profiling of natural persons that results in discrimination based on personal data that are particularly sensitive by their nature in terms of fundamental rights and freedoms is prohibited under the conditions set out in Articles 21 and 52 of the Charter (Székely et al., 2017).

8.6. International Jurisprudence on Profiling

Profiling is impacted by various decisions from both the ECtHR and the CJEU. Below, we'll delve into the most significant ones, also touching upon the stance of the German Constitutional Court on the matter.

8.6.1. Relevant ECtHR Judgments on Privacy and Data Protection

In the ECtHR's jurisprudence, Article 8 of the ECHR holds the greatest relevance concerning profiling.

- ELEMENTS OF THE PROPORTIONALITY TEST APPLIED BY THE ECTHR

The ECtHR has brought all issues involving state intervention affecting personal data protection under the rules of Article 8. Furthermore, under the scope of this Article, the court assesses the lawfulness of state measures restricting the right to identity, the free development of personality, and the right to communicate with others.

The primary reason for the state's use of personal data is that it allows for a higher degree of security (national security, public safety, etc.). Recent trends indicate that people's desire for security makes them willing to approve state interventions that restrict fundamental rights to achieve security. Such an intervention – simplified – is appropriate if the benefit achieved by the intervention is proportional to the restriction of rights caused. The ECtHR's practice has, in several cases, examined state laws on data processing from the perspective of whether the restriction of rights caused by them is proportionate to the intended goal.

Such an examination is carried out by applying the *proportionality test*, which essentially consists of four sub-tests: the legitimate aim test, the suitability test, the necessity test, and finally, the proportionality test in the strict sense (Székely et al.,

2017). Thus, to decide whether a national law can be reconciled with the ECHR, it must be subjected to this test.

According to the first sub-test, a restriction of a fundamental right can only be justified by a purpose that expresses a fundamental societal value. This typically includes the protection of fundamental human rights and the service of public interest. The suitability test examines whether the restriction of rights is suitable for achieving the set goal, whether there is a reasonable connection between the goal to be achieved by the restrictive law and the means of restriction, and whether the means are capable of achieving the goal.

The necessity test examines whether the least restrictive means possible are used in the law to achieve the goal (for clarity, for example, if something can be obtained through data acquisition activities, then coercive measures – search, seizure – are not necessary).

The last test is the true domain of judicial discretion, which involves weighing two values: the value expressed in the purpose of the restriction and the restricted fundamental right. A restriction of a fundamental right can be considered justified if the benefits achievable by realising the right-restricting purpose are appropriately proportional to the extent of the interference with the fundamental right (Burgatz v. Switzerland; and Fiedl v. Austria).

Observation aimed at increasing the level of security affects citizens by the tools and methods employed that involve the collection, storage, use, and making accessible of personal data, excluding access to one's own personal data, or limiting control over personal information (De Hert–Lammerant, 2016). The proportionality test of Article 8 states that measures defined in laws allowing state intervention into privacy to guarantee security are justified if these two values (privacy and security) are balanced.

Below, we present the legal interpretations formulated in the case law that may arise in connection with profiling. The purpose of presenting the cases is to better understand the boundaries that state interventions must not cross.

➢ THE RELATIONSHIP BETWEEN PROFILING AND PRIVACY

Regarding profiling, the first question to clarify is whether profiling even constitutes an interference with privacy.

Profiling applied in law enforcement does not only mean the collection of data but also includes the use of previously collected and available data. In the vast majority of cases, the creation of profiles during profiling occurs with data already in the possession of state authorities. In this regard, the question may arise: if the state has already legitimately acquired the data, why shouldn't it be free to do whatever it wants with it?

The ECtHR stated in this regard that the protection of private life applies not only within a person's private space (home, car, computer) but also, in certain cases, must be respected more broadly by the authorities. The court in the case of *von Hannover v. Germany* stated that a person also has a zone belonging to private life during their interactions with other persons. This was reaffirmed in the case of P.G. & J.H. v the UNITED KINGDOM. The facts of the case involved the wiretapping of a person's apartment because of a planned bank robbery. Later – after the wiretapped person refused to provide a voluntary voice sample – their conversation with an undercover detective in their cell was secretly recorded, and that recording was then compared with the recording that had been made in the apartment, establishing the identity of the two voices.

The need for privacy protection arises even if authorities obtain such a recording from a public source, that is, even if they do not obtain it through some covert measure. Although recordings are generally made to use the content of conversations, the court found that making publicly recorded recordings for the

purpose of voice samples also falls within the scope of Article 8 if the voice sample is produced from the person's voice and is specifically analysed for the purpose of identifying the person regarding their other personal data. The recording and analysis of a person's voice can be considered the processing of the data subject's personal data.

The court reached similar conclusions regarding data storage (LEANDER V. SWEDEN, ROTARU V. ROMANIA, AMANN V. SWITZERLAND), further data retention (S. AND MARPER V. UNITED KINGDOM), and the diffusion of personal data (PECK V.UNITED KINGDOM; Z. V. FINLAND).

These decisions made it clear that the use of personal data constitutes an interference with private life, and therefore such state conduct must be legitimised. Authorities have an obligation to take into account an individuals' right to respect for their private life when deciding on further use of such data. This means that if data is in the possession of an authority (be it an investigative authority or another authority), it does not mean that it can carry out any further data processing without restriction. In the case of subsequent conduct carried out on personal data, the person is also entitled to the protection of their right to respect for private life, and in connection with this, the protection of personal data, meaning such data processing can only take place based on a legal regulation that complies with the data restriction possibilities set forth in Article 8(2) of the ECHR.

Thus, the conclusion can be drawn from jurisprudence that the entire process of profiling must be properly regulated.

- LEGITIMACY OF NATIONAL LAW

An intervention is lawful if it has a legal basis in the relevant Member State law, [iv] meaning there is a legal regulation that allows the authority to apply it.

The court, as it explained in the P.G. & J.H. v. UNITED KINGDOM case, also examines the quality of the law in this context. This examination assesses whether the law provides adequate safeguards against arbitrariness during its application (for example, law enforcement is arbitrary if it disregards the law, or the law is inadequate if it allows for arbitrary interpretation and thus arbitrary law enforcement).

This requirement plays an important role in the context of profiling. If people do not know that their data has been used, they cannot take action against such state interventions. If the selection mechanism of an algorithm used during profiling cannot be understood, it is impossible to rule out arbitrary data provision or arbitrary data selection.

In the GILLAN AND QUINTON V. UNITED KINGDOM case, the court found that the right to private life had been violated because the application of identity checks and searches that could be carried out under the law it examined did not meet the criterion of restriction that it could only take place in cases specified by law. The court's position was that the restriction of rights was not properly regulated (that is, was 'not in accordance with law').

Under sections 44-47 of the Terrorism Act 2000 adopted in the United Kingdom, police were authorised to check and search private individuals, even if there was no suspicion that they had committed any unlawful conduct, for the purpose of searching for objects suited to committing a terrorist act. Persons refusing the check could be fined.

Although the investigative authority's measure was based on a legal regulation, the ECtHR later found it an insufficient legal basis for police identity checks. In its opinion, the severity of the state intervention was increased by its open nature, thereby revealing personal data merely by the identity check.

