

Biometria – zarys problematyki



Motywnym przewodnim wdrażania identyfikacji na podstawie danych biometrycznych jest obawa przed zagrożeniem terrorystycznym, postrzeganym jako problem o wymiarze globalnym, szczególnie po wydarzeniach 11 września 2001 r. Stąd też wieloletnia rola USA w promowaniu tej metody identyfikacji i koncentracja wysiłków na rzecz stworzenia efektywnego mechanizmu kontroli granicznej coraz bardziej zainteresowane krajami przed wpływem niepożądanych osób z zewnątrz. Dano temu wyraz w postaci opublikowania przez Międzynarodową Organizację Lotnictwa Cywilnego w 2003 r. nowych standardów dokumentów podróży (Machine Readable Travel Documents – MRTD). Standardy te wprowadzają do dokumentów technologie biometryczne zgodnie z propozycjami amerykańskimi i uznają za podstawowy parametr biometryczny obraz kształtu i rysów twarzy w formie obrazu cyfrowego o wysokiej rozdzielczości, przechowywanego w możliwym do odczytania bezdotykowo układzie skalonym. Ma to zapewnić globalną kompatybilność systemów identyfikacji przy kontrolach granicznych.

Aktualnie zagadnienie to, leżące wcześniej głównie w obszarze zainteresowania międzynarodowych korporacji starających się o podwyższenie poziomu bezpieczeństwa zgromadzonych danych oraz o lepszą kontrolę dostępu do swoich obiektów, stało się przedmiotem uwagi różnego rodzaju organów odpowiedzialnych za bezpieczeństwo państwa. Równolegle rozwinął się komercyjny rynek systemów i aplikacji biometrycznych, który dostarcza coraz to nowszych

rozwiązań technologicznych. Taki stan rzeczy powoduje, że warto pokusić się o pewne usystematyzowanie dyskusji wokół tej dziedziny, zarówno na płaszczyźnie jej poznania, jak i możliwości poszczególnych zastosowań.

Systematyka danych biometrycznych

Początki stosowania biometrii sięgają zamierzchłej przeszłości. W Babilonii odcisk palca na glinianej tabliczce stanowił potwierdzenie zawarcia transakcji. W starożytnych Chinach palce odciskano na urzędowych pieczęciach. Oficjalne dokumenty z XIV-wiecznej Persji były sygnowane przez decydena kciukiem maczanym w farbie, a na dworze władcy istniało stanowisko lekarza, który zajmował się weryfikacją takiego podpisu. Pierwsze próby biometrycznego oznaczania osób stosowano w Imperium Rzymskim, gdzie nacinano, wypalano lub tatuowano skórę najemników, by utrudnić im dezercję.

Jednym z najstarszych i najbardziej podstawowych sposobów identyfikacji ludzi było rozpoznawanie na podstawie twarzy, charakterystyki głosu czy sposobu chodzenia. To proste zadanie stawało się coraz bardziej znaczącym wyzwaniem wraz ze wzrostem populacji i rosnącym zjawiskiem migracji. Codziennie każdy nieświadomie wykorzystuje te cechy jako podstawę do rozpoznawania innych osobników w danym środowisku. W najnowszych zastosowaniach biometria ukierunkowana jest na metody automatycznego rozpoznawania ludzi na podstawie ich cech fizycz-

nych i behawioralnych, czyli potwierdzenie bądź odrzucenie ich tożsamości dla celów bezpieczeństwa.

Termin „biometria” wywodzi się z greckich słów *bios* – życie + *metron* – mierzyć. Zautomatyzowane systemy biometryczne mają swoje początki zaledwie w kilku ostatnich dekadach i są spowodowane znaczącym postępem technologii komputerowych. Pomiary biometryczne są matematyczno-statystycznymi metodami badania prawidłowości kierujących zmiennością populacji organizmów żywych. Wyniki pomiarów biometrycznych wykorzystywane są m. in. w antropologii, fizjologii, genetyce, hodowli i medycynie. Biometria to również technika dokonywania pomiarów istot żywych.

