https://doi.org/10.34836/pk.2025.324.2

AFIS: Perspectives from 25 Years of Experience

Major Beata Krzemińska
Central Police Forensic Laboratory
ORCID: 0009-0006-4961-6852
e-mail: beata.krzeminska@policja.gov.pl

Lieutenant-Colonel Dr Edyta Kot
Central Police Forensic Laboratory
ORCID: 0009-0006-2272-7085
e-mail: edyta.kot@policja.gov.pl

Abstract

This article examines the 25-year evolution of the Automated Fingerprint Identification System (AFIS), tracing its transition from a foundational support tool for fingerprint examiners to an advanced platform with applications extending beyond forensic science. Furthermore, it outlines the future trajectory of biometric technologies. Dactyloscopic biometric algorithms have evolved into multi-biometric technologies, yielding increasingly rapid and precise matching capabilities. This advancement has been facilitated by the integration of AI (artificial intelligence) solutions capable of real-time recognition of not only fingerprints and palm prints, but also facial features, irises, voices, and tattoos, along with the complex correlations among these modalities. This domain is undergoing continuous infrastructural development, particularly in its capacity to interact with external systems for data exchange – a paradigm defined as interoperability. However, despite the growing degree of automation, a fundamental and invariable principle remains: all final decisions regarding data processing within biometric systems ultimately rest with a human expert.

Keywords: AFIS, dactyloscopy, biometric data, Eurodac, Prüm, artificial intelligence, AI

Introduction

The original purpose of the Automated Fingerprint Identification System (AFIS) was to assist fingerprint experts in identifying criminal offenders, as well as establishing the identity of individuals and unidentified human remains. At the time of its inception, it was not anticipated that the system would serve as a catalyst for the large-scale development of biometric technologies. The accumulated experience gradually became a driver of change - extending beyond forensic identification to encompass access authentication for mobile devices, computers, facilities, banking systems, payment authorization and document security. In turn, dactyloscopic biometric algorithms laid the groundwork for the development of other biometric modalities, including facial, iris, and voice recognition, as well as the identification of tattoos. As databases expanded, so did the demand for faster, more accurate, and cross-domain data matching capabilities. This demand initiated the pursuit of multi-biometric solutions, which are now successfully deployed for identity management and real-time subject identification.

Over the past 25 years in Poland, the AFIS has not only advanced technologically but has also significantly broadened its operational scope. This progression includes the nationwide expansion of its infrastructure and the enhancement of its functionalities, specifically targeting interoperability with external systems.

Legal Basis for the Operation of the AFIS

Pursuant to Article 21h of the Police Act (Journal of Laws of 2025, items 636 and 718), the Commander-in-Chief of the Police maintains a collection for the automated processing of dactyloscopic data. This repository stores and processes information regarding fingerprint images of individuals, unidentified detected and recovered latents at crime scenes, and latents that may originate from missing persons. For the purpose of this article, “dactyloscopic data” shall be understood as “images of friction ridges of fingers or palms” originating from an individual (tenprint, palmprint) or from an incident scene (latents).

The system’s database is divided into three primary collections of dactyloscopic data, namely:

1. The Criminal Records Database, which processes the data of:

- suspects or individuals suspected of committing offenses prosecuted by public indictment,
- juveniles committing acts prohibited by law as offenses prosecuted by public indictment,
- individuals posing a threat to the life, health, or sexual freedom of others (individuals with mental disorders),
- individuals suspected of having links to terrorism-related incidents,
- individuals accused or convicted of committing offenses prosecuted by public indictment,
- wanted persons.

2. The Administrative Records Database, which processes the data of:

- foreign nationals whose fingerprints have been taken in the circumstances referred to in Article 35(2), Article 324(1), and Article 394(3) of the Act of 12 December 2013 on Foreigners, or Article 30(1)(3), Article 92(1), and Article 114(1) of the Act of 13 June 2003 on Granting Protection to Foreigners within the Territory of the Republic of Poland - Dziennik Ustaw (Polish Journal of Laws of 2025, items 1079 and 1794; of 2026, item 203), or Article 73a of the Act of 14 July 2006 on the Entry into, Residence in and Departure from the Territory of the Republic of Poland of Nationals of the European Union Member States and their Family Members - Dziennik Ustaw (Polish Journal of Laws of 2024, items 633 and 1688; of 2025, item 619).

3. The Elimination Database, which processes the data of:

- police officers and Police staff, for the purpose of eliminating fingermarks inadvertently left by them at an incident scene.

Dactyloscopic databases process information, including personal data contained on tenprint compiled by law enforcement agencies such as the Police, the Internal Security Agency, the Foreign Intelligence Agency, the Border Guard, and the Military Gendarmerie.

The Criminal Registration Database is maintained for the purpose of identifying unidentified latents (detecting criminal offenders), unknown persons, unidentified human remains, and missing persons. Data from this database is also utilized in automated international searches conducted under the Prüm Decisions (Council Decisions 2008/615/JHA and 2008/616/JHA), as well as the agreement between the Government of the Republic of Poland and the Government of the United States of America (Journal of Laws of 2019, item 2038). The international exchange of dactyloscopic data is executed in a so-called two-step process (Krzemińska, 2018, PK):

- Step I – Automatic exchange of reference and dactyloscopic data between AFIS systems located in EU Member States.
- Step II – The mutual exchange of further personal data and other information available in relation to the reference data, once a match has been established for the biometric data in Step I.

