Articles Studia Iuridica Lublinensia vol. XXIX, 5, 2020
DOI: 10.17951/sil.2020.29.5.301-309

Adam Taracha
Maria Curie-Skłodowska University in Lublin, Poland
ORCID: 0000-0001-8630-2496
adam.taracha@umcs.pl

The Use of Algorithms in Criminal Procedure (Selected Issues)

Wykorzystanie algorytmów w postępowaniu karnym (wybrane zagadnienia)

SUMMARY

The article analyzes attempts to apply mathematical methods in criminal cases since the times of J. Bentham and indicates the use of algorithms in the activities of law enforcement agencies in the detection process when it comes to the identification of people (based on the image of the face) and vehicles (based on the identification of license plates). The use of algorithms in the practice of criminal justice in the US was also discussed. In the opinion of the author, their use in a criminal trial (in the assessment of evidence and shaping the judgement) will still be only partial and sporadic for some time to come. There is no doubt, however, that their use will cause a lot of controversy. The main reason is the contradiction between the constantly increasing possibilities of collecting and using data about a person (thanks to, among others, algorithms) by law enforcement and judicial authorities and the protection of human rights and freedoms.

Keywords: algorithms; personal data; image of the face; identification; assessment of evidence

INTRODUCTION

In the modern world, we increasingly use devices that help us with everyday activities, and which operate based on an algorithm[1]. The use of algorithms is now also applied in the work of law enforcement agencies and justice administration in criminal matters. Attempts to use mathematical methods to improve the quality of judicial decisions in criminal matters have been taken for many years.

Aptly assessing the small possibilities of colloquial language in which a witness could express the degree of his conviction as to the existence of facts ("I know", "I believe", "I have reasons to believe that the matter looks like this or almost like this"), about which the witness testifies, J. Bentham wondered to what extent the language of mathematics could be helpful in this case[2]. In his opinion, two methods can be considered here. The first, a perfectly strict, based on the probability theory, which does not apply to the witness's testimony. The second is that, having given the largest amount for the final amount, it is divided into equal parts. Bentham proposed a scale to be introduced (from 0 to 10) at which witnesses would assess their degree of conviction. This scale (compared to a ladder by Bentham) would have a positive side, on which the degrees of positive conviction (i.e. confirming the existence of fact) would be noted, and the negative side, on which the degrees of negative conviction (i.e. negating the existence of this fact) would be noted. The "0" would mean a lack of conviction for both "for" and "against". Further on, Bentham proposes to apply this method to expert witnesses and to adjudicating judges as well. As regards the sentencing process, Bentham points out the advantages of the system where multiple judges are involved in the trial at first instance and the distribution of their votes is equal, then the judges in the appellate trial would have information on the strength of the conviction of the judges adjudicating at first instance. He also points to the usefulness of this method in pardon procedure – the authority deciding on the pardon would be informed on the degree of the judges' conviction as to the appropriateness of applying the right of pardon. As points out, even if the judicial decisions were based on the degrees of conviction and not on the basis of the number of votes, it could nevertheless be applied in pardon proceedings (cases of clemency)[3].

[1] The possibility of solving problems with computational technologies (especially using computers) may currently cover many areas of human activity such as air transport (autopilot), road transport (autonomous cars, license plate recognition), medicine (mainly in the area of diagnostics), banking (access through fingerprint or face recognition), etc. The term "algorithm" is now often used in the sense as defined in *The Oxford English Dictionary*: "A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer".

[2] J. Bentham, *Traktat o dowodach sądowych w opracowaniu E. Dumonta*, Gniezno [no year of release], p. 61 (English version: idem, *A Treatise on Judicial Evidence*, London 1825).

[3] *Ibidem*, pp. 61–65.

J. Bentham's proposals were not accepted (even in pardon proceedings), which is hardly surprising, as the system was too imperfect. The mere assumption of witnesses assessing their own testimonies and judges assessing their own rulings can be questioned. In such a case, it is difficult to expect that the assessments will be objective (e.g. that a witness who testified falsely assesses his testimony as "10"). On the other hand, the note that it is not possible to apply the theory of probability directly to the assessment of evidence both in criminal proceedings and the use of its rules in judging in criminal proceedings seems appropriate.