W przypadku systemów biometrycznych pod pojęciem „sprawdzenie tożsamości” kryje się dualizm znaczeń. Istnieją dwa warianty autoryzacji użytkownika:

- Identyfikacja: urządzenie ustala, kim jest sprawdzana osoba, przy czym rozpoznanie może nastąpić jedynie na podstawie cech biometrycznych. Komputer sterujący całym procesem musi porównać informacje zebrane przez sensory z bazą danych zawierającą wzorce identyfikacyjne wprowadzone wcześniej. W ten sposób można ustalić tożsamość kryminalistów czy zmasakrowanych ofiar przestępstw lub wypadków. Ten wariant pracy jest stosowany głównie przez służby policyjne, instytucje rządowe oraz wojsko.
- Weryfikacja: system komputerowy sprawdza tożsamość osoby weryfikowanej. Porównaniu

podlegają cechy biometryczne zarejestrowane przez sensory z przechowywaniem w bazie danych wzorcem referencyjnym. W porównaniu z metodą identyfikacyjną proces weryfikacji jest mniej złożony i możliwy do realizacji przy wykorzystaniu relatywnie mało wydajnych komputerów.

Biometria jest często definiowana w jej wąskim funkcjonalnym znaczeniu. Tymczasem trzeba sobie uzmysłowić, że jest to sięgająca korzeniami XIX w. nauka o prawach rządzących zmiennością cech populacji organizmów, której wyniki opracowywane są za pomocą metod statystyki matematycznej. Jak zatem słusznie wskazuje B. Soczówka, wywodzące się z nauk biologicznych klasyczne analizy i badania biometryczne, dzięki dokonującej się rewolucji technologicznej, znalazły swoje odzwierciedlenie w funkcjonalnych aplikacjach nowoczesnych technologii informacyjnych zdolnych do udostępniania i zaawansowanego przetwarzania określonych danych biometrycznych.

Komentarza wymaga stosowana systematyka danych biometrycznych istotnych dla identyfikacji człowieka. Podział na dane o charakterze fizyczno-biologicznym i behawioralnym jest zdaniem niektórych autorów bardzo nieprecyzyjny. Poniżej zamieszczono wykaz cech o identyfikacji biometrycznej.

- Cechy anatomiczne (fizyczno-biologiczne): barwa głosu, zapach, linie papilarne, geometria dłoni, geometria i rysy twarzy, rozkład temperatury twarzy, geometria ucha, geometria ust, cechy charakterystyczne tęczy i siatkówki oka, układu żył nadgarstka, identyfikacja DNA, analiza faktury powierzchni twarzy lub skóry.
- Cechy behawioralne: charakterystyka głosu, mowy, charakterystyka ruchu ust, ruchu gałki ocznej, pisma, pisanie na klawiaturze, chodu.

Wydaje się jednak, że opisywana tematyka ze względu na swą naturę i fakt, że dotyczy w sporej części or-

ganizmów żywych, nie jest tak jednoznaczna i łatwa do sklasyfikowania. Można bowiem racjonalnie argumentować, że spora część danych biometrycznych ma mieszany fizyczno-biologiczno-behawioralny charakter. Trudno bowiem inaczej zakwalifikować np. podlegające zmianom emocjonalnym fizyczne parametry głosu ludzkiego czy oddzielić obraz kształtu rysów twarzy od jej mimiki zależnej od stanów pobudzenia emocjonalnego.

Konsekwencje wdrażania systemów biometrycznych

Wielopłaszczyznowe i dalekosiężne konsekwencje powszechnego wdrożenia systemów biometrycznych poddane zostały dosyć wnikliwej analizie w opublikowanym w 2005 r. Raporcie Komisji Europejskiej pt. „Biometria na granicach: ocena wpływu na społeczeństwo” (Biometrics at the Frontiers: Assessing the Impact on Society – EUR 21585 EN), który stanowił odpowiedź na zapotrzebowanie zgłoszone przez Parlament Europejski. Celem raportu było rozważenie przyszłości biometrii nie tylko w jej najbardziej typowym obecnie zastosowaniu dla ochrony granic, lecz także w znacznie szerszej perspektywie wszelkiego rodzaju konsekwencji społecznych i cywilizacyjnych, które wywoła szerokie zastosowanie rozwiązań biometrycznych w różnych obszarach życia społecznego. Autorzy raportu usystematyzowali owe konsekwencje w czterech podstawowych aspektach (społecznym, ekonomicznym, technicznym i prawnym).