The Administrative Registration Database is maintained for the purposes of implementing EU asylum policy, namely the exchange of dactyloscopic data with the Eurodac system under Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‚Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 2013) (Krzemińska, 2018, PK)

The Architecture of the AFIS over 25 Years

The implementation of the AFIS MetaMorpho system (version 2.8.14) took place in 2000 (Moszczyński, 2009). Initially, the Central Unit of the AFIS (CU AFIS) was installed on servers located in the former Fingerprint Department of the Central Forensic Laboratory of the National Police Headquarters, alongside the first central workstations. These workstations were utilized for inputting data from tenprint cards and images of latents (which, at that time, were limited to fingerprints only). From its inception, it was assumed that the AFIS would operate in a star topology. This meant that central and remote workstations, as well as other external devices, would connect to the CU AFIS located in Warsaw. In the first place, remote computer workstations were launched in provincial forensic laboratories (lk kwp/KSP). Subsequently, work began in police units across the country to install devices for the rapid identification of individuals and identity verification, such as MorphoTouch and MorphoRapID devices, as well as L1 readers (Kot, Tomaszycki, 2015).

New development perspectives emerged in 2004, when Poland became a member of the European Union (EU) and committed to strengthening its eastern border, which also served as the external border of the EU. At that time, the AFIS was equipped with the Eurodac module. This marked the beginning of the first international data exchange with the EU's Eurodac system (Krzemińska, 2018). Simultaneously, the database began to be populated with digital tenprint cards generated on LiveScan systems, and the input of palmprint images into the system was initiated (Krzemińska, 2018, PK).

By 2010, biometric systems had evolved significantly, and consequently, the Polish AFIS was upgraded to AFIS MetaMorpho version 4.0. As part of this modernization, the system was equipped with a software-based biometric module (MetaMatcher). All previously inputted dactyloscopic friction ridge images were then re-encoded using new algorithms. Prior to this, encoding had been performed using FCP cards (a hardware-based solution). Furthermore, data migration was carried out from Versant object-oriented databases to Oracle object-relational databases (Krzemińska, 2018, PK).

Changes within the European Union resulting from globalization (e.g., the free movement of persons, acts of terrorism, cross-border crime) introduced new challenges within the Area of Freedom, Security and Justice. EU Member States initiated efforts against terrorist offenses and serious cross-border crime, which culminated in the Prüm Decisions. Consequently, the AFIS was expanded to include a Prüm interface, and in November 2015 (Council Implementing Decision (EU) 2015/2009), the automated exchange of dactyloscopic data commenced with the first EU Member States (Krzemińska, 2018, PK). This exchange continues to be conducted within a full mesh topology, with connections to subsequent countries established successively (Krzemińska, 2018). By the end of September 2025, Poland had launched cooperation in this domain with the following EU Member States: Austria (AT), Slovakia (SK), the Czech Republic (CZ), Bulgaria (BG), Lithuania (LT), Belgium (BE), Malta (MT), Cyprus (CY), Germany (DE), Slovenia (SI), Romania (RO), Hungary (HU), the Netherlands (NL), Sweden (SE), Spain (ES), Finland (FI), Estonia (EE), Luxembourg (LU), Portugal (PT), Denmark (DK), Croatia (HR), Greece (GR), and the United Kingdom (GB – under Council Decision 2020/1188).

The degradation of computer hardware, rising system maintenance costs, declining performance (due to database expansion), increasing response times, and aging algorithms necessitated a subsequent modernization of the AFIS. In 2021, the Polish Police acquired the MBIS 4.4 (Morpho Biometric Identification Solution) system, which continues to be referred to as the AFIS. At the time, it represented one of the leading innovative solutions in the field of identification biometrics, developed through a collaboration between the French company Morpho (Safran) and the American firm MorphoTrak, both specializing in multi-biometric solutions.

The AFIS/MBIS delivered a significant improvement in the accuracy and speed of dactyloscopic data matching, thereby enhancing criminal detection and identification capabilities. It provided the end-user with a multitasking Graphical User Interface (GUI), which consists of intuitive icons that streamline data processing. This interface allows for the simultaneous execution of multiple tasks through parallel operation of various functionalities (e.g., working with a latent, a tenprint card, or verifying search results) and enables seamless switching between screens dedicated to specific operations.

The MBIS software complies with a multi-tier architecture, which optimizes collaboration between system modules and ensures its scalability, as well as easier error diagnosis and troubleshooting. Furthermore, database capacity and system performance have been increased (providing faster access to stored information), while maintaining all existing business processes and functionalities and adapting them to process an expanded data model (such as the creation of the Elimination Database and the processing of additional alphanumeric data from tenprint cards).

The MBIS also increases the daily limits of executed transactions (searches) and features a license manager that regulates access to frontend and backend applications of both central and remote workstations. The MBIS is being prepared for interoperability with other external systems (e.g., SIS – Schengen Information System, introduced by Regulation (EU) 2018/1861 of the European Parliament and of the Council) and for automated international data exchange with the FBI database (Dziennik Ustaw [Polish Journal of Laws] of 2019, item 2402). Additionally, the system includes the MBSS 6 module (Morpho Biometric Storage and Search engine version 6.x), which is equipped with advanced algorithms for multi-biometric identification. It was highly rated by the National Institute of Standards and Technology (NIST) for fingerprint and palmprint matching. The results of these evaluations were published in the NISTIR 7859 report (https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7859.pdf - accessed: 16 October 2025). This module is responsible for encoding extracted minutiae (characteristic features of friction ridges, such as line beginnings or endings of ridges, bifurcations, convergences, etc.), image segmentation, sequence checking, and template generation. It also contains a database of biometric templates and executes all types of searches:

- TPTP – TenPrint-to-TenPrint (fingerprints),
- TPUL – TenPrint-to-Unknown Latent (fingerprints),
- PPUP – PalmPrint-to-Unknown Latent (palmprints),
- LTTP – Latent-to-TenPrint (fingerprints),
- LPPP – Latent-to-PalmPrint (palmprints),
- LTUL – Latent-to-Unknown Latent (fingerprints),
- LPUP – Latent-to-Unknown Latent (palmprints).

