REDAKCJA
MAŁGORZATA BUDNIK-MINIERSKA
PAWEŁ FALENTA
DAWID KOBYLAŃSKI

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI, NEUROBLASTOMA, PROPOZYCJA ZASTOSOWANIA MODELI UCZENIA MASZYNOWEGO - MEDYCYNA, EKONOMIA/BANKOWOŚĆ, NAUKI HUMANISTYCZNE

ARCHAEGRAPH
*Wydawnictwo Naukowe*

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI, NEUROBLASTOMA, PROPOZYCJA ZASTOSOWANIA MODELI UCZENIA MASZYNOWEGO
-
# MEDYCYNA, EKONOMIA/BANKOWOŚĆ, NAUKI HUMANISTYCZNE


Redakcja naukowa

MAŁGORZATA BUDNIK-MINIERSKA
PAWEŁ FALENTA
DAWID KOBYLAŃSKI

REDAKCJA
MAŁGORZATA BUDNIK-MINIERSKA
PAWEŁ FALENTA
DAWID KOBYLAŃSKI

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI, NEUROBLASTOMA, PROPOZYCJA ZASTOSOWANIA MODELI UCZENIA MASZYNOWEGO – MEDYCYNA, EKONOMIA/BANKOWOŚĆ, NAUKI HUMANISTYCZNE

ARCHAEGRAPH
*Wydawnictwo Naukowe*

REDAKCJA NAUKOWA

PRZEWODNICZĄCA KOMITETU NAUKOWEGO:
MGR MAŁGORZATA BUDNIK-MINIERSKA

WICEPRZEWODNICZĄCY KOMITETU NAUKOWEGO:
DR PAWEŁ FALENTA

WICEPRZEWODNICZĄCY KOMITETU REDAKCYJNEGO:
DAWID KOBYLAŃSKI

SEKRETARZ KOMITETU REDAKCYJNEGO:
RAFAŁ STACHYRA

REDAKCJA TECHNICZNA

MGR INŻ. RAFAŁ MINIERSKI
MGR ANETA JURSKA-GAWRYSIAK
DR MAŁGORZATA JEZIORSKA
DR DAWID PIETRAS
LEK. MAGDALENA KĘDZIORA

RECENZJA

DR JUSTYNA JASIAK
DR INŻ. RAFAŁ ŚPIEWAK

KOREKTA REDAKTORSKA, SKŁAD I PROJEKT OKŁADKI

KAROL ŁUKOMIAK



ISBN: 978-83-67527-97-2

WERSJA ELEKTRONICZNA DOSTĘPNA NA STRONIE INTERNETOWEJ WYDAWCY:
www.archaegraph.pl

ARCHAEGRAPH
*Wydawnictwo Naukowe*

ŁÓDŹ, WRZESIEŃ 2023

# SPIS TREŚCI

# PRZEDMOWA

Niniejszym przedstawiamy Państwu monografię naukową zatytułowaną *INNOWACYJNE PODEJŚCIE PŁATNOŚCI, NEUROBLASTOMA, PROPOZYCJA ZASTOSOWANIA MODELI UCZENIA MASZYNOWEGO - MEDYCYNA, EKONOMIA/BANKOWOŚĆ, NAUKI HUMANISTYCZNE,* w której znajdą Państwo pięć autorskich rozdziałów młodych adeptów nauki.

Pierwszą część monografii otwierają trzy rozdziały autorstwa Pawła Głaz. W pierwszym rozdziale monografii pt. *Innowacyjne podejście płatności część 1- technologie i trendy w płatnościach mobilnych* autor skupia się na analizie najnowszych technologii i trendów w obszarze płatności, ukazując ich wpływ na codzienne operacje finansowe. W drugim rozdziale monografii pt. *Innowacyjne podejście płatności część 2- bezpieczeństwo płatności elektronicznych: wyzwania i rozwiązania* autor tekstu skupia się na omówieniu kluczowych wyzwań, jakie stają przed bezpieczeństwem płatności elektronicznych oraz prezentuje innowacyjne rozwiązania mające na celu ochronę użytkowników przed cyberzagrożeniami. Natomiast w trzecim rozdziale ostatniej części monografii pt. *Innowacyjne podejście płatności część 3- fintechowa rewolucja w świecie finansów* autor skupia się na istocie samego ruchu FinTech oraz jego rozwoju w polskim kontekście, z uwzględnieniem determinant wpływających na jego dalszą ekspansję.

Celem kolejnego rozdziału autorstwa Marceliny Wacławskiej, Moniki Wacławskiej, Natalii Tyszczuk oraz Huberta Rogala pt. *Neuroblastoma – aktualne doniesienia dotyczące diagnostyki i leczenia* jest przegląd aktualnych badań nad leczeniem i diagnostyką nerwiaka niedojrzałego.

W ostatnim rozdziale monografii autorstwa Grzegorza Gucwa pt. *Propozycja zastosowania modeli uczenia maszynowego w analizie źródeł historycznych* autor postuluje wykorzystywanie modeli uczenia maszynowego w celu przetwarzania źródeł oraz analizy ich treści w ramach ich zbiorów.

W imieniu Komitetu Redakcyjnego niniejszego tomu, pragniemy podziękować wszystkim osobom zaangażowanym w proces jego wydania, w tym m.in. wydawnictwu, recenzentom oraz autorom.

REDAKCJA NAUKOWA:

MGR MAŁGORZATA BUDNIK-MINIERSK,
DR PAWEŁ FALENTA
DAWID KOBYLAŃSKI

**PAWEŁ GŁAZ**
UNIWERSYTET RZESZOWSKI

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI CZĘŚĆ 1- TECHNOLOGIE I TRENDY W PŁATNOŚCIACH MOBILNYCH

**Streszczenie**: W dzisiejszym dynamicznym środowisku finansowym, innowacje w płatnościach odgrywają kluczową rolę w przekształcaniu sposobu, w jaki dokonujemy transakcji. Ten tekst skupia się na analizie najnowszych technologii i trendów w obszarze płatności, ukazując ich wpływ na codzienne operacje finansowe. Poprzez dokładną analizę, praca prezentuje ewolucję od tradycyjnych metod płatności do rozwiniętych systemów opartych na cyfrowości i automatyzacji. W pracy omawiane są płatności mobilne, portfele cyfrowe, technologia blockchain oraz kryptowaluty, a także ich rosnąca rola w globalnej gospodarce. Ponadto, esej zgłębia konsekwencje zastosowania tych technologii dla użytkowników oraz przedsiębiorstw.

**Słowa kluczowe***:* blockchain, kryptowaluty, bitcoin, portfele cyfrowe, BLIK

## WPROWADZENIE

W miarę jak świat przechodzi przez cyfrową rewolucję, systemy płatności nie pozostają w tyle. Dynamiczny postęp technologiczny przyczynia się do powstawania innowacyjnych rozwiązań, które wywracają tradycyjne modele płatności do góry nogami. Od technologii blockchain i cyfrowych walut po płatności mobilne i kryptowaluty, zmiany w dziedzinie płatności rewolucjonizują nasz sposób dokonywania transakcji i oddziałują na cały ekosystem finansowy. Niniejszy rozdział skupia się na przeglądzie najnowszych innowacji w dziedzinie płatności, w tym roli technologii blockchain, płatności mobilnych, cyfrowych portfeli oraz kryptowalut. Przedstawiono zalety i korzyści

wynikające z tych technologii oraz omówione, w jaki sposób wpływają one na codzienne życie finansowe. Pierwszym etapem jest analiza technologii blockchain, która stała się fundamentem dla wielu innowacji w płatnościach. Ponadto wyjaśniono jak blockchain działa jako niezmienna i bezpieczna księga rozliczeń, zdolna do rewolucjonizowania sposobu, w jaki przekazywana jest wartość między stronami transakcji. Następnie omówiono dynamiczny rozwój płatności mobilnych i aplikacji portfeli cyfrowych, które umożliwiają płatności bezgotówkowe za pomocą smartfonów i urządzeń mobilnych. Przywołane zostały przykłady popularnych rozwiązań mobilnych i ich rosnące znaczenie w codziennych transakcjach. W kolejnym etapie przedstawiony został fenomen kryptowalut jako nowej formy płatności i środka wymiany. Praca prezentuje zalety i wyzwania płynące z wykorzystania kryptowalut oraz ich potencjalny wpływ na tradycyjne systemy finansowe. Rozdział ten jest próbą ukazania, w jaki sposób nowe technologie i trendy rewolucjonizują systemy płatności. Wyjaśnia, jakie korzyści płyną z tych innowacji, a także jakie wyzwania mogą wyniknąć w procesie adaptacji do nowych rozwiązań. Ostatecznym celem tego artykułu jest dostarczenie czytelnikowi wglądu w przyszłość płatności, która obiecuje jeszcze większą wygodę, bezpieczeństwo i dostępność w naszym globalnym społeczeństwie cyfrowym.

## ROLA I ZNACZENIE TECHNOLOGII BLOCKCHAIN

Aby możliwe było omawianie roli i znaczenia technologii blockchain, koniecznym jest usystematyzowanie wiedzy na ten temat. Blockchain jest technologią służącą do gromadzenia i przechowywania danych w sposób bezpieczny, rozproszony oraz transparentny. Upraszczając jest to rozproszona baza danych, zawierająca ciągle rosnącą ilość informacji (rekordów) pogrupowanych w bloki i powiązanych ze sobą w taki sposób, aby każdy następujący po sobie blok zawierał oznaczenie czasu (timestamp), kiedy został on stworzony. Baza danych zwiera również odnośnik w postaci linku do poprzedzającego go bloku, będący zaszyfrowanym „streszczeniem" (hash) jego zawartości (Piech 2018, s. 5). Ze względu na to, iż poszczególny blok transakcji zawiera odwołanie do poprzedniego bloku, nie istnieje możliwość, aby wprowadzić zmiany transakcji zawartej wcześniej w jakimś bloku, nie modyfikując wszystkich występujących po nim bloków. Właśnie w taki sposób tworzy się nierozerwalny łańcuch bloków danych, nazywanych blockchainem, dzięki temu niewykonalne jest dokonanie zmiany zapisów historycznych bez dokonania zmiany całej historii transakcji (Piech 2018, s.5).

Nad bezpieczeństwem transakcji kryptowalut czuwa rozwiązanie opierające się na „Proof of work" (z ang. Dowód pracy), który wymagany jest do zatwierdzenia bloku transakcji (Piech 2018, s. 6). Mechanizm konsensusu Proof of Work (PoW) jest do tej pory najszerzej wdrożonym mechanizmem stosowanym w istniejących blokach. Został on wprowadzony za pośrednictwem Bitcoina, zakładając, iż każdy „peer" (z ang. Uczestnik, komputer bądź węzeł danych w systemie) głosuje posiadaną przez siebie „mocą obliczeniową" wykorzystując rozwiązywanie przypadków pracy i tworząc odpowiednie bloki (Gervais i in. 2016, s.2). W rzeczywistości mechanizm Proof of Work skupia się na rozwiązaniu zadania matematycznego, które w swojej istocie jest skomplikowane do wykonania, lecz łatwe do sprawdzenia. „Miners" (z ang. Górnicy), konkurują pomiędzy sobą, aby jako pierwsi odnaleźć odpowiednią wartość nazywaną „nonce", która po połączeniu z zawartością nowego bloku da rezultat o określonym wzorze „hash", spełniającym pewne kryteria. Znalezienie tej wartości wymaga wielokrotnego testowania różnorakich kombinacji, wymagając znaczących mocy obliczeniowych. W momencie, gdy „miner" odnajdzie wartość „nonce", a co za tym idzie wygeneruje poprawny „hash", potwierdza wykonanie pracy obliczeniowej. Następnie zostaje wysłany nowy blok w celu weryfikacji wykorzystując inne węzły. Dzięki temu pozostałe węzły działające w sieci w łatwy sposób mogą zweryfikować czy zawarte w pracy transakcje zostały wykonane w sposób poprawny, obliczając hash bloku i sprawdzając czy nie zostały już wydane. Za poprawne wykonanie pracy „górnik" zostaje nagrodzony określoną ilością kryptowaluty (np. bitcoinów) (Rahimpour i in. 2020, s.1).

Pierwsze zastosowanie technologii blockchain miało miejsce w 2009 r. w kryptowalucie bitcoin. Określone jako sposób księgowania wszystkich transakcji nią dokonywanych bez możliwości podwójnego wydania (double spend) tych samych środków (Beck i in. 2016, s.4).

Bitcoin (BTC) jest walutą elektroniczną, działającą w oparciu o wolne oprogramowanie typu peer-to-peer. Jest to model komunikacji w sieci komputerowej, który posiada zdolność łączenia maszyn na całym świecie, przypisując im ten sam poziom uprawnień. Zastosowanie powyższych zasad pozwala na transfer wirtualnej waluty w dowolne miejsce na świecie, zaledwie w kilka sekund. Bitcoin jak wirtualna waluta nie posiada swojego materialnego odpowiednika, autorzy różnych publikacji nazywają ją zbiorem linijek kodu (Piotrowska 2014, s. 279).

Analizowany powyżej blockchain bitcoinowy posiada publiczny charakter, co w praktyce oznacza, iż każdy w sieci może posiadać do niego dostęp czy

wziąć udział w tworzeniu nowych bloków (Houben i Snyers 2018, s. 35-38). Obecnie wyróżnia się trzy podstawowe rodzaje blockchainów (Mazur 2021, s. 5):

1. **Publiczny** - Najbardziej rozpoznawalnym przykładem publicznego blockchaina jest ten, który funkcjonuje w sieci Bitcoina. Główna charakterystyka tego typu blockchaina to możliwość pobierania dowolnych fragmentów lub całej bazy danych przez każdego użytkownika, a także prawo do udostępniania swojej kopii innym węzłom (NOD'om) w sieci,
2. **Prywatny** - Główną funkcją prywatnego blockchaina jest ograniczenie dostępu do wybranej grupy uczestników. Tego rodzaju blockchainy są wykorzystywane, gdy sieć biznesowa zawiera poufne dane lub gdy regulacje prawne zabraniają korzystania z publicznego blockchaina przez każdego. Przykładem blockchaina prywatnego są platformy takie jak R3 Corda lub Hyperledger,
3. **Hybrydowy** - Teoretycznym przykładem blockchaina hybrydowego jest sieć prywatna, która posiada własny protokół konsensusu i mechanizmy kontroli dostępu do rejestru, ale korzysta z blockchaina publicznego w celach rozliczeniowych, potwierdzania istnienia danego stanu w określonym czasie (proof of existence) lub do obsługi kryptowaluty.

Blockchain zapewnia bezpieczeństwo i niezmienność danych dzięki zastosowaniu kryptografii i rozproszonej struktury. Wszystkie transakcje są zapisywane w blokach, które są połączone w łańcuch, co uniemożliwia ich modyfikację lub usunięcie. To sprawia, że transakcje są nie tylko bezpieczne, ale także transparentne, ponieważ wszystkie uczestniczące w płatnościach strony mają dostęp do tych samych danych (Wanat 2019, s. 55). Blockchain umożliwia istnienie cyfrowych walut, znanych jako kryptowaluty. Przykładem jest Bitcoin, który stał się pierwszą i najbardziej znaną kryptowalutą. Cyfrowe waluty są oparte na technologii blockchain, co pozwala na szybkie, bezpieczne i bezpośrednie transakcje między użytkownikami, bez potrzeby pośredników. Cyfrowe waluty stwarzają także możliwość bankowania dla osób, które nie mają dostępu do tradycyjnych usług finansowych (Przygoda 2021, s. 45).

## ROZWÓJ PŁATNOŚCI MOBILNYHCH I APLIKACJI PORTFELI CYFROWYCH

Rozwój płatności mobilnych oraz aplikacji portfeli cyfrowych stał się jednym z najbardziej znaczących trendów w dziedzinie finansów i technologii. Dzięki postępowi technologicznemu i rozwojowi smartfonów, coraz więcej

ludzi korzysta z płatności mobilnych, aby dokonywać transakcji w sposób wygodny, szybki ale również bezpieczny.

Przytoczenie jasno sformowanej definicji mobilnych płatności jest dość problematyczne. Powodem tego jest szerokość rozumienia obszaru mobilnych płatności. Zgodnie z pojęciem podawanym przez Europejski Bank Centralny, mobilnymi płatnościami (m-płatności) nazywamy konkretny rodzaj płatności, przy którym urządzenie przenośne (np. telefon komórkowy) używane jest przynajmniej do zainicjowania polecenia płatności, a potencjalnie również do przekazywania środków pieniężnych. Realnie urządzenie mobilne traktowane jest w tym przypadku jako narzędzie płatności elektronicznej, dzięki wykorzystaniu, którego możliwe jest zrealizowanie płatności w dowolnym miejscu (Kaszubski i Widawski 2012, s. 12).

Pierwsze płatności mobilne, wykorzystujące telefonii komórkowej, pojawiły się w 1997 roku, kiedy to Coca-Cola wraz z Merita Bank uruchomiły automaty. Umożliwiały one klientom zakup napoju, płacąc za niego za pomocą SMS-a. Ta inicjatywa była pionierskim krokiem w wykorzystaniu technologii komórkowych do dokonywania płatności. Na rynku polskim, już w 1999 roku, Wielkopolski Bank Kredytowy zaproponował abonentom sieci Plus GSM usługę informacji o saldzie konta za pośrednictwem wiadomości SMS. To był kolejny krok w rozwoju płatności mobilnych w Polsce. Pojawienie się protokołu WAP (Wireless Application Protocol) w 1998 roku umożliwiło szybki transfer danych i wyświetlanie informacji tekstowych na ekranie telefonu, choć wówczas telefony komórkowe nie były jeszcze smartfonami. WAP Forum, założone przez Ericssona, Motorolę, Nokię i Unwired Planet, odegrało kluczową rolę w standaryzacji tej technologii. W październiku 1999 roku holenderski operator telefonii komórkowej Telfort BV stał się pierwszym, który uruchomił witrynę WAP, umożliwiającą dostęp do informacji przez telefon komórkowy. Pierwszym bankiem w Polsce, który uruchomił witrynę WAP, zapewniającą klientom wgląd do konta, był WBK w 2000 roku, a później dołączył do niego mBank. Mimo że protokół WAP 2.0 został wydany w 2002 roku, szybki postęp technologii transmisji danych w telefonii komórkowej spowodował, że stał się on anachronizmem (Świecka 2015, s. 32).

Obecnie istnieje kilka rozwiązań pozwalających na wykorzystanie potencjału płatności mobilnych. Do najczęściej używanych przez konsumentów należą aplikacje bankowe zarówno w wersji podstawowej jak i te wykorzystujące BLIK-a, oraz wirtualne portfele takie jak: Apple Pay, Google Pay itp.