A similar conclusion in Polish forensics has been made by J. Konieczny. This author attributed an important role in judicial reasoning to the category of conviction, measured by subjective probability. However, he stated that it is not quite clear how to reasonably measure (express) the probability thus understood, and research is also required about pre-decision processes that transform probabilistic information. According to J. Konieczny, related problems lead to the need to modify the theoretical concept of judicial reasoning towards the use of some kind of non-probabilistic approach (presentation of such a solution would, however, go beyond the declared purpose of his paper)[4].

Confirmation of the view that it is not possible to use directly in the criminal proceedings the rules on the probability calculation can be found in the classic forensics manual by Ch.E. O'Hara and J.W. Osterburg. While the authors did not state this expressly, in chapter 46 on probability and proof, we actually find only basic information about the probability calculation. The use of mathematical methods is limited to the calculation of the degree of probability of the same traces in expert's opinions on trace evidence and forensic engineering[5]. On the other hand, in the next part of the work (chapter 47 – *Some Miscarriages of Justice Analyzed in the Light of Criminalistics*) O'Hara and Osterburg aptly assess the reasons for errors in evidence-taking which result in the conviction of innocent persons, by mentioning in the first place the erroneous diagnosis at the time of the identity parade, then insufficient circumstantial evidence, perjury, unreliable opinions of expert witnesses, excessive enthusiasm of investigating officers and prosecutors[6].

Nowadays, it can be pointed to the use of algorithms in obtaining, collecting and taking evidence in a criminal trial and (mainly in the US practice) in deciding on the use of the institution of a suspended sentence, the use of a financial guarantee, or the type of and the amount of the penalty.

[4] J. Konieczny, *Pojęcia prawdopodobieństwa ze stanowiska procesu karnego i kryminalistyki*, Katowice 1987, pp. 88–89.

[5] Ch.E. O'Hara, J.W. Osterburg, *An Introduction to Criminalistics: The Application of the Physical Sciences to the Detection of Crime*, New York 1949, pp. 666–679.

[6] *Ibidem*, p. 680.

THE USE OF ALGORITHMS IN EVIDENTIARY PROCEEDINGS AND ADJUDICATION IN CRIMINAL CASES

Modern technology allows not only for image and sound recording but also for its analysis. As regards the detection and prosecution of traffic offenders, the automatic number plate recognition system (ANPR) is essential[7]. The ANPR system is equipped with an algorithm for license plate recognition using appropriate software (optical character recognition, OCR). It allows for quick identification of the vehicle and archiving the information about the time and place of stay (movement) of the vehicle. The possibilities of this system are not only limited to the prosecution of traffic offenders[8], but also to traffic management and supervision, car park management, etc.

It is important to note the position of GIODO (Inspector General for Personal Data Protection)[9], who argues that the vehicle number should be considered as personal data within the meaning of the Polish Personal Data Protection Act. In GIODO's opinion, a specific piece of information constitutes personal data if the holder of this information is able to identify the person concerned without incurring excessive costs, time or effort. Anyone who has access to the Central Registry of Vehicles and Drivers can establish the identity of the person, e.g. the owner of the vehicle, without too much effort and expense. The view was shared by the Voivodeship Administrative Court of Warsaw in the judgement of 9 April 2013 (II SA/211/13), stating that "It can also not be assumed that the vehicle registration number cannot lead to the identification of a person and therefore does not constitute personal data within the meaning of Article 6 of the Personal Data Protection Act".

[7] Also other names for this system can be found in the Polish literature, e.g. ISKIP – *Inteligentny System Kompleksowej Identyfikacji Pojazdów* (Smart System for the Comprehensive Identification of Vehicles) developed in Instytut Badawczy Dróg i Mostów (IBDiM). The ISKIP project was carried out as part of the EU-funded programme "Innovative Economy" and was concluded in 2020. See Nauka w Polsce (https://naukawpolsce.pap.pl; Science in Poland), a news service of the Polish Press Agency on scientific matters. System VCOP (Virtual COP) is offered by P.H.U. Telsat.

[8] Polish traffic police officers (from the General Police Headquarters and five voivodeships) paid on 21–24 September 2010 a study trip to the UK under the LIFESAVER project. The officers learned about the use of the ANPR system by the Welsh police, which is considered by the Welsh an effective tool for finding and recording road traffic offences and prosecuting their perpetrators. The PolCam Mobile ANPR system was tested in 2011 by one unmarked police car from the Radom Voivodeship Headquarters of the Police. This system also enabled the use of sectional vehicle speed inspection and is used in the organization of road traffic and car park management. See *Lifesaver – polscy policjanci na drogach Walii (Wielka Brytania)*, 2010, www.policja.pl/pol/aktualnosci/59664,LIFESAVER-polscy-policjanci-na-drogach-Walii-Wielka-Brytania.html [access: 12.02.2020].

