PROBLEM NIEAUTORYZOWANYCH TRANSAKCJI W KONTEKŚCIE KWESTII ODPOWIEDZIALNOŚCI BIG TECHÓW ZA REKLAMY – SKALA ZJAWISK, ANALIZA RYZYK I PROCEDUR ODZYSKIWANIA ŚRODKÓW ORAZ ODPOWIEDZIALNOŚĆ W SYSTEMACH PŁATNOŚCI. PROPOZYCJA OPTYMALNEGO UREGULOWANIA

SYGN. PAB/WIB 2/2026

ISBN 978-83-979278-1-0

Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Warszawa, styczeń 2026 r.

PROGRAM ANALITYCZNO BADAWCZY

O Raporcie

Raport **Problem nieautoryzowanych transakcji w kontekście kwestii odpowiedzialności Big Techów za reklamy – skala zjawisk, analiza ryzyk i procedur odzyskiwania środków oraz odpowiedzialności w systemach płatności. Propozycja optymalnego uregulowania** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy

Raport został opracowany przez zespół badawczy w składzie:

prof. ucz. dr hab. Krzysztof Koźmiński
– profesor Uniwersytetu Warszawskiego, kierownik Zakładu Ekonomicznej Analizy Prawa, a także kierownik Centrum Oceny Skutków Regulacji oraz kierownik Podyplomowego Studium Zagadnień Legislacyjnych na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Radca prawny, partner zarządzający w kancelarii Jabłoński Koźmiński.

prof. ucz. dr hab. Jan Rudnicki
– profesor Uniwersytetu Warszawskiego, doktor habilitowany nauk prawnych, kierownik Katedry Europejskiej Tradycji Prawnej na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Ekspert instytucji publicznych i organizacji pozarządowych. Przez kilka lat współpracował z czołową warszawską kancelarią prawną w zakresie obsługi procesu inwestycyjnego, prawa nieruchomości i innych obszarów prawa publicznego.

dr Michał Jabłoński
– doktor nauk prawnych, adiunkt w Katedrze Prawa i Postępowania Administracyjnego Uniwersytetu Warszawskiego. Adwokat, partner zarządzający w kancelarii Jabłoński Koźmiński. Wykładowca i autor publikacji na temat prawa administracyjnego oraz administracji publicznej. Laureat nagród i rankingów prawniczych, m.in. rekomendowany prawnik w XXII i XXIII edycji Rankingu Kancelarii Prawniczych dziennika „Rzeczpospolita" w 2024 oraz 2025 r.

dr Grzegorz Keler
– doktor nauk prawnych, adiunkt w Katedrze Prawnych Problemów Administracji i Zarządzania na Wydziale Zarządzania Uniwersytetu Warszawskiego, a także wykładowca na studiach EMBA Uniwersytetu Warszawskiego oraz studiach podyplomowych z zakresu FinTech w Szkole Głównej Handlowej w Warszawie. Ekspert Centrum Oceny Skutków Regulacji na Uniwersytecie Warszawskim oraz Centrum Gospodarki i Finansów Cyfrowych na Uniwersytecie Mikołaja Kopernika w Toruniu. Adwokat, partner w kancelarii Jabłoński Koźmiński.

Jan Czarnocki, LL.M., CIPP/E
– doktorant i stypendysta Marii Skłodowskiej-Curie w KU Leuven Centre for IT & IP Law. Obecnie zajmuje się badaniem prywatności i ochrony danych, koncentrując się na danych biometrycznych i zdrowotnych w kontekście IoT-AI, w ramach projektu Horizon 2020 Privacy Matters ITN. Jego badania obejmują skrzyżowanie prawa, filozofii, technologii i polityki. Posiada tytuł magistra prawa Uniwersytetu Warszawskiego oraz tytuł LL.M. w zakresie prawa porównawczego uzyskany na China University of Political Science and Law w Pekinie.

O Programie

Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów końcowych – użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze
- Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego
- Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich
- ESG i sustainable finance
- Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt:

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

Streszczenie kierownicze

Cel przeprowadzonego badania

Celem przeprowadzonego badania jest wielowymiarowa analiza problematyki nieautoryzowanych transakcji płatniczych oraz związanej z nimi odpowiedzialności podmiotów, ze szczególnym uwzględnieniem działalności podmiotów Big Tech, w tym mediów społecznościowych. Badanie ma na celu określenie skali i charakterystyki zjawiska nieautoryzowanych transakcji płatniczych, identyfikację mechanizmów ich powstawania oraz czynników zwiększających ryzyko wystąpienia takich zdarzeń.

Analizie poddana została również rola mediów społecznościowych i podmiotów Big Tech zarówno w ułatwianiu, jak i przeciwdziałaniu oszustwom, w tym poprzez publikowanie fałszywych reklam oraz wyłudzanie danych uwierzytelniających. W ramach badania została przeanalizowana odpowiedzialność prawna tych podmiotów za szkody wynikające z nieautoryzowanych transakcji oraz działania ochronne podejmowane w celu minimalizacji ryzyka. Istotnym elementem była również ocena procedur odzyskiwania środków i systemów odpowiedzialności funkcjonujących w sektorze finansowym, w tym praktyk banków i innych instytucji w zakresie obsługi klientów poszkodowanych w wyniku cyberprzestępstw.

Badanie objęło również analizę porównawczą regulacji i praktyk w innych krajach, co pozwoliło zidentyfikować najlepsze rozwiązania oraz wskazać kierunki ewentualnych zmian w prawodawstwie krajowym. Na tej podstawie została dokonana ocena skuteczności obowiązujących ram regulacyjnych oraz ich wpływu na bezpieczeństwo użytkowników usług płatniczych. Wreszcie, badanie pozwoliło sformułować rekomendacje dotyczące przeciwdziałania zjawisku nieautoryzowanych transakcji, w tym postulaty *de lege ferenda*, które mogłyby przyczynić się do ograniczenia wyłudzania danych uwierzytelniających i wzmocnienia ochrony uczestników obrotu elektronicznego, a także poprawy efektywności regulacji i procedur stosowanych przez podmioty rynku finansowego.

Odbiorcy raportu

Raport jest przeznaczony do szerokiego grona odbiorców, obejmującego przede wszystkim podmioty rynku finansowego, w tym banki, jak również podmioty sektora technologicznego. Istotnymi adresatami Raportu są także organy władzy publicznej, takie jak Urząd Komisji Nadzoru Finansowego, Rzecznik Finansowy, Narodowy Bank Polski, Urząd Ochrony Konkurencji i Konsumentów oraz odpowiednie resorty administracji rządowej, w szczególności Ministerstwo Finansów oraz Ministerstwo Sprawiedliwości. Z uwagi na fakt, iż analizie poddano rozwiązania prawne, w tym zagadnienie odpowiedzialności odszkodowawczej oraz dochodzenie roszczeń w postępowaniu sądowym, odbiorcami mogą być również sądy oraz sędziowie Rzeczypospolitej Polskiej, a także profesjonalni pełnomocnicy zajmujący się prawem procesowym – zwłaszcza adwokaci i radcowie prawni. Zainteresowanie Raportem mogą wykazać również instytucje nauki i szkolnictwa wyższego, w tym uniwersytety, szkoły handlowe oraz Polska Akademia Nauk, a także media i komentatorzy życia publicznego.

Dokument może być również wartościowy dla organów stosujących i stanowiących prawo, jak Sejm, Senat, instytucje administracji rządowej oraz partie polityczne. W kręgu odbiorców należy również uwzględnić organizacje pozarządowe, zwłaszcza think-tanki działające w obszarze prawa i gospodarki, a także fundacje pełniące funkcję zaplecza analitycznego dla partii politycznych. Raport mógłby ponadto zainteresować kancelarie prawne, firmy doradcze oraz podmioty zajmujące się pośrednictwem finansowym.

Z uwagi na rosnącą rolę cyberbezpieczeństwa oraz skalę zagrożeń dla uczestników obrotu ze strony przestępców – raport powinien stać się elementem szeroko zakrojonej kampanii informacyjnej sektora finansowego, przyczyniając się do podniesienia świadomości społecznej, poprawy wizerunku instytucji finansowych oraz ograniczenia ryzyka nadużyć interpretacyjnych w potencjalnych sporach sądowych dotyczących nieautoryzowanych transakcji płatniczych.

Wydaje się ponadto, że niniejszy dokument może posłużyć jako podstawa do wypracowania odpowiednich wytycznych przez jednostki organizacyjne banków odpowiedzialne za zarządzanie ryzykiem oraz compliance, w szczególności w zakresie procedur obsługi klientów i kontrahentów dotkniętych wyłudzeniem danych prowadzącym do dokonania nieautoryzowanych transakcji.

Warto rozważyć również uczynienie niniejszego raportu przedmiotem wydarzeń akademickich, takich jak specjalistyczne seminaria, ogólnopolskie konferencje naukowe czy debaty z udziałem przedstawicieli administracji publicznej oraz sektora bankowego.

Przedmiot analizy

Przedmiotem analizy jest interdyscyplinarna, kompleksowa refleksja nad uwarunkowaniami prawnymi, gospodarczymi oraz społecznymi związanymi z nieautoryzowanymi transakcjami płatniczymi oraz odpowiedzialnością podmiotów za ich występowanie, ze szczególnym uwzględnieniem działalności podmiotów Big Tech, w tym mediów społecznościowych. Analiza została przeprowadzona przy zastosowaniu metody formalno-dogmatycznej, wspieranej ekonomiczną analizą prawa, metodą komparatystyczną oraz podejściem empirycznym (wywiady przeprowadzone metodą jakościową z ekspertami oraz respondentami reprezentującymi sektor bankowy).

Opracowany Raport prezentuje zarówno obowiązujące regulacje prawne dotyczące nieautoryzowanych transakcji i odpowiedzialności za nie, jak i praktyczne problemy wynikające z ich stosowania w rzeczywistym obrocie, ze szczególnym uwzględnieniem wyzwań pojawiających się w kontekście działalności podmiotów Big Tech. Dokument nie ogranicza się do opisu stanu prawnego, lecz przedstawia także krytyczną ocenę obowiązujących rozwiązań, uzupełnioną o szersze ujęcie tła gospodarczego i społecznego.

Raport zawiera ponadto postulaty *de lege ferenda* skierowane do krajowego prawodawcy, których wdrożenie mogłoby przyczynić się do skuteczniejszego ograniczenia zjawiska wyłudzania danych uwierzytelniających oraz wzmocnienia ochrony uczestników obrotu elektronicznego.

Wnioski wynikające z badania

Analiza zgromadzonego materiału – obejmującego zarówno wyniki badań jakościowych, w tym wywiadów pogłębionych, jak i dane rynkowe, działania regulatorów oraz informacje o bieżących praktykach platform społecznościowych – prowadzi do jednoznacznego wniosku, że duże platformy internetowe stanowią dziś kluczowy kanał dystrybucji oszukańczych treści, w szczególności reklam inwestycyjnych, phishingowych i innych form wyłudzeń finansowych. Skala zjawiska jest znacząca, a dynamika wzrostu utrzymuje się na poziomie wskazującym na trwałą i systemową naturę problemu. Co istotne, mimo deklaracji składanych przez największych dostawców usług cyfrowych, ich działania w praktyce nie są proporcjonalne do skali zagrożeń. Zwraca uwagę brak przejrzystych i skutecznych procedur zgłaszania podejrzanych reklam, niski poziom transparentności w zakresie rozpatrywania zgłoszeń oraz obserwowana w różnych jurysdykcjach niechęć do rzeczywistego usuwania treści stanowiących oczywiste nadużycia.

Ekonomiczna kalkulacja operatorów platform sugeruje, że eliminacja tego rodzaju treści nie jest dla nich opłacalna. Reklamy – także te generowane przez oszustów – stanowią źródło wymiernych przychodów, podczas gdy ryzyko sankcji czy konsekwencji prawnych pozostaje relatywnie niewielkie. Obserwowane w licznych raportach i postępowaniach sygnały wskazują, że deficyty bezpieczeństwa i nadzoru nie mają charakteru incydentalnego, lecz strukturalny. Liczba zgłoszeń, sygnały od sygnalistów, wyniki audytów wewnętrznych czy ostrzeżenia formułowane przez organy państwowe tworzą obraz podmiotów, które – mimo zaawansowanego zaplecza technologicznego – tolerują powtarzalne schematy oszustw lub reagują na nie w sposób opóźniony, incydentalny i niespójny. W świetle takich danych argument o „braku wiedzy" w rozumieniu art. 6 DSA traci wiarygodność. Przy tak dużej skali sygnałów i zidentyfikowanych wzorców działalności przestępczej trudno uznać, że platformy nie mają świadomości o istnieniu nielegalnych treści, szczególnie gdy dotyczą one powtarzalnych schematów, a nie jednostkowych incydentów.

W konsekwencji ciężar finansowy i operacyjny związany z nieautoryzowanymi transakcjami jest w praktyce przerzucany na sektor bankowy, który ponosi koszty zwrotów, prowadzenia postępowań wyjaśniających oraz realizacji działań edukacyjnych skierowanych do konsumentów. Oznacza to, że system nadzoru nad rynkiem cyfrowym pozostaje niewystarczający, a obowiązujące regulacje – choć formalnie rozbudowane, w szczególności po wejściu w życie DSA – nie są egzekwowane w sposób, który odpowiadałby rzeczywistym zagrożeniom.

Rekomendacje

Z perspektywy regulacyjnej i praktycznej konieczne jest więc zdecydowane wzmocnienie odpowiedzialności platform za treści o charakterze finansowym. Kluczowe znaczenie ma wyraźniejsze powiązanie obowiązków wynikających z art. 6 DSA z odpowiedzialnością odszkodowawczą określoną w art. 415 KC, tak aby platformy ponosiły odpowiedzialność w sytuacjach, w których – mimo uzyskania wiedzy o nielegalnych treściach – nie podjęły bezzwłocznych działań zmierzających do ich usunięcia. Niezbędne jest także wprowadzenie obowiązku weryfikacji reklamodawców w obszarach wysokiego ryzyka, takich jak inwestycje, pożyczki, kryptowaluty czy usługi finansowe, oraz stworzenie jednolitych procedur zgłaszania oszukańczych treści przez banki, organy nadzoru i użytkowników.

Równolegle potrzebne są działania wzmacniające transparentność – w szczególności obowiązek publikowania przez platformy regularnych raportów dotyczących liczby odrzuconych lub usuniętych reklam finansowych, sposobu ich weryfikacji oraz statystyk dotyczących zgłoszeń od użytkowników. Jedynie pełna przejrzystość pozwoli ocenić, czy deklarowane procedury mają realną skuteczność. Ponadto konieczne jest wprowadzenie mechanizmów ekonomicznych, które uczynią tolerowanie oszustw finansowych nieopłacalnym – w tym sankcji proporcjonalnych do skali przychodów z reklam oraz opłat kompensacyjnych na rzecz instytucji dotkniętych skutkami działań przestępczych.

Poprawa sytuacji w omawianym obszarze możliwa będzie wyłącznie w przypadku bardziej intensywnego zaangażowania organów władzy publicznej w nadzór nad firmami technologicznymi świadczącymi usługi internetowe – przez organy stosujące oraz stanowiące prawo, zarówno na poziomie krajowym, jak i ponadnarodowym (zwłaszcza Unii Europejskiej). Rekomendować należy zarówno większą aktywność takich organów, jak: Minister Cyfryzacji, Prezes Urzędu Ochrony Konkurencji i Konsumentów, Komisja Nadzoru Finansowego, Rzecznik Praw Obywatelskich, Prezes Urzędu Ochrony Danych Osobowych, a także działania polskich władz (m.in. Ministra Spraw Zagranicznych, Ministra Finansów i Gospodarki, Ministra Sprawiedliwości) na rzecz wypracowania rozwiązań ogólnoeuropejskich podnoszących bezpieczeństwo oraz wiarygodność treści udostępnianych w Internecie.

Duże znaczenie z perspektywy odpowiedzialności za oszustwa dokonywane poprzez reklamy na platformach społecznościowych ma doprecyzowanie pojęcia nieautoryzowanej transakcji. W obecnym brzmieniu rodzi ona wątpliwości interpretacyjne, które orzecznictwo zwykle rozstrzyga na niekorzyść banków, czyniąc je odpowiedzialnymi za transakcje, na które płatnik wyraził zgodę, choć był wprowadzony w błąd przez oszustów. Szczególnie niedopuszczalna etycznie jest sytuacja, w której bank odpowiada za naruszenia interesów płatnika, pomimo poinformowania go o zidentyfikowanym ryzyku, na które ten się godzi.

Ponadto, w celu skuteczniejszego ograniczania zjawisk nieautoryzowanych transakcji, szczególnie tych napędzanych przez reklamy publikowane na platformach społecznościowych, zasadne jest wprowadzenie zestawu nowych, bardziej zdecydowanych narzędzi oraz obowiązków regulacyjnych. Po pierwsze, platformy powinny funkcjonować na zasadach zbliżonych do instytucji finansowych (w tym banków) w zakresie AML/KYC, co oznaczałoby pełną identyfikację reklamodawców, rzetelną weryfikację dokumentów firm oraz zakaz publikacji reklam od podmiotów anonimowych. Uzupełnieniem tych wymogów może być obowiązek prowadzenia centralnego rejestru firm oferujących usługi finansowe i inwestycyjne – na wzór modelu stosowanego w Wielkiej Brytanii przez FCA (Financial Conduct Authority[1]). Wprowadzenie analogicznego rejestru w Polsce/UE umożliwiłoby weryfikację legalności podmiotów oraz ograniczenie skali nieautoryzowanych działań finansowych.

Istotnym elementem wzmocnienia systemu byłoby również wprowadzenie obowiązkowych interfejsów API (ang. Application Programming Interface[2]) umożliwiających bezpośrednią komunikację między platformami a instytucjami finansowymi oraz organami ścigania. Jego zastosowanie w obszarze bezpieczeństwa mogłoby służyć np. do zgłaszania w czasie rzeczywistym reklam związanych z oszustwem, blokowania płatności za takie reklamy, czy przekazywania danych na temat podejrzanych kont. Wprowadzenie takiego mechanizmu radykalnie skróciłoby czas reakcji i umożliwiłoby automatyczne wstrzymywanie potencjalnie szkodliwych kampanii jeszcze zanim dotrą one do konsumentów.

[1] Niezależny publiczny organ nadzoru finansowego w Wielkiej Brytanii, odpowiedzialny za autoryzację i rejestrację podmiotów świadczących usługi finansowe, nadzór nad ich działalnością oraz egzekwowanie przestrzegania standardów i regulacji. FCA określa wymagania, które firmy muszą spełnić, aby uzyskać pozwolenie na wykonywanie regulowanych czynności, monitoruje ich działalność po wpisie do rejestru oraz nakłada sankcje w przypadku naruszeń, w tym w obszarze reklam finansowych, ochrony konsumentów i standardów rynkowych.

[2] Techniczny „kanał komunikacji" między systemami, który pozwala na automatyczne i natychmiastowe przesyłanie określonych informacji.

Kolejną innowacyjną procedurą byłoby stworzenie funduszu kompensacyjnego przez największe platformy cyfrowe, Big Techy, z którego pokrywane byłyby roszczenia odszkodowawcze wypłacane w związku z nielegalnymi reklamami lub treściami wprowadzającymi w błąd. Fundusz mógłby być zasilany coroczną składką obliczaną jako procent globalnych lub europejskich przychodów reklamowych danej platformy. W razie wystąpienia pozytywnych przesłanek, tj. uznania, iż dana reklama doprowadziła użytkownika do straty finansowej (zwłaszcza w powiązaniu z nieautoryzowaną transakcją płatniczą), odszkodowanie byłoby wypłacone z funduszu w sposób znacznie szybszy i bardziej automatyczny niż w obecnych procedurach reklamacyjnych. Jednocześnie, powyższe nie zwalniałoby Big Tech z ewentualnych sankcji administracyjnych. Takie rozwiązanie zapewniłoby użytkownikom realną ochronę, a dla platform stanowiłoby ekonomiczny bodziec do zwiększania jakości weryfikacji udostępnianych treści.

Istotnym obszarem wymagającym wzmocnienia jest polityka sankcyjna. Choć DSA przewiduje kary pieniężne oraz grzywny, praktyka pokazuje, że nie są one wystarczająco skuteczne i odstraszające, zatem należałoby wprowadzić ich zaostrzenie. W tym celu warto uwzględnić wprowadzenie mechanizmu sankcji automatycznych, nakładanych z mocy prawa po przekroczeniu określonych progów naruszeń. Taki mechanizm funkcjonowałby podobnie do opłat kompensacyjnych, które mogłyby być naliczane w sposób proporcjonalny do skali działalności platform, co ma szczególne znaczenie w przypadku podmiotów Big Tech.

Uzupełniająco, system bezpieczeństwa powinien obejmować obowiązek natychmiastowego blokowania treści zgłoszonych jako fraud, wraz z oznaczeniem ich jako wstrzymanych, powiadomieniem organów ścigania oraz blokadą kont reklamodawcy do czasu pełnego wyjaśnienia sprawy. Dodatkowym rozwiązaniem mogłoby być zobowiązanie platform do ujawniania regulatorowi przejrzystych zasad dotyczących targetowania reklam oraz stosowanych mechanizmów ich priorytetyzacji. Warto również rozważyć wprowadzenie branżowego kodeksu reklamy cyfrowej, określającego minimalne standardy weryfikacji tożsamości reklamodawców, procedury audytów systemów wykrywania fraudów czy obowiązkowy 24-godzinny termin na odpowiedź na zgłoszenia instytucji finansowych.

Wśród rekomendowanych działań o charakterze systemowym kluczowe znaczenie ma wdrożenie przez sektor finansowy nowoczesnych narzędzi analitycznych, umożliwiających szybsze wykrywanie i neutralizowanie oszustw powiązanych z działalnością platform internetowych. W tym celu należy stworzyć wspólny bankowy system wczesnego ostrzegania oparty na sztucznej inteligencji, zdolny do automatycznego monitorowania platform społecznościowych i wykrywania nieautoryzowanych reklam wykorzystujących logotypy, nazwy lub identyfikację wizualną banków. System ten – działający w czasie rzeczywistym – powinien umożliwiać natychmiastowe zgłaszanie naruszeń do operatorów platform oraz ostrzeganie klientów narażonych na potencjalne ryzyko.

Powyższe powinno zostać wzbogacone poprzez stworzenie centralnej, międzybankowej bazy wzorców phishingowych. Jej zadaniem byłoby gromadzenie i aktualizacja w czasie rzeczywistym informacji o fałszywych stronach internetowych, reklamach oraz schematach oszustw, a następnie integracja tych danych z wewnętrznymi systemami antyfraudowymi wszystkich uczestniczących instytucji. Dzięki temu możliwe stałoby się automatyczne blokowanie przelewów oraz innych operacji kierowanych na adresy znane jako oszukańcze.

Przełomowym mechanizmem ochronnym mogłoby być także wprowadzenie tzw. okresów „cooling-off", czyli obowiązkowego czasu wstrzymania realizacji transakcji wysokiego ryzyka – zwłaszcza takich, które zostały zainicjowane po kliknięciu w link pochodzący z mediów społecznościowych lub w sytuacji, gdy klient loguje się po raz pierwszy z nowego urządzenia. W okresie tym bank powinien przeprowadzać dodatkową weryfikację intencji klienta z wykorzystaniem niezależnych kanałów komunikacyjnych.

Z perspektywy współpracy międzyinstytucjonalnej konieczne jest również podjęcie negocjacji na poziomie sektorowym z największymi globalnymi platformami technologicznymi. Związek Banków Polskich – oraz analogiczne instytucje w pozostałych państwach UE – powinny dążyć do zawarcia z Meta, Google, TikTok czy X umów ramowych obejmujących m. in. procedury priorytetowego zgłaszania i usuwania treści phishingowych, mechanizmy weryfikacji reklamodawców z branży finansowej, dostęp do interfejsów API umożliwiających automatyczne zgłaszanie naruszeń oraz współudział platform w pokrywaniu strat powstałych na skutek publikowania przez nie oszukańczych reklam.

Rekomenduje się powołanie sektoralnego punktu kontaktowego działającego w trybie 24/7, który stanowiłby jeden kanał komunikacji pomiędzy całym sektorem bankowym a platformami internetowymi. Jednostka ta odpowiadałaby za błyskawiczne przekazywanie zgłoszeń dotyczących nielegalnych treści,

koordynację ich usuwania oraz monitorowanie czasu i skuteczności reakcji po stronie Big Techów, co znacząco usprawniłoby proces przeciwdziałania nadużyciom.

Wreszcie, działania regulacyjne powinny zostać uzupełnione o wzmocnioną edukację użytkowników oraz o system współpracy instytucji finansowych, służb i platform cyfrowych. Wyłącznie zintegrowane podejście może prowadzić do realnego ograniczenia skali nieautoryzowanych transakcji, ich skutków i ogólnego poziomu ryzyka w systemach płatności. Wszystkie przedstawione materiały pokazują bowiem jasno, że brak reakcji ze strony platform nie jest wynikiem braku możliwości technicznych, lecz braku wystarczającej odpowiedzialności prawnej i ekonomicznej – i to właśnie te dwa elementy wymagają pilnej korekty.

Wstęp

1.1. Uwagi wprowadzające

Współczesny obrót gospodarczy jest w znacznym stopniu uzależniony od funkcjonowania usług płatniczych świadczonych w formie elektronicznej. Stanowią one kluczowy element infrastruktury finansowej, a ich realizacja jest obecnie zapewniana przez szerokie spektrum instytucji finansowych, w szczególności przez banki, które pozostają głównymi dostawcami tego rodzaju usług[3]. Jednocześnie od kilku lat obserwuje się na tym rynku dynamiczny wzrost aktywności podmiotów wywodzących się z sektora technologicznego, w szczególności przedsiębiorstw zaliczanych do grupy tzw. Big Tech[4]. Rola tych podmiotów w sektorze usług płatniczych stała się już przedmiotem licznych analiz prawno-ekonomicznych. Niezależnie jednak od dorobku badawczego, należy podkreślić, że rozwój obrotu elektronicznego – w szczególności zaś rosnące znaczenie mediów społecznościowych – generuje szereg zagrożeń zarówno dla użytkowników usług płatniczych, jak i dla podmiotów je świadczących. Nie dziwi zatem, że usługi płatnicze zostały objęte rozbudowaną regulacją prawną[5]. Polska ustawa o usługach płatniczych stanowi w tym zakresie przede wszystkim rezultat implementacji odpowiednich dyrektyw Unii Europejskiej[6], co odzwierciedla dążenie do harmonizacji tej sfery. Harmonizacja ta pozostaje kluczowa dla prawidłowego funkcjonowania jednolitego rynku.

W tym miejscu należy, dla porządku wywodu, odnotować oczywisty fakt: postęp technologiczny generuje nie tylko nowe możliwości rozwoju, ułatwień oraz innowacyjnych rozwiązań dla przedsiębiorców i konsumentów, lecz także nowe narzędzia i metody działania dla sprawców przestępstw. Można zatem uznać, że jednym z najpoważniejszych wyzwań współczesnego obrotu gospodarczego są nieautoryzowane transakcje płatnicze. Pojęcie to występuje w ustawie o usługach płatniczych – pojawia się w 27 przepisach – lecz nie zostało w niej wprost zdefiniowane, co tym bardziej uzasadnia potrzebę jego interpretacji. Rzecznik Finansowy wskazuje wprost, iż *„transakcja nieautoryzowana to taka transakcja, na którą użytkownik nie wyraził zgody"*[7]. Regulacje dotyczące odpowiedzialności za nieautoryzowane transakcje płatnicze znajdują szerokie zastosowanie w praktyce, co w konsekwencji przełożyło się na istotne zainteresowanie przedstawicieli doktryny, zarówno prawa cywilnego, jak i prawa karnego[8].

Do nieautoryzowanych transakcji płatniczych dochodzi przede wszystkim w sytuacjach, w których osoba nieuprawniona uzyskuje dostęp do danych uwierzytelniających użytkownika, takich jak numery kart płatniczych, loginy i hasła do bankowości elektronicznej czy jednorazowe kody uwierzytelniające. Jak powszechnie wiadomo, pozyskanie tych danych może następować zarówno przy użyciu tradycyjnych metod przestępczych, np. w wyniku kradzieży karty płatniczej, jak i – w coraz większym stopniu – poprzez wykorzystanie narzędzi oferowanych przez nowe technologie informacyjne. Wśród najczęściej stosowanych metod należy wskazać ataki phishingowe, tworzenie i rozpowszechnianie stron internetowych imitujących serwisy banków, instytucji finansowych czy podmiotów z sektora e-commerce, a także wysyłanie spreparowanych wiadomości tekstowych. Choć pełna skala zjawiska jest trudna do precyzyjnego oszacowania, już półtora roku temu Rzecznik Finansowy zwracał uwagę na

[3] Patrz np. A. Iwańczuk-Kaliska, *Bezgotówkowe płatności detaliczne w Polsce – rola banków i perspektywy rozwoju sektora paytech* (w:) „Finanse osobiste", red. K. Waliszewski, Warszawa 2022, s. 79-92.

[4] M. de la Mano, J. Padilla, *Big Tech Banking*, „Journal of Competition Law & Economics" 2018, t. 14, nr.4, s. 494–526; J. Padilla, *Big Tech "Banks", Financial Stability and Regulations*, „Revista de Estabilidad Financiera del Banco de España" 2020; O. Borgogno, G. Colangelo, *The data sharing paradox: BigTechs in finance*, „European Competition Journal" 2020, t. 16, nr. 2-3, s. 492-511; M. Pawłowska, *Wpływ przedsiębiorstw fintech na poziom konkurencji w sektorze finansowym. Wzrost czy osłabienie konkurencji?*, „Finanse i Prawo Finansowe" 2023 Numer specjalny 2, s. 27–56.

[5] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2024 r. poz. 30, 731, 1222, z 2025 r. poz. 146.).

