



Julia Rak¹

Specjalistka w Departamencie Współpracy Międzynarodowej Urzędu Ochrony Danych Osobowych
(ORCID: <https://orcid.org/0009-0000-5855-264X>).

Dane behawioralne jako dane osobowe w prawie Unii Europejskiej – kwalifikacja prawna, standardy przetwarzania oraz zastosowanie w procesach uwierzytelniania

Słowa kluczowe: dane behawioralne, biometria behawioralna, dane biometryczne, dane osobowe, ochrona danych osobowych, RODO, uwierzytelnianie

Artykuł podejmuje problem kwalifikacji prawnej danych behawioralnych w świetle prawa Unii Europejskiej, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)². Dynamiczny rozwój technologii opartych na analizie zachowań użytkowników prowadzi do coraz powszechniejszego przetwarzania danych behawioralnych w celach identyfikacyjnych i uwierzytelniających, m.in. w sektorze bankowym, administracji publicznej, ochronie zdrowia czy mediach społecznościowych. Analiza przeprowadzona w artykule wykazuje, że dane behawioralne co do zasady spełniają kryteria uznania ich za dane osobowe, a w określonych konfiguracjach funkcjonalnych mogą również stanowić dane biometryczne w rozumieniu art. 4 pkt 14 RODO. Analiza porównawcza standardów przetwarzania danych behawioralnych oraz klasycznych „twardych” danych biometrycznych wykazuje zarówno podobieństwa funkcji identyfikacyjnej, jak i różnice w sposobie kwalifikacji normatywnej. Artykuł szczególną uwagę poświęca podstawom prawnym przetwarzania danych behawioralnych, w tym granicom stosowania zgody, umowy oraz prawnie uzasadnionego interesu administratora, a także ryzyku obchodzenia reżimu art. 9 RODO poprzez zastępowanie klasycznych danych biometrycznych danymi behawioralnymi. Analiza przykładów zastosowań biometrii behawioralnej w procesach uwierzytelniania m.in. w sektorze bankowym ukazuje konsekwencje systemowe dla ochrony praw podstawowych jednostki, w szczególności prawa do ochrony danych osobowych i prywatności. Wnioski wskazują na potrzebę doprecyzowania standardów prawnych dotyczących przetwarzania danych behawioralnych w prawie Unii Europejskiej.

1. Wprowadzenie

Postępująca cyfryzacja usług publicznych i prywatnych, w szczególności w sektorach regulowanych, prowadzi

do dynamicznego rozwoju technologii opartych na analizie zachowań użytkowników. Coraz powszechniej wykorzystywane są rozwiązania pozwalające na identyfikację, uwierzytelnianie oraz ocenę ryzyka związanego z działaniami osoby fizycznej na podstawie jej wzorców behawioralnych, takich jak sposób poruszania kursorem, dynamika pisania na klawiaturze, charakterystyka gestów, rytm interakcji z interfejsem czy schematy nawigacyjne. Dane te, określane zbiorczo danymi

¹ Przedstawione poglądy są poglądami własnymi autorki.

² Dz.Urz. UE L 119, s. 1, ze zm. – dalej RODO.

behawioralnymi, zyskują istotne znaczenie zwłaszcza w kontekście zapobiegania nadużyciom, ciągłej autoryzacji użytkownika oraz zwiększania bezpieczeństwa procesów cyfrowych.

Funkcjonalna kwalifikacja danych behawioralnych na gruncie prawa Unii Europejskiej wymaga uwzględnienia celu i sposobu przetwarzania. Dane behawioralne zasadniczo spełniają kryteria danych osobowych w rozumieniu art. 4 pkt 1 RODO, ponieważ mogą być przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W określonych konfiguracjach technicznych i funkcjonalnych, np. przy wykorzystaniu ich do jednoznacznej identyfikacji lub uwierzytelniania użytkownika, mogą one również spełniać definicję danych biometrycznych³ podlegających szczególnemu reżimowi ochronnemu przewidzianemu w art. 9 RODO. Wątpliwości wynikają przede wszystkim z charakteru behawioralnych cech, które są dynamiczne i probabilistyczne, a nie statyczne jak klasyczne „twarde” dane biometryczne.

W praktyce prowadzi to do sytuacji, w której dane behawioralne są coraz częściej wykorzystywane w celach identyfikacyjnych i uwierzytelniających, przy możliwym jednoczesnym stosowaniu wobec nich łagodniejszych podstaw prawnych przetwarzania, charakterystycznych dla „zwykłych” danych osobowych. Zjawisko to rodzi pytanie o granice dopuszczalności takiej praktyki oraz o ryzyko obchodzenia reżimu ochronnego przewidzianego dla danych szczególnych kategorii, w szczególności w sektorach, w których użytkownik nie ma realnej swobody wyboru alternatywnych form identyfikacji.

Celem artykułu jest analiza kwalifikacji prawnej danych behawioralnych na gruncie prawa Unii Europejskiej, w szczególności ustalenie kryteriów, które pozwalają uznać je za dane osobowe oraz – w określonych okolicznościach – za dane biometryczne w rozumieniu RODO. Artykuł podejmuje próbę odpowiedzi na pytanie, w jakich konfiguracjach technicznych i funkcjonalnych przetwarzanie danych behawioralnych w procesach uwierzytelniania prowadzi do objęcia ich szczególnym reżimem ochronnym właściwym dla danych biometrycznych, a także czy praktyka wykorzystywania ich w systemach bezpieczeństwa cyfrowego może prowadzić do obchodzenia tego reżimu.

2. Pojęcie danych behawioralnych

Pojęcie danych behawioralnych nie zostało dotychczas zdefiniowane w aktach prawa Unii Europejskiej, w tym w RODO. Termin ten funkcjonuje przede wszystkim w dyskursie technologicznym oraz w praktyce rynkowej, gdzie służy do opisu informacji odnoszących się do sposobu, w jaki osoba fizyczna zachowuje się podczas korzystania m.in. z systemów cyfrowych. Dane behawioralne obejmują zatem nie tyle statyczne cechy osoby, ile dynamiczne wzorce jej aktywności, ujawniające się w trakcie interakcji z określonym środowiskiem technicznym⁴. Do najczęściej wskazywanych kategorii danych behawioralnych zalicza się w szczególności dynamikę pisania na klawiaturze, obejmującą tempo wprowadzania znaków, odstępy czasowe pomiędzy kolejnymi naciśnięciami klawiszy czy charakterystyczne sekwencje ruchów. Inną grupę stanowią dane dotyczące