[9] On 25 May 2018, with the entry into force of the Act of 10 May 2018 on Personal Data Protection (Journal of Laws 2019, item 1781), the Inspector General for Personal Data Protection was replaced by a new body, the President of the Office for Personal Data Protection, while the Office of the Inspector General for Personal Data Protection became the Office for Personal Data Protection.

As it seems, much more doubts arise as to the possibility of using automatic human face recognition software in the practice of law enforcement agencies (not only in prosecuting traffic offenders)[10]. In contemporary face recognition systems, two terms are distinguished: verification and identification[11].

Undoubtedly, the image of a person should be deemed the information enabling the identification of a natural person and thus subject to personal data protection[12]. Whereas sets of images of persons who can be identified on their basis are subject to recording in accordance with the requirements of this Act. However, as opposed to the system of registration plate identification, the use of automatic face identification systems arouses much more opposition in view of the protection of the right to privacy. For example, in connection with the tests of the camera system for the identification of individuals (on the basis of facial recognition) at the Suedkrenz railway station in Berlin in 2017, the president of the German Bar Association, Ulrich Schellenberg stated that the human facial recognition system in public places deeply interferes with the rights of citizens, which in his opinion is not lawful. Maja Smoltczyk, the representative of the Berlin city council for data protection, also pointed out the enormous potential for abuse, and she is of the opinion that the system under tests violated the constitutionally guaranteed right to move anonymously in public places[13].

[10] The provisions of road traffic law expressly allow for processing (analysing with computer software) the image of the driver of the vehicle if it has been recorded (at the time of recording the image of the traffic misconduct). The term "processing" undoubtedly comprises the use of software enabling the automatic identification of a person on the basis of an image. Under the legislation as it stands, therefore, nothing prevents the use of systems to automatically identify the image of the offender.

[11] Verification is used in situations where there is a limited number of people and the personal database contains both personal information and information of the verification (access) system. The limited personal database allows for the storage of very extensive databases of persons subject to verification, which allows for a very quick comparison of them (e.g. the verification prevents unauthorized persons from using stolen identification cards). Identification, on the other hand, is a more complex issue (compared to verification). It includes "one-to-one" or "multiple" matching functions in the facial recognition process. It is more and more used in airport (or railway and station) surveillance systems and other public buildings. Personal databases used in the identification process, are far larger than in the case of verification.

[12] Until 25 May 2018, under the Act of 29 August 1997 on Data Protection (Journal of Laws 1997, no. 133, item 833), this was pointed to by Article 6 para. 1 and 2 of the Act. Under the legislation currently in force the current legal order, personal data are defined in Article 4 point 1 of the 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 (General Data Protection Regulation) (OJ EU L 119/1, 4.05.2016).

[13] A total of three hundred people volunteered to take part in the test, whose biometric facial photos and personal data were entered into the computer. In the event that the cameras installed at the entrance and exit of the station identify a person from the database, the system will respond by

As a prerequisite for the use of the image identification system, a police database of facial profiles (as comparative data) must be built. Police forces in England and Wales have set up a database containing more than 16 million facial profiles (almost 25% of the population). Alastair MacGregor, the former Biometrics Commissioner warned that police facial search engine could pose a far greater threat to people's privacy than DNA databases or fingerprint databases[14]. This is undoubtedly an apt remark, given that the CCTV system in the UK is one of the most extensive (especially for London, which has the highest number of CCTV cameras in the world). Critical remarks are also made in the English press about the accuracy of the facial recognition systems currently in use. The English police's assessment of effectiveness of the technology used at 95% means (according to critics) that out of 1,000 indications, as many as 50 will be wrong[15]. These concerns turned out to be right. During the tests of the automatic facial recognition system by the British Police at the Notting Hill Carnival on 26 August 2017 in London, the system made 35 misidentifications (indications) of individuals, resulting in one person being arrested. Only in one case did the system make the correct recognition[16].