The court found that the police had been given excessively broad and unbounded powers by the law, while individuals were not provided with sufficient protection or guarantees to act against arbitrary law enforcement. We note that the court also found that this type of regulation carries the potential for discriminatory law enforcement, but the details of this will be discussed in the next chapter. The scope of the authorization contained in the law was too broad both geographically and temporally, and it allowed too wide a range of discretion to the members of the investigative authority. Based on this, the legal institution in question was not properly regulated.

A similar decision was made in the LIBERTY AND OTHERS V. UNITED KINGDOM case concerning digital surveillance. The judgment concerning the United Kingdom was based on the fact that a telecommunications service provider connected to the government recorded the entire communication data of several organisations linked to Ireland between 1990 and 1997.

The court found that the government-operated mass surveillance system violated the right to private life because the relevant domestic law requiring data retention did not clearly define the scope of interceptions and did not provide adequate protection against an abuse of the law.

The essence of all these decisions, when applied to profiling, requires taking the following into account: profiling requires a legal basis, and citizens need appropriate safeguards at every stage of the procedure. Through legal regulations, profiling must ensure that citizens can see and understand why the procedure took place, why they were selected within it, what data was used to create the profile, and the manner in which it was applied.

- FURTHER REQUIREMENTS FOR LEGITIMATE LEGISLATION

The next condition for a legitimate intervention is that it must have a proper purpose. This requirement does not impose unrealistic expectations; the reason

for profiling in the context of law enforcement profiling is the maintenance of public safety, the prevention of crimes, and the protection of the rights and freedoms of others, that is, reasons that comply with the conditions for limiting rights stipulated in the ECHR.

The next conditions for a legitimate intervention are *necessity* and *proportionality*, that is, proving that the intervention is necessary in a democratic society.

The concept of necessity in the court's practice does not imply the mandatory application of a strict necessity test. It allows for a certain degree of discretion, which may vary depending on the subject of the examination. It is important, however, that the method of interpretation is limited. The court has stated in several cases, including: LEANDER V. SWEDEN, SILVER V. UNITED KINGDOM, AND HANDYSIDE V. UNITED KINGDOM that an intervention is acceptable if it addresses a pressing social need and is proportionate to the legitimate aim pursued.

The measure, on one hand, must have a legitimate purpose and must be causally linked to the aims to be achieved, meaning it must be suitable for achieving them. A crucial requirement is also that it should not restrict rights more than is necessary, considering alternative ways to address the social problem. Furthermore, in the absence of a suitable alternative – taking into account the proportionality requirement – the (social) benefit achievable by the measure must be greater than its cost, that is, the (social) disadvantages caused by the restriction of rights.

In relation to profiling, it follows from the court's case law that the mere fact that the restriction of rights concerning data collection – considering the purpose of data collection – was proportionate, does not automatically mean that

the retention, storage, or other data processing operations carried out with the data also comply with the proportionality requirement.

Further actions justify considering new and different aspects of proportionality testing (the S. AND MARPER V. UNITED KINGDOM case). The data subjects in the case requested the deletion of their data (fingerprints, DNA profile) from the NDA database (used by investigative authorities to identify criminals), given that they had been acquitted in the criminal proceedings against them. The court examined the relevant rules and stated that although the data collection was lawful, the further storage of data generated during suspicion concerning persons who were acquitted or whose charges were dropped was unlawful. The court cited the risk of stigmatization inherent in data storage as a problem in its reasoning.

The essence of the stigmatization effect (labelling theories) – as is clearly perceptible in Ken Kesey's ONE FLEW OVER THE CUCKOO'S NEST – is that stigmatised people sooner or later begin to behave according to their stigma. For example, if someone is treated as a criminal, that person will tend to exhibit criminal behaviour.

According to the court's view, storing data collected for a lawful purpose even after it no longer serves that purpose is not beneficial to society, as individuals who have not committed a crime were treated the same as those who had. The harm is particularly significant for minors, whose development and social reintegration can be severely impaired by this.

In another decision, the court did not object to the use of existing data of past offenders to predict future crimes but required that the individuals concerned be limited and that specific criteria for selection be applied (VAN DER VELDEN V. THE NETHERLANDS). It also stated that the approach according to which more data in the system makes the system more effective and justifies data retention

makes the intervention disproportionate (S. AND MARPER V. UNITED KINGDOM, M.K. V. FRANCE) (De Hert–Lammerant, 2016).

8.6.2. Court Practice Regarding Adverse Discrimination

In the CARSON AND OTHERS V. UNITED KINGDOM case, the ECtHR explained that discrimination arises when a difference made in a procedure is based on an identifiable characteristic or status in analogous or substantially similar situations. Treatment is considered discriminatory if the differentiation has no objective and reasonable justification, or if it does not serve a legitimate purpose, and furthermore, if there is no reasonable relationship between the means used for the differentiation and the stated goals in terms of proportionality. The principle of non-discrimination requires that similar situations should not be treated differently, and different situations should not be treated in the same way.

Data mining algorithms fundamentally reveal relationships between data, based on which profiling identifies individuals or groups that share the characteristics of a given profile. A profile created in this way can contain several characteristics or properties that can be evaluated as relevant differences compared to the characteristics of other individuals. The prohibition of discrimination – by placing certain characteristics under protection – determines which relevant differences can be taken into account and which cannot.

Characteristics protected by the prohibition of discrimination cannot be considered relevant differences as long as their necessity for consideration is not adequately justified; thus, they cannot form the basis for differentiation. The prohibition of discrimination – as demonstrated when examining interference with privacy – is a rule valid at every phase of the profiling process, both when selecting the data necessary for creating the profile and when applying the profile.

Profiles cannot, therefore, be created based on protected characteristics, and such a created profile cannot be applied unless there is sufficient justification for doing so.

The decision of the Court of Justice of the European Union in the case of HEINZ HUBER V. FEDERAL REPUBLIC OF GERMANY is instructive from the perspective of profiling. The facts of the case were that Germany operated a register (database, AUSLANDERZEINTRALREGISTER AZR) which contained the personal data of non-German citizens (including those of EU Member States and all other citizens) who had resided in Germany for more than three months. The purpose of operating the database was to facilitate the processing of applications for residence permits for foreign citizens staying longer than three months. In addition to the person's basic data (name, birth, gender, nationality), the database also contained data generated in connection with their entry into the country, as well as their citizenship. The database also contained data on expulsion procedures carried out in relation to the person, as well as criminal data of the person related to serious crimes (drug trafficking, terrorist acts, etc.). The data processed in the database was used for several purposes, including settlement procedures, statistical purposes, and crime prevention purposes. A database of this content, and thus comparable, that specifically contained criminal data of the person concerned, did not exist for German citizens. The court found that the operation of databases containing data of foreign citizens is lawful as long as it assists in the processing and handling of residence permit applications and as long as it contains only the data necessary for decisions to be made in these procedures. Furthermore, another requirement for their lawful operation is that the data in the database are only used in those official procedures that formed the basis of the data collection, that is, the data collection took place for the purpose of carrying out these procedures.