sposobu poruszania kursorem, takie jak trajektoria ruchu, prędkość, przyspieszenie czy częstotliwość zatrzymań. W środowiskach opartych na interfejsach dotykowych analizie podlegają również gesty użytkownika, w tym sposób przesuwania palcem po ekranie, siła czy kąt nachylenia urządzenia⁵. Z perspektywy technicznej dane behawioralne mają charakter probabilistyczny i kontekstowy. Ich znaczenie ujawnia się dopiero w wyniku analizy zbiorczej, najczęściej przy wykorzystaniu algorytmów uczenia maszynowego, które pozwalają na identyfikację wzorców i odchyłeń od przyjętej normy. W przeciwieństwie do klasycznych danych identyfikacyjnych, pojedynczy element danych behawioralnych rzadko posiada samodzielną wartość informacyjną. Dopiero ich połączenie i odniesienie do konkretnego użytkownika umożliwia wykorzystanie ich w celach takich jak identyfikacja, uwierzytelnianie czy ocena ryzyka.

Kwalifikacja danych behawioralnych jako danych osobowych wymaga odniesienia się do definicji zawartej w art. 4 pkt 1 RODO, zgodnie z którą dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Kluczowym elementem tej definicji jest zatem kryterium identyfikowalności, rozumiane szeroko i funkcjonalnie, zgodnie z utrwalonym orzecznictwem TSUE⁶. Dane behawioralne, choć często nie pozwalają na bezpośrednią identyfikację osoby fizycznej w oderwaniu od kontekstu ich przetwarzania, mogą umożliwiać identyfikację pośrednią poprzez przypisanie określonego wzorca zachowań do konkretnego użytkownika⁷. Istotne jest rozróżnienie pomiędzy danymi samodzielnie identyfikującymi osobę fizyczną a danymi, które nabierają charakteru identyfikującego dopiero w określonym kontekście systemowym, tj. w połączeniu z innymi informacjami przetwarzanymi przez administratora lub podmiot trzeci.

Dane te zazwyczaj są powiązane z innymi identyfikatorami, takimi jak identyfikator sesji, numer klienta, adres IP czy dane uwierzytelniające, co znacząco zwiększa ich potencjał identyfikacyjny⁸. W praktyce oznacza to, że wzorce behawioralne są najczęściej analizowane łącznie z identyfikatorami technicznymi, takimi jak device ID, account ID, adres IP czy pliki cookies, które umożliwiają przypisanie określonej aktywności konkretnemu użytkownikowi lub urządzeniu. Nawet w sytuacjach, w których administrator deklaruje brak zamiaru identyfikacji osoby, możliwość taka może istnieć obiektywnie,

3 Zob. art. 4 pkt 14 RODO.

4 K. Gałęzowska, *Dane biometryczne a dane behawioralne*, „Monitor Prawniczy” 2022/21, s. 2079–2086.

5 A. Mahfouz, T.M. Mahmoud, A.S. Eldin, *A survey on behavioral biometric authentication on smartphones*, „Journal of Information Security and Applications” 2017/37, s. 18–39.

6 Zob. wyrok z 19.10.2016 r., C582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland, EU:C:2016:779, pkt 43–49, w którym Trybunał przyjął szerokie, funkcjonalne rozumienie pojęcia „osoby możliwej do zidentyfikowania”, odwołując się do kryterium „środków, które mogą zostać rozsądnie wykorzystane” w celu identyfikacji.

7 Wiążąca decyzja EROD 01/2023 w sprawie przetwarzania danych osobowych w celach reklamy behawioralnej przez Meta. W decyzji podkreślono, że dane behawioralne wykorzystywane w reklamach behawioralnych, nawet jeśli nie zawierają bezpośrednich identyfikatorów, mogą prowadzić do pośredniej identyfikacji użytkowników. Europejska Rada Ochrony Danych (EROD) wskazuje, że praktyki te mogą naruszać przepisy RODO, a organy nadzorcze mają prawo wydawać wiążące zalecenia, które wymagają ścisłego stosowania się administratorów danych w UE. Przykład ten ilustruje realne ryzyko identyfikowalności danych behawioralnych i konieczność proporcjonalnej ochrony prywatności.

8 ICO, *What are identifiers and related factors?*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/> (dostęp: 29.01.2026 r.).

przy uwzględnieniu testu „wszelkich rozsądnie prawdopodobnych sposobów identyfikacji”, o których mowa w motywie 26 RODO, zgodnie z którym ocena identyfikowalności powinna uwzględniać wszelkie środki, jakie mogą być racjonalnie wykorzystane przez administratora lub inny podmiot w celu ustalenia tożsamości osoby fizycznej.

Istotnym problemem pozostaje również kwestia anonimizacji i pseudonimizacji danych behawioralnych. Ze względu na unikalność i wysoką zmienność wzorców zachowań, pełna anonimizacja tych danych może okazać się w praktyce trudna do osiągnięcia. Nawet po usunięciu klasycznych identyfikatorów istnieje ryzyko ponownej identyfikacji użytkownika na podstawie zestawu cech behawioralnych, zwłaszcza gdy dane te są zestawiane z innymi zbiorami informacji. Pseudonimizacja, choć stanowi istotny środek bezpieczeństwa, nie eliminuje zatem możliwości uznania danych behawioralnych za dane osobowe.

3. Dane behawioralne a dane biometryczne

RODO definiuje dane biometryczne jako dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jej jednoznaczną identyfikację⁹. W praktyce regulacyjnej i orzeczniczej pojęcie to było dotychczas odnoszone przede wszystkim do „twardych” danych biometrycznych, opartych na względnie stałych i mierzalnych cechach osoby, takich jak odciski palców, wizerunek twarzy, geometria dłoni, cechy siatkówki oka oraz głosu. Charakterystyczne dla nich są statyczność oraz silne powiązanie z fizyczną tożsamością osoby. Cechy te, choć mogą podlegać pewnym zmianom w czasie, zachowują względną trwałość i powtarzalność, co umożliwia ich wykorzystanie jako jednoznacznych identyfikatorów.