W wymiarze społecznym rozpowszechnienie biometrii może skutkować zasadniczą zmianą relacji państwo – obywatel, istotnie pomniejszając sfery prywatności i anonimowości tego ostatniego. Z kolei z ekonomicznego punktu widzenia w dokonywaniu oceny kosztów wprowadzania biometrii powinien być brany pod uwagę nie tylko obiektywny koszt technologii, ale także inne aspekty prowadzenia procesów identyfikacji, w tym w szczególności koszty procedur rezerwowych opartych na zasobach

ludzkich. Należy także podkreślić, że identyfikacja biometryczna nie jest stuprocentowo pewna z powodów technicznych i trzeba zdawać sobie sprawę z tego, że system biometryczny jest zaledwie częścią systemu bezpieczeństwa, który może być skuteczny tylko wtedy, gdy wdrożone są prawidłowe procedury zbierania danych, zapewnione jest bezpieczeństwo ich przechowywania i istnieje odpowiednia kontrola rejestracji tych danych w systemie. Istnieje wreszcie wyraźna potrzeba modyfikacji obecnej, albo wprowadzenia nowej, legislacji związanej ze stosowaniem systemów biometrycznych, bazującej na dwóch filarach: zapewnieniu prywatności obywateli i transparentności procedur.

Aspekt prawny zagadnienia należy zatem rozpatrywać w kontekście zapewnienia ochrony praw człowieka, rozumianych szeroko jako prawa do poszanowania godności ludzkiej, prywatności, prawa do sądu, domniemania niewinności i prawa do unikania samooskarżenia. Drugim, nie mniej ważnym, problemem jest zapewnienie ochrony danych osobowych. Takie podejście jest związane z wieloma obawami wyrażanymi w związku z wprowadzaniem i powszechnym stosowaniem biometrii do celów identyfikacyjnych, w tym m. in. akumulacji nadmiernej władzy, zasad, kierunków i możliwości przyszłego wykorzystywania zgromadzonych danych, korzystania z technologii biometrycznych w sektorze prywatnym oraz ochrony obywateli przed zbyt pochopnym ujawnianiem ich danych biometrycznych.

Trzeba też nadmienić, że ochrona danych osobowych jest w ramach prawodawstwa Unii Europejskiej objęta następującymi regulacjami ramowymi:

- Konwencją nr 108 Rady Europy z 28 stycznia 1981 r. o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych,
- Dyrektywą 95/46/EC Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w za-

kresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych,

- Rozporządzeniem 45/2001/EC Parlamentu Europejskiego i Rady z 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

Inicjatywy europejskie w zakresie systemów biometrycznych

O znaczeniu, które przywiązuje Unia Europejska do rozwoju systemów zwiększających efektywność ochrony granic państwowych, świadczy Komunikat Komisji Europejskiej do Rady i Parlamentu Europejskiego z dnia 24.11.2005 r. w sprawie zwiększenia skuteczności, interoperacyjności i efektywności synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych COM (2005) 597. Celem tego komunikatu było zwrócenie uwagi na możliwość bardziej efektywnego wykorzystania systemów EURODAC, SIS II oraz VIS do realizacji polityki swobodnego przepływu osób oraz celów związanych ze zwalczaniem terroryzmu i przestępczości w sposób wykraczający poza zakładane wcześniej wykorzystanie tych systemów. Zwraca się uwagę, że jest to możliwe przede wszystkim dzięki lepszemu wykorzystaniu możliwości, które już istnieją, służące w szczególności polepszeniu kontroli wprowadzanych danych, ich większej spójności oraz ułatwieniu obsługi systemów.