It further stated that it is not problematic in itself that a Member State does not operate a database for its own citizens that contains the same data as that collected about foreign citizens in connection with residence permits. The reason for this is that the authorities needed further data to process residence permits, which legitimised the collection of data in the database. Therefore, although there was a difference between the databases containing personal data of German citizens and foreign citizens, this in itself was not discriminatory, as the differentiation served a legitimate legal purpose and the differential treatment was proportionate to this purpose. The differential treatment was reasonably connected to the differences inherent in the legal situations and was therefore justified.

The court, however, found the use of the database for law enforcement purposes by the investigative authority to be problematic. The reason for this was that, since the law enforcement purpose is independent of the perpetrator's nationality or citizenship, this purpose does not justify differential treatment between national and other EU citizens. In other words, the use of additional data, such as data relating to the person's nationality, is not necessary for law enforcement agencies to carry out their tasks.

This case was fundamentally about data managed by authorities and access to them by investigative authorities, stating that differentiation based on nationality (a protected characteristic) for law enforcement purposes is not permitted in profiling.

Discriminatory treatment related to investigative authorities' access to data may also arise at further steps of profiling, such as during the creation and application of the profile.

Barocas and Selbst's 2016 study identified five discriminatory mechanisms in data mining and profiling. These can lead to prohibited treatment if the

intervention affects groups differently, if statistical errors are not recognised during profiling, if profiling recreates previous discrimination. This also includes cases where profiling is carried out by taking insufficient factors into account, and in cases of masking. The latter case is when the person creating the profile presents intentional discrimination as an accidental error. Masking is not a general phenomenon; it can be stated that the creation of profiles leading to discriminatory results is typically caused by some act of negligence. The latter can be particularly problematic in cases where a market, non-law enforcement actor is involved in a profiling process, who fundamentally tries to use their resources based on economic rationality and not necessarily on the primacy of law, and thus is not necessarily interested in uncovering potential discriminatory models (Barocas–Selbst, 2016, p. 677).

The issue of discriminatory treatment may arise particularly in connection with profile creation whether protected data is used directly or indirectly. Based on the case presented regarding data filtering, it can be said that protected data can only be used in the presence of factually justified, specific danger.

In the German Constitutional Court's case concerning data filtering, the court did not examine the possible occurrence of discrimination in relation to the measure applied. However, the profiles created by investigative authorities were fundamentally linked to the Muslim faith, a protected characteristic, without sufficient justification.

However, differential treatment is not excluded. For example, in cases of suspected terrorist acts, which fundamentally arise on religious, ethnic, or ideological grounds, the religious, ethnic, and ideological background will be decisive, and thus this can be a sufficient reason for considering these characteristics (De Hert–Lammerant, 2016, p. 159). Profiles concerning suspect descriptions may include data such as the suspect's skin, hair, and eye colour, but only if witness statements to that effect are available. However, if investigative

authorities receive overly general suspect descriptions containing racial, ethnic, and other similar characteristics, they cannot use them as the basis for their actions (FRA, 2010, p. 63).

In their study, De Hert and Lammerant emphasise the importance of applying a so-called discrimination test to avoid discriminatory treatment, that is, evaluating the outcome of profiling. The purpose of this evaluation is to examine whether the profiling result and the actual measures implemented based on it created unjustified differential treatment.

Accurate and precise information can also reduce the risk of unlawful discriminatory profiling. If law enforcement measures are based on specific and timely information, it is more likely that objective, non-stereotypical decisions will be made.

8.6.3. Conditions for Lawful Profiling

In summary, profiling must meet the following criteria: (1) a clearly and precisely formulated legal authorization of appropriate quality is required, the details of which citizens have to be able to access; (2) the social purpose to be achieved by the profiling must be detailed, and present throughout the entire profiling process; (3)data processing during profiling is only possible if it is necessary and at the same time proportionate to the restriction of rights caused by the intervention (FRA, 2018, p. 120), and this proportionality requirement must be met at every stage of profiling.

In view of all this, the entire profiling process must be adequately regulated, including the creation of the legal basis for it and the provision of appropriate guarantees for citizens.

In relation to profiling and measures based on it, its scope must be precisely defined both geographically and temporally, including the precise limits of discretionary power.

Through legal regulations, profiling must ensure that citizens can understand and comprehend the reason for the procedure's initiation and how selection within it occurred, as well as what data was used to create the profile, and the way in which it was applied.

It is not merely the large number of collected and used data that ensures the system's effectiveness, but rather the accuracy and reliability of the data.

In the case of data processing affecting a wide range of citizens, there is a need for an independent body to oversee data processing and the use of data for criminal purposes.

Furthermore, it is advisable that the data subjects are aware that their personal data have been used in automated decision-making procedures, and in connection with this, have appropriate guarantees, especially the possibility of initiating legal remedies in connection with such interventions.

During profiling and any measures based on it, the dignity of private individuals must be respected, taking into account the conduct expected in police codes of ethics.

The reasonableness of profiling and its reliance on objective grounds must be ensured at every stage of profiling.

The suspicion necessary for the measure must be supported by objective reasons; mere intuitions are not sufficient for carrying out such measures. In this regard, it is particularly important that a protected characteristic alone or as the main reason cannot serve as a basis for any measure, thus avoiding direct discrimination.

Furthermore, in cases of legal violations occurring during the profiling process, the precise delineation of responsibilities and accountability must be guaranteed.

It is also important to comply with the rules regarding secure data processing. This includes ensuring that unauthorised persons do not access the data, do not use it for purposes other than the original purpose of data processing, and do not store it longer than necessary. For this reason, data processing records must be kept, and the regulations regarding data processing security must be complied with (Article 24 and 29 of Law Enforcement Directive). These measures are also useful for law enforcement agencies, as they can also prove lawful data processing in the event of a dispute.

Unlawful data processing must be identified and prevented. To this end, data protection impact assessments and the principles of data protection by design and by default must be applied (Article 20 and 27 of Law Enforcement Directive).

An impact assessment must be carried out before data processing begins if the type of data processing – especially using new technology – is likely to pose a high risk to the rights and freedoms of natural persons, considering its nature, scope, circumstances, and purposes.

An impact assessment can also be performed retrospectively to verify that the data processing was lawful. With static algorithms that operate according to predetermined criteria, the risk of infringement is lower than with so-called dynamic algorithms, which reveal ever newer correlations during their own redefinition. In such circumstances, there is a risk that the programmer may themselves no longer understand the modifications made by the program through artificial intelligence and machine learning.

The principle of data protection by design and by default requires the implementation of appropriate technical and organisational measures – such as

pseudonymisation – primarily aimed at the effective implementation of data protection principles, such as data minimisation.

Pseudonymisation is a measure after which personal data cannot be linked to a person in the absence of additional information. Its essence is that the information necessary for repeated identification must be treated separately and securely. Unlike anonymised data, pseudonymised data is still considered personal data and enjoys the broader protection of data protection law.

Accordingly, the principles of data protection do not apply to anonymous information, that is, information that does not relate to an identified or identifiable natural person, and to personal data that have been anonymised in such a way that the data subject is no longer identifiable (Recital 21 of Law Enforcement Directive).

According to the Law Enforcement Directive, only personal data that is necessary for the specific data processing purpose can be lawfully processed. This obligation applies to the quantity of personal data collected, the extent of their processing, their storage period, and their accessibility. The principle of data protection by design and by default must specifically ensure that personal data are not made accessible to an indefinite number of persons by default without the intervention of the natural person.