Inna, bardziej zniuansowana klasyfikacja danych biometrycznych opiera się na stopniu ich zdolności identyfikacyjnej. Wyróżnia się w tym kontekście tzw. silne identyfikatory biometryczne, które umożliwiają wysokostabilną i jednoznaczną identyfikację osoby fizycznej, takie jak odcisk palców czy obraz tęczówki oka. Obok nich wskazuje się na dane biometryczne o słabszym charakterze identyfikacyjnym, obejmujące cechy mniej unikalne lub mniej trwałe, w tym m.in. cechy głosu, określone właściwości budowy ciała oraz wzorce zachowań użytkownika. W najniższym stopniu takiej gradacji lokowane są tzw. miękkie dane biometryczne, odnoszące się do ogólnych właściwości osoby, takich jak płeć czy wiek, które same w sobie nie pozwalają na jednoznaczną identyfikację, lecz mogą pełnić funkcję pomocniczą w procesach identyfikacyjnych¹⁰. Niezależnie od powyższych klasyfikacji prawodawca unijny nie różnicuje danych biometrycznych ze względu na ich „siłę” identyfikacyjną, lecz posługuje się jednolitą definicją legalną. Dane biometryczne, jeżeli spełniają przesłanki określone w art. 4 pkt 14 RODO, zostały objęte szczególnym reżimem ochrony jako dane szczególnych kategorii w rozumieniu art. 9 ust. 1 RODO, których przetwarzanie jest co do zasady zakazane.

W konsekwencji kwalifikacja określonych informacji jako danych biometrycznych może zostać ujęta w postaci

funkcjonalnego testu obejmującego trzy elementy. Dane mogą zostać uznane za biometryczne, jeżeli: 1) stanowią dane osobowe, 2) podlegają specjalnemu przetwarzaniu technicznemu, oraz 3) umożliwiają lub potwierdzają jednoznaczną identyfikację osoby fizycznej. Spełnienie wszystkich trzech przesłanek prowadzi do objęcia ich reżimem art. 9 RODO. O zakwalifikowaniu określonych danych jako biometrycznych decyduje zatem nie tyle ich natura fizyczna, ile funkcja, jaką pełnią w procesie przetwarzania.

Biometria behawioralna opiera się na analizie wzorców zachowań użytkownika, które ujawniają się w trakcie interakcji z systemem informatycznym. Przedmiotem analizy stają się cyfrowe zachowania fizyczne i poznawcze człowieka, a nie niezmiennie identyfikatory, takie jak odciski palców czy obraz tęczówki oka, określane niekiedy mianem biometrii „drugiej generacji”¹¹. Wzorce behawioralne mają charakter dynamiczny i są modelowane przy użyciu algorytmów uczenia maszynowego, które umożliwiają przypisanie określonego profilu behawioralnego do konkretnego użytkownika¹². Analiza ta może obejmować zarówno pojedyncze cechy zachowania, jak i ich łączne konfiguracje, co pozwala na identyfikację lub uwierzytelnianie osoby z określonym poziomem prawdopodobieństwa. Granica pomiędzy biometrią klasyczną a behawioralną nie zawsze ma przy tym charakter wyraźny, zwłaszcza że systemy rozpoznawania zachowań lub emocji coraz częściej wykorzystują elementy technologii rozpoznawania twarzy.

Istotną cechą biometrii behawioralnej jest jej ciągły charakter. Dane mogą być zbierane i analizowane nie tylko na etapie jednorazowej identyfikacji, lecz również w sposób ciągły, w trakcie całej sesji użytkownika. Pozwala to na bieżącą ocenę zgodności aktualnych zachowań z wcześniej ustalonym wzorem, co znajduje zastosowanie m.in. w mechanizmach ciągłego uwierzytelniania (*continuous authentication*)¹³ oraz wykrywania nadużyć. W sytuacji, w której system porównuje aktualne zachowania użytkownika z wcześniej utworzonym profilem behawioralnym w celu potwierdzenia jego tożsamości i utrzymania aktywnej sesji, mechanizm taki może spełniać przesłankę umożliwiania lub potwierdzenia jednoznacznej identyfikacji osoby, a tym samym prowadzić do kwalifikacji danych jako biometryczne.

Biometria behawioralna bywa postrzegana jako rozwiązanie o niższym stopniu inwazyjności, gdyż nie wymaga pozyskiwania danych fizycznych w tradycyjnym rozumieniu. Jednocześnie jednak jej potencjał ingerencji w sferę prywatności może być znaczny, ze względu na możliwość tworzenia szczegółowych profili zachowań, trudności precyzyjnego określenia zakresu przetwarzania oraz ograniczoną świadomość użytkownika co do skali i ciągłości analizy jego aktywności.

11 C. Wendehorst, Y. Duller, *Biometric Recognition and Behavioural Detection. Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, Brussels 2021, s. 13–14.

12 M. Ózal, *Behavioral Biometrics: A Brief Introduction from the Perspective of Data Protection Law*, December 2020, <https://www.law.kuleuven.be/citip/blog/behavioral-biometrics-a-brief-introduction-from-the-perspective-of-data-protection-law/> (dostęp: 29.01.2026 r.).

13 A.F. Baig, S. Eskeland, B. Yang, *Privacy-preserving continuous authentication using behavioral biometrics*, „International Journal of Information Security” 2023/22, s. 1833–1847 – ciągłe uwierzytelnianie oznacza mechanizm stałej weryfikacji tożsamości użytkownika w trakcie trwania sesji na podstawie ciągłej analizy wzorców zachowań behawioralnych w celu wykrycia anomalii i nadużyć.

9 Art. 4 pkt 14 RODO.

10 *Second Generation Biometrics: The Ethical, Legal and Social Context*, red. E. Mordini, D. Tzovaras, Dordrecht 2012, s. 9.

Kluczowe pozostaje ustalenie, czy i w jakich okolicznościach dane behawioralne mogą zostać zakwalifikowane jako dane biometryczne. Prawodawca unijny uwzględnił cechy behawioralne jako potencjalną podstawę przetwarzania biometrycznego, jednak decyduje o tym spełnienie dwóch dodatkowych przesłanek: zastosowanie szczególnych środków technicznych oraz funkcja jednoznacznej identyfikacji osoby fizycznej. Nie każde przetwarzanie danych behawioralnych będzie zatem prowadziło do ich zakwalifikowania jako danych biometrycznych. Jeżeli dane będą wykorzystywane wyłącznie pomocniczo, np. w celu poprawy ergonomii interfejsu lub ogólnej analizy, brak będzie podstaw do objęcia ich reżimem art. 9 RODO. Podobnie będzie w sytuacji, gdy analiza wzorców zachowań służy jedynie ocenie poziomu ryzyka transakcji lub wykrywaniu potencjalnych nadużyć, bez przypisywania wzorca do jednoznacznie zidentyfikowanej osoby fizycznej.