Historia systemu EURODAC, będącego elementem wspólnej polityki azylowej Unii Europejskiej, sięga swymi korzeniami Konwencji Dublińskiej z 1990 r., która została znowelizowana w 2003 r. Rozporządzeniem Dublin II – 343/2003/EC. Do bazy danych wprowadzane są parametry biometryczne w postaci odcisków palców wszystkich osób w wieku powyżej 14 lat, ubiegających się o azyl w którymkolwiek z krajów Wspólnoty.

Pobrane odciski są zapisywane w postaci cyfrowej, a następnie przesyłane do centralnej bazy danych funkcjonującej przy Komisji Europejskiej, gdzie następuje ich automatycznie porównanie z odciskami, które są już w owej bazie przechowywane. W efekcie EURODAC pozwala na szybkie stwierdzenie, czy dana osoba ubiegająca się o azyl w krajach UE wjechała na obszar Wspólnoty bez wymaganych dokumentów oraz czy ubiegała się już wcześniej o prawo do azylu w którymkolwiek z krajów członkowskich.

System Informacji Schengen II to rozwinięcie funkcjonującego aktualnie w starych krajach UE systemu działającego na podstawie o podpisanej w 1955 r. Konwencji z Schengen. Do centralnej bazy danych zlokalizowanej w Salzburgu (Austria) mają dostęp policje i oddziały konsularne państw członkowskich Unii Europejskiej. Baza danych pozwala na sprawdzenie, czy osoby lub przedmioty przekraczające granicę Unii bądź już znajdujące się na jej terenie nie są poszukiwane, niejawnie nadzorowane lub czy nie dotyczy ich zakaz wstępu. Zasadniczymi podstawami prawnymi do stworzenia i operowania SIS II umożliwiającego rozszerzenie obszaru Schengen na nowe kraje Unii będą: stosowna Decyzja Rady UE oraz Rozporządzenie Parlamentu Europejskiego w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji, których projekty zostały złożone przez Komisję Europejską w czerwcu 2005 r. – odpowiednio COM (2005) 230 oraz COM (2005) 236.

System Informacji Wizowej (VIS) jest centralną bazą danych zbudowaną na podstawie Decyzji Rady UE z 8 czerwca 2004 r. w sprawie jego ustanowienia (2004/512/EC). Dostęp do niej będą miały organy kontroli granicznej, wizowe i azylowe krajów UE. Baza ta jest budowana, a docelowo ma zawierać dwa rodzaje danych biometrycznych – odciski palców oraz fotografię twarzy obywateli państw trzecich, ubiegających się o wizę w krajach UE. VIS ma za za-

danie przede wszystkim usprawnić komunikację w sprawach wizowych pomiędzy krajami członkowskimi, zapewnić efektywny przepływ informacji konsularnych, podnieść efektywność kontroli granicznych (pod kątem stwierdzenia, czy osoba legitymująca się wizą to jej faktyczny posiadacz), ułatwić ocenę nadsyłanych aplikacji (formularzy) wizowych, znacznie zmniejszyć istniejące zjawisko handlu wizami, wspomóc identyfikację osób przebywających na terytorium Wspólnoty bez wymaganej wizy oraz ułatwić ich deportację, a wreszcie – stać się przyczynkiem do wypracowania wspólnej polityki wizowej dla wszystkich krajów UE.

Komunikat podejmuje także kwestie dalszego rozwoju systemów już istniejących – w tym problematykę wyszukiwania biometrycznego o zwiększonej dokładności, szerszego dostępu do systemów przez uprawnione władze państwowe (w tym szczególnie organy odpowiedzialne za bezpieczeństwo wewnętrzne, powołane do zapobiegania terroryzmowi), a także ustanowienia w przyszłości nowych systemów – Europejskiego Systemu Informacji Daktyloskopijnej AFIS, Europejskiego Rejestru Dokumentów Podróży i Dowodów Tożsamości, a także granicznego systemu kontroli wjazdów i wyjazdów osób.