Ciągły postęp techniczny powodujący rozwój technologii mobilnych a co za tym idzie rosnące moce obliczeniowe urządzeń mobilnych oraz niskie

koszty transmisji danych oferowanych przez operatorów, spowodowały wzrost zainteresowania konsumentów, aplikacjami mobilnymi oferowanymi przez banki komercyjne. Mobilne aplikacje wydawane na urządzenia przenośne, zaraz po ich zainstalowaniu pozwalają na korzystanie z pełni dostępnych funkcji. Wykorzystując do tego połączenie sieciowe GSM bądź łącze domowego internetu Wi-Fi. Dzięki temu każdy klient banku ma pod ręką pełny dostęp do zasobów konta, bez konieczności sięgania do tradycyjnej bankowości. Zlecanie przelewów, tworzenie lokat oszczędnościowych a nawet stały kontakt z infolinią danego banku odbywa się za pośrednictwem aplikacji, dostosowanej do wymiarów urządzenia mobilnego, znacznie ułatwiając funkcjonowanie oraz komfort pracy. Dlatego właśnie mobilne aplikacje bankowe stały się nieodłącznym elementem życia konsumentów, ciesząc się coraz większym zainteresowaniem jednocześnie oferując coraz większe możliwości ich wykorzystania (Skrzyński 2011, s. 13). Jednakże rozwiązanie takie generuje koszty dla banków, w związku z koniecznością stworzenia odpowiedniego oprogramowania aplikacji, dostosowaniem go do ogólnie powszechnych platform czy systemów operacyjnych. Koniecznym zabiegiem są również aktualizacje aplikacji w celu zwiększenia bezpieczeństwa oraz zapewnienia bezawaryjnego funkcjonowania (Polasik 2013, s. 147).

Przełomowym momentem dla bankowości mobilnej był rok 2014, gdy Prezes Narodowego Banku Polskiego wyraził zgodę na uruchomienie pierwszego systemu płatności mobilnych BLIK za pośrednictwem Polskiego Standardu Płatności Sp. z o.o. (PSP zostało założone w 2013 roku za pośrednictwem 6 banków tj. Alior Bank S.A., Bank Millennium S.A., Bank Zachodni WBK S.A., ING Bank Śląski S.A., mBank S.A. oraz PKO Bank Polski S.A.) wykorzystując ustawę z dnia 24 sierpnia 2001 roku (ustawa z dnia 24 sierpnia 2001 roku). Po stworzeniu projektu został on udostępniony konsumentom w roku 2015, oferując możliwość płatności z wykorzystaniem aplikacji bankowych dostępnych na urządzaniach mobilnych. Z końcem roku 2015, została wprowadzona nowa funkcja, która do dziś jest jedną z najchętniej wykorzystywanych przez konsumentów, P2P. Od tej pory możliwe było dokonywanie mobilnych przelewów pomiędzy posiadaczami telefonów komórkowych. Aby możliwe było zlecenie owego przelewu, wystarczy wpisać jedynie numer telefonu osoby, do której skierowany jest przelew, zamiast tradycyjnego numeru bankowego. Dzięki czemu przelewy są dostarczane do obiorcy natychmiast, znacznie skracając czas oczekiwania i podnosząc komfort użytkowania. Usługa aktywowana jest w momencie, zalogowania się przez użytkownika i powiązania numeru telefonu komórkowego z dotychczasowym numerem

konta bankowego (Jagodzińska-Komar 2018, s. 107). Obecna forma działania BLIK-a opiera się na generowaniu jednorazowych kodów (6-cyfrowych) wykorzystując aplikację mobilną dostępną w bankach partnerskich. Konsumenci używają wygenerowanych kodów do dokonywania płatności w sklepach stacjonarnych, sklepach internetowych, a także do wypłacania gotówki z bankomatów bez użycia karty płatniczej czy płatności zbliżeniowych (Wolna 2018, s. 169).

Wirtualne portfele w literaturze określane są jako zbiór usług pozwalających użytkownikom na dokonywanie płatności w formie elektronicznej z wykorzystaniem urządzenia przenośnego. Istotą mobilnego portfela jest jego zdolność płatnicza, oferując wygodne, tanie, bezpiecznie oraz uniwersalne płatności. Poruszając temat wirtualnego portfela warto skupić się na formie powszechnie używanej w codziennym życiu przez konsumentów. Mowa tu o urządzeniu mobilnym posiadającym odpowiednie oprogramowanie umożliwiające dokonywanie płatności zbliżeniowych, bez użycia fizycznej karty płatniczej, jedynie za pomocą urządzania mobilnego wyposażonego w usługę NFC (Górka 2016, s. 4). Technologia NFC (Near Field Communication) to bezprzewodowa technologia komunikacji, która umożliwia wymianę danych na krótkich odległościach (zazwyczaj do 4 centymetrów) między urządzeniami wyposażonymi w chip NFC. Do nawiązania połączenia i przesyłania danych nie jest wymagane fizyczne połączenie ani kabel. Wystarczy zbliżyć urządzenia z obsługą NFC do siebie, by rozpocząć transmisję. Użycie technologii mobilnej NFC następuje tylko w sposób ograniczony, w ramach wymiany danych pomiędzy terminalem EFT-POS, następnie dalszy etap procesu komunikacji odbywa się już po stronie terminala. Warto zaznaczyć, iż w pewnych warunkach, istnieje możliwość dokonania płatności w trybie offline z wyłączeniem połączenia z serwerem banku. Co więcej główne rozwiązania wykorzystane przy płatnościach NFC bazują na instrumencie karty płatniczej (Polasik 2014, s. 199). Portfele mobilne, takie jak Apple Pay, Google Pay (Android Pay), Samsung Pay, PeoPay banku Pekao, wykorzystują technologię tokenizacji w celu zapewnienia bezpiecznych i wygodnych płatności mobilnych. W przypadku Apple Pay i Google Pay, dane karty płatniczej są zastępowane cyfrowym tokenem, który jest przechowywany na urządzeniu, natomiast rzeczywiste dane karty są przechowywane w chmurze. To znaczy, że na telefonie znajduje się jedynie bezpieczny token powiązany z danymi karty, co minimalizuje ryzyko utraty danych. Dodatkowo, portfele Apple Pay i Google Wallet oferują bardziej rozbudowane funkcje, takie jak programy lojalnościowe oraz kupony rabatowe, a także umożliwiają płatności zbliżeniowe za pomocą technologii

NFC w punktach sprzedaży wyposażonych w odpowiednie terminale. Samsung Pay idzie jeszcze dalej, wykorzystując technologię MST (Magnetic Secure Transmission), która pozwala na dokonywanie płatności za pomocą telefonu nawet w tradycyjnych terminalach, akceptujących tylko karty z paskiem magnetycznym. Innowacją w polskich rozwiązaniach płatności mobilnych jest technologia HCE (Host Card Emulation), która umożliwia przeniesienie danych karty i aplikacji płatniczej do chmury. W ten sposób eliminuje się konieczność współpracy z operatorem telefonii komórkowej. Dzięki temu smartfon wyposażony w moduł NFC może emulować kartę płatniczą, a dane są przechowywane na odległym serwerze w chmurze, co znacznie zwiększa bezpieczeństwo płatności mobilnych. Wszystkie te technologie mają na celu zapewnienie bezpiecznych, wygodnych i szybkich płatności mobilnych, które stają się coraz bardziej popularne na całym świecie. Dzięki nim konsumenci mają dostęp do nowoczesnych i innowacyjnych metod płatności, które ułatwiają codzienne transakcje (Górka 2016, s. 7).

## PODSUMOWANIE

Innowacje w dziedzinie płatności, skupiają się na rozwijających się technologiach i najnowszych trendach, które wpływają na sposób, w jaki dokonujemy transakcji finansowych. Dynamiczne zmiany w dziedzinie płatności, wskazują na rosnące zapotrzebowanie na szybsze, bezpieczniejsze i bardziej wygodne metody dokonywania transakcji. Wraz z rozwojem technologii cyfrowych i popularnością urządzeń mobilnych, konsumenci oczekują nowoczesnych rozwiązań, które będą spełniać ich potrzeby w dzisiejszym globalnym i cyfrowym środowisku. Technologia NFC (Near Field Communication) jako jedna z kluczowych innowacji, która umożliwia płatności zbliżeniowe, wykorzystuje krótki zasięg komunikacji między urządzeniami. NFC staje się coraz bardziej popularne, umożliwiając szybkie, bezdotykowe płatności zarówno za pomocą smartfonów, jak i kart płatniczych. Co za tym idzie rozwija się również rynek portfeli cyfrowych, takich jak Apple Pay, Google Wallet, Samsung Pay i PeoPay banku Pekao, które zrewolucjonizowały sposób, w jaki dokonujemy płatności. Wykorzystując technologię tokenizacji i przechowywanie danych w chmurze, portfele cyfrowe zapewniają wyższy poziom bezpieczeństwa, minimalizując ryzyko utraty danych kart płatniczych. Ponadto, wirtualne portfele oferują szeroki zakres funkcji dodatkowych, takich jak programy lojalnościowe i kody rabatowe, co zwiększa atrakcyjność i użyteczność tych rozwiązań dla klientów. Wartą uwagi kwestią jest również kwestia technologii

HCE (Host Card Emulation), która umożliwia przeniesienie danych karty płatniczej i aplikacji płatniczej do chmury, eliminując konieczność współpracy z operatorem telefonii komórkowej. Dzięki temu smartfony wyposażone w moduł NFC mogą emulować fizyczne karty płatnicze, co przyczynia się do upowszechnienia płatności mobilnych. Trendy w płatnościach, takie jak rosnąca popularność płatności zbliżeniowych, dynamiczny rozwój płatności mobilnych oraz wzrost znaczenia kryptowalut czy przenikanie nowoczesnych technologii do sektora finansowego wymusza na instytucjach finansowych ciągły rozwój i dostosowywanie się do potrzeb klientów. Wraz z rosnącym popytem na płatności cyfrowe, technologie takie jak NFC, portfele cyfrowe i HCE stają się kluczowymi graczami w przekształcaniu tradycyjnych metod płatności na rzecz bezpiecznych, wygodnych i zintegrowanych rozwiązań. Warto jednak zaznaczyć, iż decydując się na korzystanie z płatności mobilnych (elektronicznych) użytkownicy w pewnym aspekcie rezygnują z bezpieczeństwa jakie gwarantuje tradycyjna bankowość. Wybierając tradycyjne metody płatności ryzyko związane z atakami hackerskimi czy przejęciem danych ograniczane jest prawie do minimum. Przyszłość płatności zdaje się być mocno związana z technologią, a dynamiczne trendy w tej dziedzinie wyznaczają kierunek rozwoju usług finansowych na przestrzeni kolejnych lat.

## BIBLIOGRAFIA

Beck R., Chepluch J. S, Lollike N., Malone S.
2016 *Blockchain– the gateway to trust-free cryptographic transactions* [w:] Twenty-Fourth European Conference on Information Systems (ECIS), Turkey.

Gervais, A., Karame G. O., Wüst K., Glykantzis V., Ritzdorf H., Capkun S.
2016 *On the security and performance of proof of work blockchains*. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. (dostęp z dnia 26.07.2023 r.).

Górka J.
2016 *Ewolucja funkcjonalna mobilnego portfela* [w:] *Obrót bezgotówkowy w Polsce: stan obecny i perspektywy*, Warszawa.

Houben R., Snyers A.
2018 *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, Belgium.

Jagodzińska-Komar E.
2018 *Płatności natychmiastowe w Polsce na przykładzie systemu blik* [w:] Zeszyty Naukowe PWSZ w Płocku Nauki Ekonomiczne tom XXVII, Płock.

Kaszubski R., Widawski P.
2023 Mobilne systemy pieniądza elektronicznego i inne instrumenty mobilnych płatności, http://www.zbp.pl/photo/ftb/mob_systemy_pieniadza.pdf. (dostęp z dnia 15.07.2023).

Mazur M.
2021 *Non-Fungible Tokens (NFT). The Analysis of Risk and Return*, Francja.

Piech K.
2016 *Leksykon pojęć na temat technologii blockchain i kryptowalut,* Ministerstwo Cyfryzacji Warszawa.

Piotrowska A. I.
2014 *Bitcoin a definicja i funkcje pieniądza*. Annales Universitatis [w:] Mariae Curie-Skłodowska Sectio H Oeconomia nr 48, Lublin.

Polasik M.
2013 *Wykorzystanie elektronicznych kanałów dystrybucji usług bankowych w Polsce*, Toruń.

2014 *Perspektywy rozwoju mobilnych płatności NFC na rynku polskim* [w:] Annales Universitatis Mariae Curie-Skłodowska Sectio H Oeconomia nr 48, Lublin.

Przygoda M.
2021 *Wzrost znaczenia kryptowalut na międzynarodowym rynku finansowym* [w:] Administracyjno-finansowe konteksty zarządzania, Warszawa.

Rahimpour S., Khabbazian M.
2020 *Hashcashed Reputation with Application in Designing Watchtowers*, Canada.

Skrzyński P.
2011 *Mobilna bankowość – potrzeba czy moda*? Mobiltek, http://www.mobiltek.pl/wpcontent/uploads/2011/10/mobilna-bankowosc-potrzeba-czy-moda.pdf [dostęp: 24.03.2013].

Świecka B.
2015 *Płatności mobilne jako innowacje na rynku detalicznych płatności bezgotówkowych* [w:] Problemy Zarządzania nr 3, Szczecin.

Wanat E.
2019 *Bitcoin i inne kryptowaluty jako przedmiot świadczenia pieniężnego* [w:] Transformacje Prawa Prywatnego nr 2, Kraków.

Wolna J.
2015 *Rozwój systemów płatności mobilnych w Polsce* [w:] Studia Ekonomiczne nr 239, Katowice.

Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami. Dz. U. z 2013 r., poz. 246, z późn. zm.

## INNOVATION IN PAYMENTS. TECHNOLOGIES AND TRENDS

**Abstract:** In today's dynamic financial environment, innovation in payments plays a key role in transforming the way we transact. This article focuses on analyzing the latest technologies and trends in the payments area, showing their impact on everyday financial operations. Through careful analysis, the article presents the evolution from traditional payment methods to developed systems based on digitalization and automation. The article discusses mobile payments, digital wallets, blockchain technology and cryptocurrencies, as well as their growing role in the global economy. In addition, the article explores the implications of these technologies for users and enterprises.

**Keywords:** blockchain, cryptocurrencies, bitcoin, digital wallets, BLIK

**PAWEŁ GŁAZ**
UNIWERSYTET RZESZOWSKI

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI CZĘŚĆ 2- BEZPIECZEŃSTWO PŁATNOŚCI ELEKTRONICZNYCH: WYZWANIA I ROZWIĄZANIA

**Streszczenie*:*** W miarę jak płatności elektroniczne stają się powszechniejsze, wzrasta również znaczenie bezpieczeństwa transakcji online. Niniejszy tekst skupia się na omówieniu kluczowych wyzwań, jakie stają przed bezpieczeństwem płatności elektronicznych oraz prezentuje innowacyjne rozwiązania mające na celu ochronę użytkowników przed cyberzagrożeniami. Analiza obejmuje różnorodne aspekty, takie jak przechwytywanie danych, oszustwa, ataki hakerskie oraz zagrożenia związane z kradzieżą tożsamości. W tekście przedstawione są technologiczne środki obrony, takie jak autoryzacja dwuetapowa, biometria czy technologie kodowania, które mają na celu zwiększenie poziomu bezpieczeństwa płatności elektronicznych. Poprzez analizę współczesnych wyzwań i skutecznych metod obrony, ustęp stanowi przewodnik dla instytucji finansowych, dostawców usług płatniczych oraz użytkowników końcowych w budowaniu bezpiecznej przestrzeni dla płatności elektronicznych.

**Słowa kluczowe**: cyberbezpieczeństwo, zagrożenia, autoryzacja, phishing, oszustwa

## WPROWADZENIE

W dzisiejszym dynamicznym i cyfrowym świecie, płatności elektroniczne stanowią jedną z najważniejszych i nieodzownych form realizacji transakcji handlowych. Zyskując na popularności z dnia na dzień, umożliwiają szybkie, wygodne i bezpieczne dokonywanie płatności za towary i usługi wirtualnymi środkami płatniczymi. Jednak wraz z postępem technologicznym i wzrostem

wykorzystania płatności elektronicznych pojawiają się również nowe wyzwania i zagrożenia.

Wyzwaniem współczesnego świata jest analizia bezpieczeństwa płatności elektronicznych, a co za tym idzie prezentacja różnorodnych rozwiązań. Mogą przyczynić się one do zminimalizowania ryzyka i zagwarantowania ochrony dla użytkowników w trakcie realizacji transakcji online. W miarę jak nowoczesne technologie rewolucjonizują życie, konieczne jest zrozumienie potencjalnych zagrożeń i podejmowanie działań w celu utrzymania wysokiego poziomu bezpieczeństwa w świecie płatności cyfrowych.

W dalszej części tego tekstu, dokładnie przeanalizowano główne wyzwania, przed którymi stoi bezpieczeństwo płatności elektronicznych, zwracając uwagę na potencjalne ryzyka związane z cyberprzestępczością, oszustwami czy utratą danych finansowych. Ponadto, zaprezentowano innowacyjne rozwiązania technologiczne, takie jak autoryzacja wielopoziomowa, rozpoznawanie biometryczne czy rozszerzona kryptografia, które mogą znacząco podnieść poziom bezpieczeństwa transakcji online.

Celem pracy jest skupienie się także na zwiększaniu świadomości konsumentów oraz przedsiębiorstw na temat praktyk zapewniających bezpieczne płatności omówienie roli rządu i regulatorów w tworzeniu odpowiednich ram prawnych i standardów bezpieczeństwa, które wspierają rozwój i zaufanie do płatności elektronicznych.

Wraz z rosnącym znaczeniem płatności elektronicznych jako kluczowego elementu naszej codziennej aktywności, praca jest nie tylko aktualnym omówieniem bieżącej sytuacji, ale również skłonieniem do refleksji. Ważne jest zwrócenie uwagi jak wspólnie możliwe jest dążenie do stworzenia bardziej bezpiecznej i niezawodnej przyszłości płatności elektronicznych.

## ZAGROŻENIA DLA BEZPIECZEŃSTWA PŁATNOŚCI ELEKTRONICZNYCH

Wraz z rozwojem technologii informatycznych wykorzystywanych w różnych dziedzinach codziennego życia, a w szczególności płatnościach dokonywanych za pomocą „sieci", pojawiły się nowe zagrożenia związane z potencjalnymi oszustwami, kradzieżami danych czy środków zgromadzonych na kontach bankowych użytkowników. Obecnie do najczęściej wykorzystywanych ataków w intrenecie należą (Pitera 2017, s. 184):

- włamania do systemów bankowych, których celem jest malwersacja środków bądź kradzież danych klientów,
- fałszowanie firmowych stron internetowych celem wyłudzenia haseł, loginów czy kodów SMS,
- ataki *ransomware*,
- *phishing*,
- maile z plikami typu *malware*,
- wirusy dostępne na aplikacje mobilne,
- ataki hybrydowe łączące w sobie kilka technik.