[6] Przede wszystkim dyrektywy zwanej popularnie PSD2 (od ang. *Payment Services Directive 2*), czyli dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

[7] „Transakcje nieautoryzowane. Materiał o transakcjach nieautoryzowanych przygotowany we współpracy z UOKiK", na: https://rf.gov.pl/baza-wiedzy/najczestsze-pytania-i-odpowiedzi-faq/transakcje-nieautoryzowane/ [dostęp: 10 października 2025 r.].

[8] B. Wyżykowski, *Odpowiedzialność za nieautoryzowane transakcje płatnicze – wybrane zagadnienia wynikające z implementacji PSD2*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)" 2019 nr 8, s. 101-116; J. Szczerbowski, *Odpowiedzialność dostawcy usługi płatniczej za nieautoryzowaną transakcję płatniczą – uwagi na gruncie polskiej implementacji PSD2*, „Journal of Modern Science" 2021, t. 1 (46), s. 257–268; B. Wyżykowski, *Odpowiedzialność za wykonanie transakcji płatniczej z podaniem nieprawidłowego unikatowego identyfikatora na gruncie ustawy o usługach płatniczych*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)" 2021, nr 7, s. 43-62; A. Czesnowicka, *Transakcja nieautoryzowana z perspektywy prawnokarnej – kwalifikacja prawna dokonania tzw. płatności zbliżeniowej za pomocą cudzej karty płatniczej*, „Palestra" 2022, nr 7/8, s. 48-66; B. Wyżykowski, *Spory między dostawcami usług płatniczych a użytkownikami dotyczące transakcji płatniczych w świetle najnowszego orzecznictwa polskich sądów powszechnych*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)" 2022, nr 7, s. 28-47; D. Kowalski, *Europejskie ramy prawne ochrony konsumenta na rynku bankowym – aktualne problemy i wyzwania związane z rozwojem nowych technologii*, „Rocznik Administracji Publicznej" 2024, nr. 10, s. 107-118; P. Milik, G. Pilarski, *Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, „Cybersecurity and Law" 2023 t. 9, nr. 1, s. 108-126

„lawinowy wzrost liczby wniosków (…) dotyczących dochodzenia roszczeń przez banki z tytułu kredytów, które – jak twierdzą klienci – nie zostały przez nich świadomie zawarte, lecz stanowią efekt działań cyberprzestępców, wykorzystujących socjotechniki i metody hakerskie"[9]. Zapobieganie i zwalczanie tego typu nadużyć staje się jednym z kluczowych zadań państwa, co potwierdza m.in. przeprowadzona dwa lata temu kontrola Najwyższej Izby Kontroli, ukierunkowana na ocenę skuteczności realizowanych działań w tym obszarze[10].

Działania phishingowe obejmują nie tylko dane, które można uznać za klasyczne dane uwierzytelniające wykorzystywane w usługach płatniczych, lecz także informacje umożliwiające dostęp do kont w mediach społecznościowych. Zjawisko to osiąga niekiedy skalę masową, o czym regularnie informują zarówno media, jak i właściwe instytucje publiczne[11]. Jednocześnie media społecznościowe, ze względu na swoją specyfikę i oferowane narzędzia, stają się dla sprawców dogodnym środowiskiem do pozyskiwania danych uwierzytelniających, nierzadko właśnie za ich pośrednictwem. Wykorzystywane są w tym celu m.in. menedżer reklam, a także ogólnodostępne grupy czy wydarzenia[12]. W prasie i serwisach internetowych pojawiają się liczne analizy obrazujące konkretne sposoby działania przestępców w środowisku mediów społecznościowych. Informacje o takich praktykach publikują również podmioty publiczne, w tym CERT Polska[13]. Mamy więc do czynienia ze zbiegiem dwóch istotnych problemów współczesnego obrotu, ściśle związanych z rozwojem technologii informacyjnych: z jednej strony są to nieautoryzowane transakcje płatnicze, z drugiej – zagrożenia wynikające z korzystania z mediów społecznościowych oraz potencjalna odpowiedzialność za powstałe w ich wyniku szkody[14].

Dla obserwatorów współczesnej debaty publicznej nie będzie zaskoczeniem stwierdzenie, że kwestia odpowiedzialności podmiotów Big Tech ze szczególnym uwzględnieniem operatorów serwisów społecznościowych za działania ich użytkowników stanowi jeden z najbardziej złożonych i doniosłych problemów politycznych, ekonomicznych oraz prawnych o jednoznacznie globalnym charakterze. Zagadnienie to najczęściej pojawia się w kontekście procesów politycznych, a także problematyki dezinformacji i masowej manipulacji[15]. Choć sygnalizowany jest również problem publikowania w mediach społecznościowych fałszywych reklam oraz innych materiałów służących nielegalnemu pozyskiwaniu danych użytkowników[16], nie doczekał się on dotąd ani odpowiedniej uwagi medialnej, ani interdyscyplinarnych opracowań o charakterze kompleksowym. Celem proponowanego raportu jest wypełnienie tej luki i dostarczenie pogłębionej, analitycznej refleksji nad tym obszarem.

1.2. Wywiady z Respondentami

Badania poprzedzające przygotowanie raportu przeprowadzono z zastosowaniem m.in. metody empirycznej, tj. wywiadów pogłębionych, przeprowadzonych na grupie respondentów – doświadczonych ekspertów w obszarze *compliance/legal* w sektorze bankowym oraz reprezentantów sektora bankowego aktualnie zatrudnionych w polskich bankach.

Celem wywiadów było pozyskanie jakościowych danych dotyczących sposobu funkcjonowania obecnych mechanizmów rynkowych i regulacyjnych oraz lepsze zrozumienie praktycznych uwarunkowań zjawiska nieautoryzowanych transakcji.

Rozmowy obejmowały kilka kluczowych obszarów. Po pierwsze, respondenci przedstawiali swoje doświadczenia dotyczące skali i dynamiki zjawiska nieautoryzowanych transakcji, zarówno w perspektywie operacyjnej, jak i z punktu widzenia ogólnych trendów

[9] *Poradnik Rzecznika Finansowego w sprawie problematyki tzw. „kredytów na klik" i nieautoryzowanych transakcji płatniczych*, 21 grudnia 2023, na: https://archiwum.rf.gov.pl/2023/12/21/kredyt-na-klik-po/ [dostęp: 10 października 2025 r.].

[10] Informacja o wynikach kontroli: Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości, P/21/042/KPB, 7 marca 2023 r., na: https://www.nik.gov.pl/kontrole/P/21/042/KPB/ [dostęp: 10 października 2025 r.].

[11] *UWAGA! CSIRT NASK ostrzega – trwa masowa kampania phishingowa podszywająca się pod obsługę platformy Facebook*, 26 maja 2023 r., na: https://www.gov.pl/web/baza-wiedzy/uwaga-csirt-nask-ostrzega--trwa-masowa-kampania-phishingowa-podszywajaca-sie-pod-obsluge-platformy-facebook [dostęp: 10 października 2025 r.].

[12] M. Świetlińska, *Jak cyberprzestępcy maskują phishingowe reklamy na Facebooku?*, 3 września 2024 r., na: https://www.securitymagazine.pl/pl/a/jak-cyberprzestepcy-maskuja-phishingowe-reklamy-na-facebooku [dostęp: 10 października 2025 r.].

[13] CERT Polska to zespół działający w strukturach NASK – Państwowego Instytutu Badawczego, powołany w 1996 roku do reagowania na incydenty bezpieczeństwa komputerowego. Realizuje zadania CSIRT NASK, jednego z trzech takich zespołów działających na poziomie krajowym w ramach krajowego systemu cyberbezpieczeństwa: https://cert.pl/ [dostęp: 28 listopada 2025 r.].

[14] *Oszustwa reklamowe na dużych platformach internetowych*, 25 listopada 2024 r., na: https://cert.pl/posts/2024/11/Oszustwa-reklamowe-na-duzych-platformach/ [dostęp: 10 października 2025 r.].

[15] V. Jourova, *Potrzebujemy większej odpowiedzialności firm Big Tech*, 20 stycznia 2021 r., na: https://www.rp.pl/polityka/art8698221-potrzebujemy-wiekszej-odpowiedzialnosci-firm-big-tech [dostęp: 10 października 2025 r.].

[16] M.in.: M. Dzięciołowski, *Sieć pełna fałszywych reklam*, https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/9680143,siec-pelna-falszywych-reklam.html [dostęp: 10 października 2025 r.].

obserwowanych na rynku. Po drugie, zapytano o zidentyfikowane przyczyny i mechanizmy prowadzące do tych incydentów – od technik manipulacji i inżynierii społecznej, po słabe praktyki weryfikacyjne, błędy użytkowników oraz systemowe słabości infrastruktury cyfrowej. Trzecim istotnym wątkiem była rola dużych platform społecznościowych i firm technologicznych jako kanałów wykorzystywanych do dystrybucji fałszywych reklam, phishingu oraz innych treści sprzyjających popełnianiu przestępstw finansowych. Respondenci oceniali, w jakim stopniu działania lub zaniechania tych podmiotów wpływają na wzrost liczby nieautoryzowanych transakcji oraz jakie ryzyka generują stosowane przez platformy modele biznesowe. Dodatkowo, uczestników poproszono o sformułowanie opinii dotyczących środków, które powinny zostać podjęte, aby skuteczniej przeciwdziałać nieautoryzowanym transakcjom, zwłaszcza w kontekście aktywności reklamowej prowadzonej przez Big Techy. W wypowiedziach pojawiały się zarówno propozycje wzmocnienia mechanizmów nadzorczych i odpowiedzialności platform, jak i postulaty dotyczące edukacji użytkowników oraz poprawy współpracy między sektorem finansowym a podmiotami technologicznymi. Ostatnim obszarem poruszanym w ramach wywiadów była ocena aktualnego stanu regulacji prawnych w Polsce i Unii Europejskiej. Respondenci analizowali adekwatność obowiązujących przepisów – w szczególności Digital Services Act, regulacji ochrony konsumenta oraz wymogów dotyczących usług płatniczych – pod kątem ich skuteczności w ograniczaniu ryzyka oszustw finansowych oraz możliwości egzekwowania odpowiedzialności od dużych platform cyfrowych.

Zebrane wypowiedzi stanowią kluczowy wkład w dalszą część raportu, dostarczając nie tylko pogłębionych obserwacji i diagnoz, lecz także praktycznych rekomendacji dotyczących kierunków koniecznych zmian regulacyjnych oraz operacyjnych.

Łącznie przeprowadzono 6 (sześć) wywiadów z 7 (siedmioma) Respondentami, w oparciu o ustandaryzowany scenariusz (którego treść zawarto w Załączniku nr 1 raportu), uwzględniając w grupie respondentów zarówno reprezentantów banków dużych, jak i spółdzielczych, a także osoby posiadające wszechstronne doświadczenie w obszarze prawnym i zgodności, w tym zdobyte w sektorze bankowym oraz innych przedsiębiorstwach.

W badaniu udział wzięły następujące osoby: Joanna Kucharczyk (radca prawny w Departamencie Zgodności VeloBank SA), Paweł Krakowiak (Dyrektor Departamentu Przeciwdziałania Fraudom w Banku Pekao SA), Szymon Kurnicki (Dyrektor ds. Strategii Płatności Citi Handlowy – Bank Handlowy w Warszawie SA), Daria Kolenda i Ewa Billewicz (Liderki zespołów Centrum Przeciwdziałania Oszustwom ING Banku Śląskiego SA), Paulina Grala (Kierownik zespołu płatności kartowe w SGB-Bank SA), Mariusz Sudoł (adwokat i doktor nauk prawnych, w przeszłości przez kilka lat wykonywał obowiązki dyrektora departamentu compliance jednego z komercyjnych banków).

Autorzy raportu pragną jednocześnie podziękować wszystkim Respondentom, którzy poświęcili cenny czas na udział w badaniu, odpowiadając na pytania oraz dzieląc się informacjami, wiedzą, opiniami, w tym własnymi (a bardzo cennymi i inspirującymi) przemyśleniami na temat praktyki nieautoryzowanych transakcji oraz sposobów lepszego uregulowania tej materii.

***

Poniżej załączono wybrane wypowiedzi sformułowane w trakcie wywiadów.

Przede wszystkim, z przeprowadzonych wywiadów wynika jednoznacznie, że **skala nieautoryzowanych transakcji jest w Polsce duża, dynamicznie się zwiększa, a dużą rolę odgrywają tu właśnie treści w internecie**, z których znaczna część to – wyświetlane i promowane przez platformy internetowe i podmioty typu Big Tech – tzw. reklamy oszukańcze, komunikaty wprowadzające w błąd, manipulujące lub wprost instrumenty wykorzystywane przez przestępców.

„Platformy społecznościowe oraz firmy technologiczne dostarczające treści w internecie odpowiadają za duży odsetek nieautoryzowanych transakcji, wprowadzając w błąd klientów banków. Skala takich przypadków sukcesywnie rośnie i nie mamy wątpliwości, że stan ten jest efektem świadomej polityki tych podmiotów, które zdają sobie sprawę, że podnosząc „klikalność" swoich materiałów, niejednokrotnie odwołujących się do emocji odbiorców, zapewniają sobie większe wpływy, a jednocześnie nie biorąc odpowiedzialności za straty, które potem i tak zostają przerzucone na banki, a ewentualne roszczenia lub kary będzie bardzo trudno wyegzekwować. To postawa nie tylko bezprawna, ale przede wszystkim nieetyczna".

„Moim zdaniem rola platform społecznościowych i globalnych firm technologicznych (Big Tech) w eskalacji tego zjawiska jest ogromna. Stały się one kluczowym narzędziem w rękach przestępców z kilku powodów.

Skala i zasięg: platformy takie jak Facebook, Instagram czy TikTok pozwalają oszustom dotrzeć do milionów potencjalnych ofiar przy minimalnym koszcie.
Anonimowość: przestępcy mogą stosunkowo łatwo tworzyć fałszywe profile, podszywając się pod znane marki, co utrudnia ich identyfikację.
Systemy reklamowe: zautomatyzowane systemy reklamowe są masowo wykorzystywane do promowania oszustw. Algorytmy precyzyjnie targetują reklamy do grup najbardziej podatnych na manipulację, a weryfikacja reklamodawców jest często niewystarczająca.
Brak odpowiedzialności: platformy często zasłaniają się statusem pośrednika, argumentując, że nie ponoszą odpowiedzialności za treści publikowane przez użytkowników. Procesy usuwania szkodliwych treści są często powolne i nieefektywne.
W efekcie, media społecznościowe stały się głównym kanałem dystrybucji fraudów, a Big Tech, świadomie lub nie, czerpie zyski z reklam finansujących działalność przestępczą".

„Z mojej perspektywy, skala zjawiska transakcji nieautoryzowanych jest znacząca i, co najważniejsze, stale rośnie. Obserwuję ewolucję metod przestępczych – od fizycznych kradzieży kart, po wyrafinowane, wieloetapowe ataki w cyberprzestrzeni. Uważam, że wzrost ten jest napędzany przez cyfryzację usług bankowych. O ile przynosi ona ogromną wygodę klientom, o tyle otwiera nowe wektory ataku dla przestępców. Każdego dnia w bankowości analizuje się tysiące alertów z systemów monitorujących. Choć większość to fałszywe alarmy, odsetek rzeczywistych prób oszustw jest na tyle duży, że wymaga dedykowanych, zaawansowanych zespołów i technologii. Straty finansowe, choć dotkliwe, to tylko część problemu. Równie istotne są straty wizerunkowe oraz spadek zaufania klientów. Zjawisko to ma charakter globalny, a polski rynek, jako jeden z liderów innowacji, jest szczególnie narażony na ataki wykorzystujące najnowsze technologie".

„Skala jest poważna, bo jak rozmawiamy wewnętrznie, to (...) jest to jedno z ważniejszych wyzwań dla banków i ważniejsze ryzyko".

„Jeżeli chodzi o skalę nieautoryzowanych transakcji, to jest ona coraz większa. Przede wszystkim dotyka ona klientów detalicznych, ponieważ najłatwiej zmanipulować osoby fizyczne, często mniej wyedukowane lub mniej posługujące się nowoczesnymi technologiami".

„Jeśli chodzi o rolę platform internetowych i firm technologicznych – to muszę stwierdzić, że to niebagatelny element. Są to nośniki reklam, w tym właśnie fałszywych reklam. (...) Big Techy mają nie tylko przewagę faktyczną, działając globalnie i kierując się do szerokiego audytorium odbiorców, ale i dysponując jednocześnie uprzywilejowaną pozycją prawną – te podmioty funkcjonują nie tylko w ramach prawa polskiego, ale na ogół mają siedzibę za granicą, poza terenem Unii Europejskiej, co powoduje, że trudno skutecznie egzekwować ich odpowiedzialność i formułować roszczenia".

„Rola platform społecznościowych i firm technologicznych dla działań przestępczych w kontekście nieautoryzowanych transakcji jest bardzo duża. Po stronie instytucji powinny być podjęte radykalne kroki, żeby tego typu reklamy, ogłoszenia, informacje nieweryfikowalne jednak weryfikować, bo to jest istotny element. Chodzi o to, żeby takie fałszywe oferty po prostu minimalizować. Natomiast zdajemy sobie sprawę, że to jest ciężkie. Na niektórych tego typu platformach nawet trudno znaleźć jakieś elementy do odniesienia się, czy informacje w jaki sposób zgłosić coś niepokojącego, co trzeba po prostu zdjąć. A co dopiero oczekiwać, że tego typu organizacje czy platformy miałyby realizować jakieś bardziej aktywne kroki jeszcze przed umieszczeniem takich reklam, czyli po prostu je weryfikować pod kątem takich oszukańczych ofert".

„Jakie są przyczyny tego zjawiska? W pierwszej kolejności odpowiada za to niewyobrażalnie dynamiczny rozwój technologii, tzn. przestępcy mają coraz więcej narzędzi i pomysłów na to, w jaki sposób – w dodatku coraz tańszy sposób i bardziej powszechny – wykorzystywać je w swojej bezprawnej i szkodliwej działalności. To nie jest tylko AI, ale np. tworzenie call-center, oprogramowanie umożliwiające w sposób szybki tłumaczenie na różne języki komunikatów (np. z polskiego na rumuński albo z rumuńskiego na polski), co pozwala od razu dotrzeć do wielu odbiorców – przygotować atak, również za granicą, na innych kontynentach. (...) Równocześnie też istnieją zaawansowane środki socjotechniczne pozwalające połączyć je z technologią. Reasumując to wszystko – ataków na klientów jest coraz więcej. A, mimo że ostrzeżeń i kampanii informujących o ryzykach jest (zarówno inicjowanych przez banki, jak i organy władzy publicznej) coraz więcej, klienci ulegają presji, a przestępcze działania wywołują efekt, powodując że środki z kont bankowych wypływają."

Respondenci zasadniczo zgadzają się, że **celem oszustów są wszyscy odbiorcy, lecz grupami szczególnie zagrożonymi (podatnymi na popełnienie błędu i doprowadzenie do transakcji nieautoryzowanej) są osoby starsze, słabiej orientujące się w nowoczesnych technologiach i gorzej weryfikujące treści internetowe, a także nieodporne na emocjonalną manipulację**.

„Z prowadzonych analiz w obszarze fraudowym wynika, że nie ma znacząco wyróżniającej się grupy społecznej, rozproszenie jest szerokie. Są osoby z małych miejscowości i z dużych. Są osoby starsze, ale są też młodsze. Są osoby z niższym wykształceniem, ale zdarzają się też przypadki osób, które są bardzo dobrze wykształcone. Tak więc nie dominuje tutaj jakaś określona grupa społeczna, aczkolwiek jeśli chodzi o sam wiek, to najwyższy jest udział osób od pięćdziesiątego piątego roku życia w górę".

„Jednym z najpoważniejszych zagrożeń jest phishing, czyli jedna z technik inżynierii społecznej, odwołująca się do emocji, skojarzeń z osobami, w tym znajomymi, bliskimi, rodziną i instytucjami przewidywalnymi (urzędami, bankami, służbami odpowiedzialnymi za bezpieczeństwo)".

Przestępcy wykorzystują socjotechnikę, a także naiwność odbiorców oraz nadzieję szybkiego i łatwego zysku, ponadto nowoczesne technologie typu *deep-fake* lub inne instrumenty oparte o sztuczną inteligencję (AI).

„Wektor oszustw inwestycyjnych wykorzystuje systemy reklamowe platform społecznościowych do promowania fałszywych ofert inwestycyjnych. Reklamy, często opatrzone wizerunkiem znanych osób, obiecują nierealistycznie wysokie zyski. Po kliknięciu, ofiara jest kierowana na fałszywą platformę, gdzie jest nakłaniana do wpłacenia „depozytu". W rzeczywistości środki trafiają bezpośrednio do przestępców, a rzekome zyski pokazywane na fałszywym panelu mają jedynie zachęcić do dalszych wpłat".

„Już teraz widzę próby wykorzystania technologii deepfake (audio i wideo) do podszywania się pod inne osoby w celu wyłudzenia pieniędzy. Skala i wiarygodność tych ataków będzie rosła. Anonimowość i globalny charakter kryptowalut czynią je idealnym narzędziem do prania pieniędzy pochodzących z oszustw".

„W obszarze socjotechniki, inżynierii społecznej, obserwujemy dość sporo transakcji na większe kwoty. Dotyczą one na przykład „inwestycji". Klienci skądś dowiadują się, że jest możliwość zainwestowania w takim przestępczym rozumieniu, gdzieś znajdują tę informację i potwierdzenie, że to jest coś, w co warto się zaangażować. Są to media takie czy inne, czy social media. Jest to źródło informacji. Wykorzystywane są te platformy, które są nam bliskie, łatwe w obsłudze. Na przykład kontakt na popularnym komunikatorze".

„Jakość owych fałszywych reklam i wprowadzających w błąd materiałów jest niestety coraz lepsza, nieraz nawet osobie doświadczonej trudno odróżnić dane prawdziwe pochodzące od legalnie działającej, nadzorowanej instytucji finansowej od podmiotu o wątpliwej wiarygodności. Trudno się zatem dziwić, że społeczeństwo nabiera się na te sztuczki".

„Banki reagują m.in. na to, czego wymagają od nich regulatorzy i jesteśmy coraz bardziej zaawansowani pod względem technicznym, a to się przekłada na zmianę obszarów problemowych. Kiedyś większym problemem były kwestie związane z zabezpieczeniami technicznymi. Teraz istotniejsza jest kwestia poradzenia sobie z inżynierią społeczną, socjotechniką ze strony oszustów".

Respondenci są generalnie zgodni co do niesatysfakcjonującego stanu normatywnego – wskazując, że problemem nie jest tylko trudność w dochodzeniu roszczeń (pozwaniu i egzekwowaniu prawa) względem firm mających siedzibę poza Unią Europejską, lecz również niedostateczna precyzja krajowego i unijnego prawodawstwa.

„Aktualny stan prawny – zarówno na poziomie krajowym, jak i unijnym – wydaje się niesatysfakcjonujący, ponieważ z jednej strony nie zabezpiecza dostatecznie uczestników rynku przed ryzykami nadużyć, oszustw, manipulacji i innych przestępstw w internecie, z drugiej zaś strony prowadzi do niesłusznego przypisania obowiązku zwrotu środków przez banki, które nie tylko nie zawiniły, lecz ponoszą koszty budowy coraz bardziej zaawansowanej instrastruktury bezpieczeństwa, działań podnoszących świadomość

klientów oraz zagwarantowania środków, które są przeznaczane na potencjalny przyszły zwrot środków w razie zgłoszenia nieautoryzowanych transakcji. Co więcej, w opinii publicznej panuje czasem nieuzasadnione przekonanie, wzmacniane dodatkowo przez działalność niektórych urzędów (UOKiKu, Rzecznika Finansowego), że nie tylko odpowiedzialność, ale wręcz wina za nieautoryzowane transakcje obarcza bank".

„Po wielu latach obowiązywania PSD, PSD2 wciąż problematyczny jest fundament – definicja autoryzacji transakcji – gdzie jest autoryzacja, a gdzie autoryzacji nie ma i jaki jest tak naprawdę zakres odpowiedzialności za transakcje nieautoryzowane. Co bank powinien wykazać, a czego nie jest w stanie. Mam wrażenie, że cały czas kręcimy się wokół tego, czym jest ta autoryzacja. W dalszym ciągu jest rozbieżność pomiędzy tym, co uważa regulator, a tym, co racjonalnie powinno się przyjąć w zakresie wykładni przepisów".

„Źródłem problemu jest również fakt, iż Big Techy mają pochodzenie pozaeuropejskie, co przekłada się na trudność w egzekwowaniu obowiązków, roszczeń i odpowiedzialności. Zwłaszcza, że są to na ogół firmy amerykańskie, które trudno zmusić do podporządkowania się oraz efektywnego weryfikowania prezentowanych treści, które wprowadzają lub przynajmniej mogą wprowadzać w błąd. Wydaje się, że pojedyncze państwo jest zbyt słabe do skutecznego narzucenia swojej woli, zatem konieczna jest współpraca na poziomie ponadnarodowym w ramach Unii Europejskiej. (…) Wyrazem zainteresowania Unii tym problemem są akty prawne, takie jak np. DSA, czyli Digital Services Act".

„Te kwestie regulacyjne mogłyby być znacznie bardziej doprecyzowane. Żeby była większa efektywność, w tym w zakresie kontroli platform. Z tego co mi wiadomo, to nie jest właściwie uregulowane w kontekście zwiększania bezpieczeństwa konsumentów, klientów itd. Wszystko wskazuje na to, że od tej strony regulacyjnej, legislacyjnej jest sporo do zrobienia w tym zakresie".

„Sądzę, że należy wprowadzić regulacje, które nakładałyby na platformy współodpowiedzialność za straty finansowe wynikające z oszustw promowanych za pomocą ich systemów. Powinny one być zobligowane do wdrożenia solidnych procedur weryfikacji reklamodawców. (…) Konieczne jest wprowadzenie przepisów, które jasno definiowałyby odpowiedzialność platform internetowych za umożliwianie oszustw. Sformułowanie jasnego i przejrzystego prawa dotyczącego obsługi transakcji nieautoryzowanych bez zbędnych procedur sądowych".

„Oceniam, że obecny stan prawny w Unii Europejskiej, w tym w Polsce, jest krokiem w dobrym kierunku, ale pozostaje niewystarczający. Dyrektywa PSD2 wprowadziła silne uwierzytelnienie klienta (SCA), ale nie adresuje w pełni problemu transakcji autoryzowanych pod wpływem manipulacji.

Moje propozycje zmian legislacyjnych.

Nowelizacja ustawy o usługach płatniczych: wprowadzenie przepisów, które jasno definiowałyby odpowiedzialność platform internetowych za umożliwianie oszustw. Sformułowanie jasnego i przejrzystego prawa dotyczącego obsługi transakcji nieautoryzowanych bez zbędnych procedur sądowych.

Stworzenie centralnego rejestru rachunków wykorzystywanych do przestępstw: umożliwiłoby to szybsze blokowanie środków.

Uproszczenie procedur prawnych: skrócenie czasu potrzebnego na uzyskanie zgody prokuratury na blokadę środków na podejrzanym koncie.

Moim zdaniem regulacje muszą nadążać za technologią. Konieczne jest przesunięcie ciężaru odpowiedzialności z konsumenta na potężne korporacje technologiczne".

Wszyscy respondenci wskazują na okoliczność, iż **banki są świadome zagrożeń i permanentnie podnoszą poziom zabezpieczeń, wychodząc jednocześnie z inicjatywami służącymi uświadamianiu swoich klientów, co spotyka się nieraz z niezrozumieniem oraz zarzutami biurokratyzacji, formalizacji relacji bank-klient, a nawet późniejszym przerzucaniem rzekomej winy na bank, który niedostatecznie zabezpieczył klienta i umożliwił mu dokonanie wadliwej transakcji**.

„Zdarza się, że w sposób ewidentny klient banku zachował się nieroztropnie, wykazał łatwowiernością, podjął nieprzemyślaną, pod wpływem emocji i wyobrażenia łatwego i szybkiego zysku, decyzję o zainwestowaniu swoich oszczędności. Dość szybko okazuje się jednak, że nie

była to żadna inwestycja, lecz zorganizowana forma manipulacji, mającej na celu wyłudzenie pieniędzy. (…) Żal i złość tej osoby przenosi się wówczas na bank, tak jakby to właśnie bank nie zapewnił dostatecznego poziomu zabezpieczeń, a wręcz skłonił do decyzji o nieudanej inwestycji. (…) Bywa też tak, że podwyższanie poziomu zabezpieczeń przez bank – który wprowadza np. dodatkowe środki weryfikacji i ostrzeżenia – spotyka się z niezadowoleniem i krytyką ze strony klientów, którzy wyrażają niezadowolenie, że dzwoni do nich pracownik z infolinii banku zadający dodatkowe pytania o realizowaną transakcję, zabiera czas, utrudnia przeprowadzenie operacji".

„Zdarza się, że wiemy o zdarzeniu już na wcześniejszym etapie, zatrzymując takie transakcje do weryfikacji z klientem. To są klienci, którzy niestety dają się namawiać na jakieś benefity, ktoś im coś obiecuje. To jest pierwsza grupa. Są też klienci, którzy faktycznie wykonują po prostu dużo różnych transakcji, operacji i nie przywiązują ze względu na rutynę wagi do tego, że klikają w jakieś oszukańcze linki".

„Banki, poza informowaniem oraz kampaniami mającymi podnieść świadomość klientów w zakresie zagrożeń towarzyszących transakcjom, wprowadzają dodatkowe mechanizmy weryfikacji transakcji, lecz najsłabszym elementem każdego procesu jest człowiek. Zwłaszcza jeśli zastosowano wobec niego mechanizm perswazyjny, polegający na kreowaniu wyobrażenia łatwego zarobku lub pewnej i bezpiecznej inwestycji, którą jest w stanie szybko zrealizować".