Ze względu na fakt powszechnego wykorzystywania m.in. danych biometrycznych w tych systemach, stały się one także przedmiotem szczególnego zainteresowania ze strony Europejskiego Inspektora Ochrony Danych, który wydał w ich zakresie dwie opinie:

- 2005/C 181/06 w zakresie Systemu Informacji Wizowej VIS oraz wymiany informacji między państwami członkowskimi na temat wiz krótkoterminowych;
- 2006/C 91/11 w zakresie związanym z utworzeniem, eksploatacją i wykorzystaniem Systemu Informacyjnego Schengen II generacji (SIS II).

W opiniach tych zwraca się szczególnie uwagę na kwestie oceny ryzyka i potrzeby szczególnych zabezpie-

czeń systemów w związku z wykorzystaniem przez nie danych biometrycznych. Co bardzo istotne, opinia ta wskazuje także na potrzebę ogólniejszej refleksji nad problematyką korzystania z tych danych dla celów identyfikacyjnych, w tym na kwestię oddziaływania ich stosowania przez organy państwowe na społeczeństwa krajów członkowskich. Sugeruje także dokonanie pogłębionej oceny w tej mierze na podstawie tzw. siedmiu filarów wiedzy o danych biometrycznych, określonych w przywołanym wcześniej raporcie Komisji Europejskiej.

- uniwersalność – wszystkie istoty ludzkie mają te same właściwości fizyczne, takie jak palce, tęcza, twarz czy DNA, mogące być podstawą identyfikacji;
- unikalność – dla każdej osoby owe właściwości są unikalne, stanowią zatem cechy wyróżniające;
- niezmienność – właściwości te pozostają w dużej części niezmiennie przez cały czas życia osoby;
- możliwość pobrania – unikalne właściwości fizyczne osoby muszą się nadawać do pobrania w stosunkowo łatwy sposób, co umożliwi szybką identyfikację;
- wydajność – stopień dokładności identyfikacji musi być stosunkowo wysoki jeszcze przed wdrożeniem systemu;
- akceptowalność – zastosowanie systemu nie będzie sukcesem, jeśli społeczeństwo wykaże silny i długotrwały opór przed stosowaniem danych biometrycznych;
- odporność na oszukanie – dla zapewnienia dodatkowego bezpieczeństwa wdrażany system musi być trudniejszy do oszukania niż aktualnie istniejące systemy identyfikacji.

W opiniach Europejskiego Inspektora Ochrony Danych (EIOD) zwraca się ponadto uwagę na inne istotne aspekty wykorzystywania danych biometrycznych w ramach systemów EURODAC, SIS II oraz VIS, w tym na potrzebę wypracowania wspólnej

metodologii wdrażania tych danych we wszystkich wymienionych systemach i stworzenia wspólnych wymogów związanych z ich specyfiką. Poza wspomnianą powyżej ogólną ewaluacją ich oddziaływania społecznego wskazuje się również na następujące elementy, które mogłyby konstytuować takie wymogi:

- Ścisłe określenie procedury wpisywania danych: wymagane jest szczegółowe zdefiniowanie źródła danych biometrycznych i sposobu ich zbierania, gdyż bezpośrednio warunkuje to końcowe rezultaty procesu, tj. poziom błędu fałszywego odrzucenia lub błędu fałszywego przyjęcia w systemie;
- Określenie poziomu dokładności: wykorzystanie danych biometrycznych w celu identyfikacji (porównywanie jednostki ze zbiorem) może być jeszcze teraz problematyczne, gdyż wyniki tego procesu są mniej dokładne niż wykorzystanie danych biometrycznych w celu uwierzytelnienia lub kontroli (porównywanie jednostki z jednostką). Identyfikacja biometryczna nie powinna więc stanowić jedynego sposobu identyfikacji lub jedynego klucza dostępu do informacji;
- Procedury awaryjne: powinny zostać wdrożone gotowe do wykorzystania procedury awaryjne mające na celu poszanowanie godności osób, które mogły zostać błędnie zidentyfikowane.