Pierwszym z wymienionych sposobów to próba włamania do systemów informatycznych banków oraz innych instytucji, takich jak duże korporacje. Celem tych ataków jest uzyskanie dostępu do danych finansowych lub przechwycenie poufnych informacji. Takie działania są szczególnie skierowane w stronę organizacji finansowych, ze względu na ich bogactwo w informacje poufne oraz posiadane środki finansowe. Banki, zdając sobie sprawę z rosnącego zagrożenia, inwestują corocznie duże sumy w cyberbezpieczeństwo, aby zapewnić swoim klientom pełną ochronę. Najczęściej, ataki koncentrują się na ostatnim ogniwie łańcucha, a więc bezpośrednio na klientach tych instytucji. Hakerzy starają się wykorzystać ich niewiedzę lub niewłaściwe praktyki, aby zdobyć poufne dane i środki finansowe. Dlatego tak ważne jest, aby klienci byli świadomi zagrożeń związanych z płatnościami elektronicznymi i stosowali odpowiednie środki ostrożności. Polskie banki aktywnie pracują nad wdrażaniem nowoczesnych rozwiązań technologicznych w celu zabezpieczenia swoich klientów przed cyberatakami. Jednak ryzyko nadal istnieje, dlatego ważne jest, aby klienci byli uważni podczas korzystania z usług bankowych online. Przede wszystkim powinni unikać podawania swoich danych logowania i hasła na podejrzanych stronach internetowych, a także korzystać z rozsądnych haseł oraz regularnie zmieniać je w celu utrzymania bezpieczeństwa swojego konta (Pitera 2017, s. 185).

Kolejnym z stosowanych oszustw w „sieci" jest phishing. Termin ten został zapożyczony z języka internetowego, w żargonie używanym obecnie oznacza on wyłudzanie danych osobowych lub informacji finansowych dotyczących innego użytkownika komputera w celu ich wykorzystania do sfingowania płatności bądź inny rodzaj oszustwa internetowego (Akerlof i Shiller 2015, s. 18). Na przestrzeni lat oszuści stale rozwijali tego typu metody ataków, by nawet dla doświadczonych użytkowników stanowiła wyzwanie, idealnie imitowała autentyczne oraz wiarygodne źródło. W kontekście elektronicznych

płatności, w szczególności bankowości elektronicznej, metoda ta polega na podszywaniu się pod stronę internetową banku, a następnie na przyciągnięciu nieświadomych niczego użytkowników pod pretekstem zapewnienia dodatkowego poziomu bezpieczeństwa (Janin i Gupta 2016, s. 2). Typowy scenariusz ataku zaczyna się w momencie wysłania użytkownikowi wiadomości e-mail bądź powiadomienia, które wydaje się pochodzić od rzekomego banku bądź instytucji. Zazwyczaj treść takiej wiadomości sugeruje, iż konto użytkownika jest zagrożone oraz wymaga niezwłocznej reakcji w celu zabezpieczenia środków lub danych. Osoby przeprowadzające atak starają się dokładnie naśladować wygląd i treść oficjalnych wiadomości od danego. W treści owej fałszywej wiadomości zazwyczaj znajduje się link, który ma za zadanie przekierować użytkownika do spreparowanej strony internetowej umiejętnie imitującej oryginalną stronę banku. W momencie, gdy nieświadomy użytkownik zostaje przekierowany na tę stronę, jest proszony o podanie swoich danych logowania bądź poufnych informacji takich jak: login, hasło, numer karty kredytowej czy kod CVV (Card Verification Value). W momencie, gdy użytkownik podaje swoje dane, atakujący uzyskuje do nich pełen dostęp i może je wykorzystać w celach nieautoryzowanych transakcji finansowych lub kradzieży tożsamości (Protasowicki 2016, s. 38).

Kolejnym z zagrożeń z którymi spotyka się coraz więcej osób czy instytucji są ataki *ransomware*. Termin ten pochodzi z języka angielskiego i oznacza okup. Jest to rodzaj cyberataków, polegający na infiltracji systemów informatycznych przez hakerów, celem zaszyfrowania danych, uniemożliwiając dostęp do nich ich prawowitym użytkownikom. Następnie oszuści żądają okupu w zamian za odszyfrowanie danych bądź przywrócenie normalnego działania systemu. Takiego rodzaju ataki stanowią jedno z najbardziej niebezpiecznych zagrożeń w dziedzinie cyberbezpieczeństwa, gdyż mogą spowodować znaczne straty finansowe, ale również poważne zakłócenia w działaniu organizacji (Sadowski 2017, s. 62-63). Sam proces ataku rozpoczyna się bardzo podobnie jak *phishing*, mianowicie oszuści wykorzystują wiadomości e-mail, linki phishingowe, exploity[1] lub słabo zabezpieczone usługi sieciowe, by przekazać złośliwe oprogramowanie użytkownikowi a następnie zainfekować system ofiary. Po zainfekowaniu systemu, złośliwe oprogramowanie rozpoczyna proces szyfrowania danych urządzenia bądź sieci, powodując brak dostępu i nieczytelność danych bez specjalnego kodu deszyfrującego. Zwykle po

[1] Exploit to rodzaj złośliwego kodu lub techniki, które wykorzystują znane lub nieznane luki w oprogramowaniu w celu przejęcia kontroli nad systemem, aplikacją lub urządzeniem.

skutecznym zaszyfrowaniu danych, hakerzy wyświetlają komunikat mający na celu poinformowanie użytkownika o zaistniałej sytuacji, żądając okupu zazwyczaj w wymienionej kryptowalucie w zamian za klucz deszyfrujący. Dodatkowo, częstą praktyką oszustów jest określenie krótkiego terminu płatności okupu pod groźbą utraty danych lub ich upublicznienia. W przypadku, gdy ofiara decyduje się na spełnienie żądań, hakerzy dostarczają klub deszyfrujący pozwalający na odzyskanie dostępu do zaszyfrowanych danych. Niestety nie ma pewności, iż po zapłacie okupu dane zostaną przywrócone lub oszuści ich nie udostępnią (Wróblewski i Tuśnio 2023, s. 450-451).

Ostatnim przykładem analizowanych zagrożeń dla cyberbezpieczeństwa są najczęściej stosowane przez oszustów/hakerów pliki malware. Jest to nic innego jak złośliwe oprogramowanie zaprojektowane celem wyrządzenia szkód bądź wykonywania niepożądanych działań na urządzeniu mobilnym, komputerze lub sieci. Terminologia „malware" pochodzi od angielskiego wyrażenia „malicious software", czyli złośliwe oprogramowanie. Zdarza się, że pliki malware tworzone są przez hakerów, cyberprzestępców, a także organizacje i państwa w celach szpiegowskich lub sabotażu (Wołyniec 2019, s. 35). Obecnie istnieje wiele rodzajów plików malware, z których każdy z nich może działać w zupełnie inny sposób. Najczęściej spotykanymi w sieci są:

- Wirusy: Są to infekcyjne programy, działają na zasadzie łączenia się z innymi plikami, jednocześnie replikując się w systemie, powodując rozprzestrzenianie się złośliwego kodu,
- Trojany: Oprogramowanie, które precyzyjnie zostało ukryte w pozornie nieszkodliwych aplikacjach lub plikach. Po ich uruchomieniu następuje infekcja urządzenia co umożliwia hakerom na zdalne kontrolowanie komputera lub kradzież danych,
- Wormsy (robaki): samoreplikujące się pliki, rozpowszechniające się przez sieć, infekują inne komputery oraz urządzenia,
- Keyloggery: programy, których celem jest monitorowanie i rejestracja klawiszy naciskanych na klawiaturze urządzenia. Hakerom pozwala to na kradzież haseł, danych logowania lub innych poufnych danych,
- Adware: oprogramowanie, które wyświetla niechciane reklamy na komputerze lub urządzeniu.

Pliki malware mogą być rozpowszechniane za pomocą różnych metod, takich jak załączniki e-mail, pobieranie z niezaufanych źródeł, klikanie na podejrzane linki lub wykorzystując luki w zabezpieczeniach systemu.

W celu ochrony przed plikami malware, zaleca się korzystanie z oprogramowania antywirusowego i zabezpieczającego, regularne aktualizacje systemu oraz ostrożność podczas korzystania z internetu i pobierania plików (Chronowska 2022, s. 14).

## WZMOCNIENIE BEZPIECZEŃSTWA

W miarę jak technologie cyfrowe rozwijają się w szybkim tempie, płatności elektroniczne stają się nieodłącznym elementem naszego życia codziennego. Jednak zwiększenie wykorzystania płatności cyfrowych niesie za sobą nowe wyzwania związane z bezpieczeństwem danych i transakcji. W odpowiedzi na te zagrożenia, organizacje finansowe oraz firmy odpowiedzialne za usługi płatnicze nieustannie poszukują innowacyjnych rozwiązań, które wzmocnią bezpieczeństwo i zaufanie użytkowników do płatności elektronicznych.

Podstawowym narzędziem stosowanym w celu zabezpieczenia użytkowników przed potencjalnymi zagrożeniami jest uwierzytelnianie dwuetapowe zwane również dwuskładnikowym. Najczęściej ten rodzaj zabezpieczeń stosowany jest w instytucjach bankowych. Zgodnie z dyrektywą PSD2[2] (Payment Services Directive), banki zostały zobowiązanie do stosowania zabezpieczeń dwuetapowych (Penczar 2019, s. 154-155). Podstawową funkcją działania tego rodzaju gwarancji bezpieczeństwa jest uwierzytelnienie tożsamości co najmniej dwoma niezależnymi kanałami komunikacji. Na przykładzie logowania się przez użytkownika do systemu bankowego, pierwszym etapem jest podanie swojego ID a następnie hasła oraz dodatkowego zabezpieczenia w postaci kodu z kardy kodów udostępnianych przez banki, kodu tokena bądź kodu SMS przesłanego na numer telefonu użytkownika. Obecnie, rozwiązanie oparte na kartach ze zdrapywanymi kodami jest rzadko stosowane. Zamiast tego, coraz częściej wykorzystuje się tokeny, czyli urządzenia generujące ciąg cyfr za pomocą funkcji jednokierunkowej, opierającej się na dwóch parametrach: stałym identyfikatorze danego urządzenia i zmiennej wartości - ciągu cyfr generowanego w określonym czasie. Tokeny są stosowane głównie w specyficznych sytuacjach, np. do zabezpieczenia kanałów VPN (Virtual Private Network) w pracy zdalnej. Jako główne "drugie" zabezpieczenie,

[2] Dyrektywa PSD2 [Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego] jest odpowiedzią na rozwój technologii oraz nowe usługi płatnicze. Dyrektywa PSD2, której regulacje zostały wprowadzone do polskiego porządku prawnego poprzez nowelizację ustawy o usługach płatniczych, m.in. umożliwi stworzenie jednolitego rynku płatności w UE, zapewni jeszcze większe bezpieczeństwo Twoich transakcji i ochronę finansów.

najczęściej używany jest kod SMS (Short Message Service), który jest wysyłany na numer telefonu wcześniej zdefiniowany przez użytkownika. Jest to rozwiązanie zarówno praktyczne, jak i korzystne ekonomicznie. Biorąc pod uwagę powszechną dostępność telefonów komórkowych, nie ogranicza ono liczby potencjalnych klientów korzystających z bankowości internetowej. Korzystanie z kodów SMS jako drugiego etapu uwierzytelniania staje się popularne ze względu na swoją prostotę i wygodę. Po wprowadzeniu hasła użytkownik otrzymuje SMS z unikalnym kodem, który musi wprowadzić, aby dokończyć proces logowania. Dzięki temu, nawet jeśli ktoś przechwyciłby hasło użytkownika, bez dostępu do jego telefonu komórkowego nie będzie mógł ukończyć procesu uwierzytelniania (Sajler-Fudro 2022, s. 208).

Jedną z najważniejszych kwestii w działalności banków jest zapewnienie bezpieczeństwa powierzonych środków, ale również realizowanych transakcji (Cegiełko 2018, s. 167). Wyzwanie identyfikacji użytkownika i autoryzacji transakcji, także wykorzystując zabezpieczenia biometryczne, jest ściśle skorelowany z kwestią odpowiedzialności za wykonywane operacje i czynności bankowe (Bajor 2011, s. 295). Wedle ustawy o usługach płatniczych banki są zobowiązane do zapewnienia użytkownikom instytucji możliwe jak najwyższego poziomu bezpieczeństwa z wykorzystaniem odpowiednich metod służących identyfikacji (Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tj..: Dz.U.2017 poz. 2003, ze zm., art.60). Najbardziej intuicyjną i najchętniej stosowaną metodą zabezpieczenia biometrycznego jest wizerunek twarzy rozmówcy. Współcześnie zabezpieczenie biometryczne rozumiane jest jako metoda służąca do autoryzacji przelewów w aplikacjach mobilnych banków, dzięki wykorzystaniu tej metody (np. odcisk palca, skan twarzy lub tęczówki) możliwe jest ograniczenie zagrożeń związanych z cyberbezpieczeństwem. Jednakże początki takiego rozwiązania zaczynają się w momencie zakładania konta bankowego w placówce danego banku, gdzie metoda wizualnej oceny polega na weryfikacji dowodu tożsamości z zgodnością twarzy interesanta (Mlaskawa 2015, s. 113).

## SZCZEGÓLNA OSTROŻNOŚĆ

Pomimo zastosowania przez banki coraz co lepszych i skutecznych zabezpieczeń, klienci również muszą wykorzystywać wiedzę z zakresu cyberbezpieczeństwa jednocześnie przestrzegając podstawowych zasad bezpiecznego korzystania z usług oferowanych przez bankowość elektroniczną. Podstawową zasadą, na którą należy zwrócić szczególną uwagę jest to, aby nie podawać

osobom trzecim żadnych danych niezbędnych w procesie logowania do bankowości elektronicznej. Ponadto logowanie do serwisu bankowego powinno odbywać się poprzez umieszczenie odpowiedniego adresu w pasku przeglądarki. Użytkownik powinien zwrócić szczególną uwagę czy przed adresem strony internetowej znajduje się odpowiedni przedrostek „https://" a obok niego pojawia się symbol kłódki. Warto również kliknąć symbol kłódki i sprawdzić poprawność certyfikatu klucza publicznego (Górnisiewicz, Obczyński i Pstruś 2014, s. 19). Kolejną z zasad o której należy pamiętać jest łączenie się z bankowością mobilną wyłącznie za pomocą zaufanych urządzeń. Zaleca się nie korzystać z kafejek internetowych bądź ogólnodostępnych hot-spotów, za względu na ryzyko zainstalowania tam przez oszustów/hakerów złośliwego oprogramowania. Warto również pamiętać, aby urządzenia z których korzystają klienci banków posiadały możliwe najnowsze oprogramowanie antywirusowe oraz wyposażone były w zaporę sieciową.

Zabezpieczenie bankowości internetowej odpowiednim loginem i hasłem pozwala na zwiększenie bezpieczeństwa w sieci (Górnisiewicz, Obczyński i Pstruś 2014, s. 19-22). Hasło używane w banku powinno być trudne i zawierać znaki specjalne, co najmniej jedną dużą literę, oraz cyfry. Powinno ono być również zmieniane z odpowiednią częstotliwością celem uniknięcia przechwycenia hasła przez oszustów. Obowiązek dbania o zmianę hasła spoczywa stricte na barkach użytkowników, jednakże banki prowadząc swoją politykę bezpieczeństwa co jakiś czas starają się przypominać użytkownikom o konieczności zmiany hasła (Filipiak 2019, s. 22).

Podczas korzystania z usług sklepów internetowych, istnieje możliwość dokonania płatności za zakupy przy użyciu karty płatniczej. Aby zrealizować płatność, klient musi podać niezbędne dane karty, takie jak numer karty, datę ważności, dane posiadacza oraz trzycyfrowy kod CVV2/CVC2 (Card Verification Value 2/Card Verification Code 2) umieszczony na odwrocie karty. Ten trzycyfrowy kod stanowi jeden z systemów zabezpieczeń stosowanych przez banki w celu zwiększenia bezpieczeństwa płatności kartami. Warto jednak zaznaczyć, że praktyki związane z wymaganymi danymi do autoryzacji płatności mogą różnić się w różnych krajach na świecie. W niektórych regionach, zwłaszcza w niektórych krajach, kod CVC2/CVV2 może nie być wymagany podczas procesu autoryzacji płatności. Z tego powodu klienci banków muszą zachować szczególną ostrożność i pamiętać, aby nigdy nie umieszczać poufnych danych, takich jak numer karty czy kod CVC2/CVV2, w internecie. Ponieważ dane podane w internecie pozostają tam na zawsze i mogą stać się łatwym celem dla oszustów, zaleca się dokładne zapoznanie się z polityką

bezpieczeństwa sklepów internetowych i upewnienie się, że strona, na której dokonuje się płatności, jest zabezpieczona i posiada odpowiednie certyfikaty bezpieczeństwa. Korzystanie z renomowanych platform płatniczych i sklepów online o dobrej reputacji może pomóc w minimalizacji ryzyka nadużyć kart płatniczych oraz chronić dane klientów przed niepożądanym dostępem. W przypadku podejrzeń o jakiekolwiek nieprawidłowości, klient powinien natychmiast skontaktować się z bankiem w celu podjęcia odpowiednich działań w celu ochrony swoich finansów i zabezpieczenia swojego konta (Filipiak 2019, s. 22-23).

## PODSUMOWANIE

Zagadnienie bezpieczeństwa płatności elektronicznych jest bardzo ważnym aspektem codziennego życia klientów banków, analiza wyzwań i prezentacja rozwiązań ma na celu wzmocnienie ochrony transakcji online. W miarę zdobywania coraz większej popularności jaką szczycą się płatności cyfrowe, stają się one również celem coraz bardziej zaawansowanych ataków cybernetycznych. W odpowiedzi na te zagrożenia, koniecznym aspektem jest wykorzystanie innowacyjnych rozwiązań, które umożliwią utrzymanie bezpieczeństwa i zaufania użytkowników do płatności elektronicznych. Jednym z kluczowych środków w tym zakresie jest dwuetapowe uwierzytelnienie, które dodaje dodatkowy poziom weryfikacji tożsamości użytkownika, redukując ryzyko nieautoryzowanego dostępu. Kolejnym skutecznym rozwiązaniem jest wykorzystanie biometrii, takiej jak rozpoznawanie twarzy czy odcisków palców, co pozwala na bardziej precyzyjne i bezpieczne uwierzytelnianie. Dodatkowo, technologia tokenizacji zapewnia zabezpieczenie wrażliwych danych, minimalizując ryzyko ich skompromitowania. Wprowadzenie drugiego etapu uwierzytelniania, często w postaci kodów SMS, okazało się praktyczne i ekonomicznie korzystne, przy zachowaniu wygody dla użytkowników. Dzięki temu banki i firmy oferujące usługi płatnicze mogą efektywnie zabezpieczać dane swoich klientów i ograniczać zagrożenia związane z cyberatakami. Ponadto, zrozumienie zagrożeń i stosowanie świadomych praktyk bezpieczeństwa ze strony zarówno instytucji finansowych, jak i użytkowników, są kluczowe w ochronie przed potencjalnymi atakami. Edukacja i regularne szkolenia w zakresie cyberbezpieczeństwa są niezbędne w tym dynamicznie zmieniającym się środowisku. Wraz z postępem technologii, dążenie do zapewnienia bezpiecznych płatności elektronicznych jest nie tylko obowiązkiem instytucji finansowych i przedsiębiorstw, ale także wspólnym wysiłkiem całego ekosystemu płatności

cyfrowych. Poprzez stosowanie zaawansowanych rozwiązań, współpracę i rozwijanie świadomości, można razem podnosić poziom bezpieczeństwa i w pełni korzystać z potencjału płatności elektronicznych, ciesząc się wygodą i skutecznością transakcji online.

## BIBLIOGRAFIA

Akerlof G.A., Shiller R.J.
2015 *Phishing for Phools. The Economics of Manipulation and Deception*, New Jersey.