Tymczasem jednocześnie to na nie przerzucono obowiązek zwrotu środków, które stracił klient na skutek nieautoryzowanych transakcji, nawet wtedy, gdy doszło do niej na skutek nieostrożności klienta. W tej sytuacji jako niesprawiedliwe należy ocenić obowiązek zwrotu obciążający bank, który nie zawinił, a wręcz wdrożył daleko idące środki ostrożności, ściśle przestrzegał prawa i innych norm zgodności, podczas gdy wielka firma działająca globalnie w internecie zyskuje na wprowadzaniu w błąd swoich odbiorców. Uważam, że szkoda powinna być bankowi wyrównana, zrekompensowana".

„Warto zwrócić uwagę na problem z punktu widzenia ekonomicznej analizy prawa, czyli przestrzegania prawa w kontekście bilansu zysków i strat. Aktualny stan prawny oraz jego egzekwowanie prowadzić musi do wniosku, że obecnie naruszanie prawa i sprzyjanie reklamodawcom – niezależnie od tego, czy promują rzetelny produkt, czy nie – się po prostu biznesowo opłaca, ponieważ żyją one z generowania ruchu na portalach, „clickbaitu" oraz wpływów z tych reklam, które znacznie przewyższają koszt negatywnych skutków, czyli pozwów, roszczeń, kar nakładanych przez organy władzy publicznej czy strat wizerunkowych". (…) Inną, ważną do zasygnalizowania sprawą jest pytanie o to, z jakich źródeł pochodzą środki angażowane w promocję reklam oszukańczych. Nie mam konkretnych dowodów, więc nie będę formułował jednoznacznych oskarżeń, ale wiedząc, że przeznaczane są na to bardzo duże środki – naturalne wydaje się podejrzenie, że mogą być to środki z nielegalnych źródeł, podejrzane z punktu widzenia regulacji AML-owych."

Przedmiotem krytyki jest sytuacja, w której **banki – pozostając jednocześnie podmiotami zaufania społecznego, podlegającymi daleko idącej nadregulacji i nadzorowi ze strony państwa – zobowiązane są do zwrotu środków, przy jednoczesnej akceptacji dla nagannych i bezprawnych praktyk Big Techów, które niejednokrotnie w pełni świadomie oraz dla zysku udostępniają wprowadzające w błąd (oszukańcze) treści**.

Postępowanie podmiotów typu Big Tech jest nie tylko bezprawne, ale i nieetyczne – tym bardziej, że często jest to ich konsekwentna, uporczywa i świadoma polityka.

„Banki należą do najbardziej regulowanych sektorów, podlegających ścisłemu nadzorowi ze strony państwa, w tym także zjawiskom nadregulacji, a jednocześnie podejmują szerokie działania mające na celu uczulenie swoich klientów na ryzyko nieautoryzowanej transakcji i szerzej rozumianego bezpieczeństwa w sieci.

„Niestety zwrócić też trzeba uwagę, że odbiorcy treści internetowych, często nie będąc świadomymi konsekwencji prawnych, klikają w wyświetlające się komunikaty, co oznacza formalnie wyrażenie zgody na związanie się regulaminami lub zobowiązaniami wynikającymi z ich wewnętrznych polityk, co powoduje później, że – w razie sporu prawnego – prawnicy tych korporacji mają ułatwione zadanie w obronie przed roszczeniami. (…) Pojawia się zasadne pytanie o etykę takich działań, a także o konieczność szerszej ochrony

przez takimi działaniami, np. w drodze prewencyjnych akcji organów władzy publicznej lub reakcji przypominającej ostracyzm społeczny, który napiętnuje te postawy, przyczyniając się do strat wizerunkowych i kosztów rynkowych. Pamiętajmy, że mamy przecież środki do wywierania presji i egzekwowania odpowiedzialnych oraz prawnie dopuszczalnych zachowań i nie powinniśmy godzić się na to, że najpotężniejsi gracze rynkowi ignorują tak naprawdę prawa konsumentów, narażając na szwank ich interesy oraz generują zagrożenia, sprzyjając przestępcom".

W świetle przeprowadzonych wywiadów, uzasadniona jest teza, że **rozwiązaniem zidentyfikowanych problemów nie jest prawo i postawa organów je stosujących na poziomie krajowym – a niezbędna okazuje się aktywność (zwłaszcza koordynacja działań) na poziomie ponadnarodowym (unijnym, lecz również w relacjach Unia Europejska-Stany Zjednoczone-Chiny)**, ponieważ wyłącznie na poziomie globalnym wypracowane mogą być skuteczne mechanizmy zapobiegające lub ograniczające praktykę Big Techów.

„Zjawiska, o których rozmawiamy, nie występują jedynie w Europie, ale na całym świecie – więc założyć trzeba, że gdyby środowisko bankowe, wykorzystując swoje globalne relacje, a także inne podmioty: państwowe, unijne, organizacje konsumenckie itd. zaczęły wywierać nacisk – byłoby to znacznie bardziej skuteczne. I podkreślam, że powinny być to zarówno działania władcze, zinstytucjonalizowane, ale również inne, „miękkie"; wyobraźmy sobie choćby stworzenie kodeksu dobrych praktyk, który byłby jednoznacznym sygnałem dla Big Techów, że niektóre zachowania nie są i nie będą akceptowane".

„Konieczne jest stworzenie ram współpracy między sektorem bankowym, firmami Big Tech a organami ścigania. Umożliwiłoby to błyskawiczną wymianę informacji o nowych schematach oszustw".

Niezależnie od działań instytucjonalno-prawnych, **potrzebne jest dalsze prowadzenie kampanii informacyjnych oraz innych działań nakierowanych na podnoszenie wiedzy i świadomości klientów w obszarze cyberbezpieczeństwa** – najlepiej we współpracy z organami władzy publicznej, rozpoznawalnymi organizacjami pozarządowymi oraz osobami cieszącymi się popularnością i autorytetem, a także **rozwijanie wewnętrznych procedur bankowych służących ograniczeniu oszust i fraudów**.

„Banki zrobiły już bardzo dużo w kontekście różnych mechanizmów weryfikacyjnych, różnych potykaczy, na których zatrzymujemy klienta, tak żeby go uświadomić albo dodatkowo weryfikować przed wykonaniem potencjalnie fraudowej transakcji. Realizowane są też liczne kampanie edukacyjne. Wydaje mi się, że oprócz większego wpływu właściwych instytucji państwa lub odpowiednich urzędów na platformy technologiczne, UOKiK jest właściwym aktorem, który mógłby skoordynować cykliczną i ogólnopolską kampanię społeczną, radiowo-telewizyjną, która dotarłaby do znacznie szerszej grupy odbiorców. Najczęściej konsumenci zaglądają na stronę internetową banku, do aplikacji mobilnej lub też bankowości internetowej, aby dotrzeć do odpowiednich komunikatów i ostrzeżeń. Nie każdy czyta uważnie komunikaty ostrożnościowe lub autoryzacyjne push ze szczegółami transakcji. Podsumowując wydaje mi się, że taka inicjatywa ze strony UOKiK byłaby bardzo dobrym uzupełnieniem, tak żeby cyklicznie docierać do jak największej części społeczeństwa".

„Należy prowadzić ciągłe, szeroko zakrojone kampanie edukacyjne. Kluczowe jest tu hasło: »Pracownik banku nigdy nie poprosi cię o podanie hasła, kodu BLIK czy instalację oprogramowania«".

Choć nie wszyscy Respondenci wyrazili ów pogląd wprost – wydaje się, że panuje zgoda co do konieczności integracji i koordynacji różnych działań, zarówno władczych, jak i nie władczych, inicjowanych „oddolnie" (przez banki, organizacje pozarządowe i inne podmioty prywatne), jak też organy państwa i Unii Europejskiej w obszarze prewencji, ograniczania i łagodzenia skutków nieautoryzowanych transakcji.

„Uważam, że skuteczna walka wymaga zintegrowanych działań, ze szczególnym uwzględnieniem roli Big Tech:
Wymuszenie odpowiedzialności na platformach: Sądzę, że należy wprowadzić regulacje, które nakładałyby na platformy współodpowiedzialność za straty finansowe wynikające z oszustw promowanych za pomocą ich systemów. Powinny one być zobligowane do wdrożenia solidnych procedur weryfikacji reklamodawców.
Współpraca i wymiana danych: konieczne jest stworzenie ram współpracy między sektorem bankowym, firmami Big Tech a organami ścigania. Umożliwiłoby to błyskawiczną wymianę informacji o nowych schematach oszustw.

Technologia po stronie banków: banki muszą kontynuować inwestycje w zaawansowane systemy antyfraudowe oparte na sztucznej inteligencji, które potrafią w czasie rzeczywistym blokować podejrzane transakcje. Banki powinny wdrażać też systemy prewencyjne, takie jak wykrywanie spoofingu telefonicznego, biometrii czy dodatkowych kanałów potwierdzania transakcji.
Edukacja i świadomość: należy prowadzić ciągłe, szeroko zakrojone kampanie edukacyjne. Kluczowe jest tu hasło: „Pracownik banku NIGDY nie poprosi Cię o podanie hasła, kodu BLIK czy instalację oprogramowania"."

Skala i charakterystyka zjawiska nieautoryzowanych transakcji płatniczych

2.1. Nieautoryzowane transakcje – charakter i główne przyczyny zjawiska

Zjawisko nieautoryzowanych transakcji stanowi poważny problem i zarazem wyzwanie dla sektora usług finansowych.

Zgodnie z art. 40 ust. 1 ustawy o usługach płatniczych[17] transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą, przy czym zgoda może dotyczyć także kolejnych transakcji płatniczych.

> Art. 40.
>
> 1. Transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. Zgoda może dotyczyć także kolejnych transakcji płatniczych.
>
> 2. Zgoda powinna być udzielona przez płatnika przed wykonaniem transakcji płatniczej albo kolejnych transakcji płatniczych, chyba że płatnik i jego dostawca uzgodnili, że zgoda może zostać udzielona także po ich wykonaniu. Zgody na wykonanie transakcji płatniczej można również udzielić za pośrednictwem odbiorcy, dostawcy odbiorcy albo dostawcy świadczącego usługę inicjowania transakcji płatniczej.
>
> 3. Płatnik może w każdej chwili wycofać zgodę, nie później jednak niż do momentu, w którym zlecenie płatnicze zgodnie z art. 51 stało się nieodwołalne.
>
> 4. Jeżeli zgoda dotyczy kolejnych transakcji płatniczych, wycofanie dotyczy wszystkich niewykonanych transakcji płatniczych, chyba że płatnik zastrzegł inaczej.

A contrario, transakcją nieautoryzowaną jest taka transakcja, na którą płatnik nie wyraził zgody[18].

Podobny wniosek wypływa z art. 64 ust. 2 zd. trzecie Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE[19] („**PSD2**"), zgodnie z którym w przypadku braku zgody (płatnika) transakcję płatniczą uznaje się za nieautoryzowaną.

Typowym przykładem transakcji, którą można uznać za nieautoryzowaną, jest transakcja dokonana bez wiedzy płatnika, z wykorzystaniem jego danych autoryzujących pozyskanych przez przestępców w sposób nielegalny, np. poprzez zainfekowanie urządzenia płatnika.

W tym kontekście należy zwrócić uwagę na to, że nieautoryzowane transakcje stały się podstawą wszczęcia przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów („**UOKiK**") szeregu postępowań przeciwko bankom[20]. UOKiK zarzuca bankom m.in. brak zwrotu pieniędzy do końca kolejnego dnia roboczego po zgłoszeniu nieautoryzowanej transakcji[21], co oznacza, że bank nie miałby możliwości uprzedniej weryfikacji zasadności zgłoszenia. Z kolei przedstawiciele sektora bankowego argumentują, że banki nie mogą zwracać pieniędzy automatycznie, jedynie na podstawie zgłoszenia płatnika[22]. Co do zasady nie ma również podstaw do dochodzenia przez płatników roszczeń od banków w sytuacji, w której płatnik dokonał uwierzytelnienia transakcji i wyraził na nią zgodę.

Przyczyny zjawiska nieautoryzowanych transakcji

Przyczyny przeprowadzenia transakcji pomimo braku zgody płatnika mogą być różne, poczynając od wyłudzenia danych, po oszustwa polegające na wprowadzeniu klienta w błąd i skłonieniu go do dokonania transakcji, na którą w normalnych warunkach nie wyraziłby zgody. W tym drugim przypadku transakcja nie powinna jednak być kwalifikowana jako nieautoryzowana – płatnik wyraża przecież zgodę na jej dokonanie (czyli „autoryzuje" ją[23]), a bank co do zasady nie odpowiada za wprowadzenie go w błąd przez osobę trzecią lub podstęp osoby trzeciej (art. 84 § 1 i art. 86 § 2 Kodeksu cywilnego – „**KC**"). Zatem bank nie odpowiada za transakcję, która została autoryzowana, nawet jeżeli nastąpiło to pod wpływem błędu wywołanego przez osobę trzecią (np. oszusta

[17] Dz. U. z 2025 r., poz. 611 ze zm.

[18] K. Tomczyk, *Transakcje oszukańcze dokonywane przy użyciu bezgotówkowych instrumentów płatniczych jako przykłady cyberprzestępczości* [w:] *Przedsiębiorczość i konkurencyjność w dobie transformacji cyfrowej*, red. D. Dziembek, L. Ziora, Częstochowa 2023, s. 122.

[19] Dz. Urz. UE. L 2015 Nr 337, s. 35.

[20] *Nieautoryzowane transakcje – kolejne wszczęcia*, https://uokik.gov.pl/nieautoryzowane-transakcje-kolejne-wszczecia [dostęp: 21 listopada 2025 r.].

[21] *Ibidem*.

[22] *Kiedy bank musi oddać pieniądze po cyberataku? Rozstrzygnięcie sporu coraz bliżej*, Rzeczpospolita, https://www.rp.pl/banki/art43056981-kiedy-bank-musi-oddac-pieniadze-po-cyberataku-rozstrzygniecie-sporu-coraz-blizej [dostęp: 21 listopada 2025 r.].

[23] W języku polskim słowo „autoryzacja" rozumiane jest jako „zezwolenie" (tak: *Słownik Języka Polskiego PWN*, https://sjp.pwn.pl/slowniki/autoryzowa%C4%87.html, dostęp: 22 grudnia 2025 r.) lub „potwierdzenie" (tak: *Wielki Słownik Języka Polskiego PAN*, https://wsjp.pl/haslo/podglad/33278/autoryzowac/4156030/uzytkownika, dostęp: 22 grudnia 2025 r.).

namawiającego do przeznaczenia środków na rzekomo atrakcyjne inwestycje). Niemniej próby obciążania banków odpowiedzialnością za takie transakcje są przez płatników podejmowane.

Jak wskazał dyrektor departamentu przeciwdziałania fraudom jednego z banków:

„Są przykłady ataków/ wpływów manipulacyjnych na konsumentów pod przykrywką wysoko profitowych inwestycji, które są na najwyższe kwoty. Konsument dopiero po fakcie dochodzi do wniosku, że jednak go ktoś oszukał. Tymczasem my identyfikujemy jeszcze na etapie dokonywania transakcji część tego typu przypadków, kontaktujemy się z konsumentem w celach weryfikacyjnych, informujemy, o tym, że w naszej ocenie jest on oszukiwany. Najczęściej konsument pomimo ostrzeżeń zgadza się na wykonanie transakcji. Podsumowując mamy udowodnioną autoryzację transakcji, która została wykonana za zgodą konsumenta. W tego typu przypadkach nie mamy wpływu na decyzje konsumenta. Bank nie może decydować za niego, a jest wyłącznie pośrednikiem pomiędzy dwoma stronami transakcji".

Wyłudzenie danych może nastąpić na skutek m.in.:

– phishingu – „metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej"[24];

– smishingu – „rodzaj phishingu skierowanego na telefony komórkowe. Celem przestępcy jest zgromadzenie danych osobowych, takich jak na przykład numer ubezpieczenia społecznego lub numer karty kredytowej. Drogą ataku są wiadomości tekstowe lub SMS"[25];

– vishingu – „pozyskanie informacji poufnej przez przestępców z wykorzystaniem telefonu. Przestępca wyłudza dane podszywając się pod osoby lub instytucje godne zaufania"[26];

– spoofingu – „rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy. Dzięki wykorzystaniu różnych technik, oszuści mogą podszyć się pod wybrany adres e-mail, numer telefonu, a nawet adres IP i w nieuczciwy sposób osiągnąć swoje cele"[27].

Istotne znaczenie przy poszczególnych oszustwach ma inżynieria społeczna. Próbując wyłudzić dane lub skłonić ofiarę do wykonania określonego działania (np. zainicjowania transakcji) przestępcy wykorzystują ludzkie słabości. Manipulacja może polegać np. na:

– obietnicy uzyskania korzyści, głównie majątkowych, np. dzięki nadzwyczaj korzystnym inwestycjom oferowanym rzekomo przez oszusta;

– podszyciu się pod faktycznie funkcjonujący sklep internetowy;

– rzekomym oferowaniu produktów w bardzo atrakcyjnych cenach.

Jak wskazał pracownik działu compliance jednego z banków:

„Banki reagują m.in. na to, czego wymagają od nich regulatorzy i jesteśmy coraz bardziej zaawansowani pod względem technicznym, a to się przekłada na zmianę obszarów problemowych. Kiedyś większym problemem były kwestie związane z zabezpieczeniami technicznymi. Teraz istotniejsza jest kwestia poradzenia sobie z inżynierią społeczną, socjotechniką ze strony oszustów".

Jednocześnie w literaturze zwraca się uwagę, że: „manipulacja płatnikiem w celu zainicjowania oszukańczej transakcji oraz modyfikacja zlecenia płatniczego przez oszusta wydają się odgrywać bardzo ograniczoną rolę w przypadku płatności kartą, wypłat gotówki i oszustw związanych z pieniądzem elektronicznym. Natomiast w przypadku przelewów bankowych duża część oszukańczych transakcji wynikała z manipulacji płatnikiem w celu zainicjowania transakcji"[28].

Rosnące znaczenie mają manipulacje dokonywane z wykorzystaniem narzędzi sztucznej inteligencji, ze szczególnym uwzględnieniem *deepfake*[29]. Szacuje się, że w 2023 r. liczba incydentów wywołanych przez *deepfake* wzrosła o 700%.

[24] *Poradnik Rzecznika Finansowego w sprawie problematyki tzw. „kredytów na klik" i nieautoryzowanych transakcji płatniczych,* https://rf.gov.pl/wp-content/uploads/2023/12/ PORADNIK-KLIK.pdf [dostęp: 14 listopada 2025 r.], s. 8.
[25] *Ibidem*.
[26] *Ibidem*, s. 2.
[27] *Ibidem.*
[28] European Banking Authority & European Central Bank, *2024 Report on Payment Fraud*, https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf [dostęp: 16 listopada 2025 r.], s. 14.
[29] Wall Street Journal, *Deepfakes Are Coming for the Financial Sector*, 2024, https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5 [dostęp: 17 listopada 2025 r.].

Jak wskazał dyrektor ds. strategii płatności jednego z banków:

> „Już teraz widzę próby wykorzystania technologii deepfake (audio i wideo) do podszywania się pod inne osoby w celu wyłudzenia pieniędzy. Skala i wiarygodność tych ataków będzie rosła".

Poprzez *deepfake* należy rozumieć „wykorzystanie algorytmów uczenia maszynowego i technologii mapowania twarzy do cyfrowej manipulacji głosami, ciałami i twarzami ludzi"[30] Chodzi np. o przypadki, w których wykorzystując tego rodzaju narzędzia oszuści podszywają się pod osoby bliskie ofierze lub wręcz przeciwnie – pod znane postaci życia publicznego. Ta druga forma w Polsce była wykorzystywana w szczególności do tzw. oszustw inwestycyjnych[31]. Często są ono dokonywane poprzez wykorzystanie wizerunku celebrytów, sportowców czy polityków.

Zastosowanie *deepfake* zwiększa wiarygodność takiego wizerunku, szczególnie dla osób o niższym poziomie świadomości cyfrowej. Oglądając np. film wraz ze ścieżką dźwiękową, w której ciesząca się zaufaniem postać namawia do określonej inwestycji, nieświadoma oszustwa osoba nierzadko decyduje się powierzyć swoje środki z przeznaczeniem rzekomo na zakup np. kryptoaktywa czy instrumentu finansowego. W ten sposób dochodzi do przekazania środków wbrew rzeczywistej intencji płatnika.

Jak wskazał dyrektor ds. strategii płatności jednego z banków:

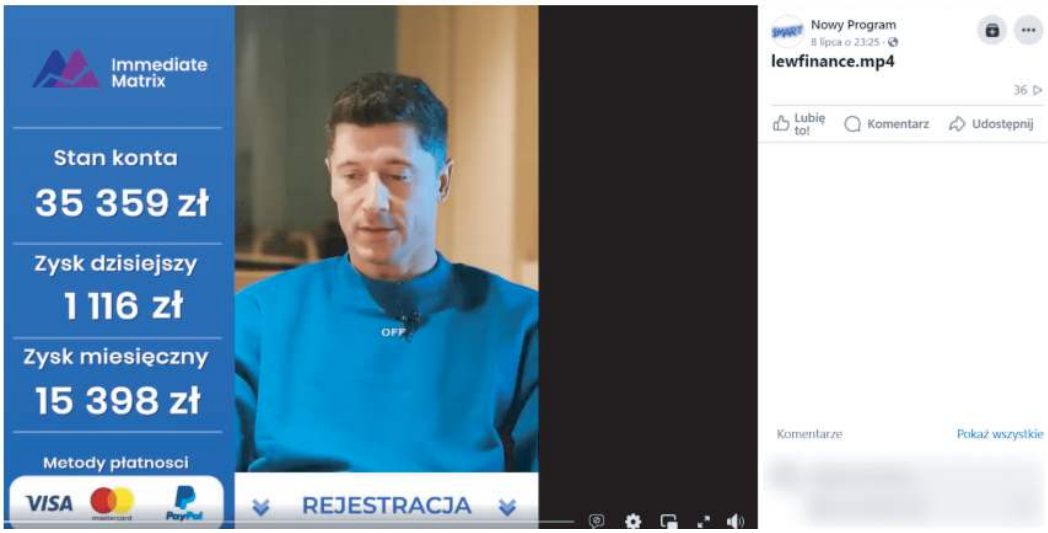
> „Wektor oszustw inwestycyjnych wykorzystuje systemy reklamowe platform społecznościowych do promowania fałszywych ofert inwestycyjnych. Reklamy, często opatrzone wizerunkiem znanych osób, obiecują nierealistycznie wysokie zyski. Po kliknięciu, ofiara jest kierowana na fałszywą platformę, gdzie jest nakłaniana do wpłacenia „depozytu". W rzeczywistości środki trafiają bezpośrednio do przestępców, a rzekome zyski pokazywane na fałszywym panelu mają jedynie zachęcić do dalszych wpłat".

Jednocześnie należy zauważyć, że na opisane oszustwa narażone są wszystkie grupy klientów. Jak wskazał dyrektor departamentu przeciwdziałania fraudom jednego z banków:

Ilustracja: Przykład reklamy wykorzystującej wizerunek znanego polityka bez jego zgody.

[30] O. Wasiuta, S. Wasiuta, *Deepfake jako skomplikowana i głęboko fałszywa rzeczywistość*, Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate 9(3) (2019), s. 19.
[31] Komisja Nadzoru Finansowego, Wykorzystanie technologii deepfake przez cyberprzestępców, https://cebrf.knf.gov.pl/falszywe-inwestycje [dostęp: 17 listopada 2025 r.].

Ilustracja: Klatka z reklamy wykorzystującej wizerunek znanych postaci życia publicznego bez ich zgody, z zastosowaniem technologii *deepfake* (w filmie zastosowano ścieżkę dźwiękową mającą imitować głos tych osób).



Ilustracja: Klatka z reklamy wykorzystującej wizerunek znanych postaci życia publicznego bez ich zgody, z zastosowaniem technologii *deepfake*.

„Z prowadzonych analiz w obszarze fraudowym wynika, że nie ma znacząco wyróżniającej się grupy społecznej, rozproszenie jest szerokie. Są osoby z małych miejscowości i z dużych. Są osoby starsze, ale są też młodsze. Są osoby z niższym wykształceniem, ale zdarzają się też przypadki osób, które są bardzo dobrze wykształcone. Tak więc nie dominuje tutaj jakaś określona grupa społeczna, aczkolwiek jeśli chodzi o sam wiek, to najwyższy jest udział osób od pięćdziesiątego piątego roku życia w górę".

Należy jednak zaznaczyć, że przypadki płatności dokonanych na skutek manipulacji nie wpisują się w pojęcie nieautoryzowanych transakcji, jeżeli wiążą się z wyrażeniem przez płatnika zgody na dokonanie transakcji. W takim przypadku są bowiem spełnione przesłanki transakcji autoryzowanej z art. 40 ust. 1 ustawy o usługach płatniczych w postaci wyrażenia zgody na transakcję.

Tego rodzaju przypadki mogą być szczególnie trudne z perspektywy banku, zwłaszcza że płatnicy próbują obciążać banki odpowiedzialnością za takie transakcje. Jak wskazał pracownik działu compliance jednego z banków:

„Na dzisiaj największym wyzwaniem jest kwestia socjotechniki. Obszar wyjątkowo trudny do „zagospodarowania".

Z kolei dyrektor departamentu przeciwdziałania fraudom jednego z banków wskazał:

„Zdarza się, że wiemy o zdarzeniu już na wcześniejszym etapie, zatrzymując takie transakcje do weryfikacji z klientem. To są klienci, którzy niestety dają się namawiać na pewne i obiecywane benefity. Są też klienci, którzy wykonują po prostu dużo różnych transakcji i nie przywiązują ze względu na rutynę wagi do tego, że klikają np. w oszukańcze linki".

Pokazuje to, że sektor bankowy jest obarczany obowiązkami i odpowiedzialnością także w przypadkach, w których weryfikacja przez banki jest poważnie utrudniona lub wręcz niemożliwa, a także takich, w których bank jest w stanie zweryfikować zagrożenie fraudem i to robi, a mimo to klient i tak decyduje się na dokonanie transakcji. Obarczanie w takim przypadku banku odpowiedzialnością za dokonanie transakcji jest niedopuszczalne. Należy zwrócić uwagę, że takie podejście stwarza ryzyko hazardu moralnego. Mając świadomość, iż koszty ewentualnego błędu poniesie ktoś inny (bank), płatnik nie będzie miał motywacji do podejmowania decyzji w sposób przemyślany, rozsądny i uważny.

2.2. Skala zjawiska oszukańczych transakcji płatniczych

Skala zjawiska oszukańczych transakcji (w tym nieautoryzowanych) stale rośnie. Jej ustalenie jest możliwe dzięki danym zbieranym i udostępnianym przez instytucje polskie i europejskie, w tym Narodowy Bank Polski, Rzecznika Finansowego oraz Europejski Bank Centralny.

Poniższe zestawienia obejmują dane liczbowe, wartości ekonomicznych strat, a także udział nieautoryzowanych transakcji w całkowitym wolumenie płatności.

Ponadto przedstawiono dominujące kanały wykorzystywane przez oszustów do realizacji oszukańczych operacji płatniczych. Analiza uwzględnia także dynamikę zmian tych wskaźników w ostatnich okresach.

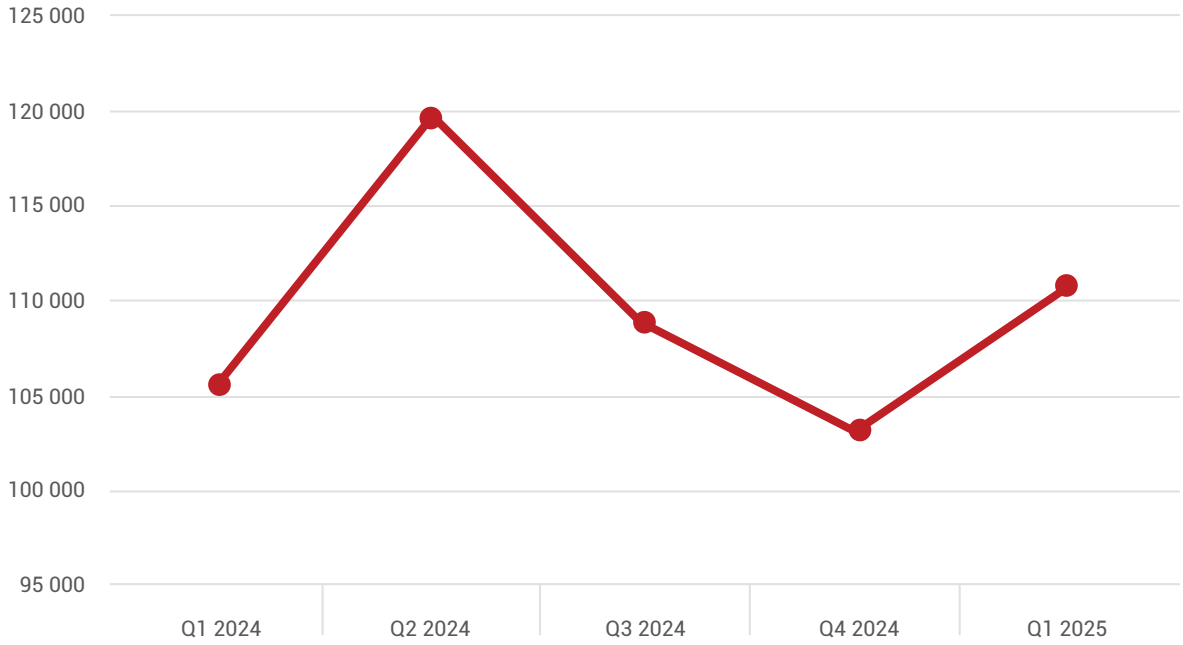
Powyższe wykresy ilustrują dynamikę zmian liczby oszukańczych transakcji w Polsce w ujęciu kwartalnym na przestrzeni 2024 r. oraz pierwszego kwartału 2025 r.