It is also worth considering the guidelines issued by the European Union Agency for Fundamental Rights (FRA) regarding the processing of PNR data, which were formulated to prevent the violation of fundamental rights during PNR data processing.

According to this, data may only be used in connection with the criminal offenses for which the data was collected. Only organisational units authorised to process the data may access the processed data. It is also important to emphasise that if a person processing data only deals with the prevention of serious crimes,

they should not be able to access, for example, data necessary for the prevention of terrorist acts.

It's crucial that data reaches information units only through accurate data collection, not automatically.

It's also important to consider that profiles based on protected characteristics are not permissible. However, conclusions about protected characteristics might sometimes be drawn from other attributes, for instance, information about dietary habits could, in some cases, reveal religious practices. Information units are prohibited from processing data related to protected characteristics. To achieve this, it's essential that information concerning, for example, dietary habits or health, be deleted. It's also necessary to check that such information isn't found in the free-text fields of PNR data disclosures.

During data processing, it's vital to test profiles using anonymised samples. Overly broad criteria used in profiles increase the occurrence of false positives, and sometimes this alone can be discriminatory. For example, information about LGBTQ+ individuals might be obtained from past criminal data, as their behaviour could be considered a crime in some non-EU countries.

Data must be accurate and factual. Inaccurate data can negatively affect individuals and create false correlations, which can diminish public trust in law enforcement activities. Furthermore, information units may only transmit data from the system to authorised law enforcement agencies (FRA, 2014, p. 2).

8.7. The Use of AI Systems in Law Enforcement, with Special Emphasis on Profiling

The use of AI in law enforcement appears to be indispensable in the rapidly changing landscape of modern crime. This chapter will briefly present the advantages and potential uses of AI in law enforcement. However, it is also

necessary to elaborate on the requirements and legal provisions that must be considered during the development of an AI system. The fundamental aim of these legal norms is to ensure that the use of an AI system does not unduly violate human rights standards, while enabling law enforcement to leverage the benefits of technology as widely as possible.

This regulation primarily takes shape in the European Union through the Artificial Intelligence Act (AI Act, Regulation (EU) 2024/1689), which is directly applicable in Member States.

The AI Act is the first-ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally. The AI Act lays down harmonised rules on artificial intelligence and is the first-ever comprehensive legal framework on AI worldwide. The aim of the rules is to foster trustworthy AI in Europe. The AI Act sets out a clear set of risk-based rules for AI developers and deployers regarding specific uses of AI. The AI Act is part of a broader package of policy measures to support the development of trustworthy AI, which also includes the AI Innovation Package, the launch of AI Factories and the Coordinated Plan on AI. Together, these measures guarantee safety, fundamental rights and human-centric AI, and strengthen uptake, investment and innovation in AI across the EU (URL2).

There are numerous definitions of artificial intelligence. The most comprehensive definition of the main characteristics of artificial intelligence is contained in the definition developed by the High-Level Expert Group on Artificial Intelligence (AI HLEG).[28] According to which:

> *As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge*

[28] AI HLEG, 'A definition of AI: Main capabilities and scientific disciplines.' 2018, URL3

> *representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).*

It can be seen that artificial intelligence has three main elements: machine learning, machine reasoning, and robotics.

Solutions that apply artificial intelligence are called AI systems. According to Article 3(1) of the AI Act:

> *AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*

A key characteristic of AI systems is their ability to infer. This capability refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved (Recital 12 of AI Act).

8.7.1. Possibilities for the Use of AI in Law Enforcement

Artificial intelligence offers many useful possibilities for increasing the effectiveness of tasks in law enforcement. These possibilities are diverse.

For example, its application offers significant support and development opportunities in the field of predictive policing activities, such as determining the

location and time of potential crimes, and also in the field of crime detection, in some cases, automating the application of covert tools and their results.

The sophisticated statistical methods used by AI systems can provide valuable new information from criminal record datasets or from events and environmental factors identified in criminological analyses. Its application allows law enforcement agencies to easily and accurately identify patterns related to the occurrence of crimes and dangerous situations, and based on this information, minimise risks by more targeted application of available resources (Europol Report, URL4).

Furthermore, artificial intelligence can help in analysing large datasets from seized devices, police reports, and otherwise unsuccessfully closed 'cold cases,' selecting relevant information in cases, enabling members of the investigative authority to faster and more accurately to uncover relevant information and connections related to a given case.

Extensive application is possible in the field of facial recognition, as its use allows for faster and more accurate identification of subjects in criminal proceedings, but it can also be applied in the processing of other biometric data.

Its application can achieve significant resource savings in the field of OSINT and Social Media Intelligence (SOCMINT); with its help, an individual's profile can be easily determined using data from open sources.

Artificial intelligence can also provide assistance in performing everyday administrative tasks. It can automate time-consuming processes that must be performed alongside actual law enforcement tasks. For example, speech recognition technology can help in preparing police reports, transcribing testimonies, and also automate the processing of written or telephoned complaints.

8.7.2. Legal Framework for the Use of AI in Law Enforcement

The development and use of AI systems for law enforcement purposes are now widely regulated. In the territory of the European Union, during the development and application of AI systems, attention must be paid to the right to private life and the protection of personal data enshrined in the Charter of Fundamental Rights of the European Union (URL5, Art. 7. Respect for private and family life; Art. 8. Protection of personal data), the rules of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, URL6), the Law Enforcement Directive (Directive [EU] 2016/680, URL7), and primarily the rules of the Artificial Intelligence Act (Regulation [EU] 2024/1689, URL8).

These rules fundamentally determine the processing and use of natural persons' personal data for law enforcement purposes in the fields of crime prevention, investigation, detection, and prosecution, as well as in the enforcement of criminal sanctions.

The Law Enforcement Directive specifically addresses the processing of personal data for the prevention, investigation, detection, or prosecution of criminal offenses, as well as the enforcement of criminal sanctions. It stipulates that these operations must always be carried out with respect for the main principles of data protection to protect individual rights and comply with legal norms.

The fundamental aim of these principles is the protection of personal data, thus the legal regime pays particular attention to the data protection principles of fairness, accountability, and transparency in relation to artificial intelligence systems, as well as the enforcement of requirements for data security, data accuracy, and non-discrimination.

In the context of data processing, the principles of purpose limitation and data minimization require that data collected for a specific purpose should not be

used for different purposes, and only the amount of data necessary to achieve the stated goals should be processed. In AI systems, data must be accurate, meaning they must faithfully reflect reality, and furthermore, they must be up-to-date, thereby ensuring the avoidance of unjustified fundamental rights interventions.

In cases where data processing is automated, including profiling, AI systems must ensure the principle of protection against automated individual decision-making, the essence of which is that automated data processing should not cause significant adverse effects on individuals without adequate safeguards, and that individual responsibility attributable to a natural person should be enforced, meaning decisions concerning individuals should always be attributable to a specific natural person.

8.7.3. Regulatory Structure of the AI Act

One of the main objectives of the Artificial Intelligence Act was to maintain and strengthen the trust of European citizens in the use of artificial intelligence through its detailed regulatory framework. To this end, a fundamental expectation of the AI Act is that its rules must be applied in accordance with the values of the European Union enshrined in the Charter of Fundamental Rights of the European Union.