Bajor B.
2011 *Bankowość elektroniczna. Studium prawne*, Warszawa.

Cegiełko S.

2018 *Kultura użytkowa zabezpieczeń biometrycznych klientów banków w Polsce na podstawie sondażu internetowego*, Bezpieczny Bank nr 72.

Chronowska E.
2022 *Selected security threats in cyberspace*, Cybersecurity and Law nr 7, Warszawa.

Filipiak M.
2019 *Postrzeganie bezpieczeństwa korzystania z usług bankowych w segmencie osób młodych*, Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych nr 31.

Górnisiewicz M., Obczyński R., Pstruś M.
2014 *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, KNF Warszawa.

Jain A.K., Gupta B.B.
2016 *A novel approach to protect against phishing attacks at client side using auto-updated white-list*, EURASIP Journal on Information Security nr 9.

Mlaskawa J.
2015 *Biometria w bankowości-szanse i zagrożenia Banku przyszłości*, Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze nr 2.

Penczar M.
2019 *Ochrona klientów i dłużników*, Polityka państwa wobec sektora bankowego w Polsce nr 147.

Pitera R.
2017 *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, Przegląd Nauk o Obronności nr 2.

Protasowicki I.
2016 *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, Zeszyty Naukowe *WSIZiA* nr 4.

Sadowski J.
2017 *Cybernetyczny wymiar współczesnych zagrożeń*, Studia nad bezpieczeństwem nr 2.

Sajler-Fudro P.
2022 *Zagrożenia bezpieczeństwa w użytkowaniu systemów informatycznych– klasyfikacja i metody zapobiegania*, Nauki Ekonomiczne tom XXXV.

Wołyniec J.
2019 *Cybersecurity in the European Union*, Prawo i Polityka nr 9.

Wróblewski W., Tuśnio N.
2023 *Redukcja ryzyka incydentu w oparciu o analizę ryzyka w cyberprzestrzeni operacyjnej straży pożarnej. Perspektywa cyberbezpieczeństwa*, Journal of Modern Science tom 50 nr 1.

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, tj.: Dz.U.2017 poz.2003, ze zm., art.60.

PAWEŁ GŁAZ

# SECURITY OF ELECTRONIC PAYMENTS: CHALLENGES AND SOLUTIONS

**Abstract:** As electronic payments become more common, the importance of online transaction security also increases. This article focuses on discussing the key challenges faced by the security of electronic payments and presents innovative solutions to protect users against cyber threats. The analysis covers various aspects such as data interception, fraud, hacking and identity theft threats. The article presents technological defenses, such as two-factor authentication, biometrics, or coding technologies, which aim to increase the level of security of electronic payments. By analyzing contemporary challenges and effective defense methods, the article is a guide for financial institutions, payment service providers and end users in building a secure space for electronic payments. Providers, and end users in establishing a secure environment for electronic payments.

**Keywords:** cybersecurity, threats, authentication, phishing, fraud

**PAWEŁ GŁAZ**
UNIWERSYTET RZESZOWSKI

# INNOWACYJNE PODEJŚCIE PŁATNOŚCI CZĘŚĆ 3 - FINTECHOWA REWOLUCJA W ŚWIECIE FINANSÓW

**Streszczenie:** Rozdział stanowi analizę głównych aspektów zmiany, jaką przynosi rewolucja FinTechu w dziedzinie usług finansowych. Rozdział skupia się na istocie samego ruchu FinTech oraz jego rozwoju w polskim kontekście, z uwzględnieniem determinant wpływających na jego dalszą ekspansję. Analizując rozwój FinTechu w Polsce, praca ukazuje, jak ten sektor staje się nieodłączną częścią krajobrazu finansowego kraju. Przedsiębiorstwa FinTech w Polsce wprowadzają innowacyjne rozwiązania, które nie tylko przyspieszają transakcje, ale także umożliwiają dostęp do usług finansowych dla szerokich grup społeczeństwa. Czynniki takie jak otwartość na innowacje, elastyczność regulacji i wzrastająca świadomość społeczeństwa wpływają na rozwój tego sektora. Determinanty rozwoju FinTechu, takie jak regulacje, inwestycje technologiczne i zmieniające się oczekiwania klientów, odgrywają kluczową rolę w dalszym kształtowaniu tego dynamicznego ekosystemu.

**Słowa kluczowe:** FinTech, determinanty rozwoju, Revolut, financial technology, usługi bankowe

## WPROWADZENIE

Współczesna era przynosi nieustanny rozwój technologiczny, który wywiera ogromny wpływ na różnorodne dziedziny życia, w tym także na sektor finansowy. Transformacja systemów płatności stanowi jedno z najbardziej dynamicznych zjawisk tego czasu, otwierając przed instytucjami finansowymi i konsumentami nowe perspektywy, wyzwania oraz możliwości. W miarę jak technologie ewoluują, tradycyjne modele płatności i usług bankowych stają w obliczu rewolucyjnych zmian, co niewątpliwie przekształca zarówno

struktury branżowe, jak i oczekiwania klientów. W ślad za zmieniającymi się oczekiwaniami i potrzebami konsumentów oraz zrewolucjonizowanymi metodami interakcji, narodził się FinTech - pojęcie, które odmienia sposób, w jaki myślimy o usługach finansowych. FinTech, krótka forma od Financial Technology, to współczesny ruch technologiczny, który w coraz większym stopniu odmienia krajobraz finansów i przekształca tradycyjne modele dostępu do usług finansowych. Współczesna Polska stała się areną dla dynamicznego rozwoju sektora FinTech. W ciągu ostatniej dekady, nowe przedsiębiorstwa i start-upy wkroczyły na rynek finansowy, wprowadzając innowacyjne rozwiązania, które nie tylko przyspieszają i ułatwiają operacje finansowe, ale również umożliwiają dostęp do usług finansowych dla nowych grup społecznych. Wykorzystując nowoczesne technologie, takie jak mobilność, sztuczna inteligencja, analiza danych czy blockchain, polskie przedsiębiorstwa FinTech odmieniają sposób, w jaki ludzie oszczędzają, inwestują, płacą rachunki i zarządzają swoimi pieniędzmi. Rozwój FinTechu w Polsce nie byłby jednak możliwy bez określonych determinant. Wpływ regulacji, inwestycji w technologię, otwartości na innowacje oraz rosnącej świadomości społeczeństwa w zakresie korzyści płynących z nowoczesnych rozwiązań finansowych - to tylko niektóre z elementów, które wpływają na rozwój FinTechu w Polsce. Analizując istotę, rozwój i determinanty FinTechu w Polsce, konieczne jest dążenie do zrozumienia, jak ta rewolucja technologiczna formuje przyszłość finansów oraz jakie możliwości otwiera przed społeczeństwem. Rozdział został oparty na analizie źródeł oraz literatury. Metoda ta polega zbieraniu, analizie i syntezie istniejących już źródeł, takich jak artykuły naukowe, książki, raporty, dane statystyczne czy dokumenty historyczne, w celu uzyskania głębszego zrozumienia danego tematu badawczego.

## ISTOTA SEKTORA FINTECH

Analizy sektora fintech, należy zacząć od wyjaśnienia pojęcia, czym w ogóle jest sektor FinTech? Fianancial Technology (w skrócie FinTech bądź fintech) określany jest jako rodzaj nowej technologii, której celem jest zautomatyzowanie transakcji a przede wszystkim stworzenie realnej konkurencji dla tradycyjnych metod świadczących usługi w zakresie finansów. Kluczową rolę w demokratyzacji usług finansowych dostępnych dla społeczeństwa odegrały różnorodne urządzenia elektroniczne dostosowane do bankowości cyfrowej oraz platformy umożliwiające inwestowanie w kryptowaluty. Wyraźnym zjawiskiem jest implementacja rozwiązań FinTech w już dobrze prosperujących

instytucjach finansowych, celem ożywienia oferowanych usług. To działanie, mające na celu poprawę pozycji na międzynarodowym rynku, staje się coraz bardziej widoczne. Termin "fintech" najczęściej określa konkretny segment rynku, który spełnia rolę dostarczyciela narzędzi przydatnych w prowadzeniu działań związanych z zarządzaniem finansami. To niewątpliwie rewolucja w sektorze usług finansowych, której wpływ jest coraz bardziej zauważalny na globalnej scenie (Seroka 2021, s. 67). FinTech w swojej istocie to stosunkowo nowy sektor działający w dziedzinie finansów, obejmujący nowe aplikacje, procesy oraz modele biznesowe w branży usług finansowych. W literaturze definiowany jest jako zbiór działań, które dostarczają kompleksowych świadczeń, prowadzonych od początku do końca poprzez internet. Analizując trendy napędzające ten sektor od 2018 roku, wyróżnia się kilka aspektów. Jednym z najbardziej istotnych trendów jest rosnące wykorzystanie technologii blockchain. Technologia blockchain najprościej mówiąc to zdecentralizowana cyfrowa księga, która rozproszona jest wśród wielu użytkowników. W tym kontekście problem, z którym trzeba się zmierzyć polega na tym, że dane nie są dostępne bez klucza dostępu dla jednostki, a zapisy są niezmienne po ich dokonaniu. Wykorzystanie technologii blockchain znajduje zastosowanie w wielu dziedzinach, w tym w sektorze opieki zdrowotnej, gdzie służy do przechowywania dokumentacji medycznej. Dzięki temu szpitale, lekarze, farmaceuci oraz laboratoria mogą zyskać dostęp do danych medycznych pacjentów w sposób przejrzysty, bezpieczny oraz kontrolowany. Wspominając o kryptowalutach, Bitcoin cieszy się największą popularnością, ale ogólna zainteresowanie różnymi kryptowalutami stale wzrasta. Wzrasta liczba kryptowalut wprowadzanych poprzez ICO (Initial Coin Offering), co otwiera nowe perspektywy rozwoju tego rynku. Jednak istnieje pewne zagrożenie związaną z rosnącą różnorodnością kryptowalut, co może prowadzić do rozproszenia rynku. Nadchodzące zmiany w tym obszarze wymagają stałej obserwacji, ze względu na przybywających niedoświadczonych inwestorów oraz pojawiających się "szybkich" sprzedawców (Seroka 2021, s. 67-68). W branży FinTech można wyodrębnić cztery główne segmenty. W obrębie tradycyjnych obszarów bankowości, do których przyporządkowuje się FinTech, należą (Dorfleitner, Hornuf i Weber 2017, s. 111):

- Finansowanie
- Płatności
- Zarządzanie Aktywami
- Inne Rodzaje FinTech

Pierwszy podział pod nazwą „Finansowanie" jest skierowany zarówno do przedsiębiorstw jak i osób prywatnych. Możliwy jest również jego podział na poszczególne podsegmenty kierowane do dużej grupy uczestników, czyli „crowfundingowy" oraz segment, który oferuje usługi „faktoringowe, pożyczkowe oraz kredytowe". Wspomniany wcześniej „crowfunding" obejmuje finansowanie, którego istotą jest zapewnienie środków finansowych potrzebnych do realizacji celu dzięki dużej liczbie współpracowników. "Crowdfunding" jest dalej dzielony na cztery podsegmenty, z uwzględnieniem rodzaju otrzymywanego wynagrodzenia. "Zarządzanie aktywami" obejmuje FinTechy oferujące doradztwo, zarządzanie aktywami oraz zagregowane wskaźniki majątku osobistego. "Boty i robo-doradcy" odnoszą się do systemów zarządzania portfelem, zapewniając zautomatyzowane doradztwo inwestycyjne. Podsegment "zarządzania finansami osobistymi" obejmuje podmioty FinTech, które oferują prywatne planowanie finansowe. Jego głównym celem jest umożliwienie klientom wizualizacji w jednej aplikacji aktywów, które zdeponowali w różnych instytucjach finansowych, a także pożyczek zaciągniętych od różnych kredytodawców. Do podsegmentu "zarządzania inwestycjami i bankowości" należą instytucje oferujące tradycyjne produkty bankowe, takie jak rachunek gotówkowy. Kolejny segment „płatności" charakteryzuje się szerokim zaznaczeniem, obejmując podmioty FinTech, w których zarówno aplikacje jak i usługi dotyczą transakcji płatniczych krajowych oraz międzynarodowych. Podsegment "blockchain i kryptowaluty" - podobnie jak w przypadku tradycyjnych środków płatniczych - umożliwia zapisywanie, użytkowanie oraz wymianę kryptowalut. "Alternatywne metody płatności" obejmują podmioty realizujące płatności mobilne. Segment "inne rodzaje FinTech" zawiera usługi, które nie są przypisane do trzech tradycyjnych funkcji bankowych. Termin "InsurTech" określa przedsiębiorstwa FinTech oferujące ubezpieczenia lub ułatwiające ich nabycie. Do "innych rodzajów FinTechów" zaklasyfikowano wyszukiwarki i strony porównawcze. Podsegment "technologia, IT i infrastruktura" oferuje rozwiązania techniczne, dedykowane dostawcom usług finansowych (Seroka 2017, s. 69).

## FINTECH W POLSCE

Stały oraz dynamiczny rozwój sektora usług bankowych w tym szczególnie sektora FinTech, odgrywa coraz większy wpływa na polską rzeczywistość związaną z bankowością. Ten ciągły postęp może być analizowany pod kątem zmian w liczbie tradycyjnych placówek bankowych na przestrzeni lat.

Analizując dane dostępne w internecie na ten temat wysuwa się stwierdzenie, iż zdecydowana większość analizowanych banków zmniejszyła liczbę swoich placówek w latach 2014-2016. Największy bank w Polsce, czyli PKO BP, dokonał redukcji liczby swoich placówek w latach 2015 i 2016. W tych okresach, bank ograniczył ilość swoich oddziałów odpowiednio o 40 i 41, co w efekcie spowodowało spadek liczby placówek o ponad 6% w ciągu dwóch lat. Drugim pod względem wielkości bankiem w Polsce jest Pekao SA, który przeprowadził jeszcze bardziej znaczącą redukcję swoich placówek. W IV kwartale 2016 roku liczba oddziałów tego banku zmniejszyła się o ponad 10% w porównaniu do IV kwartału 2014 roku. W okresie od IV kwartału 2014 roku do IV kwartału 2015 roku ilość placówek została ograniczona o 59 (prawie 6%), a w ciągu kolejnego roku zmniejszyła się o 47 (niemalże 5%) (Dec 2018, s.62). Na postawie tych badań zauważalny jest widoczny trend spadkowy w liczbie stacjonarnych placówek. Coraz wygodniejszy dostęp do bankowości mobilnej oraz dostępność usług internetowych oferowanych przez banki powoduje, iż większość użytkowników woli załatwiać sprawy bez wychodzenia z domu. Tendencja ta utrzymuje się stale co przekłada się na kolejne zamknięte placówki. Sytuację tą dobrze obrazuje analiza przeprowadzona przez Martę Czarkowską oraz Bartosza Bagniewskiego. W analizowanym okresie 2012 do II kwartału 2022 roku liczba oddziałów, filii, ekspozytur i innych placówek obsługi klienta stopniowo zmniejszała się. W okresie dziesięciu lat (od 2012 roku do drugiego kwartału 2022 roku), liczba oddziałów spadła z 7534 do 5116, co stanowi zmniejszenie o około 32%. Dane udostępnione przez Komisję Nadzoru Finansowego (KNF) pokazują, że w czerwcu 2022 roku zamknięto kolejne 21 oddziałów bankowych. Tendencję tę napędziła rewolucja technologiczna, ewolucja preferencji użytkowników w zakresie usług bankowych oraz procesy automatyzacji i przyspieszenia w sektorze finansowym. Podobne zmiany zaobserwowano w przypadku liczby filii, ekspozytur i innych placówek obsługi klienta. W 2012 roku ich liczba wynosiła 4876, a dziesięć lat później zmniejszyła się prawie o połowę, do 2516 (spadek o około 48%) (Czarkowska i Bagniewski 2022, s. 15). Za wypełnienie tej luki na rynku bankowości w Polsce odpowiadają właśnie FintTechy, przejmując część usług tradycyjnych banków i przenosząc je do świata wirtualnego. Przykładem takiego Fintechu w Polsce jest spółka Blue Media S.A., obecnie zamieniająca się w Autopay, założona w 1999 r. Spółka skupia się na dostarczaniu innowacyjnych rozwiązań związanych z płatnościami elektronicznymi oraz obsługą transakcji online dla różnych sektorów i branż. Jednym z głównych obszarów działalności Blue Media S.A. jest platforma płatnicza. Jest to zaawansowany

system, który umożliwia firmom, instytucjom oraz sklepom internetowym przyjmowanie płatności online w sposób wygodny i bezpieczny. Spółka oferuje wsparcie dla różnych metod płatności, takich jak karty płatnicze, e-portfele czy tradycyjne przelewy bankowe. Dzięki temu przedsiębiorstwa mogą zwiększyć swój zasięg i ułatwić klientom dokonywanie transakcji online. Blue Media S.A. jest również liderem w dostarczaniu rozwiązań dla sektora e-commerce. Oferuje narzędzia, które ułatwiają obsługę płatności w sklepach internetowych. Spółka dba o wydajność i bezpieczeństwo procesu płatności, co ma kluczowe znaczenie dla budowania zaufania klientów. Dzięki powszechnemu wykorzystaniu ich systemów możliwe jest dokonywanie płatności natychmiastowych między bankami pod nazwą BlueCash. Od 2019 r. posiadają w swojej ofercie również system służący do automatycznego poboru opłat na bramkach autostradowych bez konieczności czekania w kolejce na bramkach. Za ich pośrednictwem dostępna jest platforma umożliwiająca doładowanie dowolnego numeru na kartę w trybie online, 24h na dobę przez 7 dni w tygodniu. Klient podaje numer telefonu, operatora oraz kwotę doładowania, a następnie finalizuje transakcję. Po zatwierdzeniu, środki pojawiają się na jego koncie w zaledwie kilka sekund. Ten zaawansowany system wspomaga proces doładowań dokonywanych na stronach internetowych operatorów komórkowych, w bankowości internetowej oraz w aplikacjach mobilnych banków. Dzięki temu klienci mają możliwość wyboru najwygodniejszego sposobu doładowania, dostosowanego do ich aktualnych potrzeb (BlueMedia 2023).