Furthermore, it manages queues, properly allocates resources and services, collects statistical information from individual nodes, and makes it available to reporting tools. Along with the system modernization, the first test and training environment was established, containing all the functionalities of the production environment. System modifications or corrective actions following application error diagnostics are performed in the test environment first. Isolated changes or patches are deployed there, and their impact on system performance is analyzed; following successful testing, these patches are implemented into the production system. This ensures the operational stability of the MBIS system and enhances data protection without incurring unnecessary risk. The test environment also serves an educational purpose by enabling staff training. Trainees can experiment without limitations and test various procedures using test data (either artificially generated or actual anonymized data).

Four years have passed since the last AFIS modernization, and another one is already planned. This time, functionalities for transmitting and processing personal data will be implemented to meet the requirements of Recast EURODAC (Regulation (EU) 2024/1358 of the European Parliament and of the Council), the implementation of which was deadline-set for 12 June 2026. The scope of data transmitted to EURODAC will be expanded to include, among others, facial images and scans of identity/travel documents. Some of these (e.g., facial images) will be stored in the AFIS database, but will not yet serve as a component used for searches.

Four years have passed since the last AFIS modernization, and another one is already planned. This time, functionalities for transmitting and processing personal data will be implemented to meet the requirements of Recast EURODAC (Regulation (EU) 2024/1358 of the European Parliament and of the Council), the implementation of which was deadline-set for 12 June 2026. The scope of data transmitted to EURODAC will be expanded to include, among others, facial images and scans of identity/travel documents. Some of these (e.g., facial images) will be stored in the AFIS database, but will not yet serve as a component used for searches.

In 2027, further development prospects for the AFIS system will emerge in connection with the entry into force of the Prüm II Regulation (Regulation (EU) 2024/982 of the European Parliament and of the Council). The data exchange procedure will remain unchanged; however, the information transmission channels will be modified. The AFIS systems in EU Member States and Europol (the European Union Agency for Law Enforcement Cooperation) will connect with each other via a central Prüm router, managed by eu-LISA (the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – Regulation (EU) 2018/1726 of the European Parliament and of the Council). The scope of automatically exchanged data will be expanded to include facial images. To this end, a new facial image database will be established within the AFIS, and a new biometric module featuring facial recognition algorithms will be implemented.

Utilization of AFIS Databases

The primary objective of the AFIS is to support dactyloscopy experts in the identification and, *de facto*, criminal detection processes. Efficiency in this domain enhances as the tenprint database grows. Consequently, since the inception of the system, significant emphasis has been placed on the digitization of tenprint cards at the highest possible quality. Initially, inked cards were scanned, but as technology advanced, cards began to be acquired directly from LiveScan systems. Initially, it was assumed that a single digital card containing the ten best friction ridge images from rolled fingers would be stored for each individual. During data entry into the system, the friction ridge images of rolled fingers were compared against flat control prints. The evolution of encoding algorithms not only improved data classification capabilities but also accelerated data processing. The databases expanded rapidly, both quantitatively and in terms of the scope of inputted information. This

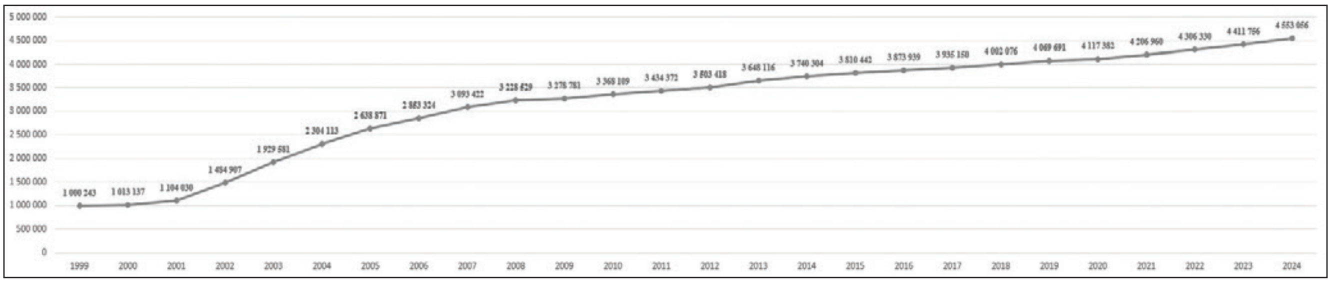

Fig. 1. Tenprint database (as of the end of 2024)

initiated the process of entering flat control prints and palmprint (PP) images, followed by all physical tenprint (TP) cards recorded for a given individual, thereby creating multi-registrations (Krzemińska, 2018, PK).