W pierwszym kwartale 2024 r. wystąpiło 105 601 transakcji o łącznej wartości 165 894 668 zł. W kolejnym kwartale liczba incydentów wzrosła do 119 500 transakcji, a wartość oszukańczych transakcji wyniosła 157 855 690 zł, co pokazuje spadek wartości oszustw pomimo wzrostu ich ilości.

W trzecim kwartale zaobserwowano spadek liczby oszukańczych transakcji do 108 982, natomiast ich wartość wzrosła o 7,8% osiągając wartość 170 176 532 zł. W czwartym okresie odnotowano dalsze spadki wolumenu transakcji do 103 178 oraz ich wartości do 160 207 696 zł. Z kolei pierwszy kwartał nowego roku przyniósł wzrost liczby transakcji oszukańczych o 7,4% do 110 797 oraz wzrost ich wartości do rekordowych 183 887 434 zł.

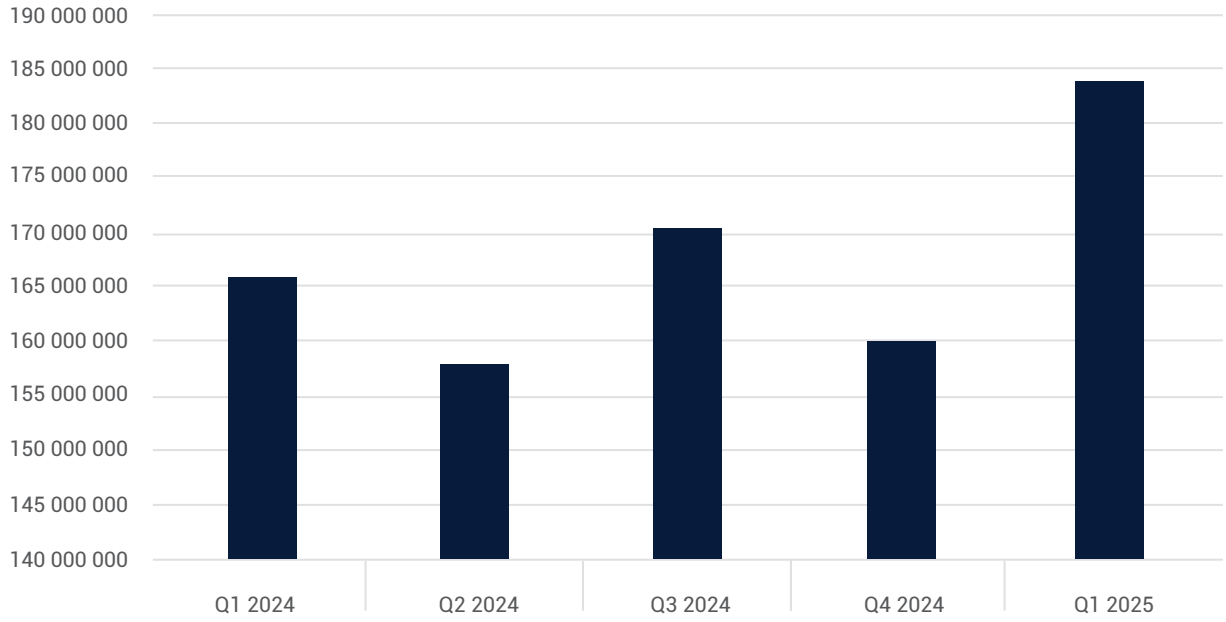
Natomiast porównując r/r, **liczba transakcji oszukańczych wzrosła o 4,9%, zaś ich wartość o 10,85%**. Zatem **pomimo, iż pomiędzy poszczególnymi kwartałami zdarzały się spadki liczby lub wartości oszukańczych transakcji, to zauważalny jest trend wzrostowy**.

LICZBA TRANSAKCJI OSZUKAŃCZYCH W PODZIALE NA KWARTAŁY



Wykres: Opracowanie własne, na podstawie danych zgromadzonych w ramach niniejszego Raportu oraz wykorzystanych w nim materiałów źródłowych.

WARTOŚĆ TRANSAKCJI OSZUKAŃCZYCH W PODZIALE NA KWARTAŁY



Wykres: Opracowanie własne, na podstawie danych zgromadzonych w ramach niniejszego Raportu oraz wykorzystanych w nim materiałów źródłowych.

Ukazuje to złożoność zjawiska oraz skalę zagrożeń związanych z fraudami płatniczymi, a także wskazuje na konieczność doskonalenia metod prewencji oszustw w polskim systemie płatniczym.

Również banki obserwują dużą liczbę oszukańczych (w tym nieautoryzowanych) transakcji. Jak wskazał dyrektor ds. strategii płatności jednego z banków:

> „Z mojej perspektywy, skala zjawiska transakcji nieautoryzowanych jest znacząca i, co najważniejsze, stale rośnie. (…) Każdego dnia w bankowości analizuje się tysiące alertów z systemów monitorujących. Choć większość to fałszywe alarmy, odsetek rzeczywistych prób oszustw jest na tyle duży, że wymaga dedykowanych, zaawansowanych zespołów i technologii. Straty finansowe, choć dotkliwe, to tylko część problemu. Równie istotne są straty wizerunkowe oraz spadek zaufania klientów. Zjawisko to ma charakter globalny, a polski rynek, jako jeden z liderów innowacji, jest szczególnie narażony na ataki wykorzystujące najnowsze technologie."

Z kolei pracownik działu compliance jednego z banków wskazał:

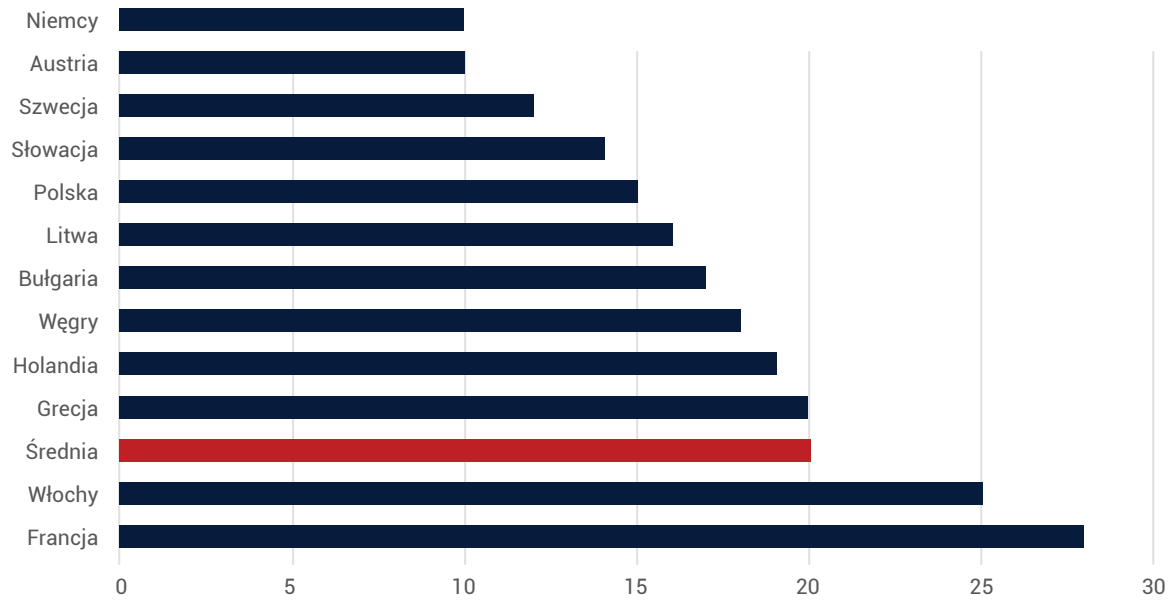
> „Skala jest poważna, bo jak rozmawiamy wewnętrznie, (…) jest to jedno z ważniejszych wyzwań dla banków i ważniejsze ryzyko."

Powyższa grafika przedstawia zestawienie średniej liczby fraudów dokonywanych na milion transakcji płatniczych w Polsce oraz wybranych krajach Unii Europejskiej, m.in.: Niemczech, Francji, Austrii, Włoszech i Irlandii w pierwszym kwartale 2025 r.

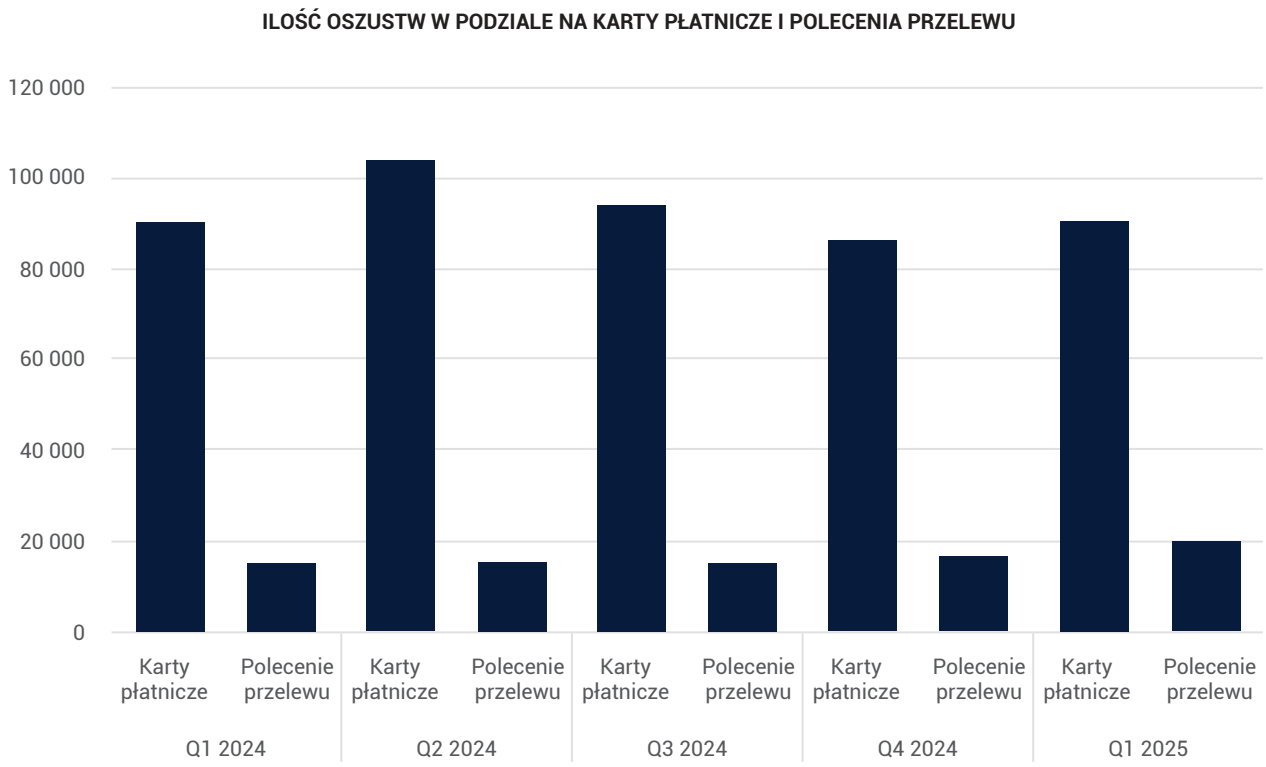
Polska odnotowała 15 przypadków fraudów na milion transakcji. Plasuje to nasz kraj poniżej średniej europejskiej, która wyniosła 20 incydentów. **Kraje o największej liczbie transakcji oszukańczych to między innymi Francja oraz Włochy, które osiągnęły odpowiednio 28 oraz 25 przypadków na milion transakcji.**

Niemcy i Austria wykazały najniższy poziom równy 10 przypadków. **Statystyka ukazuje relatywnie wysoki poziom bezpieczeństwa transakcji w Polsce na tle Europy, podkreślając skuteczność krajowych mechanizmów obronnych oraz rosnącą świadomość użytkowników**. Należy jednak zauważyć, że niektóre kraje europejskie osiągają jeszcze lepsze wyniki w zakresie ochrony przed fraudami płatniczymi, co wskazuje na możliwe różnice w efektywności systemów zabezpieczeń oraz poziomie świadomości użytkowników. Przykładem są **Niemcy i Austria, które odnotowały znacząco niższe wskaźniki fraudów, plasując się na czele w europejskim rankingu bezpieczeństwa transakcji**.

LICZBA FRAUDÓW NA MILION TRANSAKCJI: POLSKA VS INNE KRAJE UE



Wykres: Opracowanie własne, na podstawie danych zgromadzonych w ramach niniejszego Raportu oraz wykorzystanych w nim materiałów źródłowych.



Wykres: Opracowanie własne, na podstawie danych zgromadzonych w ramach niniejszego Raportu oraz wykorzystanych w nim materiałów źródłowych.

Powyższy wykres prezentuje kwartalną dynamikę zmian liczby transakcji oszukańczych w podziale na rodzaje instrumentów płatniczych: przelewy elektroniczne oraz płatności kartą.

W 2024 r. dominującym kanałem występowania fraudów były płatności kartą. Liczba oszukańczych transakcji z ich udziałem przekraczała 80 tysięcy w każdym kwartale. W tym okresie **oszustwa kartowe stanowiły około 84% wszystkich fraudów z wykorzystaniem bezgotówkowych instrumentów płatniczych**. Pokazuje to dominację tego kanału.

Na początku 2025 r. wzrosła liczba incydentów za pomocą polecenia przelewu, przekraczając 20 tysięcy przypadków, co oznacza wzrost aż o 20,1% w porównaniu do ostatniego kwartału 2024 r.

Rola mediów społecznościowych i Big Tech w ułatwianiu lub przeciwdziałaniu oszustom

3.1. Miejsce Big Tech we współczesnej gospodarce i społeczeństwie

Poprzez Big Tech rozumie się zwykle największe firmy technologiczne, które prowadzą duże platformy cyfrowe ułatwiające komunikację i dokonywanie transakcji pomiędzy znaczną liczbą użytkowników lub przeglądarki[32]. Wskazuje się, że ich wspólną cechą jest pełnienie roli pośredniczącej, łączącej użytkowników i dostawców[33].

Do Big Techów zalicza się przede wszystkim podmioty amerykańskie, takie jak Alphabet, Amazon, Apple, Meta i Microsoft[34]. Największe z nich mają większą kapitalizację niż jakakolwiek instytucja finansowa[35].

Kluczową wartością wpływającą na znaczenie Big Techów są dane, którymi dysponują. Ma to związek z liczbą użytkowników platform cyfrowych. Przykładowo Facebook ma ok. 3 mld aktywnych użytkowników miesięcznie, zaś z oprogramowania Windows korzysta 1,4 mld użytkowników[36].

Jest to istotny czynnik pozwalający na rozwijanie systemów sztucznej inteligencji, dla których big data stanowi kluczowy element. Jak wskazuje się w literaturze: „dane osobowe przekazywane przez klientów lub pozyskiwane z usług online oraz dane transakcyjne z platform handlowych i innych serwisów stanowią cenne zasoby wykorzystywane jako dane wejściowe dla algorytmów uczenia maszynowego lub innych rozwiązań opartych na analizie dużych zbiorów danych"[37].

Pozycja Big Techów wynika nie tylko z ich podstawowej działalności, ale także z rosnącego wachlarza świadczonych przez nie usług, które zwykle są komplementarne z platformami cyfrowymi czy przeglądarkami. Przykładowo większość czołowych Big Techów zajmuje się świadczeniem usług płatniczych (np. Google Pay, Apple Pay, Meta Pay), a niektóre weszły również na rynek kredytów.

Znaczenie Big Techów jest tak istotne, że – jak wskazuje się w literaturze – „mają coraz większe wpływy na gospodarkę i pośrednio również na państwową politykę wewnętrzną oraz międzynarodową"[38].

Jednocześnie rola platform cyfrowych wykracza poza obszar gospodarki czy nawet polityki. Przede wszystkim media społecznościowe stanowią kluczowe źródło informacji dla znacznej części społeczeństwa.

Jak wskazuje się w literaturze: „media społecznościowe, działające jako platformy informacyjne, dyskusyjne, rozrywkowe i komunikacyjne, są skutecznym narzędziem do wpływania na opinię publiczną, kształtowania wiedzy na określone tematy i manipulowania nastrojami społecznymi. Umiejętne prowadzenie kampanii informacyjnych i dyskusji oraz tworzenie treści dostosowanych do użytkowników (krótszych, prostszych, ze specyficznym językiem i naciskiem na grafiki i wideo) może efektywnie jednoczyć lub dzielić społeczeństwo wokół konkretnych kwestii, zachęcać do określonych działań. Zatem wzrastająca rola mediów społecznościowych oraz przeniesienie znacznej części komunikacji międzyludzkiej do Internetu wymaga refleksji nad tym, jaki jest ich wpływ na kształtowanie opinii publicznej i nastrojów społecznych, a tym samym na zmianę zachowań i postaw"[39].

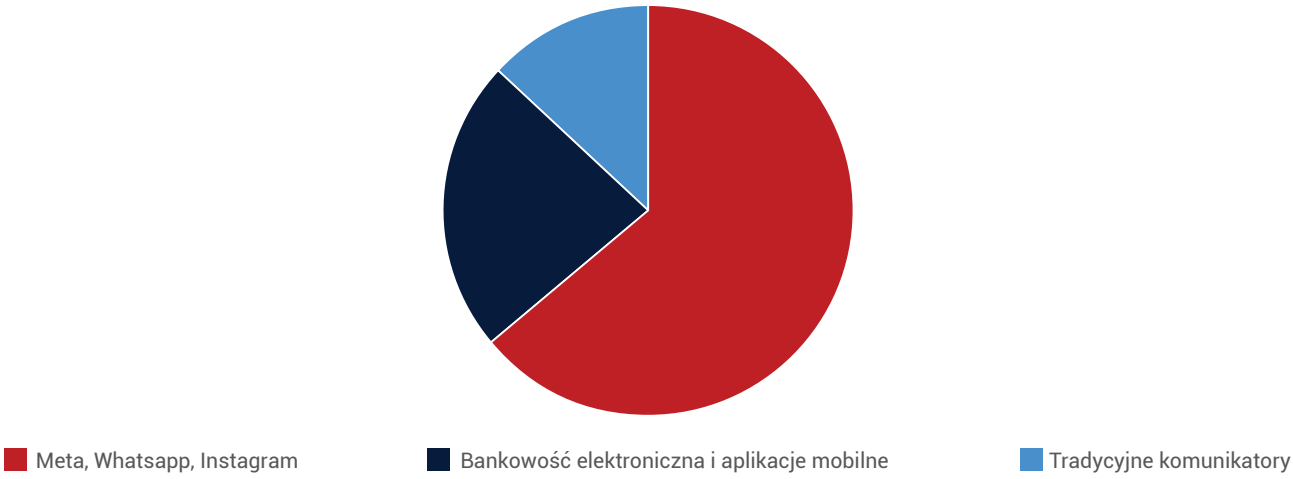
Wskazuje to na możliwość manipulacji zachowaniami odbiorców, przy czym manipulacja niekoniecznie musi być dokonywana bezpośrednio przez operatora platformy. Wystarczy, gdy akceptuje on umieszczanie na platformie treści o takim charakterze.

3.2. Media społecznościowe i Big Tech a oszustwa z wykorzystaniem transakcji płatniczych

Wskazana możliwość manipulacji zachowaniem odbiorców za pośrednictwem mediów społecznościowych stwarza zagrożenie dotyczące oszustw finansowych. Pewna część odbiorców przejawia zaufanie do informacji dotyczących kwestii finansowych, zwłaszcza inwestycyjnych, które pojawiają się w mediach społecznościowych. Szczególnie jaskrawym przykładem tego zjawiska są reklamy z udziałem influencerów, nierzadko w formie

[32] P. Armstrong, S. Balitzky, A. Harris, *BigTech – implications for the financial sector*, ESMA Report on Trends, „Risks and Vulnerabilities", 1/2020, s. 48.
[33] S. Khanal, H. Zhang, A. Taeihagh, *Why and how is the power of Big Tech increasing in the policy process? The case of generative AI*, Policy and Society, 2025, 44(1), s. 53.
[34] V. Brühl, *Big Tech, the Platform Economy and the European Digital Markets*, „Intereconomics", 58(5)/2023, s. 274.
[35] P. Armstrong, S. Balitzky, A. Harris, *BigTech – implications for the financial sector*, „ESMA Report on Trends. Risks and Vulnerabilities", 1/2020, s. 48-49.
[36] S. Khanal, H. Zhang, A. Taeihagh, *Why and how is the power of Big Tech increasing in the policy process? The case of generative AI*, „Policy and Society", 44(1)/2025, s. 5
[37] *Ibidem*., s. 53.
[38] M. Gurtowski, J. Waszewski, *Wpływ działalności gigantów technologicznych na globalne środowisko bezpieczeństwa. Studium przypadku spółki Amazon*, „Kwartalnik Bellona", 3/2020, s. 42.
[39] M. Hańczuk, G. Rybołowicz, J. Szwed, J. Wilczyńska, A. M. Olszewska, *Wpływ mediów społecznościowych na relacje międzyludzkie*, „Akademia Zarządzania", 8(2)/2024, s. 297.

GŁÓWNE KANAŁY INICJOWANIA FRAUDÓW



Wykres: Opracowanie własne, na podstawie danych zgromadzonych w ramach niniejszego Raportu oraz wykorzystanych w nim materiałów źródłowych.

kryptoreklamy[40]. Są oni angażowani nie tylko w celu promocji danej inwestycji, ale też jej uwiarygodnienia. Naturalnym miejscem tego rodzaju działań reklamowych są media społecznościowe. Znane są przypadki, w których osoby publiczne promowały oszukańcze schematy[41].

Platformy społecznościowe stały się głównym kanałem inicjowania oszustw. Nie znaczy to, że oszukańcze reklamy nie pojawiają się w innych mediach internetowych. Jednak opisana wyżej skala działania Big Techów i bardzo duża liczba użytkowników platform społecznościowych (łącznie ok. 4,41 mld[42]) sprawia, że są one najważniejszym miejscem publikacji tego rodzaju reklam.

Zaprezentowane tezy znajdują potwierdzenie w danych statystycznych zaprezentowanych poniżej.

Powyższy wykres prezentuje rozkład udziału najczęściej wykorzystywanych kanałów inicjowania oszustw płatniczych w Europie w 2024 r.

Największy udział miały serwisy i platformy społecznościowe: Meta, WhatsApp, Instagram, które odpowiadały za 62% wszystkich przypadków. Na drugim miejscu znalazła się bankowość elektroniczna i aplikacje mobilne – 25%. Pozostałe 13% przypadków transakcji oszukańczych odbyło się z wykorzystaniem innych kanałów, w tym tradycyjnych komunikatorów lub telefonu. Warto zauważyć również rosnącą rolę Telegrama, który odnotował wzrost o 121% oraz WhatsAppa (wzrost o 67%).

Dane wskazują na rosnącą rolę kanałów komunikacji internetowej, ze szczególnym uwzględnieniem platform społecznościowych i komunikatorów. Ich udział w całkowitej liczbie oszukańczych transakcji przekracza łączny udział bardziej tradycyjnych kanałów komunikacji.

Jak wskazał dyrektor ds. strategii płatności jednego z banków:

> „Moim zdaniem rola platform społecznościowych i globalnych firm technologicznych (Big Tech) w eskalacji tego zjawiska jest ogromna. Stały się one kluczowym narzędziem w rękach przestępców z kilku powodów: platformy takie jak Facebook, Instagram czy TikTok pozwalają oszustom dotrzeć do milionów potencjalnych ofiar przy minimalnym koszcie, a przestępcy mogą stosunkowo łatwo tworzyć fałszywe profile, podszywając się pod znane marki, co utrudnia ich identyfikację. Zautomatyzowane systemy reklamowe są masowo wykorzystywane do promowania oszustw. Algorytmy precyzyjnie targetują reklamy do grup najbardziej podatnych na manipulację, a weryfikacja reklamodawców jest często niewystarczająca. Ponadto platformy często zasłaniają się statusem pośrednika, argumentując, że nie ponoszą

[40] N. Jelonek, *Kryptoreklamy w mediach społecznościowych*, „Prawo Mediów Elektronicznych", 2/2023, s. 28.
[41] T. Ciechoński, *Finfluencerzy i naganiacze z Dubaju*, https://www.prawo.pl/biznes/finfluencerzy-z-dubaju-jak-rozpoznac-oszustwa-inwestycyjne,535334.html [dostęp: 22 listopada 2025 r.].
[42] S. Bharne, P. Bhaladhare, *Comprehensive Analysis of Online Social Network Frauds* [w:] *Advances in Data-Driven Computing and Intelligent Systems*, s. 24.

odpowiedzialności za treści publikowane przez użytkowników. Procesy usuwania szkodliwych treści są często powolne i nieefektywne. W efekcie, media społecznościowe stały się głównym kanałem dystrybucji fraudów, a Big Tech, świadomie lub nie, czerpie zyski z reklam finansujących działalność przestępczą".

Z kolei pracownik działu compliance jednego z banków wskazał:

„W obszarze socjotechniki, inżynierii społecznej, obserwujemy dość sporo transakcji na większe kwoty. Dotyczą one na przykład „inwestycji". Klienci skądś dowiadują się, że jest możliwość zainwestowania w takim przestępczym rozumieniu, gdzieś znajdują tę informację i potwierdzenie, że to jest coś, w co warto się zaangażować. Są to media takie czy inne, czy social media. Jest to źródło informacji. Wykorzystywane są te platformy, które są nam bliskie, łatwe w obsłudze. Na przykład kontakt na popularnym komunikatorze".

Zwraca się uwagę, że podmioty zarządzające platformami społecznościowymi nie podejmują dostatecznych działań w celu eliminacji lub istotnego zmniejszenia skali opisanych zjawisk. Wskazuje się w szczególności na brak jasnych procedur zgłaszania podejrzanych reklam czy publikacji do operatorów platform społecznościowych oraz brak transparentności w zakresie rozpatrywania takich zgłoszeń.

Dyrektor departamentu przeciwdziałania fraudom jednego z banków wskazał:

„Rola platform społecznościowych i firm technologicznych dla działań przestępczych w kontekście nieautoryzowanych transakcji jest bardzo duża. Po stronie właściwych instytucji państwa lub urzędów powinny być podjęte radykalne kroki, żeby tego typu reklamy, ogłoszenia, informacje były weryfikowane na poziomie big techów, to jest bardzo istotny element w ochronie konsumentów. Liczba fałszywych ofert, reklam lub ogłoszeń powinna być minimalizowana systemowo. Na niektórych platformach trudno znaleźć informacje pozwalające na zgłoszenie niepokojącego ogłoszenia lub reklamy w celu jest usunięcia. Organizacje typu big tech czy platformy technologiczne powinny realizować bardziej aktywne kroki jeszcze przed umieszczeniem takich reklam, czyli po prostu je weryfikować pod kątem oszukańczych ofert".

Jednocześnie w przestrzeni publicznej pojawiły się informacje, które wskazują na to, że jeden z Big Techów, Meta, świadomie czerpie zyski z oszukańczych reklam zamieszczanych na platformach społecznościowych tego podmiotu.

Informacje opublikowane przez agencję Reuters w oparciu o pozyskane przez dziennikarzy dokumenty, wskazują na niepokojące mechanizmy:

„Jak odnotowano w jednym z dokumentów z grudnia 2024 r., firma średnio wyświetla użytkownikom swoich platform szacunkowo 15 miliardów reklam oszustw dziennie – takich, które wykazują wyraźne oznaki fałszywości (»wyższego ryzyka«). Z kolei inny dokument z końca 2024 r. stwierdza, że Meta uzyskuje około 7 miliardów dolarów rocznych przychodów z tej kategorii reklam oszustw"[43].

„Znaczna część oszustw pochodziła od marketerów, którzy zachowywali się na tyle podejrzanie, że zostali oznaczeni przez wewnętrzne systemy ostrzegawcze Meta. Jednak z dokumentów wynika, że firma blokuje reklamodawców tylko wtedy, gdy jej zautomatyzowane systemy przewidują z co najmniej 95% pewnością, że dopuszczają się oszustwa. Jeśli pewność jest mniejsza – ale Meta nadal uważa, że reklamodawca prawdopodobnie jest oszustem – nalicza wyższe stawki za reklamy jako karę. Celem jest zniechęcenie podejrzanych reklamodawców do publikowania reklam"[44].

„Jednocześnie dokumenty wskazują, że z własnych badań Meta wynika, iż jej produkty stały się filarem globalnej gospodarki (*economy* – przyp. autorzy raportu) oszustw. W prezentacji przygotowanej w maju 2025 r. przez zespół ds. bezpieczeństwa oszacowano, że platformy firmy były zaangażowane w jedną trzecią wszystkich udanych oszustw w USA"[45].

„W wewnętrznych dokumentach Meta rozważa koszty wzmocnienia egzekwowania zasad dotyczących reklam oszustw w zestawieniu z ryzykiem kar finansowych nakładanych przez rządy

[43] *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, Reuters, https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/ [dostęp: 21 listopada 2025 r.].
[44] *Ibidem.*
[45] *Ibidem.*

za brak ochrony użytkowników. Dokumenty jasno wskazują, że Meta zamierza w przyszłości ograniczyć nielegalne źródła przychodów. Jednak firma obawia się, że nagłe zmniejszenie wpływów z reklam oszustw mogłoby wpłynąć na jej prognozy biznesowe, jak wynika z dokumentu z 2025 r., który omawia wpływ „naruszających przychody" – czyli dochodów z reklam naruszających standardy Meta, takich jak oszustwa, nielegalne gry hazardowe, usługi seksualne czy wątpliwe produkty zdrowotne"[46].