Compliance with this, on the one hand, promotes the protection of natural persons, businesses, democracy, the rule of law, and the environment, while also boosting innovation and employment, which is a pan-European interest (Recital 2 of AI Act). This also includes that during the operation of AI systems, the data protection rules of the General Data Protection Regulation, the Law Enforcement Directive, and the provisions on the liability rules of intermediary service providers defined in the Digital Services Act (Regulation [EU] 2022/2065, Digital Services Act, DSA, URL9) must also be complied with.

If it is not possible to determine retroactively why a particular decision of an AI system was made, or why the system performed a particular task, then its correctness and legality cannot be understood or determined. In this context, it matters whether an AI system merely provided a suggestion for reading a book based on a conclusion drawn about an individual according to its defined preferences, or if a decision was made based on the result determined by the AI system as to whether the person examined by the AI system can be released on parole or not. While in the first case, the risk of the AI system's operation is limited to the inability to understand how and on what basis the given system influences a person's habits, value judgments, and preferences, in the other case, the person's right to personal liberty is restricted.

The use of AI systems applied for different purposes and at different levels of development affects the fundamental rights defined in the Charter to varying degrees, which in itself represents a risk. The AI Act has, therefore, established different regulatory systems along these risks according to their severity and defined four risk regulatory systems that individual AI systems must comply with, depending on their functionality. These four regulatory systems apply to systems using prohibited practices, high-risk AI systems, limited-risk systems due to their transparency, and minimal-risk or general-purpose AI systems.

8.7.4. AI Systems in Law Enforcement

Regarding the application of artificial intelligence in law enforcement, it can be stated that – due to the nature of the data involved – they represent a significant interference with citizens' freedoms, particularly in areas such as predictive policing, identification based on biometric data, or assessing the risk of recidivism in criminal proceedings (Fuster, 2020; URL10). Taking this into account, the AI

Act sets out specific rules for the use of artificial intelligence for law enforcement purposes.

These rules in the AI Act regulate the use of AI systems in law enforcement and under which law enforcement includes:

Activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection, or prosecution of criminal offenses, or the execution of criminal sanctions, including the protection against and prevention of threats to public security.

The importance of considering these rules lies in the fact that the usability of information derived from AI systems operating in violation of these rules may be questioned in court. For the effective functioning of the justice system, it is necessary that data generated during the law enforcement application of AI systems can be used as evidence in criminal proceedings.

The following sections will present specific areas of the use of AI systems for law enforcement purposes and their corresponding legal regimes.

AI Systems Employing Prohibited Practices

According to the Artificial Intelligence Act, the use of the AI systems presented below for law enforcement purposes is – with some exceptions – prohibited.

- RISK ASSESSMENT OF INDIVIDUALS

In line with the presumption of innocence, decisions concerning natural persons in the European Union may in all cases be made solely on the basis of the actual conduct of those persons. Thus, the results of risk assessments from AI systems – the purpose of which are to assess or predict through profiling of individuals or evaluation of their personality traits or characteristics the risk or probability of a person committing or intending to commit a criminal offense – cannot serve as a basis for official decisions in law enforcement activities.

An exception to this is an AI system that supports human evaluation of an individual's participation in a crime. In such cases, however, the assessment must be based on objective and verifiable facts already available that are directly related to the criminal activity. Nor does this prohibition apply to risk analyses that are not based on individual profiling or on individuals' personality traits or characteristics, for example, AI systems that use risk analysis by analysing business transactions to determine the likelihood of financial crimes, or those that predict the potential location and time of illicit goods, such as drugs, being smuggled across borders based on known smuggling patterns and routes (Art 5. [1] d. and recital 42 of the AI Act).

- BIOMETRIC CATEGORIZATION SYSTEMS

Biometric categorization means the classification of natural persons into specific categories based on their biometric data, such as their face or fingerprints. Such categories can include gender, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, belonging to a national minority, sexual or political orientation. The use of biometric categorization systems is not generally prohibited.

The Artificial Intelligence Act prohibits the use of biometric categorization systems only if their purpose is to infer or deduce an individual's political opinions, trade union membership, religious or philosophical beliefs, racial origin, sexual life, or sexual orientation. However, AI systems that are used for biometric categorization based on sensitive characteristics or protected attributes under the GDPR are considered high-risk AI systems and as such fall under a strict regulatory regime (Art 5. [1] g. and recital 30 and 54 of AI Act Art. 5. [1] g).

Law enforcement activities for crime prevention purposes are not prohibited from labelling lawfully acquired biometric datasets according to biometric data, such as sorting images by hair colour or eye colour.

Use of *real-time* and *non-real-time* remote biometric identification systems [Art 5. (1) h), (2)-(5) and recital 17., 32., 33. and 95 of AI Act].

The use of remote biometric identification AI systems for law enforcement purposes represents a significant interference with the fundamental rights of individuals. Therefore, the AI Act has categorized these systems according to their mode and area of application and assigned different regulatory frameworks to them.

A *remote biometric identification system* refers to AI systems used for the identification of natural persons, where a person is identified without their active participation, typically remotely, by comparing their biometric data with biometric data in a reference database.

These systems typically identify individuals based on video or image recordings; and we can distinguish between real-time and non-real-time biometric identification systems.

A real-time remote biometric identification system is characterised by its use of *live* or *near-live* material, and the recording of biometric data, their comparison, and the identification of the person occur virtually simultaneously with the observation. The law enforcement use of such systems in publicly accessible places is – with the exceptions detailed below – prohibited.

We talk about a *non-real-time* system when identification takes place later, based on an already recorded footage. Given that the use of these systems also represents a significant interference with people's fundamental rights, such AI systems must be treated as high-risk AI systems. Consequently, the use of real-time AI systems for law enforcement purposes in publicly accessible places is

generally prohibited. With regard to the area of application the term *publicly accessible place* refers to physical areas, whether public or private property, that are accessible to an indefinite number of natural persons.

Such AI systems are particularly intrusive to the rights and freedoms of the data subjects, as they can affect the privacy of a large part of the population, create a sense of constant surveillance, and indirectly deter the exercise of freedom of assembly and other fundamental rights. Moreover, the technical inaccuracy of AI systems for remote biometric identification of natural persons can lead to distorted results and produce discriminatory effects. In addition, the immediate nature of the impact and the limited possibilities for further controls or corrections associated with the use of such real-time systems further increase the risk to the rights and freedoms of the data subjects in connection with or due to the effects of law enforcement activities.

However, this prohibition is not unlimited. These AI systems can be used to search for victims of crimes or missing persons, in cases of threats to people's lives, physical safety or under the threat of a terrorist attack, and to determine the whereabouts or identify perpetrators or suspects of certain serious crimes punishable by at least four years imprisonment.

In these cases, the identification operation can only be initiated and applied to confirm the identity of a specific target person. The application must be authorised by a judicial authority, where possible in advance, also defining the (temporal, geographical) scope of the application beyond the target person. The possibility and precise rules for this are contained in national law.