Figure 1 presents the growth of the tenprint database since the inception of the AFIS system. This chart does not reflect the total number of processed images. It should be noted that a tenprint (TP) card does not always contain 10 rolled finger images and 10 flat images, as these may include bandaged or amputated fingers (or palms). The presented statistics cover the entire AFIS database (including criminal, administrative, and elimination collections). Conversely, Figure 2 illustrates the volume of inputted tenprint cards. To ensure that the system complies with the requirements of data protection, purpose limitation, and legality, data

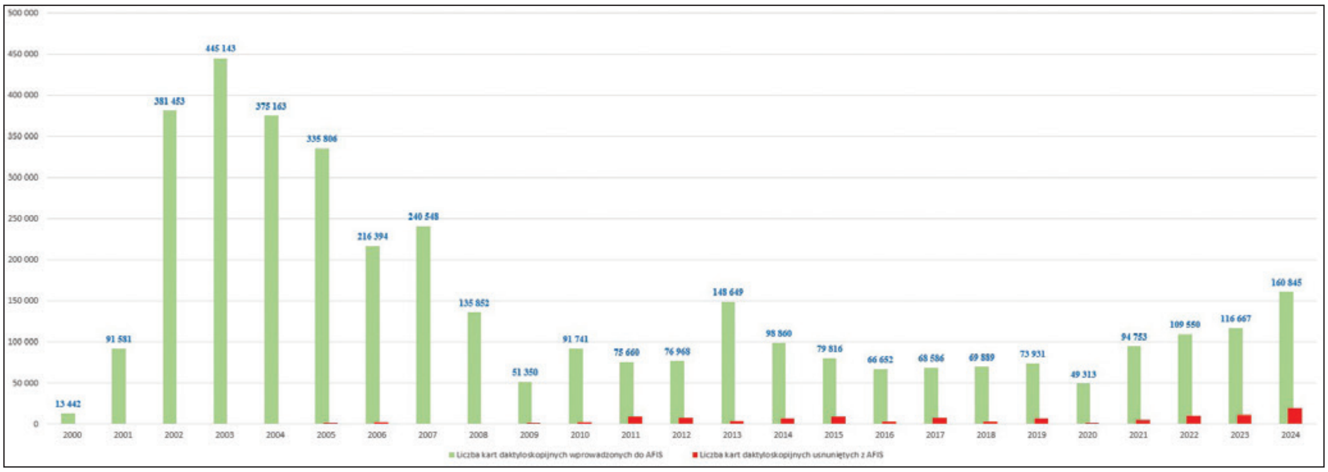

Fig. 2. Number of tenprint cards inputted and deleted in a given year

are entered into the database only when statutory conditions are met, and are deleted once the grounds for their further processing cease to exist.

Conducting similar analyses within the scope of latent print processing poses a more difficult challenge. One might say: after all, a latent print is just a single image. While this is true, the pivotal question is: "At which stage of latent print processing should the data for statistical analysis be collected?". Should statistical studies count a new finger latent (LT) or palm latent (LP) inputted by an expert (extracted from several prints present on a dactyloscopic foil or a photograph), an unknown (NN) finger latent (UL) or palm latent (UP), or rather the specific encoding version that participated in the searches?

Initially, the system clearly distinguished LT (LP) latents from UL (UP) latents. Currently, the system's multitasking capability allows the expert to submit multiple versions of the same latent print, each with a different set of minutiae, for a search against the matcher (the repository of encoded unknown latents). The expert can also decide which encoding (or how many encodings) will be added to the matcher as an unidentified latent. Consequently, a single physical latent print (LT) can be counted multiple times as a UL. It must be remembered that the minutiae configuration plays a critical role, particularly when encoding an image containing a small and additionally low-quality fragment of a latent print.

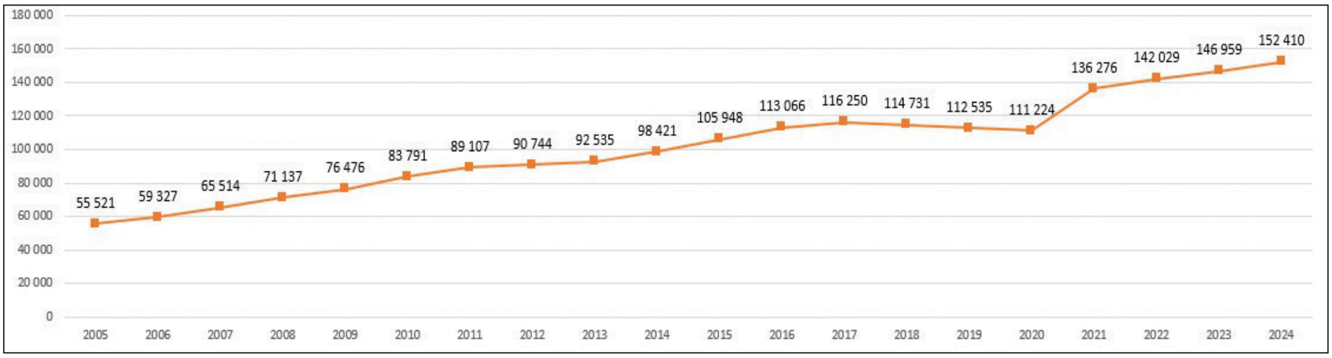

Fig. 3. Latent print database (as of the end of 2024)