„Tymczasem jak wynika z jednego z dokumentów z listopada 2024 r., firma wewnętrznie przyznaje, że kary administracyjne za reklamy oszustw są nieuniknione i przewiduje sankcje sięgające nawet 1 miliarda dolarów. Jednak te kary byłyby znacznie mniejsze niż przychody Meta z reklam oszustw. Co sześć miesięcy Meta zarabia 3,5 miliarda dolarów tylko na tej części reklam oszustw, które »niosą wyższe ryzyko prawne« – takich jak reklamy fałszywie podające się za markę konsumencką lub osobę publiczną albo wykazujące inne oznaki oszustwa. Ta kwota niemal na pewno przewyższa »koszt jakiejkolwiek ugody regulacyjnej dotyczącej oszukańczych reklam«. Ten sam dokument stwierdza, że zamiast dobrowolnie zgodzić się na bardziej rygorystyczną weryfikację reklamodawców, kierownictwo firmy zdecydowało się działać wyłącznie w odpowiedzi na działania regulatorów"[47].

Powyższe wskazuje na występowanie zjawiska tzw. *moral hazard* po stronie przynajmniej niektórych Big Techów. Wobec stosunkowo niskiego zagrożenia sankcjami za dopuszczanie do publikowania oszukańczych reklam, czerpiąc jednocześnie bardzo wysokie przychody z tego tytułu, giganci technologiczni nie mają motywacji do walki z tym zjawiskiem. Kalkulacja ekonomiczna sugeruje wręcz, by zjawisko to utrzymywać i w ten sposób zapewniać ważne źródło przychodów Big Techów. Opisana sytuacja świadczy o głębokim niedostosowaniu regulacji prawnych i ich praktycznego stosowania przez organy publiczne do rzeczywistych wyzwań w obszarze oszustw finansowych. Jednocześnie, jak wynika z przeprowadzonych analiz, faktyczny koszt fraudów jest przenoszony na banki.

Poniżej zaprezentowane zostały szacowane przychody uzyskiwane przez niektóre Big Techy z oszukańczych reklam.

Meta
Zgodnie z informacjami podanymi w raporcie Reuters, Meta z takich reklam osiągnęła przychody na poziomie 7 mld USD (ok. 25,5 mld PLN). Przyjmując globalną liczbę użytkowników platform Meta na poziomie ok. 3 mld i odpowiednio 18,7 mln w Polsce, można szacować roczny przychód Meta z oszukańczych reklam w Polsce na poziomie ok. 43,6 mln USD (ok. 159 mln PLN).

Google
Przychody Google z reklam w 2024 roku wyniosły 264,59 mld USD. Firma posiada około 5 mld użytkowników, z czego ok. 30 mln w Polsce. Gdyby przyjąć, że podobnie jak w przypadku Meta ok. 4,3% przychodów reklamowych Google pochodzi z reklam oszukańczych, to szacowana kwota przychodów z tego tytułu w Polsce wyniosłaby ok. 249 mln PLN.

Amazon
Amazon wygenerował 56,21 mld USD przychodów z reklam w 2024 roku przy 310 milionach użytkowników (ok. 22,5 mln w Polsce). Gdyby przyjąć, że podobnie jak w przypadku Meta ok. 4,3% przychodów reklamowych Amazon pochodzi z reklam oszukańczych oraz dotyczących niedozwolonych dóbr, to szacowana kwota przychodów z tego tytułu w Polsce wyniosłaby ok. 640 mln PLN.

Podsumowując, **łącznie Big Techy generują dziesiątki miliardów dolarów rocznie z oszukańczych reklam. W Polsce skala może wynosić ponad miliard złotych. Kwota ta jest wyższa niż wartość oszukańczych transakcji, co można uzasadnić faktem, iż niektóre fraudy nie są zgłaszane przez płatników i w konsekwencji nie są uwzględniane w dostępnych raportach statystycznych, szczególnie w zakresie transakcji autoryzowanych, lecz dokonanych na skutek manipulacji czy socjotechniki**.

Z powyższego wynika, że istniejące rozwiązania regulacyjne są niewystarczające dla przeciwdziałania wykorzystywaniu mediów społecznościowych i innych platform prowadzonych przez Big Techy do oszustw finansowych.

Dyrektor departamentu przeciwdziałania fraudom jednego z banków wskazał:

„Kwestie regulacyjne mogłyby być znacznie bardziej doprecyzowane, aby były widoczne rezultaty, większa efektywność, w tym w zakresie kontroli platform technologicznych. Wszystko wskazuje na to, że od strony regulacyjnej jest sporo do zrobienia w zakresie zwiększenia bezpieczeństwa i ochrony konsumentów".

[46] *Ibidem.*
[47] *Ibidem.*

Z kolei dyrektor ds. strategii płatności jednego z banków wyraził następujące zdanie:

> „Sądzę, że należy wprowadzić regulacje, które nakładałyby na platformy współodpowiedzialność za straty finansowe wynikające z oszustw promowanych za pomocą ich systemów. Powinny one być zobligowane do wdrożenia solidnych procedur weryfikacji reklamodawców. (…) Konieczne jest wprowadzenie przepisów, które jasno definiowałyby odpowiedzialność platform internetowych za umożliwianie oszustw. Konieczne jest sformułowanie jasnego i przejrzystego prawa dotyczącego obsługi transakcji nieautoryzowanych bez zbędnych procedur sądowych".

Niezależnie od rozwiązań prawnych, istotne są także działania edukacyjne. Jakkolwiek zagrożone manipulacjami czy innymi formami oszukańczej działalności są wszystkie grupy społeczne, to jednak niewątpliwie poziom edukacji ekonomicznej oraz wrażliwości na możliwe oszustwa przekłada się na ryzyko stania się ofiarą fraudu.

Dyrektor departamentu przeciwdziałania fraudom jednego z banków wskazał:

> „Banki zrobiły już bardzo dużo w kontekście różnych mechanizmów weryfikacyjnych, różnych potykaczy, na których zatrzymujemy klienta, tak żeby go uświadomić albo dodatkowo weryfikować przed wykonaniem potencjalnie fraudowej transakcji. Realizowane są też liczne kampanie edukacyjne. Wydaje mi się, że oprócz większego wpływu właściwych instytucji państwa lub odpowiednich urzędów na platformy technologiczne, UOKiK jest właściwym aktorem, który mógłby skoordynować cykliczną i ogólnopolską kampanię społeczną, radiowo-telewizyjną, która dotarłaby do znacznie szerszej grupy odbiorców. Najczęściej konsumenci zaglądają na stronę internetową banku, do aplikacji mobilnej lub też bankowości internetowej, aby dotrzeć do odpowiednich komunikatów i ostrzeżeń. Nie każdy czyta uważnie komunikaty ostrożnościowe lub autoryzacyjne push ze szczegółami transakcji. Podsumowując wydaje mi się, że taka inicjatywa ze strony UOKiK byłaby bardzo dobrym uzupełnieniem, tak żeby cyklicznie docierać do jak największej części społeczeństwa".

Z kolei dyrektor ds. strategii płatności jednego z banków wskazał:

> „Należy prowadzić ciągłe, szeroko zakrojone kampanie edukacyjne. Kluczowe jest tu hasło: »Pracownik banku nigdy nie poprosi cię o podanie hasła, kodu BLIK czy instalację oprogramowania«".

Jednocześnie istotne znaczenie ma współpraca pomiędzy interesariuszami. W szczególności warunkiem zmniejszenia skali nadużyć, w tym związanych z manipulacjami, jest zaangażowanie Big Techów.

Dyrektor ds. strategii płatności jednego z banków wskazał:

> „Konieczne jest stworzenie ram współpracy między sektorem bankowym, firmami Big Tech a organami ścigania. Umożliwiłoby to błyskawiczną wymianę informacji o nowych schematach oszustw".

Podsumowując tę część analizy, należy podkreślić, że **w świetle dostępnych danych i obserwacji uczestników rynku, platformy społecznościowe i inne prowadzone przez Big Techy są na dużą skalę wykorzystywane przez oszustów do prowadzenia działań manipulacyjnych, których rezultatem są oszustwa na szkodę użytkowników. Zjawisko to nasila się i obecnie stanowi główną przyczynę fraudów. Jednocześnie Big Techy w sposób dalece niewystarczający przeciwdziałają oszukańczym praktykom**.

Wynika to z kilku przyczyn, w tym przede wszystkim:

- **niedostatecznych regulacji;**
- **wysokich przychodów uzyskiwanych przez Big Techy z oszukańczych reklam;**
- **relatywnie niskich sankcji (z perspektywy Big Techów bardziej opłacalne jest dopuszczać oszukańcze reklamy i płacić kary niż walczyć z fraudami)**.

Jednocześnie oprócz niezbędnych zmian legislacyjnych, w celu przeciwdziałania zjawisku nieautoryzowanych transakcji **należy prowadzić stałe działania edukacyjne. Konieczne jest przy tym zaangażowanie instytucji publicznych, tak aby akcje edukacyjne miały większą skalę oraz wzbudzały większe zaufanie**.

Wreszcie, koniecznym elementem jest współdziałanie wszystkich interesariuszy: banków, organów publicznych (zwłaszcza UOKiK), Big Techów i innych.

Odpowiedzialność prawna podmiotów Big Tech za szkody wynikające z fałszywych reklam i nieautoryzowanych transakcji

4.1. Odpowiedzialność Big Tech w świetle Aktu o Usługach Cyfrowych (DSA – Digital Services Act)

Celem tego rozdziału jest analiza zasady ograniczenia odpowiedzialności prawnej podmiotów Big Tech za treści publikowane przez użytkowników na ich platformach, ze szczególnym uwzględnieniem jej zastosowania w kontekście fałszywych reklam prowadzących do nieautoryzowanych transakcji. W tym celu rozdział ten omawia główne założenia i przepisy rozporządzenia Aktu o Usługach Cyfrowych („**DSA**"), które mają zastosowanie do Big Techów jako dostawców usług pośrednich, a także bardzo dużych platform (tzw. VLOPs) oraz wyszukiwarek internetowych (tzw. VLOSEs). Rozdział skupia się na DSA jako głównej regulacji w europejskim, jak i polskim porządku prawnym, która ustanawia zasady zarządzania kwestią odpowiedzialności za treści, w tym analogicznie, za szkody z nimi związane.

W pierwszej części raportu zarysowana została ogólna problematyka regulacji odpowiedzialności za treści w Internecie, a także analizie poddano jej znaczenie dla rozwoju samego Internetu i wolności słowa w sieci, zwłaszcza w kontekście podmiotów Big Tech[48]. Podmioty te odpowiedzialne są za większość ruchu w Internecie, a więc i za dużą część pośredniczenia w zamieszczaniu i konsumpcji treści. Następnie omówiona zostaje ogólna struktura DSA, z koncentracją na celach i przedmiocie tej regulacji, a także głównych podmiotach w niej regulowanych. Kolejna część skupia się na sposobie implementacji zasady ograniczenia odpowiedzialności za treści w DSA i jakie ma ona zastosowanie w zakresie podmiotów Big Tech. DSA wyodrębnia szczególną kategorię podmiotów – bardzo duże platformy i wyszukiwarki internetowe – obejmując tym reżimem znaczną część Big Techów, które podlegają odrębnym, znacznie bardziej rygorystycznym obowiązkom regulacyjnym. W tym kontekście rozdział również omawia podejście oparte na ryzyku, na którym DSA jest strukturalnie oparte i które determinuje poprawną interpretacje tej regulacji.

W konsekwencji, rozdział ten stanowi fundament do analizy w dalszych częściach raportu kwestii roszczeń przysługujących użytkownikom bądź konsumentom za niestosowanie się podmiotów objętych regulacjami DSA do zasad należytej staranności i samego DSA. Niestosowanie się do powyższych przepisów może być podstawą do roszczeń związanych ze szkodami spowodowanymi np. fałszywymi reklamami, które prowadzą do nieautoryzowanych transakcji, ponieważ reklamy są treściami na podstawie DSA. Tym samym analiza DSA i wynikających z niej obowiązków jest pierwszym etapem do ustalenia skali odpowiedzialności podmiotów Big Tech za szkody wyrządzone w wyniku wyświetlania fałszywych reklam.

4.2. Odpowiedzialność podmiotów pośredniczących za treści w Internecie – ogólny zarys problematyki

Kwestia odpowiedzialności ponoszonej przez pośredników za treści w Internecie stanowi centralną materię regulacyjną, ponieważ sposób, w jaki egzekwowana jest odpowiedzialność za pośredniczenie, bezpośrednio determinuje zakres wolności do zamieszczania treści, a co za tym idzie – tempo i skalę rozwoju Internetu. Niemniej jednak, należy podkreślić, iż omawiana wolność w dostarczaniu treści w sieci niezaprzeczalnie przysługuje wszystkim ludziom.

Rozwój Internetu jest pochodną ilości użytkowników, jak i intensywności ich interakcji przez Internet. Takie uczestnictwo w sieci w dużej mierze odbywa się poprzez zamieszczanie materiałów takich jak komentarze, fotografie, artykuły, wideo, muzyka, lecz także reklamy lub poprzez konsumpcję tychże treści. Jeżeli zamieszczanie i konsumpcja różnego rodzaju treści jest centralną aktywnością w Internecie, to kwestia regulacji tej aktywności ma wymiar konstytucyjny dla Internetu, jeżeli przez konstytucyjność rozumiemy najbardziej fundamentalne zasady, na których dana instytucja społeczna (którą Internet w pewnym sensie jest) opiera się.

Kwestia odpowiedzialności za treści w Internecie ma fundamentalne znaczenie dla kształtowania granic wolności słowa, gwarantowanej w art. 54 Konstytucji RP i art. 11 Karty Praw Podstawowych UE.

> Art. 54.
>
> 1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji.
>
> 2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej.

[48] Termin ten pojawia się w: D. Tambini, M. Moore (red.), *Regulating Big Tech: Policy Responses to Digital Dominance*, Oxford University Press, Nowy Jork 2021.

Artykuł 11

Wolność wypowiedzi i informacji

1. Każdy ma prawo do wolności wypowiedzi. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe.

2. Szanuje się wolność i pluralizm mediów.

To sposób uregulowania tej odpowiedzialności decyduje w praktyce o tym, jakie treści mogą funkcjonować w przestrzeni cyfrowej, a które są usuwane lub blokowane. Wzrost swobody w publikowaniu i odbiorze treści w sieci przyczynia się do dynamicznego rozwoju Internetu. Jednocześnie zwiększona możliwość zamieszczania treści stanowi istotny mechanizm realizacji prawa do wolności słowa w środowisku cyfrowym, umożliwiając użytkownikom zarówno wyrażanie własnych opinii, jak i dostęp do informacji.

Dziś naturalnym wydaje się założenie, że wszystkim przysługuje praktyczna swoboda do zamieszczania treści i ich konsumpcji. Opiera się ona na czymś, co w prawie cyfrowym nazywa się zasadą ograniczenia odpowiedzialności pośredników za treści zamieszczane na ich szeroko pojętej infrastrukturze (serwery, platformy internetowe, sieci społecznościowe, fora *etc.*)[49]. Zasada ograniczonej odpowiedzialności za treści zakłada, że pośrednicy internetowi – czyli podmioty zapewniające dostęp do sieci oraz infrastrukturę umożliwiającą interakcje między użytkownikami – nie zawsze będą ponosiły odpowiedzialność za treści zamieszczane na ich platformach. Warunkiem jest dochowanie należytej staranności w moderowaniu treści nielegalnych oraz przestrzeganiu obowiązującego prawa w szerszym zakresie. Szczegółowe regulacje i wyjątki od tej zasady różnią się w zależności od jurysdykcji. Zakres pojęcia należytej staranności oraz konkretne obowiązki, które z niego wynikają, pozostają przedmiotem znaczących rozbieżności w implementacji zasady ograniczonej odpowiedzialności za treści w Internecie w tzw. świecie zachodnim.

Różnice te wynikają z funkcjonowania dwóch odmiennych tradycji prawnych. W systemach kontynentalnych, opartych na ustawach (czyli tzw. prawa stanowionego, pozytywnego, *continental law*, np. w Polsce, Francji, Niemczech), obowiązki pośredników internetowych są zazwyczaj określone wprost w przepisach prawa. W systemach anglosaskich, opartych w większym stopniu na precedensach sądowych (*common law*, np. w Wielkiej Brytanii i Stanach Zjednoczonych), wymagania dotyczące należytej staranności kształtowane są głównie przez orzecznictwo, co prowadzi do bardziej elastycznego, lecz mniej rzeczowego stosowania tej zasady.

Mimo że dziś zasada ograniczonej odpowiedzialności pośredników internetowych wydaje się oczywista, co wynika z naszego codziennego doświadczenia użytkowników Internetu – w końcu możemy publikować w sieci w zasadzie dowolne treści – w latach 90., gdy kształtowała się podstawowa struktura regulacyjna, nie była jeszcze rozwiązaniem powszechnie przyjętym. Do dzisiaj w literaturze prawa cyfrowego toczy się debata dotycząca zarówno należytego zakresu wyłączenia odpowiedzialności pośredników, jak i granic wolności słowa w Internecie[50]. Można przypuszczać, że gdyby wówczas nie podjęto decyzji o wyłączeniu odpowiedzialności pośredników, współczesny Internet wyglądałby zupełnie odmiennie, choć trudno jednoznacznie przewidzieć, w jakim dokładnie kształcie, a jeszcze trudniej określić, czy lepszym czy gorszym.

Pomimo ogólnego ograniczenia odpowiedzialności pośredników w prawie cyfrowym, obowiązującego w Stanach Zjednoczonych, Wielkiej Brytanii oraz w Unii Europejskiej, debata dotycząca szczegółowego zakresu stosowania tej zasady, jak również granic wolności słowa w sieci, ewoluuje równolegle z rozwojem samego Internetu. Znaczenie tej tematyki zmienia się wraz ze zmianami struktury samego Internetu i tego, jacy pośrednicy są typowymi w danym czasie i miejscu, a także w jaki sposób pośredniczą w dostarczaniu treści (tzn. jakie typy pośredników dominują w zapewnianiu infrastruktury dostępu i interakcji w sieci).

Od końca pierwszej dekady XXI wieku zarówno Internet, jak i charakter dominujących podmiotów pośredniczących w treściach, uległy istotnym przemianom. Pod koniec lat 90. rozwój sieci był stosunkowo zdecentralizowany, a dostarczanie treści charakteryzowało się dużym pluralizmem, wynikającym z rozdrobnienia podmiotów pośredniczących, co można mierzyć ruchem (ang. *traffic*) przechodzącym przez danego pośrednika. Również aktywność użytkowników była wówczas głównie lokalna – realizowana poprzez fora dyskusyjne lub inne formy sieciowej partycypacji ograniczonej geograficznie i językowo.

[49] Szerzej o tej zasadzie w: E. Goldman, *An Overview of the United States' Section 230 Internet Immunity* [w:] *Oxford Handbook of Online Intermediary Liability*, red. Giancarlo Frosio, Oxford University Press, Oxford 2020.

[50] Na przykład: G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, Common Market Law Review, Vol. 59, No. 2/2022.

Wraz z rozwojem technologii wyszukiwarek internetowych, takich jak Google czy Yahoo, oraz pojawieniem się sieci społecznościowych, takich jak Facebook czy MySpace, a także platform wideo, takich jak YouTube, ruch internetowy ulegał stopniowej centralizacji. Jeśli **w 2012 r. podmioty określane jako Big Tech, w tym m.in. Google, Facebook/Meta, Twitter, Netflix, TikTok czy Microsoft, odpowiadały za około 10% ruchu w sieci, to według szacunków z 2024 roku ich udział wynosi już około 70%**. Istotne z punktu widzenia niniejszego raportu jest także to, że zdecydowana większość przychodów tych platform pochodzi z reklam wyświetlanych użytkownikom, które prawnie klasyfikowane są również jako treści[51].

Biorąc pod uwagę społeczno-ekonomiczną rolę, którą Internet odgrywa w dzisiejszym świecie, oznacza to, że podmioty, przez które treści są dostarczane, mają ogromny wpływ na globalne życie, a także na zakres efektywnej wolności słowa, którą cieszymy się w Internecie. Są one po prostu infrastrukturą i medium, poprzez które ludzie komunikują się i na której spędzają dużą część swojego czasu i wartościowej ekonomicznie uwagi[52]. Jest to jedna z wielu przyczyn dla których podmioty te uważane są za posiadające efektywnie bardzo dużą siłę, często wręcz porównywalną do władzy politycznej (ang. *data power*)[53]. Efektywny wpływ, bądź nawet właśnie władza, którą posiadają te platformy, była jedną z przyczyn, które uruchomiły w Unii Europejskiej ruch w literaturze określany jako konstytucjonalizm cyfrowy – ruch intelektualny i tworzenia polityk, mający na celu ochronę praw i podstawowych zasad konstytucyjnych w sferze cyfrowej[54].

Badacze skupiający się na problematyce konstytucjonalizmu cyfrowego opisują i analizują, jak powstaje siła lub władza w Internecie i jaka jest jej natura. W konsekwencji zakresem badań zostaje również zagadnienie dotyczące kwestii regulacji tejże władzy, tak, żeby nie stanowiła ona zagrożenia dla praw podstawowych i porządku konstytucyjnego. Wolność słowa, jako jedno z najważniejszych praw podstawowych, na których oparta jest demokracja, a także, jak wyżej wspomniane, powiązana z nią kwestia odpowiedzialności pośredników za treści, są jednymi z centralnych kwestii rozważanych przez badaczy skupionych dookoła idei konstytucjonalizmu cyfrowego.

Równolegle do refleksji akademickiej, konstytucjonalizm cyfrowy jest praktyką polityki i regulacji. W wyniku realnej potrzeby poskromienia władzy Big Techów i coraz lepszego zrozumienia ich roli we współczesnej gospodarce, Unia Europejska przystąpiła do dynamicznej regulacji tychże podmiotów, szczególnie w ciągu ostatnich dziesięciu lat. Oprócz powstania szeregu regulacji dotyczących kwestii takich jak ochrona danych osobowych[55], cyberbezpieczeństwo[56] czy kwestie ochrony konsumentów[57] i konkurencji[58], nasiliła się również potrzeba uaktualnienia regulacji kwestii odpowiedzialności za treści, których większość, jak wspomniano już wyżej, dziś jest mediowana przez Big Techy.

Celem prawodawcy europejskiego w tym zakresie było uwspółcześnienie, uaktualnienie i uszczegółowienie zasady wyłączenia odpowiedzialności w sposób, który również odpowiednio adresuje specyficzne ryzyka związane z masowym pośrednictwem w zamieszczaniu treści przez Big Techy. **Koniecznym wymogiem i celem regulacyjnym było również jednocześnie utrzymanie zasady ograniczonej odpowiedzialności pośredników za treści i jej centralnych założeń, jak i z drugiej strony, wymuszenie na podmiotach Big Tech poszanowania zasad należytej staranności w zwalczaniu treści nielegalnych i szkodzących**. Osiągnięcie odpowiedniego balansu w tej kwestii jest politycznym, społecznym i ekonomicznym imperatywem, biorąc pod uwagę rolę, którą te podmioty odgrywają w drugiej i trzeciej dekadzie XXI wieku. Efektem wyżej omówionej refleksji i konkretnych działań europejskiego prawodawcy jest europejskie rozporządzenie Akt o Usługach Cyfrowych[59] (ang. Digital Services Act, czyli właśnie DSA), którego większość zasad stosuje się już od lutego 2024 r.

[51] Sandvine/AppLogic Networks (2024), *Global Internet Phenomena Report 2024.*

[52] T. H. Davenport and Beck, C. John, *The Attention Economy: Understanding the New Currency of Business*, Harvard Business School Press, Harvard 2001.

[53] O. Lynskey, *Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy*, *Theoretical Inquiries in Law*, Vol. 20, Issue 1/2-019, s. 189–220.

[54] G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*. Cambridge University Press, Cambridge 2022.

[55] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO)

[56] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.

[57] Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 2011 r. w sprawie praw konsumentów.

[58] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie konkurencyjnych i sprawiedliwych rynków w sektorze cyfrowym.

[59] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o Usługach Cyfrowych – DSA)

4.3. Ramy ogólne DSA i jego cele regulacyjne

DSA weszło w życie 16 listopada 2022 r., jednak rozporządzenie stosuje się od dnia 17 lutego 2024 r. Celem DSA jest przyczynienie się do właściwego funkcjonowania europejskiego rynku wewnętrznego w zakresie świadczenia tzw. „usług pośrednich"[60] poprzez ustanowienie zharmonizowanych przepisów dotyczących *„bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego* (…)"[61]. Dla realizacji tego celu DSA wprowadza przepisy określające ramy warunkowego wyłączenia odpowiedzialności dostawców usług pośrednich, przepisy normujące obowiązek należytej staranności, a także regulacje dotyczące wdrażania i egzekucji samego DSA[62]. Ponadto, DSA obejmuje inne szczegółowe kwestie dotyczące interakcji odbiorców (użytkowników) z dostawcami usług pośrednich.

Zakres podmiotowy DSA obejmuje wszystkich dostawców usług pośrednich działających na terenie Unii Europejskiej, co w uproszczeniu oznacza oferowanie takowych usług podmiotom i osobom fizycznym w Unii[63]. Zakres przedmiotowy rozporządzenia dotyczy natomiast usług pośrednich świadczonych w UE, które DSA klasyfikuje w trzech kategoriach: „zwykłego przekazu", „*cachingu*" oraz „*hostingu*"[64].

Zwykły przekaz polega na transmisji informacji w sieci telekomunikacyjnej lub na zapewnianiu dostępu do takiej sieci. Caching, stanowiący rozszerzenie zwykłego przekazu, obejmuje tymczasowe przechowywanie informacji wyłącznie w celu usprawnienia ich późniejszej transmisji na żądanie użytkowników. Hosting natomiast to usługa regulowana, która polega na przechowywaniu informacji przekazanych przez odbiorcę, również na jego żądanie[65]. To właśnie usługi hostingu – ze względu na ich bezpośredni wpływ na udostępnianie treści użytkownikom – podlegają najszerszemu zakresowi regulacji w DSA i stanowią kluczowy obszar zainteresowania niniejszego raportu. W ramach tej kategorii szczególne znaczenie mają platformy internetowe, rozumiane jako usługi hostingu, które na żądanie użytkownika przechowują oraz publicznie rozpowszechniają informacje. To właśnie działalność takich platform jest przedmiotem dalszych, bardziej szczegółowych obowiązków przewidzianych w rozporządzeniu. Nie mniej ważne z perspektywy tego raportu są wyszukiwarki internetowe jako usługi hostingowe, które DSA definiuje jako:

> „usługę pośrednią, która umożliwia użytkownikom dokonywanie zapytań w celu wyszukiwania – co do zasady – wszystkich stron internetowych lub wszystkich stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, zapytania głosowego, wyrażenia lub innej wartości wejściowej i która podaje wyniki wyszukiwania w dowolnym formacie, w którym można znaleźć informacje związane z zadanym zapytaniem"[66].

4.4. Zasada ograniczonej odpowiedzialności za treści

Co do zasady, głównym założeniem DSA jest utrzymanie ograniczonej odpowiedzialności dostawców usług pośrednich za treści, lecz pod warunkiem spełniania innych wymogów określonych w DSA, jak i pod warunkiem przestrzegania innych praw, takich jak prawo administracyjne i karne, wszystkich Państw Członkowskich UE. Kluczowe znaczenie dla zrozumienia odpowiedzialności Big Techów ma analiza warunkowego wyłączenia odpowiedzialności określonego w art. 6 DSA. Przepis ten przewiduje, że **dostawca usługi hostingu jest zwolniony z odpowiedzialności za przechowywane treści, o ile spełnione są dwie przesłanki**:

1. **nie ma faktycznej wiedzy o nielegalnej działalności lub nielegalnych treściach, a w odniesieniu do roszczeń odszkodowawczych** – nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o nielegalnej działalności lub nielegalnych treściach; lub

2. **podejmuje bezzwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do nielegalnych treści, gdy uzyska taką wiedzę lub wiadomość**.

Powyższe przesłanki tworzą zatem mechanizm warunkowego wyłączenia odpowiedzialności oparty na dwóch filarach: braku wiedzy faktycznej oraz szybkości działania podjętego po uzyskaniu informacji o nielegalnych treściach lub nielegalnej działalności. Stanowią one rdzeń regulacji odpowiedzialności za treści w DSA.

W literaturze obecny jest pogląd, że celem wyłączenia odpowiedzialności dostawców hostingu jest „uwzględnienie uwarunkowań świadczenia usług przez dostawców usług pośrednich (…). Ingerencja tych podmiotów w treści odbiorców usług, które transmitują lub przechowują, jest ograniczona,

[60] Art. 3 lit. g DSA.
[61] Art. 1 DSA.
[62] Art. 1 DSA.
[63] Art. 2 DSA.
[64] Art. 4, 5, 6 DSA.
[65] Art. 6 DSA.
[66] Art. 3 lit. j DSA.

a ilość treści ogromna, w związku z czym dostawcy usług pośrednich nie mają wiedzy i intelektualnej kontroli nad tymi treściami. Oczekiwanie, że będą oni sprawować nadzór nad treściami lub będą w stanie proaktywnie eliminować treści bezprawne, jest niezasadne i podważa sens świadczenia takich usług z uwagi na zbyt duże ryzyko prawne. Mogłoby również nadmiernie ingerować w swobodę wypowiedzi oraz prawo do prywatności"[67].

Podkreśla się również, że wyłączenie odpowiedzialności dostawców hostingu ma charakter horyzontalny, a zatem obejmuje wszystkie rodzaje odpowiedzialności. Oznacza to, że przy spełnieniu przesłanek określonych w art. 6 DSA wyłączona jest możliwość dochodzenia roszczeń cywilnoprawnych, nakładania kar administracyjnych, a także przypisania odpowiedzialności karnej[68]. Wiedza, do której odwołuje się omawiany przepis, musi dotyczyć konkretnej treści, której bezprawny charakter można ustalić przy zachowaniu należytej staranności albo o której dostawca został wprost poinformowany. Co istotne, chodzi tu o wiedzę człowieka, a nie automatycznego systemu czy oprogramowania[69].