High-risk AI systems for non-real-time remote biometric identification may only be used for law enforcement purposes in a targeted manner. Their application must therefore be linked to a crime, criminal proceedings, a real and actual or foreseeable danger of a crime being committed, or the search for a

specific missing person. Non-real-time remote biometric identification AI systems can also be used for the targeted search of persons suspected or convicted of committing a crime.

As a general rule, the use of these systems also require authorization, unless they are used for the initial identification of a potential suspect based on objective and verifiable facts directly related to the crime.

A further important requirement for the system is that its use must be based on a closed dataset of lawfully recorded video footage, and in all cases, it must be ensured that law enforcement authorities cannot make a decision solely based on the result provided by the non-real-time remote biometric identification system that has an unfavourable legal effect on an individual.

Regarding real-time and non-real-time systems, an important caveat is that the conditions for non-real-time remote biometric identification can in no case serve as a basis for circumventing the prohibition and strict exceptions regarding real-time remote biometric identification.

➢ HIGH-RISK AI SYSTEMS

The AI Act classifies other artificial intelligence applications used in law enforcement as high-risk, which also entails compliance with very strict requirements, acknowledging through these rules the significant dangers that the use of artificial intelligence in law enforcement can pose to fundamental rights.

Therefore, according to Point 6 of Annex III of the Artificial Intelligence Act, the following AI systems used by law enforcement authorities must be considered high-risk AI systems – if national law allows their application:

- AI systems that determine whether a natural person is at risk of becoming a victim of a criminal offense.
- AI systems used as polygraphs or for similar purposes.

- AI systems used for evaluating the reliability of evidence in criminal investigations or prosecutions.
- AI systems used for assessing, including but not limited to profiling under the Law Enforcement Directive, whether a natural person is at risk of committing or re-committing a criminal offense, or AI systems used for assessing the personality traits and personal characteristics of natural persons or groups, or their past criminal behaviour.
- AI systems used for profiling natural persons during the detection of crimes, criminal investigations, or prosecutions.

High-risk AI systems are subject to strict regulation (Chapter III, Section 2 of AI Act, Requirements for high-risk AI systems), which Member State investigative authorities must take into account when applying these systems.

Within this framework, for example, a risk management system must be operated in relation to the given AI system (Art. 9. of the AI Act). A further requirement is that data used during model creation can only be used under strict conditions (Art. 10 of the AI Act), and technical documentation must be kept up-to-date (Art. 11 of the AI Act).

High-risk systems must be designed with sufficient transparency, allowing users to understand the system's operation, including its capabilities, limitations, and the human oversight measures required for its operation (Art. 13 of the AI Act). Another essential requirement is that high-risk AI systems must be designed with appropriate human oversight tools (Art. 14 of the AI Act), allowing natural persons effective control and the possibility of intervention to prevent or minimise risks to fundamental rights. Users must also be able to adequately understand the limitations of high-risk systems and be aware of automation biases.

It is important to note, however, that AI systems intended for use in administrative procedures by tax and customs authorities, and by financial intelligence units performing information analysis under EU anti-money laundering legislation, are not to be classified as high-risk AI systems used by law enforcement authorities for the prevention, detection, investigation, and prosecution of criminal offenses. Therefore, compliance with these requirements is not mandatory for them (Recital 59 of AI Act).

- MEDIUM-RISK AI SYSTEMS

This category includes, among other things, AI systems intended for direct interaction with natural persons, as well as AI systems that create synthetic audio, image, video, or text content.

The essence of the regulation concerning AI systems in this category is to ensure transparency. For example, when using chatbots, users must know that they are interacting with a machine so they can make an informed decision about continuing the conversation.

Providers must also ensure that AI-generated content is identifiable, meaning it must always be clear that it was generated by AI.

For instance, text generated by artificial intelligence and published for informing the public in matters of public interest must be marked as artificially generated. This also applies to audio and video content that creates deepfakes.

- LOW-RISK AI SYSTEMS

The AI Act allows for the free use of minimal-risk artificial intelligence. This includes applications such as AI-powered video games or spam filters. The vast majority of artificial intelligence systems currently used in the EU fall into this category.

References

BAROCAS, S. & SELBST, A. (2016). Big Data's Disparate Impact. Vol. 104 California Law Review. p. 671. (https://canvas.stanford.edu/courses/60360/files/.../download?...frd=1)

BRAKEL, R. (2016) Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing. In Sloot-Broeders-Schrijvers: *Exploring the Boundaries of Big Data*. Amsterdam University Press, Amsterdam, pp. 117-144.

CLARK, R. (1993) Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *Journal of Law, Information and Science* 4(2) (https://digitalcollections.anu.edu.au/bitstream/1885/46248/31/07Paper06.pdf)

Consultative Committee of Convention 108 (T-PD (2005). Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, Council of Europe. (http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1)

EDENS, J.R. (2008). Misuses of the Hare Psychopathy Checklist-Revised in Court. *Journal of Interpersonal Violence*, 16(10), pp. 1082-1094.

EUROPOL REPORT (2024) AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Observatory Report from the Europol Innovation Lab. p. 15. DOI: 10.2813/0321023 | QL-01-24-000-EN-N

FERRARIS, V., BOSCO, F., CAFIERO, G., D'ANGELO, E. & SULOYEVA, Y. (2013). Defining Profiling. SSRN (https://ssrn.com/abstract=2366564 or http://dx.doi.org/10.2139/ssrn.2366564)

FRA: EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018). *Preventing unlawful profiling today and in the future: a guide*. (https://fra.europa.eu/en/publication/2018/prevent-unlawful-profiling)

FRA: EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2014). Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data (https://fra.europa.eu/en/news/2014/fra-provides-guidance-member-states-setting-national-pnr-systems)

FRA: EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2010). A hatékonyabb rendfenntartás felé. A megkülönböztető etnikai profilalkotás megértése és megelőzése [Towards more effective law enforcement. Understanding and preventing discriminatory ethnic profiling] (https://fra.europa.eu/sites/default/files/fra.../1133-Guide-ethnic-profiling_HU.pdf)

FUSTER G. G. (2020). Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights, Study for LIBE committee (http://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf)

GANEVA, T. (2012). 5 Things You Should Know About the FBI's Massive New Biometric Database (https://www.alternet.org/2014/04/what-you-should-know-about-fbis-giant-biometric-database/)

GAVISON, R. (1980). Privacy and the Limits of Law. *Yale Law Journal* 89, pp. 421-471. (http://digitalcommons.law.yale.edu/ylj/vol89/iss3/1/)

HAYES, B. (2010). *Statewatch analysis: Spying in a see through world: the 'Open Source' intelligence industry* (http://database.statewatch.org/article.asp?aid=30317)

HILDEBRANDT, M. (2008). Defining Profiling: A New Type of Knowledge? In: M. Hildebrandt and S. Gutwirth (eds.). *Profiling the European Citizen Cross-Disciplinary Perspectives*. Springer Science + Business Media B.V. (https://www.researchgate.net/publication/226744267)

IKSZR (n.d.). Az Integrált Közlekedésszervezési és Szabályozási Rendszer közbiztonsági, közlekedésbiztonsági, rendvédelmi célú informatikai fejlesztése [The IT development of the Integrated Transport Planning and Regulatory System for public safety, traffic safety, and law enforcement purposes]. Police.hu (http://www.police.hu/sites/default/files/IKSZR%20m%C5%B1szaki%20specifik%C3%A1ci%C3%B3.pdf)

INFOJEGYZET (2018). Információs önrendelkezési jog 2. [Right to informational self-determination 2.]. www.parlament.hu.