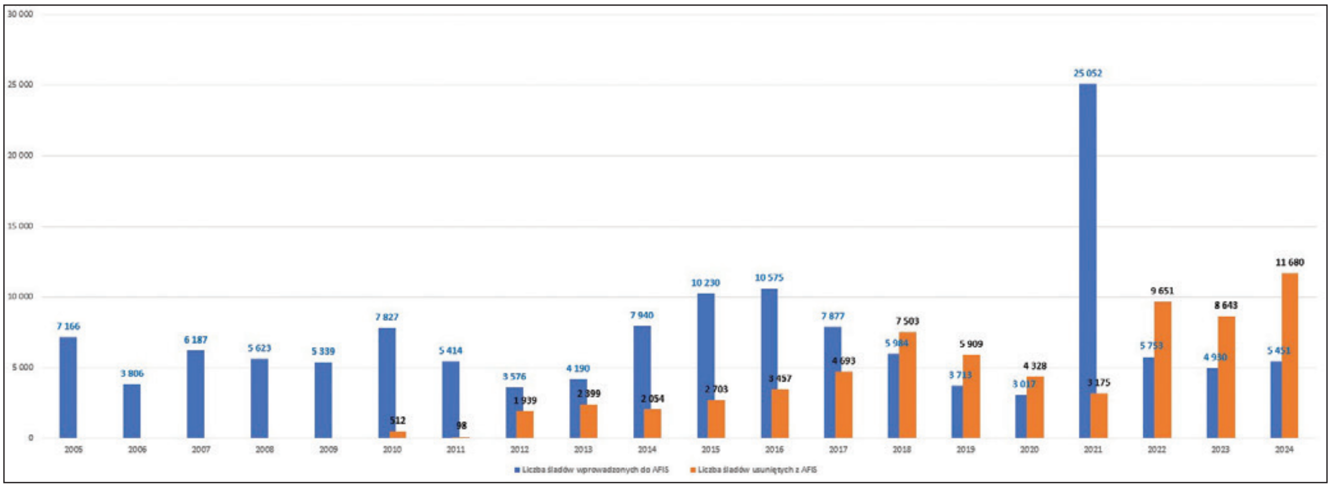

Fig. 4. Number of latent prints inputted and deleted in a given year

Figure 3 illustrates the annual quantitative changes within the latent fingerprint database (with data available from 2005 onwards), while the dynamics of their inputs and deletions are presented in Figure 4.

The database accepts latent prints that can be classified as originating from a fingertip (specifically its central area) or a palm (provided it is possible to determine its specific region). The condition for their registration is the ability to provisionally determine at least 8 characteristic features recognized by the AFIS system, so-called “AFIS minutiae” (in the case of finger latents), and at least 20 such features for palm latents. Latent prints processed in the databases are subject to deletion upon the expiration of the statute of limitations for the offense, after establishing the whereabouts of a missing person, or 55 years from the date of their entry into the database, pursuant to Article 21m of the Police Act.

When analyzing the data presented in Figure 4, it is worth noting the year 2021, which marks the period of the last system modernization. The statistical compilation presented reflects the data migration to MBIS carried out at that time, the organization of data into new database areas, the re-encoding of images, and the enablement of multi-version latent print inputting. A consequence of these actions was a significant increase in data deletions observed in subsequent years.

The percentage share of positive results (HITs) in relation to tenprint-to-tenprint searches over a 25-year period is shown in Figure 5. The presented statistical compilation does not include the results of searches conducted via mobile devices used for rapid biometric identification. Based on the compiled data, it can be concluded that the number of positive identifications in-

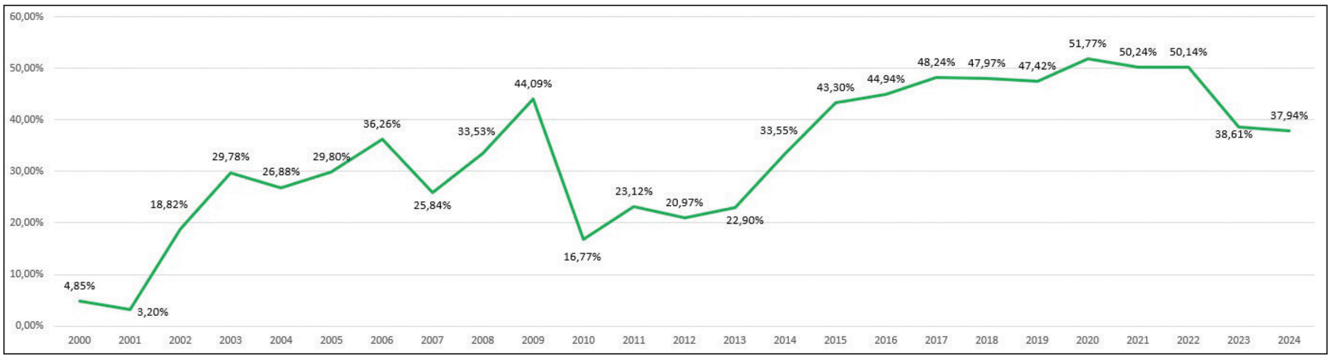

Fig. 5. Percentage share of HIT results in relation to TP/TP verifications

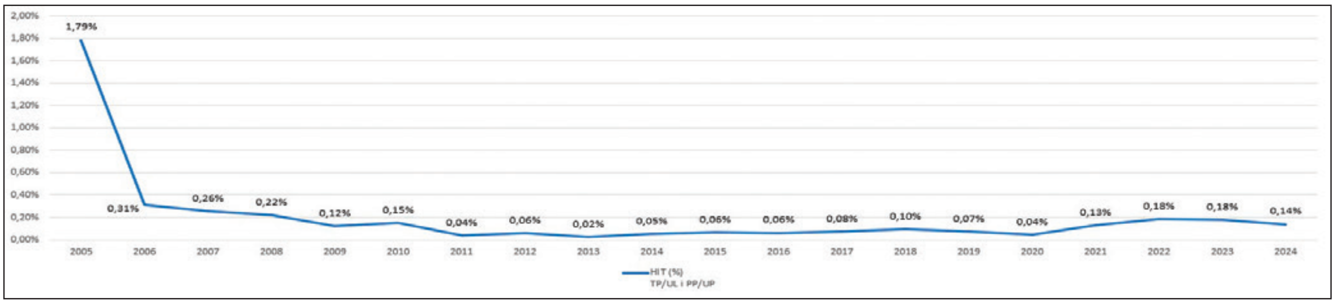

Fig. 6. Percentage share of HIT results in relation to TP/UL and PP/UP verifications