## FINTECHOWY GIGANT

Kolejnym z przykładów ekspansji przedsiębiorstw FinTechowych jest brytyjska firma finansowa o nazwie Revolut. Funkcjonuje on jako nowoczesna platforma finansowa i aplikacja mobilna, oferująca w swojej gamie szereg usług bankowych, płatności oraz usług walutowych. Revolut został założony w 2015 r. za sprawą założycieli Nika Storonsky'ego i Vlada Yatsenki, a w 2018 r. otrzymał licencję Banku Litwy. Oznaczało to nowy krok dla przedsiębiorstwa, gdyż od tego momentu w Polsce oraz krajach Europejskiego Obszaru Gospodarczego, działa on jako bank, gwarantując klientom ochronę swoich zgromadzonych środków za pośrednictwem systemu gwarancji depozytów. Swoją popularność zyskał zaledwie w ciągu 5 lat, głównie za sprawą możliwości prowadzenia konta walutowego bez dodatkowych opłat (Revolut 2023). Bank ten zapewnia wsparcie dla rachunków w 35 różnych walutach, realizując przeliczenia według kursu międzybankowego. Ponadto każdy

z użytkowników posiada możliwość dokonywania płatności za pomocą kart płatniczych wydanych za pośrednictwem renomowanych organizacji płatniczych takich jak Mastercard czy Visa. Każdy użytkownik Revoluta może natychmiastowo zasilić rachunek powiązany z kartą za pomocą innych kart płatniczych w złotówkach, jednocześnie zachowując saldo w tej walucie. Przewalutowanie transakcji odbywa się dopiero w momencie dokonywania transakcji za pośrednictwem karty płatniczej lub wypłaty gotówki z bankomatu za granicą, zgodnie z obowiązującym kursem międzybankowym. Zaletą takiego podejścia do bankowości jest możliwość uniknięcia dodatkowych kosztów dla użytkowników w postaci spreadu walutowego, który często podnosi cenę usług walutowych oferowanych przez banki (Górka 2018, s. 155). Firma codziennie otwiera 8-10 tysięcy nowych kont, a jej obroty sięgają 4 miliardów dolarów amerykańskich rocznie. Planuje zdobycie 100 milionów klientów w ciągu najbliższych pięciu lat. W planach Revoluta jest również poszerzenie swojej oferty o produkty depozytowe, pożyczki konsumenckie oraz platformę do inwestowania w akcje bez dodatkowych prowizji. Obecnie firma jest najszybciej rozwijającym się fintechiem także w Polsce. Celem zarządu jest dążenie do tego, aby stać się najpopularniejszą aplikacją bankową w Polsce, która również umożliwiać będzie zaciągnięcie pożyczki zaledwie w przeciągu kwadransa, przy jednoczesnym utrzymaniu konkurencyjnych kosztów z perspektywy klienta (Milic-Czerniak 2019, s. 41).

## DETERMINANTY ROZWOJU

Obecnie obserwuje się dynamiczny rozwój sektora FinTech, co powoduje, że od początku 21w. można mówić już o trzech generacjach FinTech. Pierwsza generacja, znana jako FinTech 1.0, zadebiutowała w połowie pierwszej dekady XXI wieku wraz z pierwszą falą start-upów. Te start-upy oferowały udoskonalony dostęp do już istniejących usług bankowych. Ich klientelą docelową były zarówno same banki, jak i podmioty rywalizujące z bankami, a także firmy dążące do stworzenia zupełnie nowych rynków usług finansowych. Począwszy od początku drugiej dekady, pojawiła się kolejna generacja znana jako FinTech 2.0. Jest to moment, w którym banki zaczęły dostrzegać potencjał, jaki niosły ze sobą firmy fintechowe. Zaczęły one nawiązywać współpracę, inwestować oraz wspierać rozwój podmiotów działających w tym sektorze. Współpraca ta pozwoliła na tworzenie synergii między tradycyjnymi instytucjami finansowymi a nowoczesnymi firmami technologicznymi. Obecnie, przemieszczając się w erę FinTech 3.0, można zaobserwować dalszą

ewolucję. W tej generacji to same banki stają się częścią ruchu fintechowego. Kreują one hybrydowe narzędzia, które łączą tradycyjne usługi bankowe z zaawansowanymi technologicznie rozwiązaniami. Ten trend umożliwia bankom przekształcenie się i dopasowanie do coraz bardziej cyfrowego i innowacyjnego środowiska finansowego. Generacje FinTech 1.0, 2.0 i 3.0 reprezentują kolejne fazy rozwoju sektora finansowego, w których technologia, innowacje i współpraca z bankami stanowią kluczowe elementy. To przykład, jak szybkie zmiany technologiczne mogą przekształcać tradycyjne usługi finansowe i kształtować nowe paradygmaty w obszarze finansów (Harasim i Mitręga-Niestrój 2018, s. 175). Rozwój sektora FinTech napędzany jest wieloma czynnikami, których analizę można rozpocząć z perspektywy popytowej, podażowej oraz instytucjonalno- regulacyjnej. Aktualnie najważniejszym motorem wzrostu FinTech jest wyraźny popyt ze strony rynku. Powszechny dostęp do internetu oraz zdolność do przeprowadzania transakcji w czasie rzeczywistym za pośrednictwem urządzeń z dostępem do sieci spowodowały wzrost oczekiwań klientów w zakresie wygody, prostoty, szybkości i kosztów usług finansowych. Wzrastające wymagania klientów w dziedzinie usług finansowych są często kształtowane przez interfejsy cyfrowe dostarczane przez firmy technologiczne, takie jak Apple, Google czy Facebook. To zjawisko jest dodatkowo wspierane przez trend demograficzny, ponieważ pokolenie Y, znane również jako milenialsi, które jest ukształtowane przez technologię i aktywność w mediach społecznościowych, obecnie osiąga etap życia, w którym potrzebuje różnorodnych usług finansowych. Często tradycyjny model tych usług nie odpowiada ich oczekiwaniom, w związku z czym poszukują oni alternatywnych rozwiązań, które lepiej pasują do ich stylu życia i sposobu myślenia (Szpringer 2019, s. 32-33). Postęp technologiczny rewolucjonizuje krajobraz finansowy, wywołując z jednej strony wzrost konkurencji wobec tradycyjnych instytucji finansowych, ze strony rozwijającego się sektora FinTech. Ten trend, choć stanowi wyzwanie, równocześnie niesie ze sobą potencjał współpracy, a nie rywalizacji, pomiędzy bankami a przedsiębiorstwami FinTech. Rozwijające się technologie nie tylko skłaniają banki do wprowadzania wewnętrznych programów innowacyjnych, ale również promują partnerstwa i kooperację. Coraz częściej, instytucje finansowe widzą w firmach FinTech potencjalnych akceleratorów, a nie zagrożenie dla ich egzystencji. Wspólna praca pozwala bankom korzystać z innowacyjnych rozwiązań i dostosować się do zmieniających się oczekiwań klientów. Niebagatelną rolę w rozwoju FinTechu odgrywa również przyjazne i proaktywne nastawienie organów regulacyjnych oraz rządów. Przejście od sceptycyzmu do wspierania

tego sektora widoczne jest na poziomie międzynarodowym, a także w obrębie Unii Europejskiej. Nowe ramy regulacyjne, jak regulatory sandbox, tworzą przestrzeń, w której zarówno nowe start-upy, jak i instytucje mogą testować innowacyjne pomysły i rozwiązania, zanim zostaną w pełni wdrożone w procesie licencyjnym. W kontekście Unii Europejskiej obserwujemy dążenie do zrozumienia i wsparcia sektora FinTech. Kompleksowe strategie oraz eliminowanie barier regulacyjnych to oznaki tego, że organy nadzorujące starają się tworzyć warunki, które pozwolą na rozwijanie się tej branży. To ukazuje, że FinTech staje się integralną częścią przyszłości sektora finansowego, a wspieranie innowacji staje się kluczowym celem działań regulacyjnych. W związku z powyższym, widzimy, że rozwój technologiczny i sektor FinTech nie tylko zmieniają oblicze finansów, ale również przyczyniają się do tworzenia nowych ekosystemów opartych na współpracy, innowacjach i elastyczności regulacyjnej. To wspólna praca banków, firm FinTech oraz organów regulacyjnych może skierować tę rewolucję w kierunku, który korzysta zarówno z instytucji tradycyjnych, jak i z nowoczesnych technologii, tworząc w ten sposób korzystne dla wszystkich środowisko finansowe (Butor-Keler 2019, s. 39-40).

## PODSUMOWANIE

W świetle analizy przedstawionej w artykule, można dostrzec, że FinTech stanowi nie tylko znaczący etap w ewolucji sektora finansowego, ale także rewolucję o globalnym zasięgu, która przekształca sposób, w jaki zarówno instytucje finansowe, jak i klienci funkcjonują w świecie finansów. Przenosząc tradycyjne usługi finansowe w erę cyfrowego ekosystemu, FinTech stwarza nowe możliwości, ale również stawia wyzwania przed wszystkimi zaangażowanymi stronami. W Polsce, FinTech stanowi siłę napędową dla przekształceń w sektorze finansowym. Świadomość wśród przedsiębiorców oraz inwestorów w zakresie potencjału, jaki niesie ze sobą nowoczesna technologia, sprawia, że polski rynek staje się atrakcyjnym polem dla innowacji. Jednakże, aby pełni wykorzystać potencjał tego sektora, konieczne jest zrozumienie determinant jego rozwoju, takich jak otwartość na innowacje, elastyczność regulacji oraz współpraca między sektorem publicznym a prywatnym. Podsumowując, FinTech to nie tylko zmiana w sposobie, w jaki zarządzamy swoimi finansami, to również nowa era, która kształtuje naszą relację z pieniędzmi, technologią i dostępem do usług. Niezaprzeczalnie, przyszłość finansów będzie zdominowana przez dalszy rozwój FinTechu, gdzie innowacyjność i elastyczność będą kluczowymi czynnikami kształtującymi branżę. Jednakże, aby ten rozwój

mógł być odpowiedzialny i zrównoważony, konieczne jest równoważenie innowacji z ochroną danych i przestrzeganiem norm regulacyjnych. Dzięki temu FinTech może pełnić swoją rolę w dostarczaniu bardziej efektywnych, dostępnych i dostosowanych usług finansowych, którymi każdy może korzystać w erze cyfrowego przekształcenia.

## BIBLIOGRAFIA

Butor-Keler A.
2019 *Nowe zagrożenia dla konsumentów wynikające z rozwoju FinTech*, Studia Ekonomiczne nr 379.

Czarkowska M., Bagniewski B.,
2022 *Wpływ rozwoju FinTech na stacjonarne oddziały instytucji bankowych w Polsce* , E-mentor. Czasopismo naukowe Szkoły Głównej Handlowej w Warszawie nr 97.

Dec P.
2018 *Rozwój sektora FinTech a tradycyjna bankowość–ujęcie ilościowe*, Warszawa.

Dorfleitner G., Hornuf I., Weber M.
2017 *Fintech in Germany*, Cham.

Górka J.
2018 *Banki, GAFAM, FinTech w gospodarce współdzielenia–equilibrium współpracy i konkurencji*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 531.

Harasim J., Mitręga-Niestrój K.
2018 *FinTech–dylematy definicyjne i determinanty rozwoju*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu nr 531.

Milic-Czerniak R.
2019 *Rola fintechów w rozwoju innowacji finansowych*, Studia BAS nr 1, Kancelaria Sejmu.

Seroka A.
2021 *Rozwój sektora FinTech w polskiej bankowości*, Przestrzeń, Ekonomia, Społeczeństwo nr 19.

Szpringer W.
2019 *Fintech i blockchain–kierunki rozwoju gospodarki cyfrowej*, Studia BAS nr 1.

**Strony Internetowe**

BlueMedia
2023 https://bluemedia.pl/ [dostęp z dnia 8.08.2023].

Revolut
2023 https://www.revolut.com/pl-PL/ [dostęp z dnia 8.08.2023].

## FINTECH - REVOLUTION IN THE WORLD OF FINANCE

**Abstract:** The article is an analysis of the main aspects of the change brought about by the FinTech revolution in the field of financial services. The article focuses on the essence of the FinTech movement and its development in the Polish context, considering the determinants affecting its further expansion. Analyzing the development of FinTech in Poland, the article shows how this sector is becoming an inseparable part of the country's financial landscape. FinTech companies in Poland introduce innovative solutions that not only speed up transactions, but also enable access to financial services for wide groups of society. Factors such as openness to innovation, flexibility of regulations and increasing public awareness influence the development of this sector. The determinants of FinTech development, such as regulations, technological investments and changing customer expectations, play a key role in further shaping this dynamic ecosystem.

**Keywords:** FinTech, determinants of development, Revolut, financial technology, banking services

MARCELINA WACŁAWSKA, MONIKA WACŁAWSKA
NATALIA TYSZCZUK, HUBERT ROGALA
UNIWERSYTET MEDYCZNY W LUBLINIE

# NEUROBLASTOMA – AKTUALNE DONIESIENIA DOTYCZĄCE DIAGNOSTYKI I LECZENIA

**Streszczenie:** Neuroblastoma jest guzem pochodzenia współczulnego o niejednorodnym przebiegu klinicznym. Jest to grupa guzów, które są prawie najczęstszymi pozaczaszkowymi guzami litymi w dzieciństwie. Nowotwory te mają niekorzystne rokowanie i są przyczyną 15% zgonów z powodu nowotworów wieku dziecięcego. Nerwiaki niedojrzałe znajdują się w dowolnym miejscu łańcucha współczulnego, ale najczęściej występują w nadnerczach. Objawy choroby nie zawsze są specyficzne, może wystąpić jedynie ogólne osłabienie lub wzrost temperatury. Jak dotąd dane dostarczane przez klinicystów są wciąż niekompletne, aby w pełni zrozumieć chorobę. Pomimo wielu badań przewidywanie pacjentów z nerwiakiem niedojrzałym pozostaje trudne. Celem artykułu jest przegląd aktualnych badań nad leczeniem i diagnostyką nerwiaka niedojrzałego. Rozpoznanie tej choroby opiera się na biopsji guza i obecności podwyższonego poziomu katecholamin w moczu. Choroba pośrednia jest leczona kilkoma cyklami chemioterapii, po których następuje resekcja chirurgiczna. Choroba wysokiego ryzyka ma złe rokowania, ale przeżycie stopniowo poprawia się dzięki terapii multimodalnej, w tym immunoterapii. Istnieje jednak potrzeba znalezienia nowych strategii terapeutycznych, które poprawią rokowanie i zmniejszą niepożądane skutki dotychczas stosowanych terapii.

**Słowa klucze:** Neuroblastoma, MIBG, MYCN, guz lity

## WPROWADZENIE I CEL

Neuroblastoma to nowotwór embrionalny obwodowego współczulnego układu nerwowego. Jest drugim najczęstszym guzem litym wieku dziecięcego

występującym poza czaszką. Aż 15 % wszystkich zgonów z powodu nowotworów u dzieci stanowi właśnie Neuroblastoma (Swift CC, 2018, 566-580).

Guzy Neuroblastoma najczęściej rozwijają się w jamie brzusznej i najczęściej są zlokalizowane w nadnerczach (Zafar A, 2021, 961-1021). Występują również wzdłuż zwojów współczulnych. Neuroblastoma, śródbrzuszne, szczególnie pochodzące z przestrzeni zaotrzewnowej, najczęściej nie prezentują żadnych objawów i stanowią bezobjawowe masy wykrywane przez rodziców lub w trakcie rutynowych badań kontrolnych. Natomiast lokalizacja guza w miednicy może uciskać pęcherz lub odbytnicowo-sigmoidalną okrężnicę co może powodować zatrzymanie moczu lub zaparcie. Obecność Neuroblastoma w klatce piersiowej zwykle nie prowadzi do zauważalnych objawów i jest rozpoznawany przypadkowo w badaniach radiologicznych.

Objawy u dzieci chorych na nerwiaka niedojrzałego zależą od liczby i lokalizacji nowotworów i mogą obejmować zarówno objawy miejscowe, jak i ogólnoustrojowe. U około połowy pacjentów występuje regionalnie natomiast u pozostałych występują przerzuty odległe do kości, szpiku kostnego. Najczęściej odnotowanym miejscem przerzutów jest wątroba. Większość nowotworów nerwiaka niedojrzałego powstaje w jamie brzusznej najczęstszą pierwotną lokalizacją nerwiaka niedojrzałego jest nadnercze. Masy brzuszne mogą przebiegać bezobjawowo lub mogą być ich następstwem przy nadciśnieniu, bólu brzucha, wzdęciach lub zaparciach z miejscowego wpływu na narządy jamy brzusznej. U około 10–15% pacjentów z nerwiakiem niedojrzałym guz szerzy się do przestrzeni zewnątrzoponowej lub wewnątrztwardówkowej, która może prowadzić do ucisku rdzenia kręgowego i paraplegii. Neuroblastoma też zwykle rozprzestrzenia się na kości oczodołowych, powodując powstawanie wybroczyn około oczodołowych charakterystycznych dla nerwiaka niedojrzałego. Towarzyszy im również wytrzeszcz i ewentualne zaburzenia widzenia. Nowotwory z obszaru szyjnego lub klatki piersiowej występują częściej u niemowląt, co może być związane z zespołem Hornera. Objawia się to jednostronnie opadającymi powiekami, anhydrozą, zwężeniem źrenic oraz objawami ze strony układu oddechowego (Whittle SB, 2017, 369-386).

Ciekawe wydają się objawy powodowane przez guza zlokalizowanego w szyjce macicy prezentujące typowy zespół Hornera (Ishola TA, 2007, 149-156). Wczesne objawy guza zazwyczaj są niespecyficzne: ogólne złe samopoczucie,spadek masy ciała i niewyjaśniona gorączka. Guz może także prowadzić do samoistnych krwotoków i prowadzić do wyniszczenia i anemii. Ciężkie objawy występują kiedy guz osiąga bardzo duży rozmiar lub zaczyna przerzutować (El Shafie M, 1983, 34-36).

Przerzuty do kości objawiają się bólami kości i ogólnym pogorszeniem sprawności oraz aktywności ruchowej. W przypadku zajęcia czaszki mogą wystąpić wybroczyny, wytrzeszcz. Bardzo niebezpieczne są guzy zlokalizowane przykręgosłupowe, ponieważ mogą uciskać rdzeń kręgowy i prowadzić do postępującej paraplegii. U niemowląt z Neuroblastoma można zauważyć podskórne,niebolesne,niebieskawe guzki zwane zespołem muffinów jagodowych. Objawy takie są charakterystyczne dla choroby w stadium 4S i wskazują na korzystną prognozę i możliwość spontanicznej regresji nowotworu,

Zespoły paranowotworowe występują stosunkowo rzadko, zazwyczaj u pacjentów z nerwiakiem niedojrzałym. Na uwadze trzeba mieć to,że Neuroblastoma wydziela wazoaktywny peptyd jelitowy przez co u pacjentów z tym guzem może rozwijać się oporna na leczenie biegunka prowadząca do odwodnienia i hipokaliemii (Hiyama E, 1994, 1821-6).

Celem prezentowanego artykułu jest przegląd i prezentacja aktualnych doniesień dotyczących właściwego rozpoznawania i leczenia Neuroblastoma. Informacje przekazane w poniższej pracy zostały uzyskane z przeszukiwania baz naukowych: PubMEd i Google Scholar. Artykuł powstał bazując na strategii wyszukiwania kluczowych słów takich jak: Neuroblastoma, MIBG, MYCN. Dostępne artykuły zostały wyselekcjonowane pod kątem ich wartości merytorycznej i związku tematycznego z tym artykułem.

## OPIS STANU WIEDZY

### Epidemiologia i etiologia

Neuroblastoma jest najczęstszym guzem litym występującym pozaczaszkowo u dzieci. Stanowi 6-8% wszystkich nowotworów wieku dziecięcego. Współczynnik zachorowalności w Polsce w ciągu roku wynosi 9,3 na 1 milion dzieci do 14. roku życia. Szczyt zachorowań przypada na 2. rok życia, natomiast 90% przypadków występuje u dzieci do 5.rż. Jednocześnie jest to najczęstszy nowotwór złośliwy okresu noworodkowego- około 37% zachorowań odnotowuje się na ten przedział wieku rozwojowego (Perek D, 2014, 624-630). Nerwiak zarodkowy współczulny rzadko występuje u starszych dzieci, a jeszcze rzadziej u młodzieży i młodych dorosłych. Statystycznie chłopcy chorują nieznacznie częściej (1,2:1). Nie ma znaczących różnic w częstości występowania tego nowotworu pod względem przynależności rasowej pacjenta, jednakże odnotowuje się wyższą złośliwość nerwiaka wśród rasy czarnej,

a zatem gorszą jego odpowiedź na leczenie i rokowanie (Henderson TO, 2011, 15-24).