Currently, facial recognition algorithms are certainly not perfect[17] and misidentifications are described in the literature. These are often funny rather than dangerous situations, such as when iPhone owner's close family members get access to their phone because the facial recognition algorithm misidentified them[18]. However, the situation is much more serious when wrong recognition occurs during the taking of evidence in criminal proceedings, which may lead to the conviction of an innocent person. This took place in the Steven Talley case of 2014, in which an expert witness (an FBI agent) in his expert opinion on identification of a person recorded on a picture (video) of the course of a criminal conduct (bank robbery) misidentified

warning of danger. See *Niemcy. Kamera zidentyfikuje podejrzanych*, 2017, www.niezalezna.pl/200036-niemcy-kamera-zidentyfikuje-podejrzanych [access: 14.03.2019].

[14] A. Michalak, *Wielka Brytania: Kontrowersje wokół systemu rozpoznawania twarzy*, „Rzeczpospolita", 17.08.2017.

[15] *Ibidem*.

[16] *Wielka Brytania: Omyłkowy areszt wynikiem systemu rozpoznawania twarzy*, www.rp.pl/Polityka/170819306-Wielka-Brytania-Kontrowersje-wokol-systemu-rozpoznawania-twarzy.html [access: 20.07.2019].

[17] For example, tests of a special system for identifying people who cross the streets unlawfully have recently been launched in Shanghai and several other Chinese cities. For the time being, the system needs improvement as out of the three hundred "recorded" people in the pilot operation of the system, only 4 have been identified and penalised. See *Czerwone światło rozpozna twarz. Będzie mandat na przejściu!*, 2017, www.fakt.pl/pieniadze/prawo/system-rozpoznawania-twarzy-dostarczy-mandat/bgqwejf [access: 22.07.2019].

[18] This applies not only to twins, siblings, but also children and parents (the literature describes a case where a ten-year-old son accessed his mother's iPhone). Undoubtedly, the iPhone's face recognition algorithm is far from perfect – I witnessed an incident when a 24-year-old son of my friends "unlocked" his eighteen-year-old brother's iPhone.

the person using facial recognition software. Talley spent two months in custody but regained his freedom when the charges were dismissed (exculpatory evidence emerged). However, a year later he was arrested again, the case was filed with the court, and the FBI agent operating the facial recognition software testified as a witness against S.Talley. He avoided being convicted owing to a testimony made by a cashier from the bank, who remembered that the perpetrator of the robbery had had distinctive warts on his hands, while the accused had no such warts, and categorically stated that it was not Talley who committed the robbery[19].

This case is very much like the story of Adolph Beck, also misidentified twice as the perpetrator of numerous matrimonial scams in London at the turn of the 20th century. Beck was wrongly identified not only by the victims, but also by police officers, which seems to have been a decisive factor in his conviction. This case, in which an innocent man was convicted, caused such a stir among public opinion that it resulted in the establishment of the first court of appeal in the United Kingdom[20]. However, unlike the case of A. Beck, the case of S. Talley went virtually unnoticed and did not give rise to any reaction in terms of increasing guarantees of the rights of the accused.

The second area where algorithms are used in criminal proceedings in the USA (as it seems, quite broadly in practice) is the process of making procedural decisions.

The use of algorithms for pre-trial detention in the USA looks particularly promising. The results of research showing that the predictions of the algorithm will be much more accurate than those of judges have been confirmed in practice. In Rhode Island, a seventeen-percent decrease in the number of detainees and a six-percent decrease in cases of recidivism has been achieved in the eight years of application of the algorithms[21]. Undoubtedly, this is a very satisfactory result which significantly reduces the economic (fewer detainees) and social (a higher number of those not detained) costs[22].

The (auxiliary) use of the COMPAS software[23] for determination of the custodial sentence is more questionable. Eric L. Loomis, sentenced to six years in prison, alleged that the district court, through using COMPAS in his case, violated his right to a fair trial. In its judgement of 13 July 2016, the Wisconsin Supreme

[19] H. Fry, *Hello world. Jak być człowiekiem w epoce maszyn*, Kraków 2019, pp. 208–210.

[20] J. Thorwald, *Stulecie detektywów*, Kraków 2009, pp. 107–119.

[21] H. Fry, *op. cit.*, p. 84.

[22] Nonetheless, it should be borne in mind that this smallest US state has relatively small population (1 million 57 thousand in 2018).