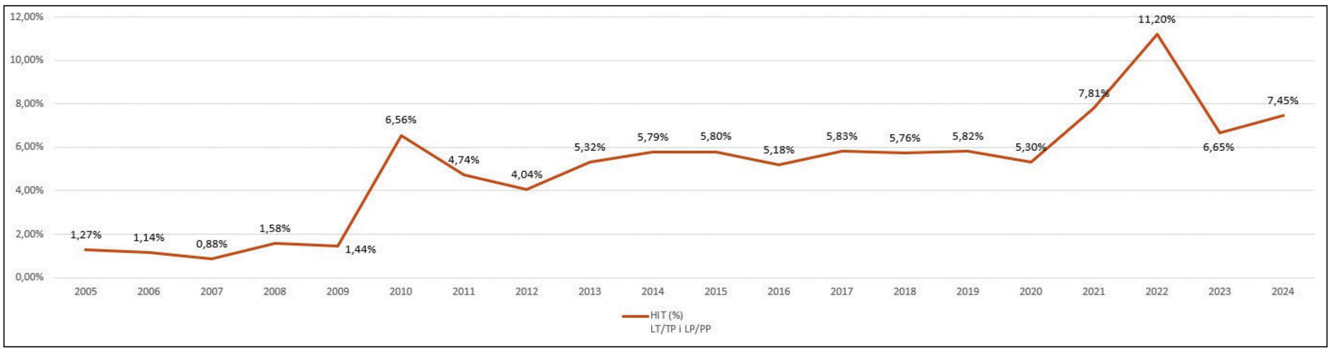

Fig. 7. Percentage share of HIT results in relation to LT/TP and LP/PP verifications

creases as the database volume expands.

Currently, each inputted tenprint card (TP) is automatically submitted for a search against unknown latents (NN). For this type of search, the highest detection rate occurred at the inception of tenprint-to-latent searches, as illustrated in Figure 6. Presently, the detection rate remains at a comparable level. In 2024, 383 unknown latents (299 UL and 84 UP) were identified out of 273,335 executed TP/UL and PP/UP verifications.

Significantly better results are observed in latent-to-tenprint searches, particularly during periods that coincided with system modernizations, i.e., in 2010 and 2021/2022 (Figure 7). During these periods, images were encoded and compared using new biometric algorithms. Searches were then conducted not only for newly inputted latents but also involved re-searching previously unknown latents. In 2022, 26,386 LT/TP and LP/PP search results were verified, yielding 2,956 HIT results (for 2,567 fingers and 389 palms). The detection rate in 2024 involved 27,865 verifications and 2,076 detected latents (1,757 fingers and 319 palms).

Since November 2015, Poland has been conducting international exchanges of dactyloscopic data under the Prüm Decisions. These searches have been and continue to be executed at the request of the unit conducting criminal or identification proceedings. Figure 8 contrasts the identification process (TP/TP searches) with the detection process (LT/TP and LP/PP searches). During the initial phase of this initiative, the results were at a higher level. This was also a period of intensive connectivity establishment with subsequent EU Member States. Currently, the automated international exchange of dactyloscopic data is maintained with 23 EU countries. From November 2015 to December 31, 2024, a total of 105,758 queries of various types were transmitted, yielding 832 HIT results. The majority of TP/TP matches originated from Germany (228 HITs), the Netherlands (142 HITs), Belgium (66 HITs), Spain (61 HITs), the Czech Republic (46 HITs), and Austria (41 HITs). In the case of latent prints, the leaders in this area are Germany (36 HITs) and Austria (35 HITs).

The presented statistics do not fully reflect the scope of activities performed by the users of the AFIS system. It must be remembered that over the course of 25 years, the system has been significantly expanded in terms of available functionalities and has automated numerous business processes previously carried out manually by experts. The fact remains unchanged that the final decision regarding the verification of data match compliance is made by a human.

AFIS and Artificial Intelligence

Artificial Intelligence (AI) is a suite of technologies utilized for autonomous learning to solve tasks and predict future actions based on data collected from various fields of life and the correlations between them. AI systems are capable of analyzing large-scale databases, modeling compiled knowledge, filtering spam, and preparing real-time responses to queries. In simple cases, they can also make decisions by extrapolating collected experiences or behavioral patterns. Research is ongoing toward creating Super Artificial Intelligence (SAI), which could make independent decisions, thereby surpassing human cognitive capabilities.

Is artificial intelligence entering the operational domains of the AFIS system? The answer is yes. The latest commercial technical biometric solutions feature matching algorithms that utilize Artificial Neural Networks (ANNs), Machine Learning (ML), and Deep Learning (DL) techniques. By mapping multiple biometric areas and supporting multibiometric correlations, the identification process can be executed not only based on dactyloscopic data but also using associated alternative modalities, such as the iris, facial features, or a facial image. Furthermore, friction ridge prints of fingers and palms are subjected to more rigorous analysis. The algorithms take into account not only minutiae