Jednak, zgodnie z motywem 18 DSA wyłączenie odpowiedzialności posiada stosowne ograniczenia, mianowicie: „w przypadku, gdy dostawca usług pośrednich zamiast ograniczać się do świadczenia usług w sposób neutralny poprzez czysto techniczne i automatyczne przetwarzanie informacji przekazanych przez odbiorcę usług, odgrywa aktywną rolę, która może pozwolić mu na powzięcie wiedzy o tych informacjach lub sprawowanie nad nimi kontroli. Wyłączenia te nie powinny zatem być dostępne w przypadku odpowiedzialności za informacje przekazane nie przez odbiorcę usługi, lecz przez samego dostawcę usługi pośredniej, w tym w przypadku, gdy odpowiedzialność redakcyjną za opracowanie tych informacji ponosi dany dostawca"[70].

Jak podkreślają komentatorzy[71], również orzecznictwo wskazuje, że określone działania dostawcy usług nie stanowią sprawowania takiej aktywnej kontroli nad treściami, która mogłaby prowadzić do uzyskania wiedzy o bezprawnym charakterze konkretnych danych lub ofert. Za czynności niewskazujące na kontrolę treści uznaje się w szczególności:

1. ustalanie warunków świadczenia usług, pobieranie opłat oraz informowanie użytkowników o ogólnym charakterze oferowanej usługi[72];

2. weryfikację zgodności pomiędzy deklarowanym hasłem a hasłem zapisanym przez użytkownika, rozumianą jako ustalenie, czy operator posiada dostęp do haseł wprowadzanych przez reklamodawców i przechowywanych w jego systemie, czy też nie sprawuje nad nimi żadnej kontroli[73];

3. korzystanie z oprogramowania służącego do wykrywania treści bezprawnych, a więc stosowanie narzędzi technologicznych przeznaczonych do identyfikacji nielegalnych materiałów[74].

Ponadto DSA wyraźnie wskazuje, że określone czynności techniczne związane z przetwarzaniem treści, takie jak automatyczne indeksowanie, funkcje wyszukiwania czy systemy rekomendacji – nie mogą być uznawane za dowód posiadania wiedzy o bezprawnym charakterze materiałów przechowywanych przez dostawców[75].

Jednocześnie rozporządzenie podkreśla, że działania podejmowane w dobrej wierze i z należytą starannością, których celem jest wykrywanie, identyfikacja, usuwanie lub uniemożliwianie dostępu do treści nielegalnych[76], nie prowadzą do utraty ochrony wynikającej z wyłączenia odpowiedzialności. Z drugiej strony DSA nie nakłada na dostawców usług pośrednich obowiązku aktywnego monitorowania, czy systematycznej kontroli użytkowników w celu zapobiegania publikacji treści nielegalnych. Niemniej jednak **dostawcy ci są zobowiązani do podejmowania odpowiednich działań w każdym przypadku, gdy otrzymają stosowny nakaz od właściwych organów władzy publicznej**[77].

Wyłączenie odpowiedzialności przewidziane w DSA przysługuje dostawcom usług pośrednich pod warunkiem dochowania należytej staranności, rozumianej jako ustawowy standard zachowania. Rozporządzenie precyzuje, co dochowanie tego standardu oznacza w praktyce oraz w jakich sytuacjach dostawca powinien uznać, że posiada wiedzę o treściach nielegalnych[78]. W świetle DSA **należyta staranność polega na kumulatywnym stosowaniu środków i procedur**

[67] M. Piech [w:] *Akt o usługach cyfrowych. Komentarz*, red. J. Gołaczyński, R. Skibicki, Warszawa 2024, art. 6.
[68] *Ibidem*, art. 6.
[69] M. Piech, *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019, s. 162.
[70] Motyw 18 DSA.
[71] M. Piech [w:] *Akt o usługach cyfrowych. Komentarz*, red. J. Gołaczyński, R. Skibicki, Warszawa 2024, art. 6.
[72] Wyrok TSUE z 12 lipca 2011 r., C-324/09, L'Oréal i inni, EU:C:2011:474, pkt 115.
[73] Wyrok TSUE z 23 marca 2010 r. w sprawach połączonych C-236/08 do C-238/08, Google France, EU:C:2010:159, pkt 117.
[74] Wyrok TSUE z 22 czerwca 2021 r., C-682/18 i C-863/18, Frank Peterson, EU:C:2021:503, pkt 109.
[75] Motyw 22 DSA.
[76] Art. 7 DSA.
[77] Art. 9 DSA.
[78] Art. 11 DSA.

określonych dla poszczególnych kategorii usług pośrednich. Do najważniejszych z nich – które zostaną omówione w kolejnych częściach raportu – należą w szczególności mechanizmy zgłaszania treści nielegalnych, obowiązki przejrzystości, systemowe zarządzanie ryzykiem oraz współpraca z organami publicznymi.

4.5. Dodatkowe obowiązki dostawców usług pośrednich w zakresie zarządzania treściami

Dostawcy usług pośrednich mają obowiązek utworzenia pojedynczego punktu kontaktowego dla organów Państw Członkowskich UE, a także utworzenia punktu kontaktowego dla odbiorców usług (użytkowników), który ma zapewnić szybką i bezpośrednią komunikację z dostawcą[79]. Ponadto, muszą desygnować przedstawiciela prawnego w UE, przez dostawców bez siedziby w UE.

Oprócz samej regulacji odpowiedzialności za treści DSA ma na celu ustandaryzowanie poziomu ochrony, jakim cieszą się użytkownicy w relacji z podmiotami świadczącymi usługi pośrednie i ograniczanie arbitralności w usuwaniu treści, jak i kont użytkowników. Dlatego jedną z prawdopodobnie najważniejszych innowacji prawnych wprowadzonych przez DSA jest obowiązek publikacji przez dostawców usług pośrednich transparentnych i zrozumiałych warunków korzystania z usług (ang. *terms of use or terms of service*), które wiążą prawnie i dostawców, i użytkowników[80]. Jest to też jeden z warunków określających to, czy dostawcy dochowali zasad należytej staranności.

Warunki te muszą jasno określać zasady i kryteria używane do moderowania treści, lecz także ujawniać istotne informacje dotyczące warunków użytkowania i co wpływa na użytkowanie, jak np. podanie informacji na temat przejrzystości systemów rekomendacyjnych, w przypadku bardzo dużych platform internetowych[81]. Użytkownicy muszą jednocześnie być poinformowani o wszelkich zmianach dotyczących tych warunków. Jednocześnie dostawca usług pośrednich ma obowiązek zapewnienia mechanizmu odwoławczego od decyzji na podstawie warunków korzystania z usług, np. dotyczącej usunięcia danych treści, bądź samego konta[82]. Jest to duża zmiana, ponieważ **dostawcy usług pośrednich, jak np. Facebook czy Reddit byli (i często są) notoryczni w nietransparentnym, zmiennym i nieprzewidywalnym sposobie, w jaki zarządzają treściami i kontami użytkowników**. Podczas egzekwowania warunków korzystania z usług, art. 14 ust. 4 DSA określa, że: „Dostawcy usług pośrednich, stosując i egzekwując ograniczenia, o których mowa w ust. 1, działają z należytą starannością, w sposób obiektywny i proporcjonalny oraz z należytym uwzględnieniem praw i prawnie uzasadnionych interesów wszystkich zaangażowanych stron, w tym zapisanych w Karcie praw podstawowych odbiorców usługi, takich jak wolność wypowiedzi, wolność i pluralizm mediów i inne prawa podstawowe i wolności"[83].

Oznacza to *explicite*, że warunki korzystania z usług i ich egzekwowanie nie mogą naruszać istoty praw podstawowych, w tym wolności słowa. Jednocześnie DSA nakłada obowiązek uzasadnienia każdej decyzji dotyczącej usuwania treści, w odniesieniu do warunków korzystania z usług, bądź w odniesieniu do prawa *sensu largo*[84]. Takie uzasadnienie ma ponadto być *„jasne i konkretne"*. Mimo wprowadzenia wyżej wymienionych ograniczeń formalnych co do moderacji treści, DSA pozwala na podejmowanie odpowiednich środków przeciwko odbiorcom (użytkownikom) notorycznie łamiącym prawo i zamieszczającym nielegalne treści[85]. Ponadto, w przypadku powzięcia akcji względem danej treści, dostawca hostingu musi odpowiednio uzasadnić odbiorcy swoją decyzję[86].

Co istotne, **za każdym razem, kiedy dostawca usług hostingu poweźmie informacje na temat możliwości istnienia treści nielegalnych, w szczególności, jeśli chodzi o przestępstwa zagrażające życiu lub bezpieczeństwa, musi on niezwłocznie poinformować odpowiednie organy władzy publicznej**[87].

Dostawcy usług pośrednich podlegają również obowiązkowi sprawozdawczemu dotyczącym moderacji treści. Obejmuje on w szczególności konieczność ujawniania informacji o nakazach wydanych przez państwa członkowskie w sprawie usunięcia treści nielegalnych, a także przedstawiania ogólnego opisu stosowanych praktyk moderacyjnych, w tym wykorzystania narzędzi automatycznych oraz polityki prowadzenia moderacji treści nielegalnych[88].

Co więcej dostawcy są zobowiązani do raportowania liczby skarg dotyczących sposobu moderowania treści, podejmowanych w ich następstwie decyzji

[79] Art. 12 DSA.
[80] Art. 14 DSA.
[81] Art. 27 DSA.
[82] Art. 20 DSA.
[83] Art. 14 ust. 4 DSA.
[84] Art. 17 DSA.
[85] Art. 23 DSA.
[86] Art. 17 DSA.
[87] Art. 18 DSA.
[88] Art. 15 DSA.

oraz mediany czasu potrzebnego na ich rozpatrzenie[89]. Szczegółowe wymogi w zakresie raportowania zostały doprecyzowane przez Komisję Europejską w akcie wykonawczym[90].

Kolejnym interesującym ograniczeniem w DSA **jest zakaz tzw. złych patternów (ang. *dark patterns*), które literatura identyfikuje jako architekturę interakcji z usługą w sieci, która manipuluje użytkownika w sposób, który zwiększa prawdopodobieństwo podejmowania decyzji szkodliwych bądź niekorzystnych dla użytkownika**[91]. DSA zakazuje platformom internetowym używania takich rozwiązań[92]. W kontekście tego raportu może to oznaczać, że architektura samych platform nie powinna pozwalać na prominentne wyświetlanie się treści i reklam szkodliwych bądź manipulujących w szkodliwe decyzje, również finansowe.

DSA uzupełnia również regulacje RODO, nakładając na dostawców platform internetowych **obowiązek zapewnienia małoletnim użytkownikom podwyższonego poziomu bezpieczeństwa i ochrony prywatności**. Jednocześnie rozporządzenie wprowadza zakaz wyświetlania małoletnim reklam opartych na profilowaniu, rozumianym jako „*zautomatyzowane przetwarzanie danych osobowych mające na celu ocenę określonych czynników dotyczących osoby fizycznej, w szczególności analizę lub prognozę jej sytuacji ekonomicznej, zdrowia, preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się*"[93].

W praktyce oznacza to, że reklamy kierowane do małoletnich nie mogą być dostosowywane na podstawie profilu użytkownika tworzonego poprzez analizę jego aktywności. Innymi słowy, platformy nie mogą oceniać, jakie treści reklamowe z największym prawdopodobieństwem wpłyną na zachowanie małoletniego w sposób pożądany przez reklamodawcę, przykładowo skłaniając go do kliknięcia reklamy.

Wszystkie powyżej omówione zasady wynikające z DSA tworzą istotne tło interpretacyjne dla zasady ograniczenia odpowiedzialności dostawców usług pośrednich. Jednocześnie są kluczowe dla zrozumienia, w jaki sposób DSA reguluje działalność Big Techów oraz jaka jest ich praktyczna odpowiedzialność za treści wyświetlane za pośrednictwem platform – a zatem również w jakim zakresie mogą **ponosić odpowiedzialność za szkody powstałe w wyniku publikowanych lub reklamowanych tam treści**.

Według komentatorów, i co istotne dla przedmiotu tego raportu, istotną innowacją DSA w kwestii regulacji odpowiedzialności za treści jest regulacja tejże odpowiedzialności w kontekście platform internetowych, które umożliwiają konsumentom zawieranie z przedsiębiorcami umów na odległość[94]. DSA stanowi, że wyłączenie odpowiedzialności dla dostawców:

> „nie ma zastosowania w odniesieniu do odpowiedzialności na mocy prawa ochrony konsumentów platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, w przypadku, gdy taka platforma internetowa przedstawia określoną informację lub w inny sposób umożliwia zawarcie danej transakcji w sposób, który wzbudzałby u przeciętnego konsumenta przekonanie, że informacja, produkt lub usługa będące przedmiotem transakcji są dostarczane lub świadczone przez samą platformę internetową albo przez odbiorcę usługi działającego z jej upoważnienia lub pod jej kontrolą"[95].

Oznacza to między innymi, że **w sytuacji, gdy tzw. przeciętny konsument może odnieść wrażenie, iż treść – na przykład reklama – prezentowana na platformie i będąca podstawą dokonania nieautoryzowanej transakcji pochodzi bezpośrednio od samej platformy, a nie od podmiotu trzeciego, wyłączenie odpowiedzialności za treści może nie znaleźć zastosowania**.

Choć DSA nie definiuje pojęcia „*umożliwiania zawierania transakcji*", komentatorzy wskazują, że powinno ono być interpretowane możliwie szeroko – jako stworzenie przez platformę warunków do zawarcia umowy lub umożliwienie jej zainicjowania[96].

Motyw 24 DSA dodatkowo precyzuje, że platformy umożliwiające konsumentom zawieranie z przedsiębiorcami umów na odległość nie powinny korzystać z wyłączenia odpowiedzialności przewidzianego dla dostawców hostingu w sytuacjach, w których

[89] Art. 15 ust. 1 lit. d DSA.
[90] https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations [dostęp: 6 listopada 2025 r.].
[91] European Data Protection Board, Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them (14 lutego 2023 r.), w: https://www.edpb.europa.eu/
[92] Art. 25 DSA.
[93] Art. 4 pkt. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – RODO).
[94] M. Piech [w:] *Akt o usługach cyfrowych. Komentarz*, red. J. Gołaczyński, R. Skibicki, Warszawa 2024, art. 6.
[95] Art. 6 ust. 3 DSA
[96] Art. 6 ust. 3 DSA

prezentują istotne informacje dotyczące transakcji w sposób mogący wzbudzić u przeciętnego konsumenta przekonanie, że to platforma – a nie przedsiębiorca – jest źródłem tych informacji lub że przedsiębiorca działa z jej upoważnienia bądź pod jej kontrolą.

Za przykłady takiej sytuacji DSA wskazuje m.in.:

- brak wyraźnego ujawnienia tożsamości przedsiębiorcy, mimo że wymaga tego rozporządzenie,
- ujawnianie danych identyfikujących przedsiębiorcę dopiero po zawarciu umowy,
- wprowadzanie produktu lub usługi do obrotu przez platformę we własnym imieniu, a nie w imieniu faktycznego sprzedawcy lub usługodawcy.

W takich przypadkach należy – w oparciu o wszystkie relewantne okoliczności – ustalić obiektywnie, czy sposób prezentacji informacji mógł wzbudzić u przeciętnego konsumenta przekonanie, że zostały one przekazane przez samą platformę lub przez przedsiębiorcę działającego z jej upoważnienia lub pod jej kontrolą.

W kontekście niniejszego raportu kluczowe znaczenie ma fakt, że platformy umożliwiające konsumentom zawieranie umów na odległość muszą zapewnić możliwość jednoznacznej identyfikacji przedsiębiorców, których oferty prezentują[97]. Motyw 72 DSA podkreśla, że przedsiębiorcy są zobowiązani do przekazywania takim platformom określonych istotnych informacji zarówno dla celów prezentowania ofert, jak i promowania produktów lub usług. Obowiązek ten obejmuje również przedsiębiorców działających na podstawie umów bazowych, którzy promują produkty lub usługi w imieniu marek.

Platformy powinny zatem gromadzić m.in.:

1. dokumenty potwierdzające tożsamość przedsiębiorcy,
2. informacje dotyczące rachunku płatniczego,
3. numer wpisu w odpowiednim rejestrze handlowym.

Motyw 73 DSA precyzuje, że **dostawcy platform powinni „dołożyć wszelkich starań" w celu oceny wiarygodności tych danych. Obejmuje to w szczególności korzystanie z oficjalnych, publicznie dostępnych baz danych i rejestrów – takich jak krajowe rejestry handlowe czy system wymiany informacji o VAT – a także żądanie od przedsiębiorców dokumentów potwierdzających, takich jak kopie dokumentów tożsamości, uwierzytelnione wyciągi z rachunku płatniczego, zaświadczenia o prowadzeniu działalności gospodarczej czy wyciągi z rejestrów**. DSA dopuszcza również korzystanie z innych wiarygodnych źródeł dostępnych zdalnie.

Motyw 74 DSA dodaje, że platformy muszą projektować i organizować swoje interfejsy internetowe w taki sposób, aby umożliwiać przedsiębiorcom realizację obowiązków wynikających z odpowiednich przepisów prawa unijnego (m.in. dyrektyw 2011/83/UE, 2005/29/WE, 2000/31/WE oraz 98/6/WE). Wymaga to podjęcia starań, aby ocenić, czy przedsiębiorcy udostępniają kompletne informacje wymagane przez te regulacje, a także aby uniemożliwiać oferowanie produktów lub usług do czasu, gdy informacje te zostaną przez przedsiębiorcę w pełni uzupełnione.

Jednocześnie DSA wyraźnie wskazuje, że obowiązki te nie oznaczają nałożenia na platformy ogólnego obowiązku monitorowania treści ani kontrolowania prawdziwości informacji przekazywanych przez przedsiębiorców. Interfejsy powinny pozostać przyjazne i łatwo dostępne zarówno dla przedsiębiorców, jak i konsumentów.

Ponadto, po dopuszczeniu przedsiębiorcy do oferowania produktów lub usług, **platformy powinny podejmować „rozsądne starania" w celu losowego sprawdzania, czy dane produkty lub usługi nie zostały oznaczone jako nielegalne w oficjalnych, ogólnodostępnych rejestrach lub bazach danych dostępnych w państwach członkowskich lub na poziomie unijnym**.

W praktyce oznacza to, że każdy reklamodawca publikujący treści za pośrednictwem platformy powinien być możliwy do jednoznacznego zidentyfikowania, a sama platforma ma obowiązek zachowania należytej staranności przy weryfikacji tożsamości takiego przedsiębiorcy. DSA wzmacnia ten obowiązek również poprzez art. 30 ust. 5, zgodnie z którym:

> „Dostawcy platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość przechowują w sposób bezpieczny informacje uzyskane na podstawie ust. 1 i 2 przez okres sześciu miesięcy po zakończeniu stosunku umownego z zainteresowanym przedsiębiorcą".

Dla przedmiotu tego raportu oznacza to, że ważnym kryterium określenia potencjalnej odpowiedzialności

[97] Art. 30 DSA.

platformy za nieautoryzowane transakcje, które wynikły poprzez treści prezentowane przez platformę, jest to, czy sama platforma dołożyła odpowiednich starań by przedsiębiorca, który zamieszcza takie treści, był identyfikowalny**.** DSA w motywach przedstawionych powyżej przedstawia bardzo konkretne kryteria, które pozwalają ocenić, czy w tym kontekście te zasady należytej staranności są respektowane. Można przypuścić, że taka **staranność nie jest zachowywana, jeżeli nieautoryzowane transakcje są cały czas notorycznym problemem**.

4.6. Reżim odpowiedzialności i nadzoru wobec bardzo dużych platform oraz usług wyszukiwania

DSA wyodrębnia tzw. bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe, które są przedmiotem dodatkowych obowiązków ponad te, które mają zastosowanie do zwykłych platform i wyszukiwarek. Jednym z kluczowych warunków dla kwalifikacji przez Komisję Europejską na podstawie DSA platformy lub wyszukiwarki jako bardzo dużej jest posiadanie co najmniej 45 milionów odbiorców (użytkowników) w Unii Europejskiej. Ta klasyfikacja zazwyczaj pokrywa się z tym, co potocznie określa się jako Big Tech. **Dotychczas, na podstawie informacji z 10 października 2025 r., za bardzo dużą platformę bądź wyszukiwarkę internetową uznane przez Komisję Europejską zostały: AliExpress, Amazon, Apple, Booking, Google i rodzina jego usług (np. YouTube czy Google Play), Shein, LinkedIn, Meta (Facebook, WhatsApp, Instagram), Microsoft, Pinterest, Snapchat, TikTok, Twitter/X, Temu, Wikipedia, Zalando i ponadto inne strony hostujące i udostępniające treści nieodpowiednie**[98].

Tego typu podmioty mają obowiązek wprowadzenia i utrzymywania procesu oceny i zarządzania ryzykiem systemowym[99]. Przez powyższe należy rozumieć identyfikację o należytej staranności opartej na analizie oraz ocenie ryzyka systemowego wynikającego z funkcjonowania konkretnej usługi i powiązanych z nią systemów. Ocena ryzyka musi uwzględniać specyfikę usług, a także być proporcjonalna do samego ryzyka, biorąc pod uwagę jego wagę i prawdopodobieństwo[100]. Obowiązek prowadzenia i utrzymywania procesów oceny i zarządzania ryzykiem jest motywowany filozofią regulacyjną, którą określa się w literaturze podejściem opartym na ryzyku (ang. *risk-based approach*)[101].

Podejście regulacyjne przyjęte wobec bardzo dużych platform i wyszukiwarek odchodzi od tradycyjnego modelu, w którym przepisy szczegółowo określają, co jest dozwolone, a co zakazane. Zamiast tego **DSA opiera się na mechanizmie zarządzania ryzykiem, w ramach którego to sam podmiot regulowany ma obowiązek zidentyfikować ryzyka wynikające z własnej działalności, a następnie dobrać adekwatne i praktycznie wykonalne środki służące ich ograniczeniu. W praktyce oznacza to konieczność samoograniczenia się platform i wyszukiwarek poprzez wdrażanie działań odpowiadających skali i charakterowi zagrożeń, które generują**.

Rola organów publicznych polega z kolei na nadzorowaniu tego procesu, analizie przedstawionych przez platformy ocen ryzyka oraz ocenie, czy zastosowane środki spełniają standard należytej staranności, biorąc pod uwagę cele regulacji. Przykładowo, jeżeli DSA – przyjmując podejście oparte na ryzyku – ustanawia obowiązek zwalczania treści nielegalnych przy jednoczesnym zachowaniu zasady ograniczonej odpowiedzialności, a bardzo duże platformy i wyszukiwarki mają w tym obszarze szczególne obowiązki, to zadaniem regulatora jest sprawdzenie, czy przyjęte przez nie działania rzeczywiście odpowiadają poziomowi zagrożeń i czy skutecznie prowadzą do ich ograniczenia.

W tym celu **ocena ryzyka i sposób zarządzania nim muszą być odpowiednio udokumentowane i udostępniane na wniosek odpowiednich władz publicznych**[102]. Oznacza to, że prawo przyjmuje scenariusz, w którym pewne nielegalne treści „przemkną się" przez system oceny i zarządzania ryzykiem, tak długo jeżeli podmiot regulowany jest w stanie wykazać, że racjonalnie i w dobrej wierze zrobił wszystko, co było możliwe, tak aby ryzyko tychże szkodliwych zdarzeń zmniejszyć.

Do konkretnych ryzyk, które DSA wprost wymienia, a które powinny być zarządzane przez bardzo duże platformy oraz wyszukiwarki zgodnie z art. 34 ust. 1 pkt a) b) c) d) zalicza się:

a) ryzyko rozpowszechniania nielegalnych treści za pośrednictwem ich usług;

b) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla wykonywania praw podstawowych, w szczególności prawa podstawowego do godności ludzkiej zapisanego w art. 1 Karty, do poszanowania życia prywatnego i rodzinnego zapisanego w art. 7 Karty, do ochrony danych osobowych zapisanego w art. 8 Karty,

[98] https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses [stan na 25 listopada 2025]
[99] Art. 34 ust. 1 DSA.
[100] Art. 34 ust. 2 DSA.
[101] O podejściu opartym na ryzyku w prawie ochrony danych osobowych i w ogóle, zobacz: R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford Data Protection & Privacy Law (Oxford: Oxford University Press, 2020).
[102] Art. 34 ust. 3 DSA.

do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, zapisanego w art. 11 Karty, do niedyskryminacji zapisanego w art. 21 Karty, do przestrzegania praw dziecka zapisanego w art. 24 Karty i do wysokiej jakości ochrony konsumentów zapisanego w art. 38 Karty;

c) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych oraz dla bezpieczeństwa publicznego;

d) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków w odniesieniu do przemocy ze względu na płeć, ochrony zdrowia publicznego i małoletnich, oraz poważnych negatywnych skutków dla fizycznego i psychicznego dobrostanu osoby.

DSA precyzuje, jakie elementy działalności bardzo dużych platform i wyszukiwarek muszą zostać objęte oceną ryzyka. Chodzi przede wszystkim o to, w jaki sposób zaprojektowane są systemy rekomendacji, moderacji treści, reklamy oraz jak przetwarzane są dane użytkowników[103].

Regulacja zwraca również uwagę na sam charakter usługi – zwłaszcza na to, czy sprzyja ona szybkiemu i szerokiemu rozpowszechnianiu nielegalnych treści. W oparciu o te czynniki platformy mają obowiązek wdrażać środki adekwatne do poziomu ryzyka. DSA nie nakazuje konkretnych rozwiązań, ale wskazuje katalog możliwych działań – od zmian w interfejsie lub zasadach korzystania z usług, przez dostosowanie procesów moderacji, testowanie algorytmów i zmianę sposobu wyświetlania reklam, aż po wzmocnienie nadzoru wewnętrznego czy współpracę z zaufanymi sygnalistami i innymi platformami. Celem tego katalogu nie jest „checklista", lecz podpowiedź, jakie typy interwencji mogą być adekwatne do określonego ryzyka systemowego. **Zadaniem platform jest więc samodzielne dobranie proporcjonalnych i skutecznych środków, natomiast zadaniem regulatora – ocena, czy dokonana przez platformę analiza ryzyka i dobrane przez nią działania rzeczywiście prowadzą do jego ograniczenia, zgodnie z celami DSA**[104].

Cały system zarządzania ryzykiem musi być poddawany co najmniej corocznemu audytowi, który ma weryfikować, czy platforma stosuje odpowiednie środki i czy faktycznie minimalizuje ryzyko związane z jej funkcjonowaniem[105].

DSA reguluje również zasady prezentowania reklam przez platformy internetowe. **Reklamy muszą być wyświetlane w sposób zapewniający pełną rozpoznawalność i przejrzystość: użytkownik powinien jasno widzieć, że dana informacja jest reklamą, w czyim imieniu jest prezentowana, kto ją sfinansował oraz na podstawie jakich kluczowych parametrów została skierowana właśnie do niego**[106].

W przypadku bardzo dużych platform i wyszukiwarek powyższy obowiązek jest rozszerzony, ponieważ **podmioty te muszą utworzyć publicznie dostępne repozytorium wszystkich wyświetlanych reklam i tych, które były wyświetlane aż do roku wcześniej**[107]. W teorii wymóg ten powinien w dużym stopniu przeciwdziałać wyświetlaniu szkodliwych reklam, ponieważ zbieranie takich informacji powinno zniechęcać podmioty prezentujące nielegalne treści poprzez reklamy.

Finalnie koordynator cyfrowy, desygnowany przez dane Państwo Członkowskie, powinien mieć dostęp do wszystkich danych pozwalających na ocenę zgodności praktyk bardzo dużej platformy i wyszukiwarki z prawem[108]. Ponadto, **bardzo duże platformy i wyszukiwarki muszą regularnie publikować sprawozdania na temat zgodności z DSA**, którego elementy zostały określone w art. 42 DSA.

[103] Art. 34 ust. 2 DSA.

[104] art. 35 DSA.
[105] Art. 37 ust. 1.
[106] Art. 26 DSA.
[107] Art. 39 DSA.
[108] Art. 40 DSA.

Procedury odzyskiwania środków i systemy odpowiedzialności w sektorze finansowym

5.1. Hipotetyczny stan faktyczny – fałszywa strona internetowa banku reklamowana na platformie internetowej

Ta część raportu przybierze formę studium przypadku, którego celem jest udzielenie odpowiedzi na pytanie, czy bank lub inna instytucja finansowa, która poniosła koszty nieautoryzowanej transakcji dokonanej przez swojego klienta, może dochodzić odszkodowania od platformy internetowej, na której udostępniono materiał phishingowy.

W pierwszej kolejności przedstawiony zostanie hipotetyczny scenariusz, w którym uczestniczą cztery podmioty: platforma internetowa, konsument będący jednocześnie klientem tej platformy i banku, oszust oraz sam bank. Następnie – odwołując się przede wszystkim do wniosków z poprzedniej części raportu – omówione zostaną ramy prawne, w jakich bank musiałby formułować swoje roszczenia wobec platformy.

Na końcu zaprezentowane zostaną informacje i analizy eksperckie, które wskazują, że wykazanie przez bank przesłanek odpowiedzialności platformy internetowej może być, przynajmniej w niektórych konfiguracjach faktycznych, realne i potencjalnie skuteczne.