LAMMERANT, H. & DE HERT, P. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. In B. van der Sloot, D. Broeders & E. Schrijvers (eds.). *Exploring the boundaries of big data*. (32), pp. 145-173. Amsterdam University Press/WRR

PERRY, W., McInnis, B., Price, C. C., Smith, S. C & Hollywood, J. C. (2013) Predictive Policing: The Role of Crime Forecasting. (https://www.rand.org/content/dam/rand/pubs/research_reports/../RAND_RR233.pdf)

PRIVACYINTERNATIONAL.ORG (2015). *GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal* (https://privacyinternational.org/press-release/1544/gchq-nsa-intelligence-sharing-unlawful-says-uk-surveillance-tribunal)

ROESSLER, B. & MOKROSINSKA, D. (2013). Privacy and Social Interaction, Philosophy Social Criticism (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.875.4434&rep=rep1&type=pdf)

ROßNAGEL, A. & RICHTER, P. (2016). Big data and informational self-determination. Regulative approaches in Germany: the case of police and intelligence agencies. In Sloot-Broeders-Schrijvers: *Exploring the Boundaries of Big Data*. Amsterdam University Press, Amsterdam. 261-282.

SÁRI, J. & SOMODY, B. (2008). Alapjogok. Alkotmánytan II. [Fundamental Rights. Constitutional Law II.] (www.tankonyvtar.hu)

SIMITIS, S. (1987) Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review*, 135, pp. 707-746. (https://scholarship.law.upenn.edu/penn_law_review/vol135/iss3/)

SZÉKELY, I. (2014). Surveillance – a megfigyeléstől a megfigyelő társadalmakig és a megfigyeléstudományig [Surveillance – from observation to surveillance societies and the science of surveillance]. *Replika*, 89(4-5), 7-13. (https://replika.hu/system/files/archivum/89_01_szekely.pdf)

URL1: https://rm.coe.int/1680a2353d

URL2: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

URL3:https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

URL4: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing

URL5:https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:12016P/TXT

URL6:https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679

URL7:https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex:32016L0680

URL8: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

URL9:https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2065

URL10:http://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

About the Authors

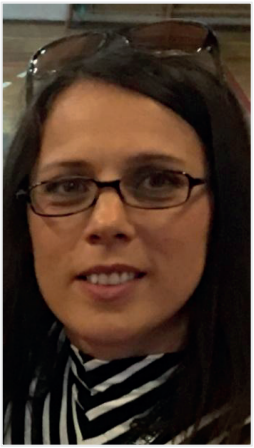
Zoltán György Bács, a D.Univ. in History and Ph.D. in Military Sciences, Dr. Bács is assistant professor of the Ludovika University of Public Service and the Head of the Secretariat of the Vice Rector for International Affairs. The author of almost seventy publications in four languages, he specialises in terrorism, national security, dynamic networks as innovative assessment and evaluation systems, radicalization, as well as drug problems and organised crime in Latin America.

He has previously served as a diplomat in Moscow, Kiev, Baku, Minsk and Buenos Aires. Between foreign assignments, he worked for international and national private companies in Hungary. Dr. Bács is fluent in Spanish, English and Russian.

Anita Bückő has been working in various fields of security for over a decade. She studies artificial intelligence and predictive analytics solutions, with a particular focus on their integration into physical security systems. The centre of her attention lies in the examination of the security structures of law enforcement, municipal policing, and multinational corporations. She believes that the true significance and value of numerical data lies in revealing strategic advantages, predictive insights, and preventive opportunities. Her goal is to develop prediction-based security systems that contribute to strengthening organisational security and enhancing the effectiveness of crime prevention.

Orsolya Czenczer Ph.D. is a legal professional and academic specialising in national and international prison law and penology. She is an associate professor and correctional lieutenant colonel at Ludovica University of Public Service, teaching and researching since 2008. Her work focuses on prison systems, criminal justice reforms, and European legal policy. She represents Hungary at the Council of Europe's Penological Co-operation Council. She holds law degrees from Hungary and Romania, a Ph.D. in Criminal Law, and a psychology degree. Early in her career, she practiced criminal law and was a Ph.D. research fellow. Fluent in English, Italian, and Romanian, she applies strong intercultural skills in international and academic settings.

Csaba Zágon Ph.D., is dedicated to enhancing the academic performance and international visibility of the Law Enforcement Faculty at Ludovika University. He contributes to European Commission programmes focused on the advancement of higher education in law enforcement. His involvement includes participation in CEPOL's Research and the Science Correspondents' Network. With over thirty years of experience as a former customs officer, he has engaged in capacity building across EU Member States and Accession States. For more than a decade, Dr. Zágon has taught cadets, mid-level law enforcement practitioners, and civilian candidates in various Bachelor's, Master's, and Doctoral programmes. His research interests include risk management in law enforcement environments, crime analysis, international cooperation in criminal matters, and infrastructure networks.



Zsanett Fantoly Ph.D. is a law professor at the Ludovika University of Public Service, specialising in criminal justice systems and the efficiency of the criminal procedurals. She teaches courses on the Hungarian and the European Union's criminal law of proceedings in addition to AI decision-making in criminal cases. She is the author of numerous scientific studies and books, and a regular speaker at domestic and international conferences.

A member of several scientific societies (e.g. International Association of Penal Law) she is also committed to modern legal education and scientific research in her public life.

István Giczi is a security technology engineer, senior security coordination expert, and AI engineer with extensive experience in integrated security systems and risk management solutions. His professional focus is on the practical application of artificial intelligence, particularly predictive analytics, machine learning, and image analysis.

He applies an engineering mind-set and data-driven approach to enhance security system development, leveraging innovative technological opportunities. His core belief is that the true value of technological advancements lies in their ability to effectively address real-world problems.

Kristina A. Krasnova Ph.D. Cand. Sci. (Law), Associate Professor

Associate Professor of Criminal Law Department, North-West branch of the Federal State Budgetary Educational Institution of Higher Education "Russian State University of Justice named after V.M. Lebedev" (St. Petersburg)

Chair of the St. Petersburg Branch of the Russian Criminological Association named after A.I. Dolgova. Vice-President of the International Criminological Geographical Association (ICGA). Independent Expert, authorized by the Ministry of Justice of Russia to conduct anti-corruption expertise of normative legal acts and draft normative legal acts in cases stipulated by the legislation of the Russian Federation. Member of the Editorial Board of the journal Member of the Editorial Boards of the journals "Bulletin of the Academy of Law and Management" (Russia), "Criminal Geographical Journal" (Hungary), "European Law Announcements" (Hungary).

Róbert Major Ph.D. A police colonel, associate professor, and head of the department of Public Safety of the Ludovika University of Public Service, as well as a traffic engineer, lawyer, traffic engineering specialist, road safety auditor. He has been dealing with the opportunities for preventing traffic accidents for decades, with a particular focus on police activity. His research areas include the examination of the adequacy of traffic engineering designs, the methodology, techniques and tactics of road traffic control, as well as the safety of pedestrians and other vulnerable road users. He has published numerous publications on these topics and regularly gives scientific lectures. He is a member of and senior official for several scientific societies.