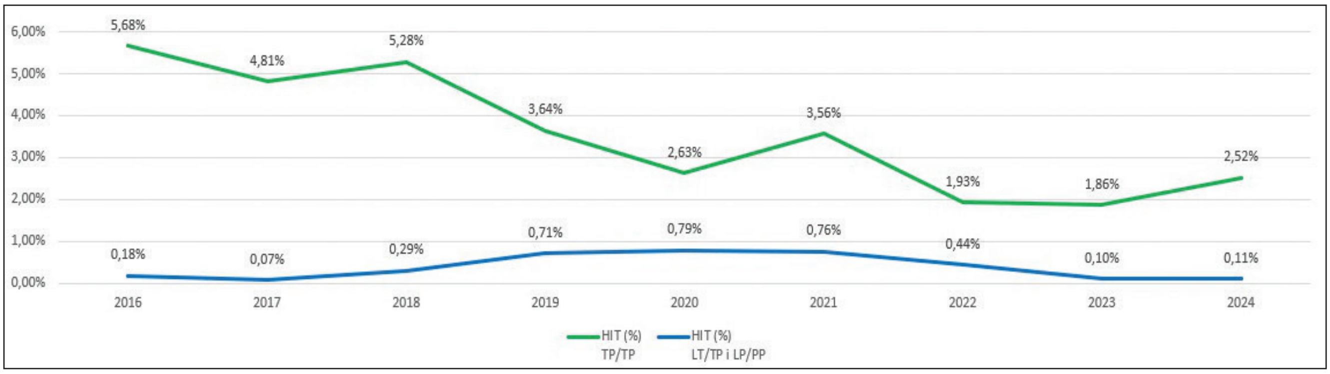

Fig. 8. Percentage share of HIT results in relation to executed TP/TP, LT/TP, and LP/PP verifications within searches under the Prüm Decisions

and patterns but also such friction ridge peculiarities as ridge thickness, edge shape, or the presence of pores.

Biometric system manufacturers boast that by leveraging neural networks and machine learning, their fingerprint recognition technologies are more accurate and efficient; however, they do not disclose the specific operational details of these algorithms, citing proprietary copyright protections. A glimpse into this obscured area is provided by researchers who present various machine learning approaches in their publications, such as Support Vector Machines (SVMs), Genetic Algorithms (GAs), or Learning Vector Quantization (LVQ). More information can be found in the publication: „Artificial Intelligence in Forensic Science" – DOI:10.4324/9781003287810-3 (accessed: October 15, 2025). A compelling approach to analyzing dactyloscopic images is presented there; however, from a practical standpoint, it should be noted that the algorithms are trained and tested on small samples. This can lead to sample bias and raises doubts as to whether they will perform effectively in large-scale systems. Nevertheless, such research must be monitored, as the scientific community drives innovation.

Mentions can already be found online regarding artificial intelligence challenging the thesis of friction ridge uniqueness (https://www.bbc.com/news/technology-67944537, accessed: October 15, 2025). In the article, a team of American researchers trained an AI tool to analyze fingerprints based on the orientation of ridges in the center of the finger, utilizing the curvatures and swirl angles at the core. The study was conducted on 60,000 fingerprint images. In the same article, doubts were raised concerning the permanence of the markers the AI tool focused on, depending on how the finger skin distorted upon contact with a surface.

Crucial to AI models is the training process, which involves not only providing input data but also implementing Retrieval-Augmented Generation (RAG) mechanisms that connect a Large Language Model (LLM) with a knowledge base. Systems based on LLMs have a tendency to „invent" information (hallucinate) by predicting outcomes based on the highest statistical probability. RAG models partially mitigate such behaviors. OpenAI researchers explain that AI hallucinations occur because during training, knowledge vectors (or their components) are not correctly labeled with „true" or „false" tags (https://itwiz.pl/halucynacje-w-ai-badacze-openai-tlumacza-skad-sie-biora-i-jak-je-ograniczac/, accessed: October 15, 2025). In such cases, machine models may adopt flawed assumptions and present false hypotheses, considering them to be highly probable.

The eu-LISA agency could play a significant role in the implementation of artificial intelligence within the EU. Supporting the development and deployment of AI in the domains of borders, migration, and security, the agency manages large-scale IT systems. A report from July 2020 published at DOI:10.2857/58386 (accessed: October 15, 2025) outlines the application areas of AI. One such area involves training biometric machine learning algorithms on datasets from large-scale systems (Krzemińska, 2018). Machine learning techniques will include an automated biometric data matching component, focusing primarily on facial images and the identification of individuals at border crossings. Solutions optimizing the performance of neural networks are intended to ensure high quality, precision, and speed of data recognition within databases containing millions of biometric templates.

Summary

The integration of classical dactyloscopy with advanced hardware and software solutions, embodied by the AFIS system, has proven to be highly successful. Subjecting friction ridge prints of fingers, and subsequently palms, to digital processing laid the foundation for creating systems that are effective not only in identifying criminal perpetrators but also in verifying identity in real time. Over the course of 25 years, it appeared that AFIS would undergo a „renaissance" in its operations. However, the criminal environment also adapts, leaving fewer latents at crime scenes. While this decline is reflected in the volume of inputted data, the system's identification efficacy continues to rise. The highest increases in efficiency serve as a measure of the improved performance of biometric algorithms and coincide with key upgrades to the AFIS system's biometric modules. Both hardware and software solutions continue to be developed. The resulting enhancement of system performance and data processing speed paves the way for mutual interoperability.

The integration of biometric solutions into border control and migration movements has become a major catalyst for the development of multibiometric systems that compare not only finger and palm prints but also facial images, irises, voices, and even DNA profiles (deoxyribonucleic acid – molecules containing the unique genetic blueprint of every human being). Along with the evolution of computer science, AI technologies have entered biometric algorithms. Consequently, contemporary AFIS systems are no longer limited to the traditional analysis of minutiae and ridge patterns; instead, they account for more subtle features during searches, such as ridge thickness, edge shape, and surface porosity. By mapping manifold biometric features and processing multibiometric correlations, identification can be based on a combination of the aforementioned data modalities.

Nonetheless, the fact remains that key decisions are still made by a human. Granted, an increasing number of data processing areas within AFIS are being automated, and the system is approaching a super-intelligent version (SAI AFIS); however, there appears to be a long road ahead.