Etiologia rozwoju nerwiaka zarodkowego nie jest do końca poznana. Naukowcy stale poszukują czynników ryzyka, które zaburzają różnicowanie i dojrzewanie pierwotnych komórek grzebieni nerwowych. Z tej przyczyny kluczowe wydaje się zakwalifikowanie tego guza do grupy chorób związanych z zaburzeniami rozwoju cewy nerwowej. Niejednokrotnie podłożem neuroblastoma są czynniki genetyczne przekazywane dziecku przez rodzica. Około 1% do 2% pacjentów z neuroblastoma posiada dodatni wywiad rodzinny z tą chorobą. Wśród nich nowotwór zazwyczaj ujawnia się w młodszym wieku (ok. 9 miesiąc życia przy zdiagnozowaniu) i możliwe jest wystąpienie choroby pierwotnie wieloogniskowej nawet u 20%. U dzieci ozdrowieńców w 50% przypadków istnieje ryzyko rozwoju tego nowotworu. W badaniach cytogenetycznych najczęściej mówi się o delecji dystalnego odcinka krótkiego ramienia 1 chromosomu- del 1p36, mutacji genu kinazy anaplastycznego chłoniaka ALK (Anaplastic Lymphoma Kinase), amplifikacji w rejonie dystalnego odcinka chromosomu drugiego zawierającego protoonkogen MYCN, jak też wielu innych (Mossé YP,2008, 883-4).

**Diagnostyka**

Za rozwój Neuroblastoma odpowiada wiele czynników genetycznych (np. amplifikacja genu MYCN), a także okołoporodowych i ciążowych. Niestety do tej pory nadal nie potwierdzono żadnego konkretnego narażenia środowiskowego lub rodzicielskiego odpowiedzialnego za rozwinięcie NB(6). MYCN jest amplifikowany w 20% do 25% nerwiaka niedojrzałego, ponadto Neuroblastoma z amplifikacją MYCN przyczynia się do dużego odsetka zgonów. Wzmocniony MYCN wzmacnia napływ żelaza do komórki poprzez zwiększoną ekspresję receptora transferyny. Nagromadzenie żelaza powoduje wytwarzanie reaktywnych form tlenu (ROS) (Floros KV, 2021, 1896-1908).

U pacjentów z podejrzeniem nerwiaka niedojrzałego oprócz USG szyi, śródpiersia i brzucha oraz prześwietlenia klatki piersiowej, przeprowadza się badania kliniczne. Badania fizykalne z oceną lokalizacji i wielkości masy znajdującej się w jamie brzusznej i ocena stopnia hepatomegalii też są istotne. Poziomy swoistej dla neuronów enolazy (NSE) i dehydrogenazy mleczanowej (LDH) są badane, a także wydalanie katecholamin z moczem (Simon T, 2017, 147-167).

Ocena określenia stopnia zaawansowania choroby u dzieci z nerwiakiem niedojrzałym zwykle jest możliwa dzięki obrazowaniu guza pierwotnego za pomocą CT lub MRI ( Bleeker G, 2015, 9). W celu identyfikacji rozprzestrzeniania się guza do innych odległych miejsc obrazuje się klatkę piersiową. brzuch i miednicę. Meta-jodobenzyloguanidyna (MIBG) może być wykorzystywana do wykrywania guzów pierwotnych i miejsc przerzutowych, przy czym około 90% pacjentów ma guzy MIBG dodatnie ( Taggart DR, 2009, 131). Dla pacjentów bez MIBG stosuje się skany pozytonowej tomografii emisyjnej z [18F]-fluorodeoksyglukozą (FDG-PET) (Sharp SE, 2009, 1237-1243).

W przypadku podejrzenia przerzutów wewnątrzczaszkowych należy również wykonać CT głowy lub MRI mózgu. Oprócz badań obrazowych, rekomenduje się aspiracje szpiku kostnego i biopsje z co najmniej dwóch niezależnych miejsc aby określić stopień zaawansowania guza. Oczywiście ostateczne rozpoznanie stawiane jest na podstawie biopsji z rozpoznaniem histopatologicznym w połączeniu z podwyższonym poziomem katecholamin w moczu lub surowicy, bądź dodatni skan MIBG plus aspirat szpiku kostnego lub biopsja z wykrywalnymi komórkami nowotworowymi (Cheung NK, 1999, 84-87).

**Stopień zaawansowania**

Opracowanie i wykorzystanie międzynarodowych systemów oceny stopnia zaawansowania, takich jak INSS-International Neuroblastoma Staging System, zapewniło spójność oceny stopnia zaawansowania pacjentów z Neuroblastoma na całym świecie (Whittle SB, 2017, 369-386). Neuroblastoma został podzielony na cztery główne stadia to jest: zlokalizowane stadia L1 i L2, rozsiane stadium M i rozsiane stadium MS. Stadium MS występuje u pacjentów poniżej 18 miesiąca życia. W klasyfikacji guzów Neuroblastoma bierze się pod uwagę stopień zróżnicowania,obecność lub brak zrębu, wiek pacjenta, status onkogenu MYCN, pliodię DNA i status chromosomu 11q.21,22 (Shimada H, 1984, 405-416).

**Rola MYCN w Neuroblastoma**

Wśród zaawansowanych przypadków Neuroblastoma, prawie 25% przypadków dotyczy amplifikacji onkogennego MYCN. Rolą MYCN jest kodowanie wiążącego E-BOX czynnika transkrypcyjnego typu basic-helix-leucyn

(bHLH-LZ). Wykazano, że MYCN kieruje transkrypcyjnym przekształceniem receptora importującego żelazo i sprawia, że Neuroblastoma staje się zależny od szklaku GSH. Zaobserowano,że NB z amplifikacją MYCN są wrażliwe na celowanie w ten szlak, chemicznie lub genetycznie, i że ten szlak jest aktywowany przez MYCN, przynajmniej częściowo, w celu detoksykacji ROS z nadmiernego importu żelaza. Przez powyższe uważa się, że zastosowanie zatwierdzonego przez FDA leku na reumatoidalne zapalenie stawów, auranofina, oraz lek SAS na reumatoidalne zapalenie stawów i wrzodziejące zapalenie jelita grubego, są skuteczne przeciwko Neuroblastoma z amplifikacją MYCN, poprzez ukierunkowanie aktywności przeciwutleniającej (Floros KV, 2021, 1896-1908).

**Leczenie**

Nisko zróżnicowane guzy o korzystnej biologii są zwykle leczone wyłącznie przez resekcję chirurgiczną. Nowotwory o słabym profilu biologicznym po leczeniu chirurgicznym są poddawane agresywnej chemioterapii (Nakagawara A, 2018, 214-241). Leczenie nerwiaków zarodkowych wysokiego ryzyka dzieli się na 3 fazy: indukcja remisji, konsolidacja remisji, i faza konserwacji skoncentrowana na zwalczeniu minimalnej choroby resztkowej. Wyniki badań wykazują, że zwiększenie intensywności chemioterapii indukcyjnej wiąże się z poprawą odsetka odpowiedzi i całkowitego przeżycia. Podstawowy schemat chemioterapii indukcyjnej obejmuje intensywne cykle cisplatyny ietopozyd na przemian z winkrystyną, doksorubicyną i cyklofosfamidem (Maris JM, 2010, 2202-11).

Neuroblastoma to nowotwór promieniowrażliwy i radioterapia jest krytycznym elementem terapii po leczeniu indukcyjnym. Obecne protokoły zwykle stosują dawkę 2100 cGy w leczeniu konsolidacyjnym w schematach frakcjonowanych lub hiperfrakcjonowanych. Połączenie chemioterapii o dużej dawce, zabiegu chirurgicznego i radioterapii hiperfrakcjonowanej w miejscu pierwotnym w dawce 2100 cGy powoduje zmniejszenie wskaźnika nawrotów,który wynosi<10% (Wolden SL, 2008, 369-386). W Neuroblastoma występuje GD2 czyli powierzchniowy antygen glikolipidowy, który jest idealnym celem immunoterapii. Jednakże immunosupresja wywoływana przez schematy chemioterapii NB stwarzają niekorzystne warunki do stosowania immunoterapii czynnej, ale pozwala na zastosowanie immunoterapii biernej po zakończeniu chemioterapii indukcyjnej lub ASCT. MoAb anty-GD2 stanowią obecnie podstawę immunoterapii Neuroblastoma i jego profil

bezpieczeństwa znajduje się na optymalnym poziomie (Cheung NK, 1998, 3053-60).

## PODSUMOWANIE

Neuroblastoma staje się guzem uleczalnym ze względu na postępy w leczeniu, dobrze opracowane strategie a także dość dobrą diagnostykę. Niestety należy pamiętać, że nawet po zakończeniu sukcesywnej terapii pacjenci z nerwiakiem niedojrzałym zazwyczaj cierpią z powodu toksyczności stosowanych leków i prowadzonych badań. Istnieje potrzeba współpracy różnych środowisk klinicznych w podejmowaniu nowych strategii, które powinny skutkować bardziej precyzyjnymi i skutecznymi opcjami terapeutycznymi.

## BIBLIOGRAFIA

Bleeker G, Tytgat GAM, Adam JA, et al. 123I-MIBG scintigraphy and18F--FDG-PET imaging for diagnosing neuroblastoma. Cochrane-Database Syst Rev. 2015:CD009263. DOI:10.1002/14651858.CD009263.pub2

Cheung NK, Heller G, Kushner BH, et al. Detection of neuroblastoma in bone marrow by immunocytology: is a single marrow aspirate adequate? Med Pediatr Oncol. 1999;32:84-87

Cheung NK, Kushner BH, Cheung IY, et al. Anti-G(D2) antibody treatment of minimal residual stage 4 neuroblastoma diagnosed at more than 1 year of age. J Clin Oncol 1998;16.

El Shafie M, Samuel D, Klippel CH, et al. Intractable diarrhea inchildren with VIP-secreting ganglioneuroblastomas. Journal of Pediatric Surgery 1983;18.

Floros KV, Cai J, Jacob S, Kurupi R, Fairchild CK, Shende M, Coon CM, Powell KM, Belvin BR, Hu B, Puchalapalli M, Ramamoorthy S, Swift K, Lewis JP, Dozmorov MG, Glod J, Koblinski JE, Boikos SA, Faber AC. MYCN-Amplified Neuroblastoma Is Addicted to Iron and Vulnerable to Inhibition of the System Xc-/Glutathione Axis. Cancer Res. 2021 Apr 1;81(7). doi: 10.1158/0008-5472.CAN-20-1641. Epub 2021 Jan 22. PMID: 33483374; PMCID: PMC9281612.

Henderson TO, Bhatia S, Pinto N, et al.: Racial and ethnic disparities in risk and survival in children with neuroblastoma: a Children's Oncology Group study. J Clin Oncol (1):, 2011.

Hiyama E, Yokoyama T, Ichikawa T, et al. Poor outcome inpatients with advanced stage neuroblastoma and coincident opsomyoclonus syndrome. Cancer 1994;74.

Ishola TA, Chung DH. Neuroblastoma. Surg Oncol. 2007 Nov;16(3). doi: 10.1016/j.suronc.2007.09.005. Epub 2007 Oct 31. PMID: 17976976.

Mallepalli S, Gupta MK, Vadde R. Neuroblastoma: An Updated Review on Biology and Treatment. Curr Drug Metab. 2019;20(13). doi: 10.2174/1389200221666191226102231. PMID: 31878853.

Maris JM. Recent advances in neuroblastoma. N Engl J Med. 2010 Jun 10;362(23). doi: 10.1056/NEJMra0804577. PMID: 20558371; PMCID: PMC3306838.

Mossé YP, Laudenslager M, Longo L, et al.: Identification of ALK as a major familial neuroblastoma predisposition gene. Nature 455 (7215): , 2008.

Nakagawara A, Li Y, Izumi H, Muramori K, Inada H, Nishi M. Neuroblastoma. Jpn J Clin Oncol. 2018 Mar 1;48(3). doi: 10.1093/jjco/hyx176. PMID: 29378002.

Perek D. Choroby nowotworowe u dzieci. W: Pediatria, Kawalec W, Grenda R, Ziółkowska H ( red.).PZWL, Warszawa 2014.

Sharp SE, Shulkin BL, Gelfand MJ, et al. 123I-MIBG scintigraphy and 18F-FDG PET in neuroblastoma. J Nucl Med. 2009;50.

Shimada H, Chatten J, Newton WA, et al. Histopathologic prognostic factors in neuroblastic tumors: definition of subtypes of ganglioneuroblastoma and an age-linked classification of neuroblastomas. J Natl Cancer Inst. 1984;73(2).

Simon T, Hero B, Schulte JH, Deubzer H, Hundsdoerfer P, von Schweinitz D, Fuchs J, Schmidt M, Prasad V, Krug B, Timmermann B, Leuschner I, Fischer M, Langer T, Astrahantseff K, Berthold F, Lode H, Eggert A. 2017 GPOH Guidelines for Diagnosis and Treatment of Patients with Neuroblastic Tumors. Klin Padiatr. 2017 May;229(3),

English. doi: 10.1055/s-0043-103086. Epub 2017 May 30. PMID: 28561228.

Swift CC, Eklund MJ, Kraveka JM, Alazraki AL. Updates in Diagnosis, Management, and Treatment of Neuroblastoma. Radiographics. 2018 Mar-Apr;38(2). doi: 10.1148/rg.2018170132. PMID: 29528815.

Taggart DR, Han MM, Quach A, et al. Comparison of iodine-123metaiodobenzylguanidine (MIBG) scan and [18F]fluorodeoxyglucose positron emission tomography to evaluate response afteriodine-131 MIBG therapy for relapsed neuroblastoma. J Clin Oncol. 2009.

Whittle SB, Smith V, Doherty E, Zhao S, McCarty S, Zage PE. Overview and recent advances in the treatment of neuroblastoma. Expert Rev Anticancer Ther. 2017 Apr;17(4). doi: 10.1080/14737140.2017.1285230. Epub 2017 Mar 15. PMID: 28142287.

Wolden SL, Barker CA, Kushner BH, et al. Brain-sparing radiotherapy for neuroblastoma skull metastases. Pediatr Blood Cancer 2008;50.

Zafar A, Wang W, Liu G, Wang X, Xian W, McKeon F, Foster J, Zhou J, Zhang R. Molecular targeting therapies for neuroblastoma: Progress and challenges. Med Res Rev. 2021 Mar;41(2). doi: 10.1002/med.21750. Epub 2020 Nov 6. Erratum in: Med Res Rev. 2022 Jan;42(1):641. PMID: 33155698; PMCID: PMC7906923.

# NEUROBLASTOMA – CURRENT REPORTS ON DIAGNOSTICS AND TREATMENT

**Abstract:** Neuroblastoma is a tumor of sympathetic origin with a heterogeneous clinical course. It is a group of tumors that are almost the most common extracranial solid tumors in childhood. These tumors have an unfavorable prognosis and cause 15% of deaths in childhood cancers. Neuroblastomas are located anywhere in the sympathetic chain, but are most common in the adrenal glands. The symptoms of the disease are not always specific, there may only be general weakness or an increase in temperature. So far, the data provided by clinicians is still incomplete to fully understand the disease. Despite many studies, predicting patients with Neuroblastoma remains difficult. The aim of this article is to review current research into the treatment and diagnosis of Neuroblastoma. Diagnosis of this disease is based on tumor biopsy and the presence of elevated levels of urinary catecholamines. Intermediate disease is treated with several cycles of chemotherapy followed by surgical resection. High-risk disease has a poor prognosis, but survival gradually improves with multimodal therapy, including immunotherapy. However, there is a need to find new therapeutic strategies that improve the prognosis and reduce the undesirable effects of the therapies used so far.

**Key word:** Neuroblastoma, MIBG, MYCN, solid tumor

**GRZEGORZ GUCWA**
UNIWERSYTET JAGIELLOŃSKI

# PROPOZYCJA ZASTOSOWANIA MODELI UCZENIA MASZYNOWEGO W ANALIZIE ŹRÓDEŁ HISTORYCZNYCH

**Streszczenie:** Metodologia historii wymaga szczegółowej analizy dużych zbiorów danych dla rzetelności badań o szerokim zakresie merytorycznym. W XX i XXI wieku poczyniono postępy w dziedzinach gromadzenia i przechowywania danych. Jasnym jest, że ich odkrywcza manualna analiza staje się w miarę progresu historiografii zadaniem coraz trudniejszym do wykonania przez pojedynczego badacza. W obliczu tego problemu niniejsza praca postuluje wykorzystywanie modeli uczenia maszynowego w celu przetwarzania źródeł oraz analizy ich treści w ramach ich zbiorów. Przytoczone zostaną w niej przykłady skutecznego użycia uczenia maszynowego w badaniach o metodologii pokrewnej do stosowanej w historiografii. Zastosowanie modeli przetwarzania języka naturalnego w wyraźny sposób może zwiększyć możliwości analityczne historyka, jednakże nie może go w pełni zastąpić na żadnym etapie procesu badawczego ani tym bardziej w jego całości.

**Słowa kluczowe:** uczenie maszynowe, przetwarzanie języka naturalnego, historia, historiografia, analiza źródeł

## WSTĘP

Historia jako dziedzina nauki zajmująca się (w najszerszym skrócie) opisaniem przeszłych działań i wytworów ludzkich bazuje w znacznej mierze na badaniu źródeł pisanych bądź mówionych. Wymaga to od historyków długotrwałych analiz wielkich zbiorów danych składających się z materiałów sporządzonych domyślnie w języku naturalnym celem rzetelnego rozpoznania przeszłych zdarzeń oraz stworzenia narracji je opisujących lub konfrontowania już istniejących z ich treścią. W obliczu coraz powszechniejszego

dostępu do danych oraz progresu, jaki współcześnie poczyniono w kwestii ich katalogowania to zadanie staje się coraz trudniejsze. Niniejsza praca ma na celu omówienie tego problemu oraz przedstawienie jego potencjalnych rozwiązań przy zastosowaniu modeli uczenia maszynowego wyspecjalizowanych w przetwarzaniu języka naturalnego. W sposób ogólny zostanie tu opisane uczenie maszynowe i jego wybrane działy oraz metody, a także zastosowanie go w przetwarzaniu wielkich zbiorów danych. W tym celu przedstawione zostaną przykłady badań wykorzystujących z powodzeniem uczenie maszynowe w analizie materiałów sporządzonych w języku naturalnym, a także zaproponowane na ich bazie zastosowanie metodologii przez nie wykorzystywane w badaniach historycznych.

## Podstawy funkcjonowania uczenia maszynowego i jego roli w przetwarzaniu języka naturalnego

Przetwarzanie języka naturalnego (ang. *Natural Language Processing*, NLP) jest dziedziną nauki z pogranicza informatyki oraz lingwistyki. Jego celem jest umożliwienie programom komputerowym rozpoznawania i rozumienia języka w formie pisanej i mówionej, a w bardziej zaawansowanej formie także wykorzystywanie go. Jedną ze współcześnie stosowanych metod NLP jest tworzenie tzw. modeli przetwarzania języka naturalnego, bazujące w swoim założeniu na technologiach uczenia maszynowego.