Odmierna sytuacja występuje, gdy dane behawioralne stanowią zasadniczy element procesu identyfikacji lub uwierzytelniania użytkownika, a ich analiza pozwala na potwierdzenie jego tożsamości z wysokim stopniem prawdopodobieństwa. Granica pomiędzy danymi osobowymi a danymi biometrycznymi w przypadku danych behawioralnych ma charakter płynny i zależy od kontekstu przetwarzania. Te same kategorie danych mogą podlegać odmiennej kwalifikacji prawnej w zależności od celu i sposobu ich wykorzystania. Taka sytuacja rodzi ryzyko niejednolitego stosowania przepisów RODO oraz sprzyja powstawaniu praktyk polegających na funkcjonalnym zastępowaniu klasycznej biometrii rozwiązaniami behawioralnymi, bez poddania ich odpowiadającemu im reżimowi ochronnemu.

4. Podstawy prawne przetwarzania danych behawioralnych

W sytuacji, w której dane behawioralne nie spełniają przesłanek uznania ich za dane biometryczne w rozumieniu art. 4 pkt 14 RODO, ich przetwarzanie podlega ogólnym zasadom wynikającym z art. 6 RODO. W takim przypadku konieczne jest ustalenie jednej z przesłanek legalizujących przetwarzanie określonych w art. 6 ust. 1 RODO, w praktyce największe znaczenie mają przesłanki wykonania umowy oraz prawnie uzasadnionego interesu administratora.

Podstawą przetwarzania danych behawioralnych może być art. 6 ust. 1 lit. b RODO, jeżeli przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą. W sektorze bankowym oraz w innych sektorach regulowanych argument ten bywa wykorzystywany w odniesieniu do danych przetwarzanych w celu zapewnienia bezpieczeństwa transakcji lub dostępu do usług elektronicznych. Należy jednak podkreślić, że zakres zastosowania tej podstawy jest ograniczony do danych rzeczywiście niezbędnych do realizacji zobowiązania umownego, co wymaga każdorazowej oceny proporcjonalności. W szczególności nie każde przetwarzanie danych służące zwiększeniu poziomu bezpieczeństwa systemu może zostać uznane za niezbędne do wykonania umowy w rozumieniu art. 6 ust. 1 lit. b RODO.

Inną podstawą może być art. 6 ust. 1 lit. f RODO, czyli prawnie uzasadniony interes administratora polegający na zapobieganiu nadużyciom, ochronie systemów informatycznych lub minimalizacji ryzyka operacyjnego. W przypadku danych behawioralnych zastosowanie tej podstawy wymaga jednak

przeprowadzenia testu równowagi, uwzględniającego charakter danych, skalę ich przetwarzania oraz stopień ingerencji w sferę prywatności użytkownika. Ze względu na potencjał identyfikacyjny i profilujący danych behawioralnych wynik takiego testu nie zawsze będzie oczywisty. Szczególne znaczenie mają w tym kontekście zakres i ciągłość monitorowania zachowań użytkownika, które mogą prowadzić do tworzenia szczegółowych profili aktywności w środowisku cyfrowym.

Zgoda, o której mowa w art. 6 ust. 1 lit. a RODO, teoretycznie stanowi trzecią możliwą podstawę przetwarzania danych behawioralnych. W praktyce jej zastosowanie napotyka jednak istotne ograniczenia, zwłaszcza w relacjach asymetrycznych, takich jak relacja klient – instytucja finansowa. Wątpliwości budzi w szczególności realność dobrowolności zgody, jeżeli odmowa jej wyrażenia prowadzi do ograniczenia dostępu do kluczowych usług.

Odmierna ocena prawna jest konieczna w sytuacji, w której dane behawioralne spełniają przesłanki uznania ich za dane biometryczne, a więc gdy są przetwarzane przy użyciu szczególnych środków technicznych w celu jednoznacznej identyfikacji lub uwierzytelnienia osoby fizycznej. W takim przypadku zastosowanie znajduje art. 9 ust. 1 RODO, ustanawiający generalny zakaz przetwarzania danych szczególnych kategorii. Zakwalifikowanie danych behawioralnych jako biometrycznych skutkuje koniecznością spełnienia zarówno przesłanki legalności przetwarzania z art. 6 ust. 1 RODO, jak i jednej z dodatkowych przesłanek wskazanych w art. 9 ust. 2 RODO. Samo powołanie się na podstawę z art. 6 RODO nie jest wówczas wystarczające do uznania przetwarzania za zgodne z prawem.

Legalność przetwarzania wymaga wówczas oparcia się na jednej z wyjątkowych podstaw wskazanych w art. 9 ust. 2 RODO. Najczęściej rozważaną podstawą jest wyraźna zgoda osoby, której dane dotyczą¹⁴. Jednak również w tym przypadku pojawia się problem rzeczywistej dobrowolności zgody, zwłaszcza gdy biometria behawioralna stanowi domyślny lub jedyny dostępny mechanizm uwierzytelniania. W określonych przypadkach możliwe jest również powołanie się na przetwarzanie niezbędne ze względów związanych z ważnym interesem publicznym¹⁵, na podstawie prawa Unii lub państwa członkowskiego. Podstawa ta ma jednak charakter wyjątkowy i wymaga wyraźnej podstawy normatywnej, która w odniesieniu do biometrii behawioralnej występuje obecnie jedynie fragmentarycznie. Z kolei art. 9 ust. 2 lit. f RODO, dotyczący dochodzenia lub obrony roszczeń, ma znaczenie marginalne i nie może stanowić podstawy systematycznego przetwarzania danych behawioralnych w celach uwierzytelniania.

Zestawienie powyższych podstaw prawnych pokazuje istotny problem konstrukcyjny w obecnym modelu regulacyjnym. Dane behawioralne, mimo że mogą pełnić funkcję zbliżoną do klasycznych danych biometrycznych, mogą być często kwalifikowane jako „zwykłe” dane osobowe, co pozwala na ich przetwarzanie bez podwyższonego reżimu ochronnego. Zjawisko to bywa określone jako tzw. ukryta biometria, polegająca na wykorzystywaniu systemów analizy zachowań, które w praktyce umożliwiają identyfikację użytkownika, lecz formalnie są kwalifikowane jako

¹⁴ Zob. art. 9 ust. 2 lit. a RODO.

¹⁵ Zob. art. 9 ust. 2 lit. g RODO.

narzędzia analizy ryzyka lub monitorowania bezpieczeństwa¹⁶. W takich przypadkach formalna kwalifikacja systemu jako narzędzia analizy zachowań nie powinna przesłaniać jego rzeczywistej funkcji identyfikacyjnej, gdyż mogłoby to prowadzić do funkcjonalnego obejścia reżimu ochronnego przewidzianego w art. 9 RODO.