[23] COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) is an algorithm designed to forecast the risk of defendant's recidivism within two subsequent years. It is used by, among others, courts in New York, Wisconsin, California, Florida. It operates using the information provided by the defendant as an answer to questionnaire questions. This algorithm achieved an accuracy rate of 70%.

Court dismissed the Loomis' action, pointing out that by this ruling was based on a number of grounds (in this case, the defendant's criminal record became as important as COMPAS)[24]. Loomis appealed against the ruling to the Supreme Court, but the Supreme Court refused to hear the case.

CONCLUSION

Despite the fast development of mathematical sciences, applied in a growing number of areas of human activity, their use in criminal proceedings (evaluation of evidence and preparing the judgement) will be for some time (longer rather than shorter) of only a partial and sporadic nature. However, there is no doubt that their application will arouse much controversy. The main reason is the contradiction between the ever-increasing possibilities for collecting and the use (including through algorithms) of personal data by law enforcement agencies and the judiciary, and the protection of human rights and freedoms.

REFERENCES

Literature

Bentham J., *Traktat o dowodach sądowych w opracowaniu E. Dumonta*, Gniezno [no year of release].

Czerwone światło rozpozna twarz. Będzie mandat na przejściu!, 2017, www.fakt.pl/pieniadze/prawo/system-rozpoznawania-twarzy-dostarczy-mandat/bgqwejf [access: 22.07.2019].

Fry H., *Hello world. Jak być człowiekiem w epoce maszyn*, Kraków 2019.

Konieczny J., *Pojęcia prawdopodobieństwa ze stanowiska procesu karnego i kryminalistyki*, Katowice 1987.

Lifesaver – polscy policjanci na drogach Walii (Wielka Brytania), 2010, www.policja.pl/pol/aktualnosci/59664,LIFESAVER-polscy-policjanci-na-drogach-Walii-Wielka-Brytania.html [access: 12.02.2020].

Michalak A., *Wielka Brytania: Kontrowersje wokół systemu rozpoznawania twarzy*, „Rzeczpospolita", 17.08.2017.

Niemcy. Kamera zidentyfikuje podejrzanych, 2017, www.niezalezna.pl/200036-niemcy-kamera-zidentyfikuje-podejrzanych [access: 14.03.2019].

O'Hara Ch.E., Osterburg J.W., *An Introduction to Criminalistics: The Application of the Physical Sciences to the Detection of Crime*, New York 1949.

Thorwald J., *Stulecie detektywów*, Kraków 2009.

[24] *Loomis v. Wisconsin*, 881 N.W. 2d 749 (Wis. 2016).

Legal acts

Act of 29 August 1997 on Data Protection (Journal of Laws 1997, no. 133, item 833).
Act of 10 May 2018 on Personal Data Protection (Journal of Laws 2019, item 1781).
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 (General Data Protection Regulation) (OJ EU L 119/1, 4.05.2016).

Case law

Judgement of the Voivodeship Administrative Court in Warsaw of 9 April 2013, SA/211/13.
Loomis v. Wisconsin, 881 N.W. 2d 749 (Wis. 2016).

STRESZCZENIE

W artykule dokonano analizy prób zastosowania metod matematycznych w sprawach karnych od czasów J. Benthama oraz wskazano na wykorzystanie algorytmów w działalności organów ścigania w procesie wykrywczym, gdy chodzi o identyfikację osób (na podstawie wizerunku twarzy) oraz pojazdów (na podstawie identyfikacji tablic rejestracyjnych). Omówiono także zastosowanie algorytmów w praktyce wymiaru sprawiedliwości w sprawach karnych w USA. Zdaniem autora wykorzystanie ich w procesie karnym (w ocenie dowodów i kształtowaniu orzeczenia) będzie miało jeszcze przez pewien czas jedynie cząstkowy i sporadyczny charakter. Nie ulega jednak wątpliwości, że ich zastosowanie będzie wywoływać liczne kontrowersje. Główną przyczyną jest sprzeczność między stale wzrastającymi możliwościami gromadzenia i wykorzystywania danych o osobie (m.in. dzięki algorytmom) przez organy ścigania i wymiaru sprawiedliwości a ochroną praw i wolności człowieka.

Słowa kluczowe: algorytmy; dane osobowe; wizerunek twarzy; identyfikacja; ocena dowodów