W kontekście drugiego z przedstawionych wymogów poziomu dokładności procesów porównywania danych biometrycznych ważne jest dokonanie analizy tych danych. Mimo że przyjmuje się powszechnie, że są one w dużej części niezmiennie w całym okresie życia istoty ludzkiej, to nie jest to stwierdzenie w pełni adekwatne. Faktem jest, że przynajmniej niektóre parametry charakteryzujące poszczególne cechy biometryczne podlegają mniej lub bardziej daleko idącym zmianom w różnym czasie. Determinantami tych zmian mogą być zarówno wiek osobniczy, jak

i chwilowe pobudzenie emocjonalne, na które dodatkowo nakłada się niedoskonałość systemów informatycznych obsługujących systemy identyfikacji biometrycznej.

Wnioski

W ramach podsumowania nasuwa się refleksja, że biometria widziana oczami prawnika i kryminalistyka powinna być oceniana przez pryzmat rozwoju innych metod nowoczesnej kryminalistyki. Jednocześnie należy zauważyć, że wykorzystywanie w kryminalistyce nowych metod proponowanych przez nauki przyrodnicze i techniczne nie może być dokonywane bez należytą ostrożności, gdyż ich proste i bezrefleksyjne przełożenie na grunt czynności dowodowych w ramach procesu karnego może zakończyć się niepowodzeniem. Sprawa jest na tyle skomplikowana, że już samo hasło „dane biometryczne” niesie za sobą konotacje sięgające, wydawałoby się, odległych dziedzin i gałęzi prawa krajowego:

- kwestii karnoprawnych (problematyka związanych z danymi biometrycznymi działań, które mają charakter przestępstwa, np. przetwarzanie danych bez stosownego uprawnienia, udostępnianie ich bez upoważnienia);
- kwestii administracyjnoprawnych (problematyka ogólnej ochrony danych osobowych oraz decyzji administracyjnych Głównego Inspektora Ochrony Danych Osobowych);
- kwestii cywilnoprawnych (problematyka ochrony danych biometrycznych mających charakter dóbr osobistych, np. wizerunku osoby).

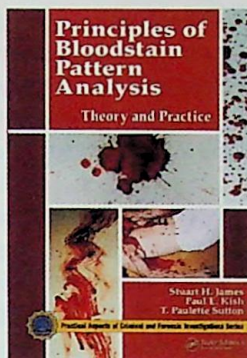
Biometria nie może abstrahować od konsekwencji i problemów, jakie niesie ze sobą każda nowa, chociażby najskuteczniejsza, metoda ustalania tożsamości ofiar czy sprawców czynów zabronionych albo też eliminacji osób z kręgu podejrzewanych o ich popełnienie. Praktyczne wdrożenie i ostateczny sukces każdej metody jest bowiem uwarunkowany

w dużej mierze świadomością faktu istnienia jej słabości (choćby statystycznej stopy błędu) oraz sposobem ich oszacowania wraz ze stworzeniem mechanizmu poprawnego wykorzystania metody w realiach systemu prawnego. Podsumowując, trzeba powiedzieć, że biometria może stać się skutecznym narzędziem kryminalistyki, dołączając do innych uznanych i sprawdzonych metod identyfikacji człowieka.