Mechanizmy oparte na biometrii behawioralnej mogą również prowadzić do ciągłego monitorowania aktywności użytkownika pod pozorem zapewniania bezpieczeństwa systemów informatycznych. W takich sytuacjach zakres i intensywność przetwarzania danych mogą pozostawać w napięciu z zasadami minimalizacji danych oraz proporcjonalności określonymi w art. 5 RODO, zwłaszcza gdy użytkownik nie posiada realnej możliwości wyboru alternatywnej metody uwierzytelniania lub ograniczenia zakresu monitorowania.

W konsekwencji poziom ochrony prawnej osoby, której dane dotyczą, może zależeć nie od stopnia ingerencji w jej sferę prywatności, lecz od przyjęcia przez administratora kwalifikacji prawnej danych. Szczególne znaczenie ma to w sektorach regulowanych, takich jak bankowość, gdzie użytkownik często może nie mieć realnej możliwości wyboru alternatywnej metody uwierzytelniania. W takich przypadkach zastosowanie łagodniejszych podstaw prawnych może prowadzić do osłabienia standardów ochrony danych osobowych oraz naruszenia zasady minimalizacji i proporcjonalności.

5. Dane behawioralne w procesach uwierzytelniania

Sektor bankowy należy do obszarów, w których technologie oparte na analizie danych behawioralnych znalazły najszerze zastosowanie. Wynika to z rosnącej skali zagrożeń związanych z nadużyciami finansowymi, rozwojem bankowości elektronicznej oraz wymogów regulacyjnych dotyczących bezpieczeństwa transakcji, w szczególności obowiązku stosowania silnego uwierzytelniania klienta. Są wykorzystywane zarówno jako element systemów wykrywania nadużyć, jak i jako narzędzie wspierające lub zastępujące tradycyjne mechanizmy uwierzytelniania¹⁷. W praktyce bankowej służą przede wszystkim do oceny zgodności aktualnych zachowań użytkownika z wcześniej zidentyfikowanym profilem behawioralnym. W przypadku wykrycia istotnych odchyśleń od wzorca system może zainicjować dodatkowe mechanizmy weryfikacyjne, ograniczyć dostęp do usług lub oznaczyć transakcję jako potencjalnie podejrzaną¹⁸. Szczególne znaczenie ma wykorzystanie danych behawioralnych w kontekście ciągłego uwierzytelniania; rozwiązania te pozwalają na zwiększenie poziomu bezpieczeństwa bez konieczności każdorazowego angażowania użytkownika

w aktywne czynności uwierzytelniające. Jednocześnie jednak prowadzą do stałego monitorowania zachowań klienta, co rodzi pytania o proporcjonalność takiego przetwarzania oraz zakres informacji faktycznie niezbędnych do osiągnięcia celu¹⁹.

Poza sektorem bankowym dane behawioralne są coraz częściej wykorzystywane w obszarach takich jak administracja publiczna, ochrona zdrowia, platformy cyfrowe czy handel elektroniczny. W e-administracji mogą wspierać procesy uwierzytelniania użytkowników korzystających z usług publicznych online, zwłaszcza w kontekście zdalnego dostępu do wrażliwych danych. W sektorze ochrony zdrowia bywają wykorzystywane do zabezpieczenia systemów telemedycznych oraz kontroli dostępu do dokumentacji medycznej. Na platformach cyfrowych oraz w e-commerce dane behawioralne są stosowane zarówno w celach bezpieczeństwa, jak i w procesach personalizacji oraz profilowania użytkowników²⁰. Granica pomiędzy uwierzytelnianiem a innymi formami analizy zachowań bywa w takich przypadkach nieostra, co zwiększa ryzyko rozszerzenia zakresu przetwarzania poza pierwotnie deklarowane cele. Z perspektywy prawa ochrony danych osobowych istotne jest zatem precyzyjne określenie celu przetwarzania oraz zapewnienie, aby dane behawioralne nie były wykorzystywane w sposób niezgodny z zasadą ograniczenia celu.

Zastosowanie danych behawioralnych w procesach uwierzytelniania wiąże się z wieloma konsekwencjami prawnymi i regulacyjnymi. Przetwarzanie wymaga spełnienia wymogów wynikających z zasad ogólnych RODO, w szczególności zasady minimalizacji danych²¹, przejrzystości²² oraz rozliczalności²³. Administratorzy powinni być w stanie wykazać, że zakres i intensywność przetwarzania danych behawioralnych są adekwatne do realizowanego celu oraz że nie istnieją mniej inwazyjne środki pozwalające osiągnąć porównywalny poziom bezpieczeństwa. Stosowanie danych behawioralnych w charakterze mechanizmu uwierzytelniania może rodzić obowiązek przeprowadzenia oceny skutków dla ochrony danych, zwłaszcza gdy przetwarzanie ma charakter systematyczny, na dużą skalę i dotyczy monitorowania zachowań osób fizycznych²⁴. Obowiązek ten jest szczególnie istotny w sektorach regulowanych, gdzie przetwarzanie danych behawioralnych może prowadzić do daleko idących konsekwencji dla sytuacji prawnej użytkownika. Praktyka zastępowania lub uzupełniania klasycznych metod uwierzytelniania rozwiązaniami behawioralnymi wymaga krytycznej oceny z punktu widzenia zasady równego traktowania i niedyskryminacji. Modele behawioralne mogą różnie klasyfikować zachowania użytkowników, w zależności od ich cech indywidualnych, stanu zdrowia czy sposobu korzystania z technologii²⁵. Ma to szczególne znaczenie w kontekście

16 G. Orrù, A. Rattani, I. Rida, S. Marcel, *Recent advances in behavioral and hidden biometrics for personal identification*, „Pattern Recognition Letters” 2021/185, s. 108–109.

17 P. Kałużny, P. Stolarski, *Biometria behawioralna i „tradycyjna” w mobilnych usługach bankowych – stan oraz przyszłe możliwości zastosowania*, „Bezpieczny Bank” 2019/1(74), s. 139–161.

18 A. Biger-Levin, *What is behavioral biometrics?*, Bio Catch, <https://www.biocatch.com/blog/what-is-behavioral-biometrics> (dostęp: 29.01.2026 r.) – instytucje finansowe stoją przed wyzwaniem pogodzenia innowacji w kanałach cyfrowych i poprawy doświadczenia klienta z koniecznością skutecznego zarządzania ryzykiem nadużyć; dane behawioralne stanowią skuteczne narzędzie ochrony sesji cyfrowych, pozwalając równocześnie wspierać rozwój usług cyfrowych i minimalizować ryzyko oszustw.