Uczenie maszynowe (dalej: UM) jest dziedziną badań nad sztuczną inteligencją. Skupia się ona na tworzeniu i rozwijaniu algorytmów samodzielne wyciągających wnioski, tworzących prognozy oraz podejmujących decyzje wykraczając poza swoją pierwotne możliwości. Proces ten jest nazywany tworzeniem modeli uczenia maszynowego. W ogólnym kontekście badań nad SI celem UM jest umożliwienie nie tylko autonomicznego podejmowania przez nią decyzji, ale również usprawnienie tego procesu i *per procura* całkowitej jej wydajności. Modele uczenia maszynowego są „szkolone" za pomocą uprzednio przygotowanych odpowiednio dużych baz danych, by umożliwić im swobodne rozpoznawanie wielości zawartych w nich wzorów, korelacji oraz trendów. Wówczas mogą one wykorzystać zgromadzone informacje do tworzenia prostych prognoz lub podejmowania decyzji na bazie nowych, dotychczas przezeń nieprzetworzonych danych. Stworzenie modelu UM zakłada przedstawianie algorytmom odgórnie przygotowanych „treningowych" danych i modyfikowanie na podstawie odpowiedzi zwrotnej parametrów modelu aby przybliżyć jego prognozy do wartości rzeczywistych.

Istnieją różne rodzaje tzw. klasycznego uczenia maszynowego, z których można wyróżnić podstawowe: nadzorowane uczenie się (ang. *supervised learning*), nienadzorowane uczenie się (ang. *unsupervised learning*) i uczenie się wzmacniające (ang. *reinforcement learning*). W przypadku nadzorowanego uczenia się algorytmy korzystają z oznakowanych przykładów, gdzie każdy z nich ma przypisany ustalony wynik lub wartość docelową. W założeniu tworzy on uogólnienie na bazie podanych mu przykładów i na jego podstawie stara się stawiać trafne prognozy na bazie nowych danych z którymi dotychczas nie miał kontaktu. Nienadzorowane uczenie się z kolei zakłada podstawianie algorytmom nieoznakowanych przykładów, w których ma on znaleźć nieznane wcześniej dla siebie właściwości tworzące poszczególne zależności i struktury wewnątrz zbioru danych. Uczenie się wzmacniające zaś stanowi etap pośredni między obydwoma, gdzie algorytm nadal prowadzi pewną interakcję z otoczeniem, lecz w budowie modelu nie jest oceniana zgodność z odgórnie oczekiwanym wynikiem: odpowiedzią zwrotną jest poziom spełnienia niesprecyzowanych z góry oczekiwań nadzorcy. (Simeone 2018, s. 649-650). O krok dalej idzie natomiast uczenie głębokie (ang. *deep learning*). Bazuje ono bowiem na zaawansowanych mechanizmach sieci neuronowych, wzorowanych w swojej konstrukcji na zasadach funkcjonowania faktycznych, biologicznych układów nerwowych. Choć jest to rozwiązanie wymagające większego nakładu mocy obliczeniowej, oferuje ono dzięki swojej unikatowej architekturze możliwości przekraczające osiągi klasycznych metod uczenia maszynowego. Poszczególne warstwy „neuronów" odpowiadają za przypisaną im część zadania pod które była projektowana sieć (np. rozpoznawania poszczególnych elementów twarzy na zdjęciach), współpracując ze sobą w określaniu końcowego rezultatu (He i in. 2016, s. 770-771). Tak potężne narzędzia pozwalają na przeprowadzenie w krótkim czasie dokładnych analiz na wielkich pakietach danych, przekraczając w znaczny sposób możliwości ludzkie.

Wyróżnić w tym miejscu trzeba dwa rodzaje sieci neuronowych wykorzystywanych często w przetwarzaniu języka naturalnego. Szczególnym typem, który zostanie poruszony w niniejszej pracy, jest sieć o przedłużonej pamięci krótkotrwałej (ang. *Long Short-Term Memory,* dalej: LSTM). W przetwarzaniu języka naturalnego często wykorzystywane są sieci neuronowe o charakterze rekurencyjnym, to jest sieci wykorzystujące na nowo własną odpowiedź zwrotną celem modyfikacji danych wejściowych. Taka architektura czyni je idealnymi do analizy powtarzalnych danych pokroju odręcznego pisma lub rozpoznawania mowy, a także wyróżniania różnych stylów językowych (Dupond 2019, s. 218-230). Technologia LSTM powstała jako odpowiedź

na jeden z kluczowych mankamentów sieci rekurencyjnej, to jest zatracanie gradientu – sytuację, w której przez przeuczenie modelu różnica między odpowiedzią zwrotną a danymi wejściowymi na które ma ona wpływ jest niewielka, niwelując tym samym proces uczenia. LSTM przedłuża żywotność tej „pamięci krótkotrwałej", zachowując część dawnej odpowiedzi zwrotnej do dalszego użytku modelu. Czyni to ją niezwykle użyteczną w procesie analizy dużych zbiorów danych i korelacji między nimi (Graves i in. 2009, s. 855-858). Alternatywą dla sieci rekurencyjnych jest architektura uczenia głębokiego *transformer*, która przetwarza dane wejściowe równolegle względem siebie zamiast w sekwencji, symulując nadal ludzkie procesy odpowiedzialne za uwagę – tym samym wymagając mniejszej ilości czasu na uczenie modelu niż sieci LSTM (Vaswani i in. 2017). Na architekturze *transformer* bazuje BERT (Bidirectional Encoder Representations from Transformers), rodzina modeli językowych stworzona przez pracowników Google, a także modele GPT popularne dzięki OpenAI.

Uczenie maszynowe ma swoje zastosowanie w wielu obszarach życia codziennego, biznesu oraz zarządzania państwowego, stanąwszy się już teraz nieodwracalnie stałym elementem cyberprzestrzeni oraz biznesu IT. Ciężko wyobrazić sobie dla przykładu funkcjonowanie portali społecznościowych oraz wyszukiwarek pokroju Google, będących podstawą dzisiejszego Internetu, bez komputerowego rozpoznawania obrazów, przetwarzania języka naturalnego, rozpoznawania mowy, a także systemu rekomendacji treści (w tym reklamowych). Wszystkie te rozwiązania oparte są w niebagatelnym stopniu na technologii *machine learning* lub przynajmniej korzystają z niej pomocniczo (Hazelwood i in. 2018, s. 620-622). Można też bez cienia przesady powiedzieć, że inne gałęzie gospodarki rozwinęły się dynamicznie dzięki możliwości przystępnej i szybkiej analizy wielkich zbiorów danych, zautomatyzowanemu podejmowaniu decyzji przez komputery i innych możliwości wynikających z uczenia maszynowego. Nie znaczy to jednak, że jest ono rozwiązaniem technicznie doskonałym. Kluczowym trudem związanym z funkcjonowaniem wielu algorytmów *machine learning* pozostaje oprócz ich właściwej architektury kwestia dokładnego przetworzenia wstępnego analizowanych przez nie zestawów danych, ich miarodajności oraz załatania w nich ewentualnych luk: model uczenia maszynowego tworzony na wadliwym zbiorze danych nie będzie w stanie spełniać swoich ról. Kolejnym problemem pozostaje kwestia „przeuczenia" i „niedouczenia" (ang. *overfitting* and *underfitting*) modeli, to jest nadmiernego ich dostosowania lub niedostosowania do „szkolnych" danych, tym samym zaburzając dokładność prognoz opartych na nowych porcjach

(Hastie i in. 2008, s. 10.10). Coraz częściej jest również poruszania kwestia etyczności zastosowania uczenia maszynowego: krytycy zwracają uwagę między innymi na potencjalne naruszenia prywatności osób trzecich, niedostateczną ich zdaniem transparentność w korzystaniu z uczenia maszynowego przez instytucje publiczne oraz prywatne oraz niewspółmierne do ryzyka błędu opieranie swoich działań na prognozach SI (Mittelstadt i in. 2016).

## Zastosowanie prostych modeli UM w wykrywaniu trendów wewnątrz zbioru źródeł

Unikatowe właściwości uczenia maszynowego mogą zmienić na zawsze nasze podejście do danych, ich przetwarzania, a także korelacji występujących wewnątrz nich. Nie sposób zatem nie łączyć nauki skupiającej się właśnie w dużej mierze na analizie danych i tworzeniu na ich podstawie narracji z technologią informatyczną zakładającą szybkie, sprawne i samodzielne ich przetworzenie przez oprogramowanie. W tej części niniejszej pracy zamierzam zidentyfikować kilka problemów, z jakimi mierzy się współczesna historiografia i zaproponować ich rozwiązania wykorzystujące UM.

Jednym z nich jest niewspółmierność możliwości, jakimi dysponują badacze do ilości danych potrzebnych do stworzenia kompletnej analizy. Na pierwszy rzut oka ta tendencja może wydawać się nieuzasadniona. Dzięki takim postępowi współczesnej archiwistyki w dziedzinach gromadzenia i przechowywania materiałów archiwalnych, ekstensywnemu katalogowaniu nowych informacji, stale trwającej digitalizacji opracowań, globalizacji systemów bibliotecznych, rosnącej liczbie publikacji i pism wydawanych w Internecie (za opłatą lub w wersji *open access*) i wreszcie właściwego naszym czasom fenomenu, jakim jest *big data*, badacz w roku 2023 może cieszyć się dostępem do informacji na większą skalę niż kiedykolwiek. I chociaż ten stan rzeczy słusznie można oceniać pozytywnie z perspektywy metodologii historii, nie jesteśmy w stanie wykorzystać go w pełni przez nasze obecne ograniczenia narzucone przez warsztat pracy historyka.

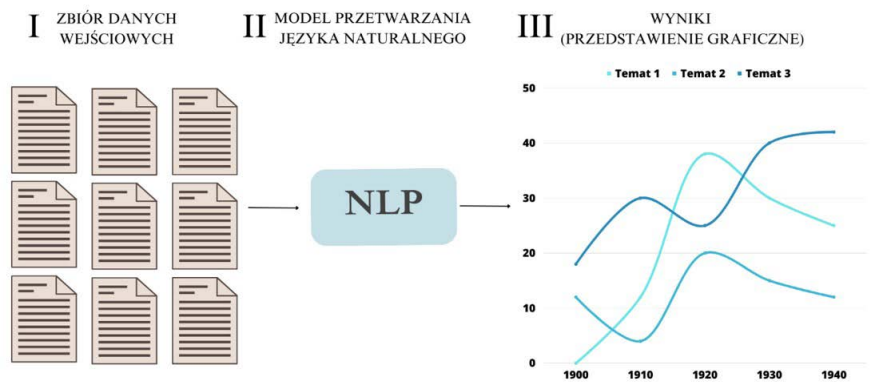
Do tej pory badania historyczne polegają w znacznym stopniu na przeprowadzaniu osobistych kwerend i samodzielnej analizie materiałów zgromadzonych w ich wyniku. Te metody stają się nieadekwatne do wyzwań i możliwości, jakie oferuje coraz większa ilość dostępnych dla nas informacji, zwłaszcza w dziedzinie historii najnowszej. Manualna analiza wielkich zbiorów danych wolna od uciekania się przez badaczy do wybiórczości w doborze materiałów i poleganiu na arbitralnie uznawanej reprezentatywności części informacji

względem dostępnej całości jest niemożliwa bez gigantycznego nakładu sił i środków. Jednocześnie nawet wtedy nie ma gwarancji, że w badaniu dużych zbiorów źródeł nie dojdzie do pomyłek w przetwarzaniu oraz wyciąganiu wniosków z danych używanych przez badacza lub zespół badawczy, narażając tym samym narrację zawartą w opracowaniach podsumowujących badania na błędność merytoryczną lub tworzenie konkluzji na wątpliwych przesłankach. W efekcie konflikt narracji, napędzający dyskurs naukowy, musi opierać się w znacznej mierze na badaniach bazujących na analizach reprezentatywnych zbiorów danych zamiast ich całości. Sprowadza się to często do zderzania się osobnych rzeczywistości bazowanych na tychże narracjach, nie współgrających ze sobą i nie budujących konsensusu, tym bardziej odrębnych od siebie, im większy jest zestaw danych do przeanalizowania w danym obszarze.

Zmianę tego stanu rzeczy oferuje potencjał, jaki technologia uczenia maszynowego posiada w kwestii analizy danych. Najlepszym przykładem, przedstawiającym wzorowo sposób wykorzystania uczenia maszynowego i przetwarzania języka naturalnego w badaniach historycznych jest wydana w dwóch częściach praca Petera Grajzla i Petera Murrella *A machine-learning history of English caselaw and legal ideas prior to the Industrial Revolution.* Uczenie maszynowe jest w niej wykorzystywane do oszacowania kształtu modelu tematycznego i analizy zbioru 52 949 protokołów angielskich spraw sądowych powstałych w okresie 1485-1765. Badacze stosują w nim technikę modelowania tematycznego, która jest rodzajem algorytmu nienadzorowanego uczenia maszynowego, szczególnie odpowiedniego dla badania dużych tekstowych zestawów danych, wykrywając w nim trendy o wielkiej skali. Modelowanie tematyczne traktuje dokumenty jako, w słowach samych badaczy, „worki słów", nie zważając *a priori* na kolejność wyrazów i wykorzystując współwystępowanie poszczególnych zwrotów w różnych dokumentach celem identyfikacji tematów. Te tematy w tym przypadku oznaczają rozkłady prawdopodobieństwa w słownictwie zbioru reprezentujące występowanie zwrotów często poruszanych w dokumentach. Algorytm uczenia maszynowego szacuje najbardziej prawdopodobne wartości parametrów w modelu opierając się na analizowanym zespole danych. Użyty tutaj został konkretny typ modelu tematycznego zwany strukturalnym modelem tematycznym (ang. *Structural Topic Model,* STM), integrujący metadane na poziomie dokumentu (takie jak rok sprawy) i metadane na poziomie treści protokołu celem oszacowania tematu (Grajzl i Murrell 2020a, s. 11-14). Ta integracja poprawiła identyfikację i interpretację tematów, a także zwiększyła dokładność i efektywność szacowania wpływu metadanych na ich rozpowszechnienie (Ilustracja 1). Oszacowanie tematów

i ich rozpowszechnienia w czasie zapewniło wgląd w ewolucję idei prawnych i ich znaczenia w protokołach spraw. Następnie autorzy badali słowa związane z każdym tematem i osobiście zapoznali się z treścią materiałów, aby nazwać i zinterpretować istotę poszczególnych tematów. Pozwoliło to tym samym na odkrycie i wstępne scharakteryzowanie idei w brytyjskim prawie precedensowym właściwych dla poszczególnych okresów oraz regionów Anglii bazując na zbiorze danych zawierającym w sobie zawrotną liczbę prawie 53 tysięcy protokołów sądowych sporządzonych w języku angielskim używanym we wczesnej nowożytności (Grajzl i Murrell 2020b, s. 8-13).

Ilustracja 1. Przedstawienie graficzne procesu wykrywania tematów wewnątrz zbioru danych.




Źródło: opracowanie własne.

Wykorzystanie w tej pracy uczenia maszynowego, a w szczególności modelowania tematycznego, umożliwiło badaczom przeanalizowanie dużego zestawu protokołów i pism sądowych w systematyczny i wydajny sposób. Zautomatyzowany proces identyfikowania tematów i oszacowywania ich rozpowszechnienia w historii prawa angielskiego oszczędziło według badaczy w porównaniu z ręcznym przeprowadzeniem takiej analizy zasoby i czas w sposób „znaczący", oferując nowe spojrzenie na dzieje angielskiego prawodawstwa z wielu nowych perspektyw.

Praca P. Grajzla i P. Murrella zatem oferuje nam przykład udanego wykorzystania uczenia maszynowego do rzetelnej makroanalizy wielkiego zbioru danych, jednocześnie demonstrując jego potencjał. Obywając się bez zwiększenia nakładu sił z własnej strony badacze są w stanie wykryć powiązania między informacjami bazując na materiale wyczerpującym badane przez nich zagadnienie, bez wyznaczania arbitralnie prób reprezentatywnych lub bez odrzucania *a priori* części materiałów. Warto nadmienić, że dzięki swobodzie

w konstruowaniu modeli UM możliwym jest dostosowywanie ich do własnych potrzeb badawczych ze względną łatwością. Ponadto przy stosowaniu *reinforcement learning* algorytmy są w stanie wykrywać wzorce i relacje w danych, których istnienie może nie być z góry założone przez badaczy. W ten sposób zarówno można znacznie wzbogacić wartość swojej pracy, jak i otworzyć nowe perspektywy badań nad tym samym korpusem danych.

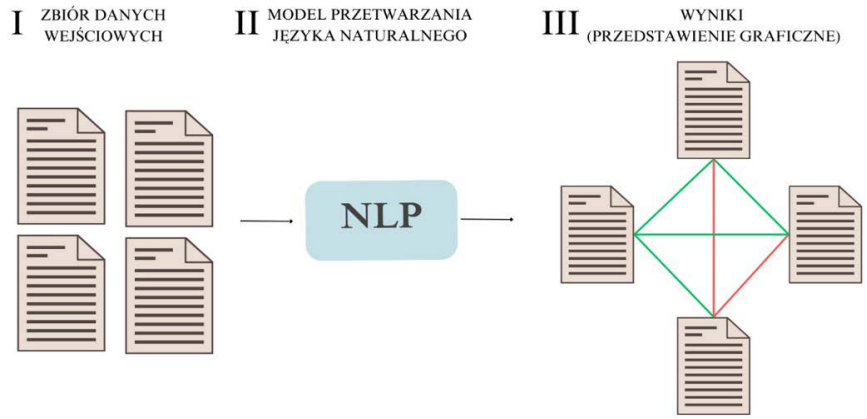
## Wykrywanie sprzeczności w zbiorach źródeł za pomocą sieci neuronowych

Nie oznacza to jednak, że praktyczne możliwości jakie technologia uczenia maszynowego ma do zaoferowania historii ograniczają się jedynie do znajdywania korelacji w gigantycznych zbiorach danych. Na analogicznej zasadzie bowiem modele UM są w stanie wykrywać wszelkie rozbieżności wewnątrz analizowanych przez siebie treści, ułatwiając tym samym pracę historyka w dwójnasób. Badania historyczne bowiem nie tylko zakładają ustalanie jednolitej wersji wydarzeń w formie narracji na podstawie relacji bądź innego rodzaju źródeł traktujących o zgłębianym przez historyków zagadnieniu. Równie ważna w pracy historyka jest krytyka samych źródeł, ich rzetelności oraz zgodności z innymi materiałami obejmującymi sobą podobny zakres (jeśli takie istnieją). Krytyka źródeł ma swoje zastosowanie pomocnicze w badaniach, może nawet być również ich nawet przedmiotem: odrzucając błędne lub wręcz fałszywe wersje wydarzeń, historyk tworzy narrację opartą na materiałach, których spójności i wzajemnej zgodności nie da się podważyć. Ta właściwość jest jedną z podstaw, na których można oceniać rzetelność narracji prowadzonej w opracowaniu historycznym i *per procura* rzetelność samego opracowania. Idąc tym tropem, krytyka źródła jest jednym z najważniejszych zadań stojących przed badaczem podczas jego pracy, mając bezcenne znaczenie dla jakości opracowania wieńczącego proces badawczy. Jedną z metod krytyki źródeł jest falsyfikacja relacji przez nie prezentowanych. Falsyfikacja w ujęciu ogólnym jest sprawdzaniem negatywnym polegającym na wykazaniu fałszywości, to jest sprzeczności z ustaloną i zweryfikowaną wiedzą, twierdzenia lub twierdzeń zawartych (trzymając się omawianego tu kontekstu) w relacji przekazywanej przez źródło historyczne. Specyfika samej historii jako nauki zajmującej się przeszłymi zdarzeniami utrudnia jednakże falsyfikację relacji, gdyż wykazywanie ich nieprawidłowości w oparciu o dorobek innych nauk nie wyklucza wzajemnego konfliktu ich treści. W związku z tym jedną z metod falsyfikacji źródeł historycznych jest analiza porównawcza relacji

w nich zawartych: zestawienie wszystkich dostępnych dla badacza materiałów traktujących o podjętym przez niego zagadnieniu. W ten sposób możliwym jest ustalenie podobieństw oraz różnic między wersjami wydarzeń prezentowanymi przez każde z nich. Chociaż nie jest to jeszcze jednolita podstawa do falsyfikacji lub koroboracji materiałów, stanowi ona cenną odpowiedź zwrotną dla ich oceny.