Pierwszym bohaterem hipotetycznego stanu faktycznego jest platforma internetowa świadcząca usługi elektroniczne, w tym przede wszystkim hostingowe, spełniająca kryteria uznania jej za bardzo dużą platformę internetową (VLOP) w rozumieniu DSA. Na platformie tej oszust zamieszcza reklamę lub inny rodzaj posta zawierającego link do fałszywej strony banku. Strona została przygotowana w sposób profesjonalny – wykorzystuje nazwę, logo oraz charakterystyczną szatę graficzną banku – i stanowi klasyczny przykład phishingu, mającego na celu wyłudzenie danych uwierzytelniających.

Użytkownik platformy, będący jednocześnie klientem banku, ulega wrażeniu autentyczności strony – zarówno ze względu na udane wykorzystanie brandingu banku, jak i fakt, że link udostępniony jest na znanej i powszechnie używanej bardzo dużej platformie internetowej. Po przejściu na stronę użytkownik podaje swoje dane logowania oraz kod autoryzacyjny, co umożliwia oszustowi dokonanie przelewu, a więc nieautoryzowanej transakcji.

Ponieważ oszustwo było przygotowane niezwykle starannie, użytkownikowi nie można przypisać rażącego niedbalstwa. W konsekwencji – zgodnie z PSD2 oraz polską ustawą o usługach płatniczych – bank zwraca klientowi utracone środki. Tym samym to bank staje się ostatecznym podmiotem ponoszącym szkodę, obejmującą zarówno kwotę zwróconą klientowi, jak i koszty obsługi transakcyjnej.

Podsumowanie ról czterech podmiotów:

a) Oszust („reklamodawca") – bezpośredni sprawca czynu zabronionego i szkody, którą poniósł klient, a finalnie bank;

b) Platforma internetowa (BigTech) – dostawca usług hostingowych, objęty obowiązkami wynikającymi z DSA (w szczególności art. 16, 30, 34–35) oraz zasadą ograniczonej odpowiedzialności za informacje przechowywane na wniosek użytkownika (art. 6 DSA);

c) Klient – równocześnie użytkownik platformy, odbiorca usług płatniczych banku i bezpośrednia ofiara phishingu;

d) Bank – podmiot pośrednio poszkodowany, niebędący odbiorcą usług platformy, który jednak z mocy prawa pokrył stratę klienta i rozważa roszczenie regresowe wobec platformy internetowej.

5.2. Stan prawny – przypomnienie i rozwinięcie w kontekście polskiego prawa cywilnego

Ponieważ problematyka odpowiedzialności Big Techów w Unii Europejskiej została szczegółowo omówiona w poprzedniej części raportu, na tym etapie wystarczy przypomnieć kluczowe zasady wynikające z DSA oraz odnieść je do ogólnych reguł odpowiedzialności cywilnej prawa polskiego, które muszą znaleźć zastosowanie w dalszej analizie.

Zgodnie z przepisami DSA hosting jest centralną kategorią dla określania zakresu odpowiedzialności za treści publikowane w Internecie, a działalność platform internetowych – w tym bardzo dużych platform – polega w istotnej mierze na świadczeniu usług hostingu (art. 6 DSA). Warto również odnotować art. 54 DSA, który przyznaje odbiorcom usług pośrednich prawo dochodzenia odszkodowania od dostawców tych usług za szkody wynikłe z naruszenia przez nich obowiązków określonych w DSA. Roszczenia takie są dochodzone zgodnie z prawem Unii oraz prawem krajowym.

W analizowanym stanie faktycznym przepis ten ma jednak ograniczone znaczenie. „Odbiorcą usług pośrednich" w rozumieniu art. 54 DSA jest bowiem klient banku i platformy internetowej – a więc to on, co do zasady, mógłby rozważać

dochodzenie roszczeń wobec platformy. Ponieważ jednak jego szkoda została w całości pokryta przez bank zgodnie z PSD2 i ustawą o usługach płatniczych, klient nie tylko nie ma już szkody, ale również utracił interes prawny w samodzielnym dochodzeniu jakiegokolwiek roszczenia wobec platformy. Z jego perspektywy skorzystanie z szybkiego i pewnego trybu zwrotu środków przez bank wyczerpuje problem.

Z tego względu art. 54 DSA można wyłączyć z dalszych rozważań.

Zasadnicze pytanie brzmi natomiast, czy bank, jako podmiot pośrednio, lecz realnie poszkodowany działaniem oszusta, który wykorzystał usługę oferowaną przez platformę internetową, może dochodzić wobec tej platformy roszczeń regresowych. To właśnie ta kwestia – relacja pomiędzy zasadą ograniczonej odpowiedzialności dostawców usług hostingu a reżimem odpowiedzialności odszkodowawczej na gruncie prawa polskiego – stanowi przedmiot dalszej analizy.

Należy podkreślić, że **przypomniana powyżej zasada ograniczonej odpowiedzialności dostawcy usług hostingowych, wyrażona w art. 6 DSA, nie wyłącza bynajmniej zasad odpowiedzialności cywilnej znanych prawu polskiemu lub też innym porządkom prawnym państw członkowskich Unii Europejskiej. Przepisy DSA modyfikują jedynie ogólne zasady odpowiedzialności cywilnej, w szczególności wprowadzając jej wyłączenia, jak i w zakresie doprecyzowania przesłanki zawinienia, w tym „miernika staranności" specyficznego podmiotu profesjonalnego, jakim jest przedsiębiorca prowadzący platformę internetową lub inne usługi cyfrowe**. Innymi słowy, jako punkt wyjścia dla ewentualnego roszczenia banku wskazać należy niewątpliwie przepisy ogólne polskiego prawa cywilnego, a następnie wskazać, w jaki sposób przepisy DSA modyfikują ich możliwą interpretację i zastosowanie.

Ze względu na to, że w praktyce nie istnieje żadna szczególna umowa między bankiem a platformą internetową – poza standardową, wzorcową umową użytkownika, jaką platforma zawiera z każdym rejestrującym konto – **należy uznać, że reżim odpowiedzialności kontraktowej nie znajduje tu zastosowania**. Nie sposób bowiem wykazać naruszenia zobowiązania wynikającego z umowy łączącej te dwa podmioty. Tym samym **analiza musi zostać przeniesiona na grunt odpowiedzialności deliktowej**.

Podstawą prawną jest art. 415 Kodeksu cywilnego, stanowiący generalną klauzulę deliktową:

Art. 415.

Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.

W doktrynie przyjmuje się, że z art. 415 KC, odczytywanego w systemowym kontekście przepisów o odpowiedzialności odszkodowawczej, wynikają trzy przesłanki, których spełnienie jest konieczne do przypisania odpowiedzialności deliktowej:

1) powstanie szkody po stronie podmiotu pragnącego wystąpić z roszczeniem;

2) adekwatny związek przyczynowy pomiędzy szkodą a działaniem lub zaniechaniem podmiotu, do którego kierowane jest roszczenie;

3) wina w działaniu lub zaniechaniu tego podmiotu.

W analizowanym hipotetycznym stanie faktycznym **niewątpliwie spełniona jest przesłanka powstania po stronie banku szkody w opisanym wyżej wymiarze (kwota wypłacona klientowi oraz koszty obsługi transakcyjnej)**.

Możliwy do wykazania wydaje się być **również związek przyczynowy między dopuszczeniem reklamy phishingowej przez platformę internetową a faktem powstania tej szkody**. To bowiem fakt umieszczenia reklamy na platformie spowodował, że klient trafił na fałszywą stronę internetową banku, ujawnił na niej swoje dane uwierzytelniające, skutkiem czego doszło do nieautoryzowanej transakcji, a bank musiał spełnić swój prawny obowiązek zwrócenia klientowi utraconych środków.

Jednocześnie możliwość zastosowania art. 415 KC jest ograniczona przez art. 6 DSA, który ustanawia zasadę ograniczonej odpowiedzialności dostawców hostingu. Przepis ten nie działa jednak w oderwaniu od reszty rozporządzenia. Powinien być interpretowany łącznie z obowiązkami nałożonymi na platformy, w szczególności art. 16, 30 oraz 34–35 DSA, które precyzują zakres wymaganej od nich należytej staranności. To właśnie te obowiązki wyznaczają granice, w których art. 6 DSA może chronić platformę przed odpowiedzialnością – lub przeciwnie, w których ochrona ta przestaje działać.

Art. 16 DSA nakłada na dostawców hostingu – w tym platformy internetowe – obowiązek zapewnienia łatwo dostępnego, efektywnego i przyjaznego dla użytkownika mechanizmu zgłaszania treści uznawanych za nielegalne. Mechanizm ten jest bezpośrednio powiązany z przesłanką wyłączającą odpowiedzialność z art. 6 DSA: **platforma może powoływać się na brak**

wiedzy o nielegalnych treściach tylko wtedy, gdy wykazała należytą staranność w stworzeniu i utrzymaniu takiego mechanizmu. Jeżeli mechanizm jest wadliwy, niewystarczający lub w praktyce nieskuteczny, argument o „braku wiedzy" traci swoje znaczenie.

Art. 30 DSA wprowadza z kolei standard *„know your business user"*, zobowiązując platformy do weryfikowania tożsamości przedsiębiorców oferujących za ich pośrednictwem towary lub usługi. Obowiązek ten ma ograniczać ryzyka związane z nadużyciami i umożliwiać identyfikację podmiotów dopuszczających się działań nielegalnych.

Natomiast art. 34 i 35 DSA nakładają na bardzo duże platformy obowiązek systematycznej identyfikacji, oceny i minimalizowania ryzyk systemowych, obejmujących wprost ryzyko dokonywania oszustw finansowych przy użyciu ich usług. Niewypełnienie tych obowiązków może zatem podważać możliwość powołania się przez platformę na ograniczenie odpowiedzialności z art. 6 DSA, skoro brak reakcji na przewidywalne ryzyka jest w istocie zaniechaniem naruszającym DSA.

Innymi słowy, **formułując swoje roszczenia na podstawie art. 415 KC w związku z art. 6 DSA, bank musiałby udowodnić, że po stronie platformy internetowej doszło do zawinionego działania lub zaniechania, polegającego w szczególności na tym, że mimo uzyskania wiedzy o nielegalnej działalności lub treści (w tym wypadku: umieszczonym na platformie odnośniku do fałszywej strony banku, wykorzystanej przez oszusta do dokonania ataku phishingowego) nie zareagowała bezzwłocznie usuwając lub blokując dostęp do nielegalnych treści**. Ocena, czy do takich działań lub zaniechań doszło i czy były one zawinione, zostałaby dokonana zwłaszcza w oparciu o wskazane unormowania DSA określające szczegółowe obowiązki przedsiębiorców wskazane powyżej.

Osobną kwestią są problemy praktyczne związane z czasem zgłoszenia fałszywej reklamy lub wprowadzającej w błąd informacji. Tytułem przykładu: wyzwaniem jest sytuacja, w której następczo, tj. dopiero po transakcji oszukańczej i jej zgłoszeniu przez klienta, bank oraz platforma dowiadują się, że fałszywa reklama została zamieszczona, natomiast jeszcze w momencie zajścia zdarzenia brak było podstaw do takiej kwalifikacji. Pojawia się zatem pytanie czy pierwsze zdarzenie, następujące przed zgłoszeniem, może rodzić skutek odszkodowawczy oraz jak dalekie środki zapobiegawcze powinny wdrożyć platformy i banki, by niejako prewencyjnie ograniczać ryzyka i chronić społeczeństwo przed oszustami.

Wydaje się, że podmioty typu Big Tech powinny – z uwagi na wielkość, zasięg społecznego oddziaływania oraz związaną z tym odpowiedzialność i wiarygodność – podejmować maksymalnie staranne działania, również na etapie prewencyjnego weryfikowania treści, w celu zapobieżenia aktywności przestępców. Zaniedbanie w tym zakresie może być ocenione, w zależności od indywidualnych okoliczności faktycznych konkretnej sprawy, jako zaniechanie.

5.3. Działania bardzo dużych platform internetowych w kontekście przesłanek z art. 6 DSA oraz przesłanki zawinienia

Dla porządku wywodu warto zaznaczyć rzecz oczywistą: analizowany stan faktyczny ma charakter hipotetyczny. Oznacza to, że nie jest możliwe „wykazanie" jakichkolwiek faktów, w tym takich, które wspierałyby tezę o konkretnych zaniechaniach po stronie platformy internetowej. W dalszej części analizy chodzi zatem nie o rekonstrukcję faktów, lecz o ocenę, czy znane i publicznie dostępne informacje na temat funkcjonowania bardzo dużych platform internetowych pozwalają zbliżyć się do odpowiedzi na pytanie o spełnienie przesłanek wyłączających ich odpowiedzialność z tytułu hostingu w rozumieniu art. 6 DSA.

Już na wstępie można sformułować hipotezę, że liczne dane dostępne w przestrzeni publicznej wskazują na występowanie systemowych trudności bardzo dużych platform z bezzwłocznym reagowaniem na zgłoszenia dotyczące nielegalnych treści i działalności prowadzonej za pośrednictwem ich usług.

Należy równocześnie podkreślić, że przedstawione w dalszej części zestawienie nie pretenduje do wyczerpania całego spektrum problemów. Obejmuje ono przede wszystkim zagadnienia najlepiej udokumentowane oraz weryfikowalne w oparciu o wiarygodne, ogólnodostępne źródła – takie jak publikacje organów publicznych, analizy eksperckie czy materiały uznanych mediów.

Problem *celeb-bait scam ads* w Australii

W 2022 r. *Australian Competition and Consumer Commission* (ACCC)[109] wszczęła postępowanie przed Sądem Federalnym przeciwko właścicielowi

[109] ACCC to australijski, niezależny organ publiczny odpowiedzialny za ochronę konkurencji i praw konsumentów. Jego zadaniem jest egzekwowanie przepisów dotyczących uczciwych praktyk rynkowych, przeciwdziałanie nadużyciom dominacji, kartelom, wprowadzającym w błąd działaniom handlowym oraz oszustwom konsumenckim. ACCC może prowadzić dochodzenia, nakładać kary, pozywać przedsiębiorstwa (w tym platformy internetowe), a także wydawać wytyczne regulacyjne dla rynku.

Facebooka, Meta Platforms, Inc. oraz Meta Platforms Ireland Limited, zarzucając im dopuszczenie się fałszywych, wprowadzających w błąd lub oszukańczych działań poprzez publikację spreparowanych reklam z udziałem prominentnych australijskich osobistości publicznych[110]. Kluczowym zarzutem było to, że Meta miała wiedzieć o wyświetlaniu na Facebooku fałszywych reklam promujących kryptowaluty, w których biorą rzekomo udział gwiazdy, ale nie podjęła wystarczających kroków w celu rozwiązania problemu. Reklamy te nadal były wyświetlane na Facebooku, mimo że osoby publiczne z całego świata skarżyły się, że ich nazwiska i wizerunki były wykorzystywane w podobnych reklamach bez ich zgody.

Postępowanie przed australijskim sądem federalnym ciągle trwa, jednak w jego następstwie Meta podjęła stosowne działania przeciwko tego typu oszustwom. Podmiot objęty postępowaniem wprowadził nowy mechanizm raportowania nadużyć, stworzony specjalnie dla instytucji finansowych[111]. Pomimo podjętych działań, zjawisko to pozostaje w Australii na tyle poważnym problemem, że władze państwowe regularnie publikują oficjalne ostrzeżenia dotyczące tego typu oszustw [112]. Na początku bieżącego roku *Australian Banking Association*, skupiające 20 największych banków w kraju, skrytykowało Meta za brak działań zapobiegających opisywanym degeneracjom. Stowarzyszenie prowadzi własne badania i eksperymenty, testując systemy zgłaszania nielegalnych treści i wskazuje, że bardzo łatwo znaleźć można wiele przykładów oszukańczych treści na stronie, w tym tzw. kont mułów (*money mules*, czyli elementu łańcucha przestępczego) – wykorzystywanych przez przestępców do prania skradzionych środków. Stowarzyszenie twierdzi, że większość zgłoszeń dotycząca owych nielegalnych treści spotyka się z brakiem reakcji ze strony platform należących do Meta, wskazując np., że w jednym z przypadków: „na trzy podejrzane reklamy na Facebooku zgłoszone jako oszustwa, jedna z nich pozostawała aktywna przez co najmniej cztery dni. Pozostałe dwie zostały usunięte w ciągu 24 godzin, ale jedno z tych kont mogło szybko ponownie opublikować niemal identyczną reklamę i nadal promować inne podejrzane reklamy". Stowarzyszenie skonkludowało, że „te przykłady [oszustw finansowych] są otwarcie widoczne na platformie, a łatwość, z jaką je zidentyfikowano, budzi poważne wątpliwości co do zaangażowania platformy w walkę z oszustwami"[113].

Oczywiście należy mieć na uwadze fakt, że omówiony *casus* dotyczy sytuacji w państwie nie będącym członkiem Unii Europejskiej, a zatem taki, do którego trudno byłoby odnieść bezpośrednio standardy wynikające z DSA. Niemniej całkowicie uprawniony jest zabieg odwrotny, tj. odniesienie wskazanych w nim niedostatków w praktykach zwalczania oszustw finansowych przez Meta, mających przecież w znacznej mierze charakter globalny, do standardów prawa unijnego. Opisana sytuacja uprawdopodabnia tezę o wadliwości systemów zgłaszania nielegalnych treści oraz braku bezzwłocznej reakcji po stronie dostawcy usług hostingowych.

5.4. Wątpliwości Komisji Europejskiej Odnośnie do stosowania DSA przez bardzo duże platformy internetowe

Kolejne przykłady nie będą ograniczać się wyłącznie do treści związanych z usługami finansowymi. Obejmą również materiały o charakterze nielegalnym lub społecznie szkodliwym innego rodzaju, które również pojawiają się na platformach internetowych. To, w jaki sposób platformy reagują (lub nie reagują) na tego typu treści, ma bezpośrednie znaczenie dla oceny realizacji przez nie obowiązków przewidzianych w DSA. W szczególności wpływa na ocenę, czy mogą one skutecznie powoływać się na przesłanki wyłączające odpowiedzialność z art. 6 DSA.

W pierwszej kolejności warto podkreślić, że istotne wątpliwości co do skuteczności działań platform w tym zakresie podnosi sama Komisja Europejska. W 2023 r. wszczęła ona z tego właśnie tytułu postępowanie przeciwko X (dawniej Twitter) w celu oceny, czy X mógł naruszyć ustawę o usługach cyfrowych (DSA) w obszarach związanych z zarządzaniem ryzykiem, moderowaniem treści, ukrytymi wzorcami (*dark patterns*), przejrzystością reklam i dostępem badaczy do danych[114]. Pierwotnym kontekstem, który wpłynął na wszczęcie postępowania, było nieusuwanie nielegalnych treści w kontekście ataków terrorystycznych Hamasu na Izrael[115]. Z uwagi na

[110] https://www.accc.gov.au/media-release/accc-takes-action-over-alleged-misleading-conduct-by-meta-for-publishing-scam-celebrity-crypto-ads-on-facebook [dostęp: 21 listopada 2025 r.].

[111] https://ia.acs.org.au/article/2024/meta-and-australian-banks-tackle-ai-celeb-bait-scams.html [dostęp: 21 listopada 2025 r.].

[112] https://www.nsw.gov.au/departments-and-agencies/id-support-nsw/learn/scams/celebrity-deepfake?utm_source=chatgpt.com [dostęp: 21 listopada 2025 r.].

[113] https://www.news.com.au/finance/money/costs/failing-banks-hit-out-at-meta-over-scams/news-story/c7140aa2ef2d633e42179eadf1ccbaca [dostęp: 21 listopada 2025 r.].

[114] https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-x-under-digital-services-act [dostęp: 22 listopada 2025 r.].

[115] https://tvn24.pl/biznes/tech/komisja-europejska-wszczela-postepowanie-przeciwko-platformie-x-dlaczego-st7591548#:~:text=Komisja%20Europejska%20wszcz%C4%99%C5%82a%20formalne%20post%C4%99powanie%2C%20w%20kt%C3%B3rym,pojawiaj%C4%85ce%20si%C4%99%20w%20niej%20nielegalne%20tre%C5%9Bci%20terrorystyczne [dostęp: 22 listopada 2025 r.].

przedmiot raportu warto obszernie zacytować, jak Komisja Europejska zakreśliła zakres toczącego się postępowania[116]:

1. przestrzeganie obowiązków wynikających z DSA dotyczących przeciwdziałania rozpowszechnianiu nielegalnych treści w UE, w szczególności w zakresie oceny ryzyka i środków zaradczych przyjętych przez X w celu ograniczenia rozpowszechniania takich treści, a także funkcjonowania mechanizmu zgłaszania i usuwania treści nielegalnych przewidzianego przez DSA, w tym z uwzględnieniem dostępności zasobów moderacji treści po stronie X;

2. skuteczność działań podejmowanych w celu zwalczania manipulacji informacją na platformie, w szczególności skuteczność systemu tzw. „Community Notes" w UE oraz adekwatność powiązanych polityk mających ograniczać ryzyka dla debaty publicznej i procesów wyborczych;

3. działania podjęte przez X w celu zwiększenia transparentności platformy. Przedmiotem postępowania są domniemane uchybienia w zakresie udostępniania badaczom publicznie dostępnych danych, zgodnie z art. 40 DSA, a także nieprawidłowości związane z repozytorium reklam X;

4. podejrzenie stosowania zwodniczych rozwiązań projektowych w interfejsie użytkownika, w szczególności w odniesieniu do oznaczeń (*checkmarks*) powiązanych z określonymi produktami subskrypcyjnymi – tzw. niebieskich odznak (*blue checks*).

Postępowanie wciąż trwa, a w jego toku opinia publiczna była wielokrotnie informowana zarówno o uprawdopodobnieniu stawianych zarzutów[117], jak i o rozszerzeniu zakresu prowadzonego śledztwa[118].

Po stwierdzeniu wątpliwości odnośnie przestrzegania przepisów DSA przez X podjęto kroki w stosunku do kolejnych dwóch czołowych platform internetowych. W kategorii niemal najnowszego newsa z branży prawno-technologicznej można traktować to, że w dniu 23 października 2025 r. Komisja Europejska ogłosiła, iż „wstępnie uznała, że zarówno TikTok, jak i Meta naruszyły obowiązek zapewnienia badaczom odpowiedniego dostępu do publicznych danych zgodnie z aktem o usługach cyfrowych (DSA). Komisja stwierdziła również wstępnie, że Meta – zarówno w przypadku Instagrama, jak i Facebooka – naruszyła swoje obowiązki w zakresie zapewnienia użytkownikom prostych mechanizmów zgłaszania treści nielegalnych oraz umożliwienia im skutecznego kwestionowania decyzji dotyczących moderacji treści"[119].

Co szczególnie istotne w kontekście tego raportu i *case study*, zdaniem Komisji: „w odniesieniu do firmy Meta ani Facebook, ani Instagram nie wydają się zapewniać przyjaznego dla użytkownika i łatwo dostępnego mechanizmu „zgłaszania i działania" (Notice and Action), który umożliwiałby użytkownikom oznaczanie treści nielegalnych. (...) W związku z tym mechanizmy Meta służące zgłaszaniu i usuwaniu treści nielegalnych mogą okazać się nieskuteczne". Ponadto, podniesiono, że: „Facebook, Instagram i TikTok mogły wprowadzić uciążliwe procedury i narzędzia umożliwiające naukowcom ubieganie się o dostęp do danych publicznych. Często pozostawia im to częściowe lub niewiarygodne dane, co wpływa na ich zdolność do prowadzenia badań, takich jak to, czy użytkownicy, w tym małoletni, są narażeni na nielegalne lub szkodliwe treści. Umożliwienie naukowcom dostępu do danych platform jest zasadniczym obowiązkiem przejrzystości wynikającym z aktu o usługach cyfrowych, ponieważ zapewnia publiczną kontrolę potencjalnego wpływu platform na nasze zdrowie fizyczne i psychiczne"[120].

Jak widać, we wskazanej sprawie zarzuty dotyczą przestrzegania przepisów DSA w ogólności, bez rozróżnienia, o jakiego typu treści i dane chodzi.

5.5. Zarzuty wobec platform internetowych związane z materiałami dot. wykorzystywania seksualnego dzieci (CSAM)

Gradacja naruszeń prawa czy też „stopień nielegalności" materiałów mogących być udostępnianymi w Internecie są oczywiście poniekąd względne i zależą w znacznej mierze nie tylko od rodzaju i stopnia sankcji przewidzianych w poszczególnych porządkach prawnych, ale również od przyjętej optyki. Niemniej jednak można zaryzykować tezę, że znaczna część światowej opinii publicznej zgodziłaby się

[116] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709 [dostęp: 22 listopada 2025 r.].

[117] https://www.bankier.pl/wiadomosc/Komisja-Europejska-z-trzema-zarzutami-do-X-Jest-grozba-grzywny-8781899.html#:~:text=Komisja%20Europejska%20poinformowa%C5%82a%20w%20pi%C4%85tek%2C%20%C5%BCe%20wed%C5%82ug,kont%20na%20platformie%2C%20przejrzysto%C5%9Bci%C4%85%20reklam%20i%20dost%C4%99pem [dostęp: 22 listopada 2025 r.].

[118] https://digital-strategy.ec.europa.eu/en/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services [dostęp: 22 listopada 2025 r.].

[119] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503 [dostęp: 22 listopada 2025 r.].

[120] https://poland.representation.ec.europa.eu/news/tiktok-i-meta-blokuja-dane-2025-10-27_pl [dostęp: 22 listopada 2025 r.].

ze stwierdzeniem, że na platformach internetowych udostępniane są materiały, których szkodliwość znacznie przekracza tę choćby najzmyślniejszych i najskuteczniejszych oszustw finansowych, a za przykład takowych uznałaby materiały powiązane z wykorzystywaniem seksualnym dzieci (CSAM – ang. *Child Sexual Abuse Material*).

W ostatnich latach w Stanach Zjednoczonych miała miejsce cała seria zdarzeń związanych z tym właśnie problemem. Od kwietnia 2024 r. Kongres pracuje nad projektem ustawy „STOP CSAM Act"[121]. W styczniu Mark Zuckerberg zeznawał przed komisją Senatu[122] m.in. w sprawie wykorzystywania platform należących do Meta przez przestępców seksualnych.

Równolegle, od grudnia 2023 r. toczy się postępowanie sądowe w Nowym Meksyku, którego Prokurator Generalny Raúl Torrez „wniósł pozew przeciwko Meta Platforms, Inc., dyrektorowi generalnemu Markowi Zuckerbergowi oraz w pełni zależnym spółkom córkom – w tym Instagram, LLC oraz Facebook Holdings, LLC – w celu ochrony dzieci przed wykorzystywaniem seksualnym, uwodzeniem w Internecie oraz handlem ludźmi"[123]. Organ twierdzi, że „zebrał materiał dowodowy potwierdzający, że platformy należące do Meta":

- Aktywnie dostarczały i kierowały do nieletnich użytkowników strumień rażących, pornograficznych zdjęć – nawet gdy dziecko nie wyrażało zainteresowania tymi treściami.
- Umożliwiały dziesiątkom dorosłych odnajdywanie, kontaktowanie się i wywieranie presji na dzieci, aby dostarczały im pornograficzne zdjęcia lub oglądały filmy.
- Zalecały dzieciom dołączenie do niemoderowanych grup na Facebooku poświęconych ułatwianiu komercyjnego seksu.
- Umożliwiały użytkownikom Facebooka i Instagrama wyszukiwanie, udostępnianie i sprzedaż ogromnej ilości pornografii dziecięcej.
- Umożliwiały fikcyjnej matce oferowanie swojej 13-letniej córki handlarzom ludźmi w celach seksualnych i utworzenie profesjonalnej strony, na której córka mogła dzielić się przychodami z reklam.

W 2025 r. seria pozwów zarówno osób prywatnych, jak i organów władzy publicznej wniesiona została w Stanach Zjednoczonych przeciwko platformom gamingowym Discord i Roblox[124]. We wszystkich tych postępowaniach powtarzają się zarzuty niedostatecznych zabezpieczeń, braku realnej weryfikacji wieku użytkowników i wadliwych domyślnych ustawień prywatności, ułatwiających przestępcom kontakt z dziećmi.

W Wielkiej Brytanii różnego typu działania prawne przeciwko platformom internetowym w związku z dostępnością na nich CSAM podejmuje organizacja pozarządowa 5Rights Foundation[125], której raporty i ustalenia były m.in. przedmiotem obrad komisji parlamentarnych[126].

Praktycznie **we wszystkich wskazanych tutaj sprawach powtarzają się zarzuty, że platformy internetowe nie stworzyły adekwatnych rozwiązań do przeciwdziałania udostępniania CSAM, nie reagują adekwatnie na zgłoszenia bardzo poważnych nadużyć, a wręcz projektują środowisko sprzyjające tym nadużyciom**.

5.6. Zarzuty celowego projektowania algorytmów naprowadzających na szkodliwe treści i świadomego ignorowania naruszeń prawa

W 2021 r. pracowniczka Facebooka, Frances Haugen, udostępniła mediom oraz Kongresowi USA szereg wewnętrznych dokumentów swojego pracodawcy, które natychmiast stały się przedmiotem wielu analiz, a sama sygnalistka zeznawała potem zarówno przed Kongresem[127], jak i przed Parlamentem Zjednoczonego Królestwa[128] oraz Parlamentem Europejskim.