19 M. Anderson, S. Reynolds, J. Carter, O. Bennett, C. Paul, *AI-Powered Behavioral Biometrics for Zero Trust Authentication*, September 2025 – dodatkowymi wyzwaniami są ryzyko *biasu* (stronniczości) z powodu niereprezentatywnych danych treningowych, potrzeba przejrzystych polityk zarządzania danymi, konieczność stosowania technik prywatności (*federated learning, differential privacy*), wysokie wymagania obliczeniowe i trudności integracyjne z istniejącymi systemami i politykami dostępu.

20 Z. Zhang, H. Yin, S.X. Rao i in., *Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights*, „Data Science and Engineering” 2025/10, s. 24–39.

21 Zob. art. 5 ust. 1 lit. c RODO.

22 Zob. art. 5 ust. 1 lit. a RODO.

23 Zob. art. 5 ust. 2 RODO.

24 Zob. art. 35 RODO.

25 C. Wendehorst, Y. Duller, *Biometric Recognition...*, s. 50–52.

rosnącej automatyzacji procesów decyzyjnych i wykorzystania algorytmów w systemach bezpieczeństwa. W sytuacjach, w których system uwierzytelniania prowadzi do automatycznego blokowania dostępu do usługi, odmowy realizacji transakcji lub zakwalifikowania użytkownika jako podmiotu wysokiego ryzyka bez udziału człowieka, może powstać pytanie o zastosowanie art. 22 RODO dotyczącego decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych.

6. Dane behawioralne jako potencjalny substytut klasycznej biometrii

Z perspektywy technologicznej biometria behawioralna oferuje wiele cech, które czynią ją atrakcyjną w kontekście projektowania systemów bezpieczeństwa²⁶. W przeciwieństwie do „twardych” danych biometrycznych nie wymaga ona specjalistycznych urządzeń ani aktywnego zaangażowania użytkownika w proces identyfikacji, co pozwala na jej integrację z istniejącymi systemami informatycznymi. Istotnym argumentem przemawiającym za wykorzystywaniem danych behawioralnych jest ich ciągły charakter. Podczas gdy klasyczne dane biometryczne są zazwyczaj wykorzystywane w ramach jednorazowego aktu uwierzytelniania, dane behawioralne umożliwiają stałą weryfikację tożsamości użytkownika w trakcie całej sesji. Pozwala to na wykrywanie przejęcia konta lub innych anomalii w czasie rzeczywistym, bez konieczności ponownego inicjowania procesu logowania. Z technologicznego punktu widzenia dane behawioralne bywają również postrzegane jako trudniejsze do podrobienia lub przejęcia, ponieważ opierają się na złożonych i dynamicznych wzorcach zachowań, a nie na pojedynczym identyfikatorze. Jednocześnie ich wykorzystanie może być przedstawiane jako mniej inwazyjne dla prywatności użytkownika, ponieważ nie wiąże się z przetwarzaniem fizycznych danych biometrycznych.

Z perspektywy prawnej biometria behawioralna może być przedstawiana jako rozwiązanie pozwalające na osiągnięcie porównywalnego poziomu bezpieczeństwa przy zastosowaniu łagodniejszego reżimu ochronnego. Jeżeli dane behawioralne nie zostaną zakwalifikowane jako dane biometryczne w rozumieniu art. 4 pkt 14 RODO, możliwe staje się ich przetwarzanie na podstawach przewidzianych w art. 6 RODO, bez konieczności spełnienia rygorystycznych warunków wynikających z art. 9 RODO. Funkcjonalne podobieństwo danych behawioralnych i klasycznych danych biometrycznych, polegające na odgrywaniu przez nie analogicznej roli identyfikacyjnej lub uwierzytelniającej, podważa zasadność różnicowania poziomu ochrony wyłącznie na podstawie technicznej charakterystyki danych²⁷. Jeżeli dane behawioralne umożliwiają jednoznaczną identyfikację osoby fizycznej, to brak objęcia ich reżimem art. 9 RODO może prowadzić do osłabienia ochrony prawnej jednostki. Problem ten nabiera szczególnego znaczenia w kontekście zasady proporcjonalności oraz równości ochrony danych osobowych. Różnicowanie standardów ochrony wyłącznie ze względu na formalną kwalifikację danych może prowadzić do niespójności systemowych.

Sytuacja w której, biometria behawioralna może pełnić funkcję substytutu klasycznej biometrii, bez jednoczesnego poddania jej odpowiadającemu jej reżimowi ochronnemu, stwarza ryzyko tzw. *regulatory arbitrage*, polegającego na wyborze rozwiązań technologicznych nie ze względu na ich rzeczywistą inwazyjność, lecz na możliwość zastosowania wobec nich łagodniejszych wymogów prawnych²⁸. Ryzyko jest szczególnie widoczne w sektorach, w których stosowanie biometrii klasycznej napotyka istotne bariery prawne lub społeczne. W takich przypadkach dane behawioralne mogą być wykorzystywane jako alternatywa pozwalająca na osiągnięcie podobnych efektów przy mniejszym obciążeniu regulacyjnym. Prowadzi to do sytuacji, w której ochrona danych osobowych staje się pochodną przyjętej architektury systemu, a nie rzeczywistego wpływu przetwarzania na prawa i wolności jednostki.

7. Konsekwencje systemowe dla ochrony praw podstawowych jednostki

Upowszechnienie przetwarzania danych behawioralnych w celach identyfikacyjnych i uwierzytelniających rodzi konsekwencje systemowe dla ochrony praw podstawowych jednostki, w szczególności prawa do prywatności oraz prawa do ochrony danych osobowych, gwarantowanych w art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej²⁹. Kluczowym problemem jest stopień przejrzystości przetwarzania danych behawioralnych. Ze względu na złożoność algorytmów i probabilistyczny charakter analizy zachowań, osoba, której dane dotyczą, może mieć ograniczoną świadomość zarówno zakresu przetwarzania, jak i jego rzeczywistych konsekwencji. Utrudnia to skuteczne korzystanie z praw informacyjnych oraz prawa kontroli przewidzianych w RODO, takich jak prawo dostępu do danych czy prawo sprzeciwu wobec przetwarzania. Szczególne znaczenie ma również wpływ na autonomię jednostki; przetwarzanie o charakterze ciągłym, polegające na nieustannej analizie zachowań użytkownika, może prowadzić do efektu stałego monitorowania, który wykracza poza klasyczne modele identyfikacji oparte na jednorazowym uwierzytelnianiu. Taki model przetwarzania sprzyja normalizacji nadzoru i może wpływać na sposób korzystania z usług cyfrowych, ograniczając swobodę zachowania użytkownika w środowisku cyfrowym³⁰.