BIBLIOGRAFIA

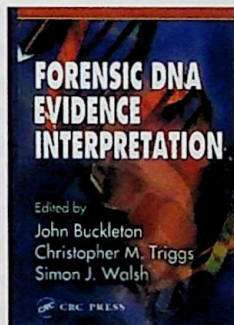
1. **Chrostowski J.:** Uważne oko biometrii, „Wiedza i Życie” 2006, nr 4, s. 20.
 2. **European Commission, Joint Research Centre, Institute for Prospective Technological Studies:** Technical Report „Biometrics at the frontiers: Assessing the impact on Society”, 2005 – EUR 21585 EN.
 3. **Goliński T.:** Biometria w dokumentacji, „Człowiek i Dokumenty” 2006, nr 2, s. 2.
 4. **Hanuszek T.:** Kryminalistyka w Polsce przełomu wieków, „Problemy Kryminalistyki” 2001, nr 232, s. 5.
 5. **Kasprowski P.:** Identyfikacja osobnicza na podstawie ruchu oka – autoreferat rozprawy doktorskiej, Instytut Informatyki Wydziału Automatyki, Elektroniki i Informatyki Politechniki Śląskiej, Gliwice 2004, s. 2.
 6. **Koziczak A.:** Karnoprawne uwarunkowania biometrii, Materiały Konferencji Naukowej Biometria 2003 – Technologia, Prawo, Społeczeństwo, Instytut Maszyn Matematycznych 2003.
 7. **Krysowaty I., Niedziejko P.:** Biometria – Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie, „Zabezpieczenia” 2006, nr 4, artykuł dostępny na stronie portalu: www.zabezpieczenia.com.pl
 8. **Popławski P.:** Co to jest biometria?, artykuł dostępny na stronie portalu: www.geokat.com.pl
 9. **Soczówka B.:** Czym jest biometria, artykuł dostępny na stronie portalu: www.twojafirma.pl
 10. **Swarcewicz R.:** Identyfikacja biometryczna – blaski i cienie, „Logistyka” 2002, nr 4, artykuł dostępny na stronie portalu: www.czasopismologistyka.pl
- Przywoływane akty prawne zostały wykazane w treści artykułu.

Nowe nabytki Biblioteki Naukowej CLK KGP

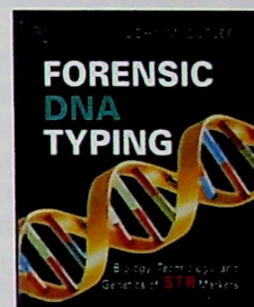


- S. Zubański – AFIS, wybrane zagadnienia
- J. Kosiński – Przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych
- M. Kaczmarek – Zbiory daktyloskopijne i ich praktyczne wykorzystanie
- J. Jerzewska – ABC daktyloskopowania
- A. Misiuk – Instytucje policyjne w Polsce. Zarys dziejów
- J. Clement, K. Marks – Computer – Graphic Facial Reconstruction
- M. Cassidy – Footwear Identification

- D. Hilderbrand – Footwear, the Missed Evidence
- H. James, P.E. Kish, T.P. Sutton – Principles of Bloodstain Pattern Analysis. Theory and Practice



- H.H. Braess, U. Seiffert – Vieweg Handbuch Kraftfahrzeugtechnik
- K. Łagoda – Vadecurum interwencji policyjnych

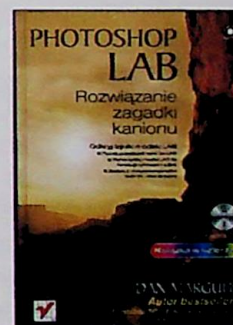


- D. Sklyara – Łamanie zabezpieczeń cyfrowych
- B. Long – Fotografia cyfrowa
- J.M. Butler – Forensic DNA Typing

- J. Buckleton, Ch.M. Triggs, S.J. Walsh – Forensic DNA Evidence Interpretation
- L. Barken – Wireless hacking
- D. Margulis – Photoshop LAB. Rozwiązanie zagadki kanionu
- A. Chodała – Trening militarny żołnierzy
- G. Kędzierska – Technika kryminalistyczna. Tom 2



- J. Kasprzak, B. Młodziejowski, W. Brzęk, J. Moszczyński – Kryminalistyka
- J. Pieprzyk – Teoria bezpieczeństwa systemów komputerowych
- J. Cowger – Friction Ridge Skin
- D. Ashbaugh – Quantitative – Qualitative Friction Ridge Analysis



Biblioteka Naukowa CLK KGP
Al. Ujazdowskie 7
00-583 Warszawa
godziny otwarcia: 8.15–12.15