Szabolcs Mátyás Ph.D. is a police lieutenant colonel and an associate professor at the Ludovika University of Public Service. He obtained a degree in geography and regional development at the University of Debrecen in 1999, a Ph.D. in 2011, completing his habilitation in 2023. Alongside his role as associate professor he also teaches at the University of Debrecen. He lectures on the Predictive Policing course in both English and Hungarian, and is the author of numerous studies on the subject. He led the research team that developed the predictive traffic policing software Sopianae. A member of the editorial board of several Hungarian and international scientific journals, he is also the founder and editor-in-chief of the *Criminal Geographical Journal* and *Bűnözésföldrajzi Közlemények*, the world's only English and Hungarian language crime geography journal. He was the founder and Vice President (formerly President) of the International Criminal Geographical Association.

Endre Nyitrai Ph.D. A researcher, associate professor, and acting head of department, Dr. Nyitrai earned his degree in criminal investigation from the College of Police Officers in 2004. He went on to graduate from the Faculty of Law at the University of Pécs. From 2004 to 2012, he served with the Organised Crime Division of the Budapest Metropolitan Police Headquarters, followed by a post at the Pest County Police Headquarters. Since 2013 he has been a member of the teaching staff at the Ludovika University of Public Service. He obtained his Ph.D. in 2018. He has presented extensively both domestic and international conferences. His current research interests include smart cities and smart policing, artificial intelligence, and criminalistics/forensic science.

Máté Sivadó Ph.D., A police major, associate professor, doctorate in law, police officer, university lecturer, and researcher, he has more than 20 years of practical experience in law enforcement work and training. He is an associate professor at the Department of Criminology of the Faculty of Law of the University of Public Service. In 2015, he defended his doctoral dissertation entitled 'Drug Policies in Hungary and Europe, with an overseas perspective.' Alongside a published monograph, he has over a hundred independently and jointly written publications to his credit. His main research areas continue to be drug policy, law enforcement crime prevention, and the impact of religious conversion on prisoners. He has participated in numerous professional trips abroad and regularly visits foreign universities to teach within the framework of the Erasmus program. He speaks English at an intermediate level.

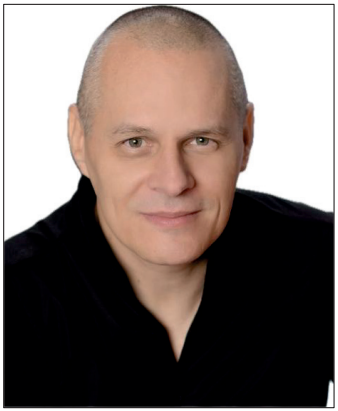
Imre Szabó Ph.D., is a prosecutor at the Metropolitan Chief Prosecutor's Office. He is a member of the National Association of Prosecutors, who, in addition to his prosecutorial work, is also engaged in scientific research and teaching activities. He teaches the 'Predictive Policing' course at the Doctoral School of Law Enforcement of the Ludovika University of Public Service, His main research area is predictive policing. In addition, he researches criminal law, with a particular focus on cybercrime. He regularly participates in Hungarian and international conferences and has published studies in Hungarian, English, and German.

Nikiforosz Packosz is a Ph.D. student at the University of Public Service in Hungary. He holds degrees in law and law enforcement. Over the course of a 12-year investigative career, he spent 8 years at the National Bureau of Investigation, specialising in organised crime and crimes related to online payments. During this time, he served for several years as a delegated national expert in the EUROPOL EMPACT working group on non-cash means of payment fraud. After leaving the field of law enforcement, he worked as a legal advisor in the private sector. He is currently employed at the Office of the President of Hungary. His continued Ph.D. studies reflect his strong commitment to the field of law enforcement.

Miklós Tihanyi Ph.D. A police lieutenant colonel and associate professor at the Ludovika University of Public Service, lecturing at both the Faculty of Law Enforcement of the Ludovika University of Public Service and at the Károli Gáspár University of the Reformed Church. His areas of expertise are law enforcement and church law. His research focuses on public safety, organisational efficiency, and the relationship between religion and law enforcement. He is a member of the editorial boards of several Hungarian and international journals and serves as the president of the International Criminal Geographical Association. He has taught as an Erasmus instructor in many countries around the world. He has published his research findings in Hungarian, English, Serbian, and Russian.

Levente Tóth Ph.D. is an assistant professor at the Department of Private Security and Municipal Policing at the Faculty of Law Enforcement, Ludovika University of Public Service. He has been teaching at universities for 27 years. Alongside his academic career, he has gained 35 years of experience working in the private security sector and is currently the Operational Director of one of the largest security companies, which specialises in the installation of intrusion detection, video surveillance, access control, and fire alarm systems. His main research interests include video surveillance systems and artificial intelligence-based image processing (video content analysis).

Zita Traub is a second-year BA student at the Ludovika University of Public Service, where she is studying International Public Management. She has shown a keen interest in computer science since her high school years and was part of the university research team that developed the Sopianae software system that operates based on predictive algorithms. In 2024, she designed the structure of the traffic safety software operating in Pécs. She has published several studies on this program in both English and Hungarian. She has also participated in numerous Hungarian and international conferences.



Endre Vajda is a former police officer and certified criminologist. He is currently the CEO and owner of a security company. In addition to his police degree, he has participated in several multi-week online training courses held by renowned universities and training institutions around the world on the topic of terrorism and security policy. His research interests include crime geography and Islamic terrorism. He has published numerous articles in English and Hungarian on the above topics. He is a high-level martial arts practitioner, a 3rd Dan Kempo and 2nd Dan Ju Jitsu master.

Vince Vári Ph.D., a lieutenant colonel and associate professor at Ludovika University of Public Service, and a leading figure in the study of police organisational effectiveness in Hungary. He has pulished more than 170 scientific works, with around 300 independent citations recorded in the MTMT (Hungarian Scientific Works Database, ID: 10033318). His research has appeared in several peer-reviewed, Q-ranked academic journals, and he is also the author of multiple monographs, including works published in foreign languages. Dr. Vári is actively engaged in professional and public life, serving as editor-in-chief or board member on prominent Hungarian and international journals, and as a member of major scientific societies. His research contributions and academic leadership have been acknowledged through several professional awards. Currently, he is preparing his habilitation, further strengthening his academic achievements and influence in police science.

Contents

The research presented in this paper focuses on various aspects of the application of artificial intelligence in predictive policing.

Since profiling is already used to identify perpetrators of crimes, the examples included in the paper, although mostly drawn from the Hungarian experience, demonstrate its usefulness in prevention, as well as the technical, forensic, legal, and ethical implications.

The considerations presented in various areas inspire the use of AI that conciliates crime prevention, fundamental rights and the rule of law.

Using AI to obtain a more precise profile in time and space, while maintaining the final interpretation by a human being, enables a better identification of risks and potential perpetrators, and consequently, protects both the security and freedom of citizens.

Yves Vandermeer
founder of the European Cybercrime
Training and Education Group