Istotne jest również ryzyko związane z profilowaniem oraz automatyzacją decyzji. Dane behawioralne ze względu na swoją granularność³¹ i kontekstowość umożliwiają tworzenie bardzo szczegółowych profili użytkowników, które mogą być wykorzystywane nie tylko do celów bezpieczeństwa, lecz także do oceny wiarygodności, ryzyka czy przewidywania przyszłych zachowań. W sektorach regulowanych, takich jak bankowość, konsekwencje takich ocen mogą mieć bezpośredni wpływ na sytuację prawną

26 P. Chandre, S. Joshi, R. Rathod, J. Nandimath, B. Shendkar, Y. Nikam, *Beyond Passwords: Enhancing Security with Continuous Behavioral Biometrics and Passive Authentication* [w:] *Demystifying AI and ML for Cyber-Threat Intelligence. Information Systems Engineering and Management*, red. M. Yang, S.N. Mohanty, S. Satpathy, S. Hu, Cham 2025, s. 161–173.

27 C. Wendehorst, Y. Duller, *Biometric Recognition...*, s. 20–22.

28 E. Pollman, *Tech, Regulatory Arbitrage, and Limits*, „European Business Organization Law Review” 2019/20(3), s. 7–10.

29 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389 – dalej KPP.

30 G.G. Fuster, M.N. Peeters, *Person identification, human rights and ethical principles – Rethinking biometrics in the era of artificial intelligence*, Brussels 2021, s. 6–8.

31 S. Somepalli, D. Siramgari, *Unveiling the Power of Granular Data: Enhancing Holistic Analysis in Utility Management*, „International Journal of Intelligent Systems and Applications in Engineering” 2020/8(4), s. 284–289 – granularność danych oznacza poziom szczegółowości, z jakim dane są rejestrowane i analizowane; im wyższa granularność, tym bardziej szczegółowe i drobne jednostki informacji, co umożliwia tworzenie precyzyjnych profili użytkowników.

i ekonomiczną jednostki³². Istnieje również ryzyko dyskryminacji pośredniej. Modele behawioralne oparte na danych historycznych i statystycznych mogą różnie klasyfikować zachowania użytkowników w zależności od ich cech indywidualnych, takich jak wiek, stan zdrowia, poziom sprawczości czy sposób korzystania z technologii. W rezultacie osoby odbiegające od przyjętego „wzorca” behawioralnego mogą być częściej poddawane dodatkowym weryfikacjom lub ograniczeniom, co rodzi pytanie o zgodność z zasadą równego traktowania³³.

Z perspektywy systemowej problematyczne jest rozmycie granic pomiędzy danymi osobowymi a danymi szczególnych kategorii. Sytuacja, w której dane behawioralne, pełniące funkcję zbliżoną do biometrii, nie są konsekwentnie obejmowane podwyższonym reżimem ochronnym, może prowadzić do erozji standardów ochrony danych osobowych. Ochrona praw podstawowych staje się wówczas zależna od przyjętej przez administratora architektury technologicznej, a nie od rzeczywistej intensywności ingerencji w sferę prywatności. Przetwarzanie danych behawioralnych wymaga szczególnej ostrożności regulacyjnej oraz interpretacyjnej. Skala potencjalnych zagrożeń dla praw i wolności jednostki uzasadnia potrzebę bardziej spójnego i funkcjonalnego podejścia do kwalifikacji tych danych oraz określenia standardów ich dopuszczalnego wykorzystania.

8. Wnioski

Przeprowadzona analiza aspektów prawnych i technicznych prowadzi do następujących wniosków. Dane behawioralne, ze względu na swój charakter oraz funkcję pełnioną w nowoczesnych systemach informatycznych, co do zasady mieszczą się w zakresie pojęcia danych osobowych w rozumieniu art. 4 pkt 1 RODO. Ich przetwarzanie zazwyczaj umożliwia identyfikację lub co najmniej możliwość identyfikacji osoby fizycznej, niezależnie od tego, czy identyfikacja ma charakter bezpośredni, czy pośredni. Brak jest podstaw do generalnego wyłączenia danych behawioralnych spod reżimu ochrony danych osobowych.

Kluczowe znaczenie dla kwalifikacji prawnej danych behawioralnych ma analiza funkcjonalna. W sytuacjach, gdy dane te są wykorzystywane przy użyciu szczególnych środków technicznych w celu jednoznacznej identyfikacji lub uwierzytelniania osoby fizycznej, mogą one spełniać przesłanki uznania za dane biometryczne w rozumieniu art. 4 pkt 14 RODO. W takich przypadkach zastosowanie znajduje podwyższony reżim ochronny przewidziany w art. 9 RODO, niezależnie od ich niematerialnego i dynamicznego charakteru.

Obowiązujące ramy prawne pozostawiają istotny margines niepewności interpretacyjnej, w szczególności w zakresie odróżnienia danych behawioralnych wykorzystywanych w celach analitycznych od danych pełniących funkcję biometryczną. Brak jednoznacznych kryteriów sprzyja rozbieżnościom w praktyce stosowania prawa i może prowadzić do kwalifikowania danych w sposób umożliwiający zastosowanie łagodniejszych podstaw przetwarzania, co rodzi ryzyko osłabienia ochrony przewidzianej dla szczególnych kategorii danych.

Zasadne jest doprecyzowanie standardów dotyczących danych behawioralnych na poziomie unijnym, w szczególności poprzez wyraźne odniesienie do nich w aktach *soft law* lub przyszłych regulacjach sektorowych. Pożądane byłoby przyjęcie podejścia

funkcjonalnego, w którym decydujące znaczenie mają cel i skutek przetwarzania, a nie wyłącznie techniczna natura danych, co pozwoliłoby zapewnić spójny poziom ochrony wszystkich form biometrii.

Niezależnie od ewentualnych zmian legislacyjnych konieczne jest wzmocnienie standardów praktyki stosowania prawa, zwłaszcza w zakresie oceny skutków dla ochrony danych oraz realizacji zasady *privacy by design*³⁴. W przypadku systemów opartych na danych behawioralnych ocena ta powinna obejmować nie tylko ryzyka techniczne, lecz także długofalowe konsekwencje systemowe dla praw i wolności jednostki, tak aby zapewnić spójność systemu ochrony danych w warunkach dynamicznego rozwoju technologii.