List of Figures and Sources

Figs. 1–8. Author's own work.

Bibliography

1. Kot, E., Tomaszycki, K. (2015). Funkcjonowanie automatycznego systemu identyfikacji daktyloskopijnej AFIS. W: (red.) E. W. Pływaczewski, W. Filipowski, Z. Rau (red.), Przestępczość w XXI wieku zapobieganie i zwalczanie. *Problemy technologiczno-informatyczne* (s. 332–348). Warszawa, Wolters Kluwer SA.
2. Krzemińska, B. (2018). *System AFIS w polskiej Policji – wczoraj, dzisiaj, jutro. Problemy Kryminalistyki*, nr 300(2), s. 33-43.
3. Krzemińska, B. (2018). Współpraca AFIS z systemami wielkoskalowymi. W: E. Gruza, K. Borkowski (red.), *Horyzonty Daktyloskopii* (s. 151-168). Warszawa, Wydawnictwo Centralnego Laboratorium Kryminalistycznego Policji.
4. Moszczyński, J. (2009). Polska daktyloskopia na przełomie wieków. W: P. Rybicki, T. Tomaszewski, *Daktyloskopia 100 lat na ziemiach polskich* (s. 215-223). Warszawa, Wydawnictwo Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW.
5. Widacki, J. (2008). *Kryminalistyka,* Warszawa, Beck, Warszawa.
6. Gruza, E., Goc, M., Moszczyński, J. (2011), *Kryminalistyka – czyli rzecz o metodach śledczych,* Warszawa, Oficyna Wydawnicza Łośgraf.

Legal acts

1. The Act of 6 kwietnia 1990 r. o Policji (Dz. of Laws of 2025, item 636.718) shall expire.
2. Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach (Dz. U. z 2025 r. poz. 1079, 1794, z 2026 r. poz. 203).
3. Ustawa z dnia 14 lipca 2006 r. o wjeździe na terytorium Rzeczypospolitej Polskiej, pobycie oraz wyjeździe z tego terytorium obywateli państw członkowskich Unii Europejskiej i członków ich rodzin (Dz. U. z 2024 r. poz. 633, 1688, z 2025 r. poz. 619).
4. Agreement between the Government of the Republic of Poland and the Government of the United States of America *on enhancing cooperation in preventing and combating serious crime*, signed in Washington on 12 June 2019 (Journal of Laws of 2019, item 2038).
5. Agreement between the Government of the Republic of Poland and the Government of the United States of America *on cooperation on border security and immigration*, signed in Washington on 16 August 2019 (Journal of Laws of 2019, item 2402).
6. Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 *on the establishment of Eurodac for the comparison of fingerprints for the effective application of* Regulation (EU) No 604/2013 *establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes,and amending* Regulation (EU) No 1077/2011 *establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice* (OJ EU L 180, 2013).
7. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), *and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA* (OJ EU L 135/53, 2016).
8. Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 *on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011* (OJ EU L 295/99, 2018).
9. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006* (OJ EU L 312/14, 2018).
10. Regulation (EC) No 2024/982 of the European Parliament and of the Council of 13 March 2024 *on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council* (OJ EU L, 5.4.2024).
11. Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 *on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council* (OJ EU L, 22.5.2024).
12. Council Decision 2008/615/JHA of 23 June 2008 *on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime* (OJ EU L 210/1, 2008).
13. Council Decision 2008/616/JHA of 23 June 2008 *on the implementation of* Decision 2008/615/JHA *on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime – containing an annex specifying the technical parameters for the exchange of DNA profiles, dactyloscopic data and vehicle registration data* (OJ EU L 210/12, 2008).
14. Council Implementing Decision (EU) 2015/2009 of 10 November 2015 *on the launch of automated data exchange with regard to dactyloscopic data in Poland* (OJ EU L.294/70, 2015) and Corrigendum to Council Implementing Decision (EU) 2015/2009 of 10 November 2015 *on the launch of automated data exchange with regard to dactyloscopic data in Poland* (OJ EU L.2015.312.26/1, 2015).
15. Council Implementing Decision (EU) 2020/1188 of 06 August 2020 *on the launch of automated data exchange with regard to dactyloscopic data in the United Kingdom* (OJ EU L.265/1, 2020).

Websites

1. *https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7859.pdf* – Report: NISTIR 7859, "ELFT-EFS Evaluation of Latent Fingerprint Technologies: Extended Feature Sets [Evaluation#2]", published: May 2012, (accessed: October 16, 2025).
2. DOI:10.2857/58386 – "*Artificial Intelligence in the Operational Management of Large-scale IT Systems*", Research and Technology Monitoring Report: Perspectives for eu-LISA, published: July 2020, (access: 15 October 2025).
3. *https://www.bbc.com/news/technology-67944537* – "Our fingerprints may not be unique, claims AI", Author: Zoe Kleinman, published: 11 January 2024, (accessed: October 15, 2025).
4. DOI: 10.4324/9781003287810-3 – "*Artificial Intelligence in Fingerprint Identification*", Authors: Apoorva Singh, Vinay Aseri, Varad Nagar, Sneha Lohar, Poonam Kumari, Surya Shekhar Daga, Mahipal Singh Sankhla, Chandra Shekhar Yadav, Kumud Kant Awasthi, published: July 2024, (accessed: October 15, 2025).
5. *https://itwiz.pl/halucynacje-w-ai-badacze-openai-tlumacza-skad-sie-biora-i-jak-je-ograniczac/*– „Halucynacje w AI – badacze OpenAI tłumaczą, skąd się biorą i jak je ograniczać", Author: Mikołaj Marszycki, published: 09 September 2025, (accessed: October 15, 2025).