Jednakże przy analizie porównawczej źródeł ilość potrzebnej do przetworzenia przez historyka informacji może być przeszkodą. Jak w przypadku omawianego wcześniej w niniejszej pracy problemu, przetworzenie wielkich zbiorów źródeł stanowi poważne wyzwanie, wymagające znacznego nakładu czasu, sił oraz środków ze strony badacza. Również i w tej kwestii pomocnym może być zastosowanie UM: na podstawie funkcjonowania modeli przetwarzania języka naturalnego możliwym jest znalezienie sprzecznych informacji wewnątrz analizowanych danych, w jednoczesnym odniesieniu do całości zestawu zamiast jedynie do jego poszczególnych części – tym samym tworząc przejrzysty obraz wszystkich nieścisłości i konfliktów zarówno między poszczególnymi relacjami, jak i w odniesieniu jednego materiału względem całości (Ilustracja 2).

Ilustracja 2. Przedstawienie graficzne procesu wykrywania sprzeczności pomiędzy poszczególnymi elementami zbioru danych.




Źródło: opracowanie własne.

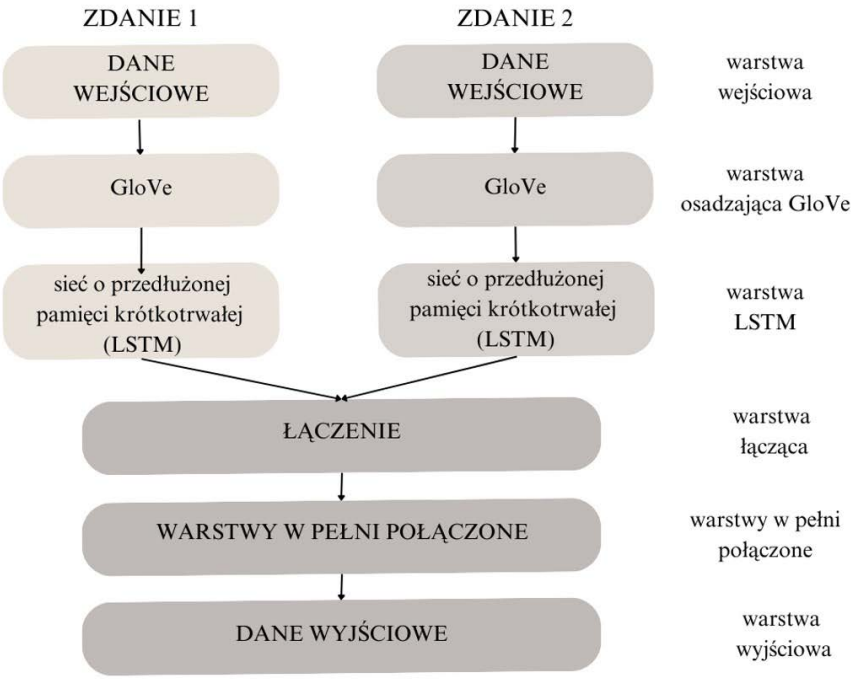
Jedna z nowoczesnych metod wykrywania sprzeczności wewnątrz tekstu lub zbioru tekstów przy zastosowaniu technologii uczenia maszynowego została opisana szczegółowo przez badaczy Uniwersytetu Aśoki w pracy pt. *Deep learning for conflicting statements detection in text* (Lingam i in. 2018). Pionierskość tej pracy wynika z zastosowanej przez autorów nowatorskiej

metodologii wykorzystującej moc uczenia głębokiego, w szczególności wykorzystując sztuczne sieci neuronowe o architekturze bazującej na technologii LSTM w połączeniu z zastosowaniem GloVe, to jest modelu uczenia nienadzorowanego osadzającego poszczególne słowa w przestrzeni wektorowej, umożliwiającej szacowanie różnic semantycznych na bazie dystansów między poszczególnymi wektorami reprezentującymi przetworzone słowa (Pennington i in., 2014, s. 1532-1535). Opierając się na trzech publicznie dostępnych zbiorach danych zawierających teksty poruszające różne tematy (SemEval 2014, Stanford Natural Language Processing Corpora, PHEME), badacze zastosowali z powodzeniem kombinację sieci neuronowej opartej na LSTM oraz wspierających ją zaprojektowanych przez nich funkcji językowych skupiających się na wykrywaniu zaprzeczeń, antonimów oraz mierzenia współczynnika podobieństwa Jaccarda, tj. podobieństwa między zbiorami. Obydwa zastosowania po przetworzeniu tekstu za pomocą osadzania wektorowego GloVe w celu stworzenia danych wejściowej wykrywają we współpracy ze sobą pary zdań o treści sprzecznej ze sobą, przekazując binarną odpowiedź zwrotną stwierdzającą niezgodność między analizowanymi zdaniami lub jej brak (Ilustracja 1). Stworzone przez autorów narzędzie do wykrywania przeciwieństw w tekstach wykazało się dużą skutecznością: poprawność odpowiedzi zwrotnej w przypadku zbioru Stanforda wynosiła 71,9%, SemEval 91,2%, a przy analizie zbioru PHEME aż 96,85%. Tym samym udowodniono, że możliwym jest stworzenie modelu uczenia maszynowego wykrywającego z dużą dozą poprawności konflikt treści pomiędzy poszczególnymi zdaniami (Lingam i in., 2018, s. 2-12). Analogiczne badanie przeprowadzone przez Niroja Ghimire i Surendry Shrestha pokazuje skuteczność stosowania sieci neuronowych LSTM oraz GloVe w wykrywaniu nieprawdziwych wiadomości (ang. *fake news*) w sieci: skuteczność sieci neuronowej w wykrywaniu sprzecznych informacji wewnątrz zbioru danych FNC-1 zawierającego w sobie artykuły z poszczególnych stron internetowych wynosiła 93,69% (Ghimire i Shrestha 2022, s. 49-53). Można zatem stwierdzić, że użycie technologii sieci neuronowych LSTM w zestawieniu z GloVe w celu wykrywania sprzeczności w tekście ma wysoką efektywność, choć nie osiąga jeszcze idealnych rezultatów.

Alternatywą dla przedstawionych powyżej rozwiązań jest stosowanie modeli BERT. Praca F.S. Yazi i in. postuluje zastosowanie ich jako efektywniejszego rozwiązania względem stosowania sieci LSTM w przypadku wyspecjalizowanej literatury medycznej celem wykrycia przeciwieństw w postulowanych przez nie tezach oraz założeniach. Stosując na przygotowanym uprzednio przykładowym zbiorze częściowo sprzecznych względem siebie

tekstów naukowych ManConCorpus traktujących o medycynie zarówno połączenie GloVe+LSTM oraz zmodyfikowany model BERT, autorzy badania ustalili, że technologia BERT jest w stanie efektywniej wykrywać zaprzeczające sobie nawzajem zdania wewnątrz zestawu danych traktującego o jednolitej tematyce (aczkolwiek w nieznacznym stopniu, nie przekraczając pod żadnym kątem 110% efektywności drugiego modelu, z dokładnością pomiędzy 88,9% a 92,2%) (Yazi i in. 2021a, s. 118-120). Te wyniki trzeba jednak traktować ostrożnie: ten sam zespół w innym badaniu wykazał, że w przypadku większych monotematycznych zbiorów testowych niż ManConCorpus (w tym przypadku EBMSum) technologia BERT nie zwiększa swojej skuteczności, co badacze wywodzą z jej niedostosowania do wielkich zasobów danych (Yazi i in. 2021b, s. 72-75).

Ilustracja 3. Ogólne przedstawienie przetwarzania języka naturalnego przy wykorzystaniu sieci neuronowej i osadzania wektorowego GloVe.




Źródło: opracowanie własne.

Wykrywanie sprzeczności wewnątrz tekstu za pomocą przetwarzania języka naturalnego o satysfakcjonującej skuteczności jest zatem w zasięgu możliwości współczesnej nauki. Odkrywanie potencjału, jaki to rozwiązanie oferuje w takich sferach jak zwalczanie dezinformacji w Internecie lub

rozwijanie metodologii medycyny daje także nadzieję na zaimplementowanie jej we współczesnej historiografii. Analiza dużych zestawów źródeł pod kątem wykrywania trendów lub korelacji w danych w znaczący sposób usprawni proces opracowywania ich w ujęciu narracyjnym, wzbogacając jego złożoność i oferując nowe spojrzenie na znane już zjawiska i procesy. Wzmocnienie jej o możliwość komputerowego wykrycia nieścisłości bądź przeciwieństw wewnątrz zbioru danych umożliwi jednoczesne przeprowadzenie wzajemnej krytyki źródeł oraz może jeszcze zwiększyć liczbę potencjalnych interpretacji przedstawionych w nich wydarzeń. Zastosowanie modeli uczenia maszynowego zmniejszy w wydatny sposób wymagane nakłady sił i środków, jakie badacze powinni wkładać w takie przedsięwzięcie.

## Potencjalne przeszkody, wyzwania i trudności w zastosowaniu UM w historii

Dotychczas w niniejszej pracy skupiono się na przedstawieniu konceptu i właściwości uczenia maszynowego oraz pozytywnego potencjału, jaki może ono wnieść w rozwój metodologii historii. Nie powinno natomiast ono być traktowane jako narzędzie uniwersalne, a we wszelkich projektach praktycznego zastosowania go w analizie źródeł poniższe informacje powinny być brane pod uwagę.

Podstawowym problemem, przed którym stoi historiografia w stosowaniu UM jest natura przetwarzania języka naturalnego. Celem przeprowadzenia skutecznej analizy zbioru danych każde źródło tekstowe, które się na niego składa powinno uprzednio ulec digitalizacji. Nie powinno się to ograniczać wyłącznie do zapisania skanu dokumentu w formie obrazu lub temu podobnych prostych technik zapisywania źródeł w przestrzeni cyfrowej. Sama ich treść powinna ulec cyfryzacji celem sprawnego przetworzenia tych informacji przez modele UM. Dzięki nowoczesnym systemom OCR (*Optical Character Recognition*, ang. optyczne rozpoznawanie znaków) archiwa są w stanie konwertować obrazy dokumentów na pliki tekstowe, znacznie usprawniając wyszukiwanie informacji przez badacza, chociaż nie jest to jeszcze w przypadku archiwów niemieckich w pełni skończony proces (Vafaie i in., 2022, s. 15-18). Dopiero całkowita digitalizacja zbiorów archiwalnych w formie w pełni przetwarzalnej przez modele uczenia maszynowego pozwoli wykorzystać ich pełny potencjał. Warto z tego miejsca zauważyć, że nie zawsze digitalizacja formami pokroju OCR idzie w parze z uporządkowaniem tych danych. Diana Kim w swojej pracy pochyla się między innymi nad niekonsekwencją, z jaką

brytyjskie archiwa katalogują tak przetworzone dokumenty, utrudniając tym samym według niej kwerendę poprzez (według niej) niedostateczne możliwości szukania danych względem ilości materiałów (Kim 2022, s. 531-535). Taki stan rzeczy może utrudnić tworzenie zbiorów danych koniecznych dla stworzenia i funkcjonowania modeli UM.

Dalszym problemem, który trzeba mieć na uwadze, są ograniczenia techniczne modeli. Szczególnie należy się tu pochylić nad wykrywaniem sprzeczności między zdaniami, gdyż wykazany tu niedostatek skuteczności, chociaż oscylujący pomiędzy badaniami w granicach *circa* 10%, stanowi wciąż lukę w kompletności analizy. Nadal wymagają one również osobistego zapoznania się z dokładną treścią analizowanych materiałów dzięki ograniczonej formie informacji zwrotnej. Jak wykazała praca P. Grajzla i P. Murrella, podstawowym zastosowaniem opracowanego przez nich modelu było wykrycie i umiejscowienie wewnątrz zbioru przypadków występowania korelacji (Grajzl i Murrell 2020a, s. 17). Wyciągnięcie wniosków na ich bazie stanowi nadal pracę, którą historyk musi wykonać samodzielnie, tym samym ściśle relegując modele przetwarzania języka naturalnego do roli potężnych narzędzi pomocniczych dla badacza – natomiast nie są w stanie go zastąpić bądź wyręczyć w kwestii najważniejszej: formułowania wniosków i tworzenia na ich podstawie narracji.

## Podsumowanie

Uczenie maszynowe i jego zdolności w przetwarzaniu języka naturalnego niewątpliwie mają zastosowanie praktyczne w dziejopisarstwie, a także potencjalnie zmienić jej oblicze. Godnym uwagi wydaje się oferowane przez nie szerokie spektrum narzędzi, które historyk mógłby wykorzystać w swojej pracy: od modeli o prostej architekturze po zaawansowane sieci neuronowe *transformer*. Możliwości analityczne, jakie NLP otwiera przed badaczami, są olbrzymie: duże zbiory danych mogą ze wsparciem modeli UM zostać przeanalizowane dogłębnie przez pojedynczego historyka lub niewielki zespół, utrzymując tym samym jednolity kurs badań. Całkowite przetworzenie dostępnych źródeł, zarówno pod kątem trendów występujących między nimi jak i niespójności umożliwia spojrzenie na omówione już zjawiska z wielu nowych perspektyw. Jednakże, jak podkreślono w niniejszej pracy, UM oferuje przeważnie możliwości analityczne, nie zastępując tym samym historyka w tworzeniu narracji oraz wyciąganiu zaawansowanych wniosków z wyników badań. Specyfika pracy z wielkimi zbiorami danych wymaga również osobistej

weryfikacji odpowiedzi zwrotnej modeli UM, co również nie wykreśla całkowicie czynnika ludzkiego z procesu analizy źródeł. Podsumowując, przetwarzanie języka naturalnego modelami UM może stać się potężnym narzędziem pomocniczym w ręku historyka, w znaczny sposób ułatwiając mu pracę oraz poszerzając zakres jego możliwości badawczych.

## Bibliografia

Dupond S.
2019 *A thorough review on the current advance of neural network structures*, „Annual Reviews in Control" 14.

Ghimire N., Shrestha S.
2022 *Fake News Stance Detection using DeepNeural Network*, „LEC Journal" 2022, 4(1).

Grajzl P., Murrell P.
2020 *A machine-learning history of English caselaw and legal ideas prior to the Industrial Revolution I: generating and interpreting the estimates*, „Journal of Institutional Economics", vol. 17, issue 1.

Grajzl P., Murrell P.
2020 *A machine-learning history of English caselaw and legal ideas prior to the Industrial Revolution II: applications*, „Journal of Institutional Economics", vol. 17, issue 2.

Graves A., Liwicki M., Fernandez S., Bertolami R., Bunke H., Schmidhuber J.
2009 *A Novel Connectionist System for Unconstrained Handwriting Recognition*, „IEEE Transactions on Pattern Analysis and Machine Intelligence", 31 (5).

Hastie T., Tibshirani R., Friedman J.H.
2009 *The Elements of Statistical Learning: Data mining, Inference, and Prediction*, Stanford.

Hazelwood K., Bird S., Brooks D., Chintala S., Diril U., Dzhulgakov D., Fawzy M., Jia B., Jia Y., Kalro A., Law J., Lee K., Lu J., Noordhuis P., Smelyanskiy M., Xiong L., Wang X.
2018 *Applied Machine Learning at Facebook: A Datacenter Infrastructure Perspective*, [w:] *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, Wiedeń.

He K., Zhang X., Ren S., Sun J.
2016 *Deep Residual Learning for Image Recognition,* [w:] *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* Las Vegas.

Kim D.S.
2022 *Taming Abundance: Doing Digital Archival Research (as Political Scientists)*, „PS: Political Science & Politics", 55(3).

Lingam V., Bhuria S., Nair M., Gurpreetsingh D., Goyal A., Sureka A.
2018 *Deep learning for conflicting statements detection in text*, „PeerJ" vol. 6.

Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L.
2016 *The Ethics of Algorithms: Mapping the Debate*, „Big Data & Society", 3(2).

Simeone O.
2018 *A Very Brief Introduction to Machine Learning With Applications to Communication Systems*, „IEEE Transactions on Cognitive Communications and Networking", 4/2018.

Pennington J., Socher R., Manning C.
2014 *GloVe: Global Vectors for Word Representation* [w:] *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Doha.

Vafaie M., Bruns O., Pilz N., Waitelonis J., Sack H.
2022 *Handwritten and printed text identification in historical archival documents*, „Archiving Conference" 19(1).

Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A., Kaiser Ł., Polosukhin I.
2017 *Attention Is All You Need,* [w:] *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, Long Beach.

Yazi F.S., Vong W., Raman V., Hui Then P.H., Lunia M.J.
2021 *Towards Automated Detection of Contradictory Research Claims in Medical Literature Using Deep Learning Approach,* [w:] *2021 Fifth International Conference on Information Retrieval and Knowledge Management (CAMP).*

Yazi F.S., Vong W., Raman V., Hui Then P.H., Lunia M.J.
2021 *An Experimental Evaluation of Deep Neural Network Model Performance for the Recognition of Contradictory Medical Research Claims Using Small and Medium-Sized Corpora*, „Malaysian Journal of Computer Science", wyd. spec. 2/2021.

# PROPOSAL FOR THE APPLICATION OF MACHINE LEARNING MODELS IN THE ANALYSIS OF HISTORICAL SOURCES

**Abstract:** The methodology of history requires a detailed analysis of large-scale datasets for the reliability of research with a wide substantive scope. In the 21st century, with the advances that have been made in the fields of data collection and preservation, it is clear that their revealing manual analysis becomes a task more and more difficult for a single researcher as historiography progresses. In the face of this problem, this paper postulates the use of machine learning models to process sources and analyze their content within their collections. It will present examples of the effective use of machine learning in research with a methodology similar to that used in historiography. The use of natural language processing models can clearly increase the historian's analytical capabilities, but it cannot replace it at any stage of the research process, and even more so in its entirety.

**Keywords**: machine learning, natural language processing, history, historiography, source analysis

ISBN 978-83-67527-97-2