Abstract

Julia Rak

Specialist in the International Cooperation Department,
Personal Data Protection Office, Poland
(ORCID: <https://orcid.org/0009-0000-5855-264X>).

Behavioural Data as Personal Data under EU Law – Legal Classification, Processing Standards and Application in Authentication Processes

Keywords: behavioural data, behavioural biometry, biometric data, personal data, personal data protection, GDPR, authentication

The article presents an analysis of the issue of legal classification of behavioural data in the light of EU law, in particular 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). The dynamic development of technologies based on user behaviour analysis is leading to the increasingly common processing of behavioural data for identification and authentication purposes, including in the banking, public administration, healthcare or social media sectors. The analysis conducted in this article shows that behavioural data in general meet the criteria for recognising them as personal data, and in certain functional configurations, can also constitute biometric data within the meaning of Article 4(14) GDPR. The comparative analysis of the processing standards for behavioural data and classic “hard” biometric data reveals both similarities in their identification function and differences in the normative classification method. The article focuses especially on the legal basis for the processing of behavioural data, including the limits of consent, contract and the controller’s legitimate interest, as well as the risk of evading the regime of Article 9 GDPR by replacing classic biometric data with behavioural data. An analysis of examples of behavioural biometrics application in authentication processes, including in the banking sector, shows the systemic implications for the protection of fundamental rights of an individual, in particular the right to the protection of personal data and privacy. The conclusions point to the need for clarifying the legal standards for the processing of behavioural data in EU law.

The views and opinions expressed are those of the author.

32 W. Macierzyński, M. Macierzyński, *Using Behavioral Biometrics in the Context of Cybersecurity of Polish Banking Sector (2019–2024)*, „Journal of Finance and Financial Law” 2025/3(47), s. 103–128.

33 Motyw 71 RODO.

34 Pojęcie *privacy by design* zostało wprowadzone w art. 25 RODO, który nakłada na administratorów obowiązek uwzględniania ochrony danych już na etapie projektowania systemów i procesów.

Bibliografia/References

- Anderson M., Reynolds S., Carter J., Bennett O., Paul C., *AI-Powered Behavioral Biometrics for Zero Trust Authentication*, September 2025.
- Baig A.F., Eskeland S., Yang B., *Privacy-preserving continuous authentication using behavioral biometrics*, „International Journal of Information Security” 2023/22.
- Biger-Levin A., *What is behavioral biometrics?*, Bio Catch, <https://www.biocatch.com/blog/what-is-behavioral-biometrics> (dostęp: 29.01.2026 r.).
- Chandre P., Joshi S., Rathod R., Nandimath J., Shendkar B., Nikam Y., *Beyond Passwords: Enhancing Security with Continuous Behavioral Biometrics and Passive Authentication* [w:] *Demystifying AI and ML for Cyber-Threat Intelligence. Information Systems Engineering and Management*, red. M. Yang, S.N. Mohanty, S. Satpathy, S. Hu, Cham 2025.
- Fuster G.G., Peeters M.N., *Person identification, human rights and ethical principles – Rethinking biometrics in the era of artificial intelligence*, Brussels 2021.
- Gałęzowska K., *Dane biometryczne a dane behawioralne*, „Monitor Prawniczy” 2022/21.
- Kałużny P., Stolarski P., *Biometria behawioralna i „tradycyjna” w mobilnych usługach bankowych – stan oraz przyszłe możliwości zastosowania*, „Bezpieczny Bank” 2019/1(74).
- Macierzyński W., Macierzyński M., *Using Behavioral Biometrics in the Context of Cybersecurity of Polish Banking Sector (2019–2024)*, „Journal of Finance and Financial Law” 2025/3(47).
- Mahfouz A., Mahmoud T.M., Eldin A.S., *A survey on behavioral biometric authentication on smartphones*, „Journal of Information Security and Applications” 2017/37.
- Second Generation Biometrics: The Ethical, Legal and Social Context*, red. E. Mordini, D. Tzovaras, Dordrecht 2012.
- Orrù G., Rattani A., Rida I., Marcel S., *Recent advances in behavioral and hidden biometrics for personal identification*, „Pattern Recognition Letters” 2024/185.
- Özal M., *‘Behavioral Biometrics’: A Brief Introduction from the Perspective of Data Protection Law*, December 2020, <https://www.law.kuleuven.be/citip/blog/behavioral-biometrics-a-brief-introduction-from-the-perspective-of-data-protection-law/> (dostęp: 29.01.2026 r.).
- Pollman E., *Tech, Regulatory Arbitrage, and Limits*, „European Business Organization Law Review” 2019/20(3).
- Somepalli S., Siramgari D., *Unveiling the Power of Granular Data: Enhancing Holistic Analysis in Utility Management*, „International Journal of Intelligent Systems and Applications in Engineering” 2020/8(4).
- Wendehorst C., Duller Y., *Biometric Recognition and Behavioural Detection. Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces*, Brussels 2021.
- Zhang Z., Yin H., Rao S.X. i in., *Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights*, „Data Science and Engineering” 2025/10.

REKLAMA



TOŻSAMOŚĆ KONSTYTUCYJNA W WYBRANYCH PAŃSTWACH CZŁONKOWSKICH UNII EUROPEJSKIEJ

Cena: 99 zł

redakcja naukowa Andrzej Wróbel, Michał Ziółkowski

Kamila Doktor-Bindas, Dominika Ewa Harasimiuk
Szymon Pawłowski, Jarosław Sułkowski, Michał Ziółkowski

JAK PAŃSTWA UE CHRONIĄ TOŻSAMOŚĆ KONSTYTUCYJNĄ?

- Publikacja prezentuje **różne sposoby rozumienia tożsamości konstytucyjnej** przez sądy konstytucyjne w Unii Europejskiej.
- Autorzy analizują koncepcje ochrony tej tożsamości w wybranych państwach członkowskich (Niemcy, Francja, Czechy, Austria, Hiszpania, Włochy), a także przywołują ich cechy wspólne i różniące.
- Przedstawiono rozważania na temat podstaw prawnych tożsamości konstytucyjnej oraz inspiracji i **odniesień istotnych dla Trybunału Konstytucyjnego** w sprawie konstytucyjności przepisów Traktatu z Lizbony.

ZAMÓW KSIĄŻKĘ Z RABATEM 20% W KSIĘGARNI PROFINFO.PL
W FORMULARZU ZAMÓWIENIA WPISZ KOD: WKCZA20