[121] https://www.congress.gov/bill/118th-congress/senate-bill/1199/text [dostęp: 22 listopada 2025 r.].
[122] https://eu.usatoday.com/story/money/2024/01/31/senate-social-media-hearing-kids-safety/72413205007/ [dostęp: 22 listopada 2025 r.].
[123] https://nmdoj.gov/press-release/attorney-general-raul-torrez-files-lawsuit-against-meta-platforms-and-mark-zuckerberg-to-protect-children-from-sexual-abuse-and-human-trafficking/ [dostęp: 22 listopada 2025 r.].
[124] Pozew rodziców nastolatki ze stanu Washington: https://www.fox13seattle.com/news/snohomish-county-family-sues-roblox-discord [dostęp: 22 listopada 2025 r.]; Pozew rodziców nastolatki z Kalifornii: https://www.business-humanrights.org/en/latest-news/usa-roblox-and-discord-sued-for-allegedly-facilitating-the-sexual-exploitation-of-a-child/ [dostęp: 22 listopada 2025 r.]; Pozew Prokuratora Generalnego New Jersey: https://www.wired.com/story/new-jersey-sues-discord/ [dostęp: 22 listopada 2025 r.].
[125] https://5rightsfoundation.com/5rights-foundation-escalates-legal-action-against-meta-over-ai-generated-child-sexual-abuse-material-on-instagram/ [dostęp: 22 listopada 2025 r.].
[126] https://committees.parliament.uk/writtenevidence/132894/html/ [dostęp: 22 listopada 2025 r.].
[127] https://www.theguardian.com/technology/2021/oct/05/facebook-harms-children-damaging-democracy-claims-whistleblower [dostęp: 22 listopada 2025 r.].
[128] https://committees.parliament.uk/committee/534/draft-online-safety-bill-joint-committee/news/157979/facebook-whistleblower-frances-haugen-to-give-evidence-to-uk-parliament/ [dostęp: 22 listopada 2025 r.]; https://www.bbc.com/news/technology-59038506 [dostęp: 22 listopada 2025 r.].

Podmioty analizujące dokumenty postawiły na ich podstawie tezy, że z działalnością platform należących do Meta związany jest cały szereg następujących problemów[129]:

- **Wpływ na zdrowie psychiczne nastolatków:** wewnętrzne badania Meta miały wykazać, że w szczególności Instagram miał negatywny wpływ na zdrowie psychiczne i postrzeganie własnego ciała przez nastoletnie dziewczęta – znaczący odsetek badanych zgłaszał, że platforma pogłębia ich problemy z samooceną.

- **Przemoc polityczna i dezinformacja:** dokumenty ujawniły, że platformy Facebooka były wykorzystywane do podżegania do przemocy oraz szerzenia dezinformacji w wielu krajach, m.in. podczas ataku na Kapitol Stanów Zjednoczonych 6 stycznia 2021 r., a także w związku z przemocą etniczną w Etiopii i Mjanmie. Firma z opóźnieniem wprowadzała środki mające ograniczyć szkodliwe treści.

- **Algorytmiczne promowanie treści skrajnych:** ustalono, że algorytmy Facebooka priorytetowo traktowały treści wywołujące silne reakcje emocjonalne (takie jak gniew), ponieważ zwiększały one zaangażowanie użytkowników. Często prowadziło to do promowania mowy nienawiści oraz treści polaryzujących.

- **System XCheck:** dokumenty ujawniły istnienie systemu o nazwie „XCheck" (*cross-check*), który zapewniał specjalne wyjątki moderacyjne użytkownikom o wysokim profilu (celebrytom, politykom itp.), pozwalając im naruszać zasady dotyczące treści bez natychmiastowych konsekwencji.

- **Handel ludźmi:** wewnętrzne raporty Facebooka wskazywały, że platforma była wykorzystywana przez handlarzy ludźmi do rekrutacji i sprzedaży pracowników domowych, szczególnie na Bliskim Wschodzie i w Azji Południowej, a działania Facebooka w celu powstrzymania tego zjawiska były niewystarczające ze względu na brak zasobów moderacji w lokalnych językach.

- **Priorytet dla zysków kosztem bezpieczeństwa:** zarzut przewodni z analiz dokumentów brzmiał, że choć zespoły wewnętrzne identyfikowały potencjalne rozwiązania tych poważnych problemów, ich uwagi i propozycje były często ignorowane przez kierownictwo na rzecz dalszego wzrostu i zysków.

Zarzuty sformułowane na podstawie ujawnionych dokumentów wewnętrznych pojawiały się następnie w szeregu innych postępowań oraz analiz, dotyczących nie tylko platform należących do Meta, ale także innych czołowych serwisów internetowych. W sierpniu 2025 r. prokurator generalny Minnesoty pozwał TikToka zarzucając, że: „gigant mediów społecznościowych i platform wideo narusza prawo stanowe oraz żeruje na młodych mieszkańcach Minnesoty poprzez celowo manipulacyjne i wprowadzające w błąd praktyki"[130]. W październiku natomiast do sądu w Mediolanie wpłynął pozew zbiorowy włoskich rodzin „przeciwko Facebookowi, Instagramowi (Meta) i TikTokowi, oskarżając platformy o niewłaściwe egzekwowanie ograniczeń wiekowych oraz stosowanie uzależniających funkcji, które szkodzą zdrowiu psychicznemu dzieci"[131].

Na szczególną uwagę zasługują działania podjęte przez bezprecedensowo szerokie koalicje prokuratorów generalnych z wielu amerykańskich państw związkowych. W październiku 2023 r. koalicja 33 prokuratorów generalnych: „wniosła federalny pozew przeciwko firmie Meta za wyrządzanie szkody zdrowiu psychicznemu młodych osób oraz za przyczynianie się do kryzysu zdrowia psychicznego wśród młodzieży. **W pozwie zarzuca się, że firma świadomie zaprojektowała i wdrożyła szkodliwe funkcje na Instagramie, Facebooku i innych swoich platformach społecznościowych, które celowo uzależniają dzieci i nastolatków. Pozew, wniesiony do Federalnego Sądu Okręgowego dla Północnego Dystryktu Kalifornii, zarzuca również, że Meta rutynowo gromadzi dane dotyczące dzieci poniżej 13. roku życia bez informowania rodziców lub uzyskania ich zgody, co stanowi naruszenie prawa federalnego**. (…) Kolejnych dziewięciu prokuratorów generalnych wnosi pozwy w swoich stanach, co oznacza, że łącznie 42 prokuratorów generalnych podjęło działania przeciwko Meta"[132]. Co istotne, rok później rozpatrujący sprawę sędzia federalna dla Dystryktu Kalifornii dopuściła ją do dalszego rozpatrzenia[133].

[129] https://time.com/6110234/facebook-papers-testimony-explained/ [dostęp: 22 listopada 2025 r.]; https://www.wired.com/story/facebook-papers-internal-documents/ [dostęp: 22 listopada 2025 r.]; https://www.theguardian.com/technology/2021/oct/30/facebook-papers-meta-analysis-zuckerberg [dostęp: 22 listopada 2025 r.].

[130] https://www.cbsnews.com/minnesota/news/minnesota-ag-keith-ellison-announces-lawsuit-against-tiktok/ [dostęp: 22 listopada 2025 r.]; https://www.mprnews.org/story/2025/08/19/minnesota-attorney-general-sues-tiktok-for-preying-on-minnesota-young-people [dostęp: 22 listopada 2025 r.].

[131] https://www.reuters.com/sustainability/boards-policy-regulation/italian-families-target-facebook-instagram-tiktok-over-child-safety-2025-10-07/ [dostęp: 22 listopada 2025 r.].

[132] https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-sue-meta-harming-youth [dostęp: 22 listopada 2025 r.].

[133] https://news.bloomberglaw.com/litigation/meta-must-face-some-claims-by-state-ags-in-addiction-lawsuit [dostęp: 22 listopada 2025 r.].

Z punktu widzenia przedmiotu niniejszego raportu jeszcze istotniejsza jest inna inicjatywa koalicji prokuratorów generalnych. Otóż w czerwcu 2025 r. **„ponadpartyjna koalicja 42 prokuratorów generalnych wysłała list do Meta Platforms, Inc. (Meta), wzywając firmę do podjęcia natychmiastowych i realnych działań w celu przeciwdziałania szerzeniu się oszukańczych reklam inwestycyjnych na Facebooku i WhatsAppie**. List skierowany do dyrektor ds. prawnych Meta, Jennifer Gillian Newstead, przedstawia powszechne obawy dotyczące wprowadzających w błąd reklam, które nakłaniają użytkowników do dołączania do fałszywych grup inwestycyjnych, często podszywających się pod znane postacie ze świata finansów. Oszustwa te doprowadziły do poważnych strat finansowych wśród konsumentów w całym kraju. Takie oszustwa mogą być inicjowane i rozpowszechniane na Państwa platformach z niepokojącą łatwością, a ich celem stają się najczęściej najbardziej podatne grupy społeczne – napisali prokuratorzy generalni. Wpływ na ofiary jest druzgocący – prowadzi nie tylko do utraty pieniędzy o potencjalnie życiowej wartości, lecz także do poważnych konsekwencji psychologicznych i społecznych. Koalicja podkreśliła, że **obecne systemy Meta – zarówno automatyczne, jak i ręczne – są niewystarczające, by zatrzymać rozprzestrzenianie się takich oszustw. Jeżeli Meta nie jest w stanie wdrożyć skuteczniejszego systemu, to powinna po prostu zaprzestać publikowania reklam inwestycyjnych jako kategorii** – czytamy w liście. Prokuratorzy generalni wezwali Meta do wzmocnienia procesów weryfikacji reklamodawców oraz zwiększenia udziału ludzi w nadzorze nad reklamami związanymi z inwestycjami"[134].

5.7. Outsourcing moderowania treści przez bardzo duże platformy internetowe

W kontekście oceny staranności działań podejmowanych przez platformy internetowe w celu zdobywania wiedzy o nielegalnych treściach udostępnianych za ich pośrednictwem oraz należytego reagowania na nie istotne jest również to, jak zaprojektowane i wdrożone zostały systemy moderowania treści. O zrzutach odnoszących się do tego problemu była już mowa powyżej, przede wszystkim w kontekście CSAM. Warto jednak poruszyć jeszcze inne związane z tym wątki, w tym zwłaszcza problem zasobów kadrowych, które są do tego celu wykorzystywane.

Zacząć należy od tego, iż jest raczej powszechną wiedzą, że duże platformy (Meta, TikTok, Google/YouTube, także firmy od AI) prawie zawsze korzystają z pośredników – firm takich jak Genpact, Sama, Teleperformance, Majorel, Accenture, Telus – którzy z kolei kontraktują lokalne firmy z krajów o niższych kosztach pracy (Filipiny, Indie, Kenia, Ghana, Kolumbia), zatrudniające na lokalnych rynkach tysiące moderatorów.

Problem został szerzej zauważony przez światową opinię publiczną już przed kilku laty, m.in. za sprawą publikacji na łamach Guardiana, W artykule „*Revealed: catastrophic effects of working as a Facebook moderator*"[135] opublikowanym 17 września 2019 r. autor Alex Hern opisał sytuację pracowników kontraktowych zajmujących się moderacją treści w centrach Facebook Inc. w Berlinie oraz innych lokalizacjach, którzy zeznają, że codzienna ekspozycja na graficzne materiały (przemoc, pornografia, wykorzystywanie dzieci) spowodowała u nich traumy, zmiany światopoglądowe, a nawet uzależnienie od tego typu zawartości. Artykuł opiera się zarówno na wywiadach z byłymi i obecnymi moderatorami, jak i na wcześniejszych publikacjach m.in. w The Verge, które ujawniały warunki pracy w centrach moderacji Facebooka i wskazywały, że moderatorzy pozostają w kontaktach z treściami ekstremalnymi lub traumatycznymi nawet po godzinach pracy.

W podobnym czasie do dystrybucji trafił film *The Cleaners* (2018, reż. Hans Block i Moritz Riesewieck)[136]. Jest to dokument ujawniającym realia pracy moderatorów treści zatrudnianych przez zewnętrzne firmy w Manili na Filipinach, którzy na zlecenie takich platform jak Facebook, Twitter czy YouTube codziennie muszą podejmować szybkie decyzje dotyczące usuwania materiałów zawierających przemoc, pornografię, mowę nienawiści czy treści polityczne. Podobnie jak w ujawnieniach cytowanych w artykule The Guardian, film opiera się głównie na bezpośrednich relacjach moderatorów, przedstawiając ich doświadczenia psychiczne – w tym PTSD, zaburzenia snu i emocjonalną obojętność – wynikające z ciągłej ekspozycji na drastyczne treści oraz presję norm jakościowych narzucanych przez pracodawców. Jednocześnie *The Cleaners* wprowadza szerszy kontekst polityczny, wskazując, że systemy moderacji treści mają realny wpływ na debatę publiczną i mogą prowadzić do mechanicznej cenzury sztuki, dziennikarstwa czy dokumentowania naruszeń praw człowieka, jeśli zostały zaprojektowane bez zrozumienia kontekstu kulturowego i z myślą przede wszystkim

[134] https://www.naag.org/press-releases/42-state-and-territory-attorneys-general-urge-meta-to-take-action-against-investment-scam-ads/ [dostęp: 22 listopada 2025 r.]

[135] https://www.theguardian.com/technology/2019/sep/17/revealed-catastrophic-effects-working-facebook-moderator#:~:text=Revealed:%20catastrophic%20effects%20of%20working%20as%20a%20Facebook%20moderator%20%7C%20Facebook%20%7C%20The%20Guardian. [dostęp: 23 listopada 2025 r.]

[136] https://www.abc.net.au/news/science/2018-09-29/the-cleaners-documentary-social-media-moderation-the-philippines/10300098 [dostęp: 23 listopada 2025 r.].

o skalowalności. Analogiczne doświadczenia moderatorów zatrudnianych przez Genpact w indyjskim stanie Hyderabad opisywał szeroko Reuters[137].

Wskazany problem nie dotyczy jednakże tylko moderatorów pochodzących z krajów rozwijających się. W 2021 roku sąd w Kalifornii ostatecznie zatwierdził ugodę w sprawie Scola przeciwko Facebookowi[138]. Ugoda zakończyła proces sądowy, w którym zarzucano Facebookowi, że nie zapewnił ochrony moderatorom, którzy oglądali drastyczne treści, zapewniając odszkodowanie finansowe i nakazując wprowadzenie ulepszeń w miejscu pracy dla ponad 14 000 członków grupy w całych Stanach Zjednoczonych. Łączna kwota wynagrodzeń wyniosła 85 mln dolarów.

Głośne stały się również sprawy pozwów, które przeciwko swoim bezpośrednim pracodawcom oraz przeciwko Meta wnieśli moderatorzy z krajów afrykańskich. W 2022 r. pozew zbiorowy wnieśli pracownicy podwykonawcy z Kenii[139]. W obu sprawach powodowie przedstawiają analogiczne zarzuty i argumenty, wskazując na nieregularne wynagrodzenie, brak należytego wsparcia psychicznego, tłumienie działalności związkowej, skrajnie niekorzystne warunki pracy oraz naruszenie godności i prywatności pracowników.

Na chwilę obecną opisane tu pokrótce zjawisko podsumowuje obszerny raport z maja 2025 r., zatytułowanym *Scroll. Click. Suffer. The hidden human cost of content moderation and data labelling*, sporządzony przez pozarządową organizację Equidem[140]. Autorzy przedstawiają skalę i warunki pracy tysięcy moderatorów i pracowników „*data labeling*" dla platform cyfrowych i firm AI, zatrudnionych w państwach takich jak Filipiny, Kenia, Ghana czy Kolumbia. Raport wskazuje, że pracownicy często muszą przeglądać nawet 700-1000 treści dziennie, są narażeni na materiały zawierające przemoc, wykorzystywanie dzieci i tortury, przy niskich stawkach płacowych i minimalnym wsparciu psychologicznym. Autorzy zwracają uwagę na globalny model „taśmowej produkcji" moderacji, gdzie outsourcing, brak odpowiedniego przeszkolenia i presja czasu skutkują pogorszeniem warunków pracy, wysoką rotacją i możliwym naruszeniem praw pracowniczych oraz zdrowia psychicznego pracowników. Raport używa m.in. bezpośrednich wywiadów z moderatorami, analiz dokumentów z kontraktorów moderacji oraz danych NGO-owych, by pokazać, że system moderacji treści jest obciążony kosztami ludzkimi, które firmy technologiczne często przerzucają na pracowników.

Oczywiście we wszystkich wskazanych źródłach i wątkach dominuje – co nie dziwi – narracja o kosztach ludzkich przyjętego modelu moderacji treści na platformach internetowych, w tym w szczególności o naruszaniu praw pracowniczych i konsekwencjach zdrowotnych tego typu pracy. Z punktu widzenia przedmiotu naszego raportu trzeba jednak zauważyć, że wskazany model nie może pozostawać bez wpływu na **efektywność i jakość pracy moderatorów**. Na wskazany problem nakłada się ponadto to, że **outsourcing moderacji prowadzić może do problemów z należytym zrozumieniem materiałów udostępnianych na platformach, a to przede wszystkim z uwagi na konteksty językowe i kulturowe**.

Sporo miejsca poświęcono temu wątkowi w opublikowanym w 2023 r. przez międzynarodową organizację pozarządową Article 19 raporcie zatytułowanym „*Content Moderation and Freedom of Expression: Bridging the Gap between Social Media and Local Civil Society*", co istotne, wspartym finansowo przez Unię Europejską oraz UNESCO[141]. Na łamach publikacji analizowano praktyki Facebooka w Bośni, Kenii, Indonezji i Kolumbii. W konkluzjach czytamy: „Analizując obecny stan praktyk moderacji (...) ze szczególnym uwzględnieniem „treści szkodliwych" („mowy nienawiści" i dezinformacji), projekt ten uwypuklił **istnienie rozdźwięku między globalnymi firmami mediów społecznościowych a lokalnymi interesariuszami. Gdy firmy te nie uwzględniają różnorodnych (językowych, politycznych, społecznych, kulturowych i ekonomicznych) wymiarów kontekstów lokalnych, procesy moderacji treści mogą mieć dramatyczne konsekwencje dla dotkniętych nimi społeczeństw**, takie jak rosnąca polaryzacja i ryzyko przemocy". W 2024 r. w publikacjach prasowych zwrócono z kolei uwagę na to, jakie trudności sprawia moderowanie treści w języku hebrajskim[142].

Nie można wszakże zapominać, że opisany outsourcing dotyczy jednak przede wszystkim treści publikowanych w języku angielskim, natomiast odnośnie do mniejszych języków lokalnych (w tym

[137] https://www.reuters.com/article/world/some-facebook-content-reviewers-in-india-complain-of-low-pay-high-pressure-idUSKCN1QH15D/?utm_source=chatgpt.com [dostęp: 23 listopada 2025 r.].
[138] https://www.impactfund.org/social-justice-blog/scola-v-facebook [dostęp: 23 listopada 2025 r.].
[139] https://www.reuters.com/technology/content-moderator-kenya-sues-meta-over-working-conditions-2022-05-10/?utm_source=-chatgpt.com [dostęp: 23 listopada 2025 r.].
[140] https://equidem.org/reports/scroll-click-suffer-the-hidden-human-cost-of-content-moderation-and-data-labelling/?utm_source=chatgpt.com [dostęp: 23 listopada 2025 r.].
[141] www.article19.org/wp-content/uploads/2022/06/Summary-report-social-media-for-peace.pdf [dostęp: 23 listopada 2025 r.].
[142] https://www.theguardian.com/technology/article/2024/aug/15/meta-content-moderation-hebrew?utm_source=chatgpt.com [dostęp: 23 listopada 2025 r.].

europejskich) platformy internetowe niejako zmuszone są korzystać z wykonawców umocowanych na lokalnych rynkach. Niemniej jednak i w tym zakresie zaobserwowano i opisano istotny problem praktyczny. W raporcie zleconym przez Grupę Lewicy w Parlamencie Europejskim opublikowanym w 2024 r.[143] grupa naukowców z kilku krajów europejskich wskazała, że typową cechą branży moderatorów treści w państwach europejskich jest to, że zatrudnia ona wielu migrantów. Naukowcy przeprowadzili wywiady z moderatorami treści pracującymi w firmach outsourcingu usług Telus i Accenture w Niemczech (w Berlinie i Essen) oraz w anonimowej firmie w Portugalii. W portugalskiej lokalizacji każdy pracownik, z którym rozmawiali, był migrantem z Rosji, Polski, Indii lub Turcji. W niemieckich lokalizacjach większość pracowników stanowili migranci, w tym wielu z Azji i Afryki.

Oczywiście nie sposób nie zauważyć, że problemy opisane we wszystkich wskazanych tu źródłach dotyczą przede wszystkim moderowania treści zgoła innych niż możliwe oszustwa finansowe. Niemniej jednak **całokształt polityki w zakresie moderacji stosowanej przez daną platformę internetową niewątpliwie może być argumentem za tezą dotyczącą stopnia staranności, z jakim to dana platforma podchodzi do swoich obowiązków wynikających z przepisów DSA**.

5.8. Podsumowanie *case study*

Powyżej opisane przykłady kontrowersji wokół działań bardzo dużych platform internetowych oraz stawianych im zarzutów stanowią pewne tło empiryczne dla rozważań o problemach prawnych wynikających z przepisów DSA oraz polskiego prawa krajowego. W tym miejscu przykłady te należy podsumować wskazując na powtarzające się wzorce zarzutów kierowanych wobec bardzo dużych platform internetowych:

1. Systemowe zaniedbania w zakresie reagowania na zgłoszenia nielegalnych treści. Z wielu opisanych przypadków wynika wspólna teza, że **platformy internetowe nie realizują w sposób skuteczny i bezzwłoczny obowiązków związanych z mechanizmem zgłaszania i usuwania treści nielegalnych. Zastrzeżenia dotyczą zarówno powolnego tempa reakcji, jak i braku realnego sprawdzenia zgłoszeń lub ich ignorowania**. Ten zarzut dotyczy różnych kategorii treści: od reklam oszustw finansowych, przez materiały związane z wykorzystywaniem seksualnym dzieci (CSAM), po szeroko rozumiane treści szkodliwe społecznie (dezinformacja, ekstremizm, nawoływanie do przemocy).

2. **Niewystarczająca prewencja i brak adekwatnych mechanizmów bezpieczeństwa**. Platformy są krytykowane nie tylko za brak reakcji na zgłoszenia, lecz także za to, że architektura ich usług umożliwia lub wręcz sprzyja nielegalnym praktykom. Zarzut ten obejmuje m.in. brak właściwej weryfikacji reklamodawców i kont, tolerowanie kont wykorzystywanych w oszustwach finansowych, a także brak obowiązkowej weryfikacji wieku użytkowników w przypadku treści obarczonych ryzykiem (np. związanych z CSAM lub treściami wpływającymi na zdrowie psychiczne nieletnich).

3. **Nadużywanie algorytmów ukierunkowanych na maksymalizację zysków kosztem bezpieczeństwa użytkowników**. W wielu opisanych źródłach wskazuje się, że platformy celowo projektują systemy rekomendacji i targetowania reklam w sposób zwiększający skalę i widoczność treści kontrowersyjnych, emocjonalnych lub ryzykownych — ponieważ zwiększają one zaangażowanie użytkowników i przychody z reklam. Ten zarzut pojawia się także w kontekście materiałów nielegalnych, takich jak reklamy oszustw inwestycyjnych czy treści związane z wykorzystywaniem dzieci, co prowadzi do tezy o konflikcie interesów między przychodem a bezpieczeństwem użytkowników.

4. **Brak przejrzystości i utrudniony dostęp do danych na temat procesów moderacji**. Wiele organów publicznych, badaczy i organizacji pozarządowych wskazuje, że platformy utrudniają dostęp do danych niezbędnych do oceny realnej jakości moderacji i wpływu ich algorytmów na użytkowników. Zarzuty dotyczą również utrudniania reklamacji użytkowników oraz błędów w procedurach odwoławczych od decyzji moderacyjnych. Wskazuje to na brak transparentności jako funkcjonalny element działania platform, a nie incydentalne nieprawidłowości.

5. **Wadliwy model moderacji treści oparty na outsourcingu i niskich kosztach pracy**. W opisanych materiałach powtarza się motyw, że bardzo duże platformy powierzają moderację treści podmiotom zewnętrznym działającym w krajach Globalnego Południa lub bazującym na taniej sile roboczej. Warunki pracy moderatorów odbiegają od standardów właściwych dla prac o porównywalnej odpowiedzialności i obciążeniu

[143] https://hal.science/hal-04662589v1/file/Report_EnCOre-final.pdf [dostęp: 23 listopada 2025 r.].

psychicznym. Przekłada się to na niski poziom jakości moderacji, brak kompetencji kulturowych, językowych oraz presję na szybkość kosztem poprawności decyzji.

6. **Powtarzające się sygnały, że platformy miały wiedzę o problemach, lecz nie podejmowały wystarczających działań**. W wielu przypadkach występuje wspólny schemat: platformy miały dostęp do zgłoszeń, analiz wewnętrznych, danych i dowodów wskazujących na naruszenia, lecz reakcje były opóźnione, fragmentaryczne albo nieskuteczne. Ten element narracji wzmacnia potencjalną tezę o co najmniej prawnym niedbalstwie, a w niektórych przypadkach — o świadomym ignorowaniu ryzyka.

7. **Podejrzenia świadomego tolerowania nielegalnych treści ze względu na korzyści finansowe**. Ostatni, lecz istotny wzorzec obejmuje zarzut, że istnieje ekonomiczna motywacja do tolerowania nielegalnych treści, ponieważ generują one ruch użytkowników lub przychód z reklam. Najsilniej ta teza pojawia się w przypadku oszustw finansowych oraz treści „wysokiego ryzyka", które mogą stanowić istotny procent przychodów platform.

Wszystkie powtarzające się wątki sprowadzają się do jednej wspólnej konkluzji: analizowane materiały przedstawiają obraz platform, które – niezależnie od publicznych deklaracji – charakteryzują się systemowymi deficytami w zakresie bezpieczeństwa, nadzoru i odpowiedzialności, a ich działania często są postrzegane jako spóźnione, niespójne lub nakierowane przede wszystkim na optymalizację przychodów, a nie na ochronę użytkowników czy zgodność z przepisami.

W odniesieniu do przesłanek wyłączenia odpowiedzialności na gruncie art. 6 DSA należy postawić tezę, iż „brak wiedzy" może nie być wiarygodną linią obrony, gdy istnieją dowody systemowej świadomości ryzyk, a na takową wskazują przypadki i zarzuty przytoczone w tej części raportu. Skala otrzymywanych zgłoszeń o nielegalnych treściach, prowadzone przez platformę badania wewnętrzne na ich temat, materiały sygnalistów, ostrzeżenia kierowane do platform przez organy władzy publicznej – nawet jeśli nie dotyczą „konkretnej jednostkowej treści" – mogą zostać uznane za wiedzę o nielegalnej działalności w rozumieniu art. 6, zwłaszcza jeśli dotyczą schematów, nie incydentów.

Ponadto, nawet jeśli wiedza została skutecznie pozyskana, wzorce opóźnień i nieskutecznych reakcji mogą podważać warunek „niezwłoczności". W wielu przytoczonych źródłach powtarzały się zarzuty o długi czas reakcji na zgłoszenia, niekompletność działań moderacyjnych, pozwolenie na recydywę. Stwierdzenie istnienia takich wzorców może prowadzić do wniosku, że działania platformy były reaktywne, fragmentaryczne i nie odpowiadały wymogowi działania „bezzwłocznego" w rozumieniu art. 6 DSA.

Wreszcie, przesłanka winy, a zatem zachowania profesjonalnej staranność w kontekście art. 6 DSA musi być oceniana przez pryzmat skali, zasobów i możliwości technologicznych platform. DSA w swojej konstrukcji zakłada, że od platform oczekuje się nie abstrakcyjnej staranności, lecz „staranności adekwatnej do rozmiaru, zasobów i wpływu" (co wynika z całokształtu przepisów oraz motywów rozporządzenia, w tym zwłaszcza przepisów dot. VLOP/VLOSE).

W świetle zaprezentowanych ustaleń można wyobrazić sobie argumenty sugerujące zaniedbanie tego standardu, które mogłyby zostać użyte w konkretnej sprawie odszkodowawczej. Jako jednoznaczne dowody niestaranności posłużyć mogłyby informacje, że platforma internetowa outsourcinguje moderację w sposób zagrażający jakości (np. brak kompetencji językowych), toleruje znane błędy systemowe algorytmów rekomendacji i reklam, nie zapewnia wystarczających zasobów kadrowych do moderacji lokalnych rynków, projektuje procesy w sposób utrudniający użytkownikom zgłaszanie naruszeń, nie wdraża proporcjonalnych technicznych środków prewencji mimo wiedzy o ryzykach.

Konkludując, stwierdzić należy, że zestawione informacje – choć nie stanowią dowodu w konkretnej sprawie, tym bardziej, że ma ona jedynie charakter hipotetyczny – wskazują na powtarzalne wzorce, które mogą podważać skuteczność powołania się przez platformę na wyłączenie odpowiedzialności z art. 6 DSA.

Analiza porównawcza – praktyki i regulacje w innych krajach

6.1. Czynniki wpływające na rozszerzenie mechanizmów oszustw finansowych oraz potencjalne działania prewencyjne

Oszustwa płatnicze to rodzaj oszustw finansowych lub internetowych, w których przestępcy wykorzystują nieautoryzowane metody do kradzieży pieniędzy lub poufnych informacji finansowych. Oszustwa płatnicze są jednym z głównych wyzwań, przed którymi stoją obecnie organizacje i przedsiębiorstwa, a zrozumienie ich wielowymiarowego charakteru ma kluczowe znaczenie dla poruszania się w dzisiejszym środowisku finansowym.

Polski Rzecznik Finansowy trafnie wskazuje, że problem ten powoduje straty finansowe i podważa zaufanie do globalnego systemu finansowego. Choć bezpośrednio to banki są obarczone kosztami, prawdziwym źródłem podatności na zagrożenia jest często coś innego: w dużej mierze nieuregulowane ekosystemy cyfrowe, w których powstają oszustwa[144].

Oszustwa płatnicze były kilkadziesiąt lat temu niszową działalnością przestępczą, a obecnie stanowią globalne zagrożenie. Przewiduje się, że globalne straty spowodowane oszustwami bankowymi wzrosną o 153% w ciągu najbliższych pięciu lat, z 23 mld dolarów w 2025 r. do 58,3 mld dolarów w 2030 r.[145]

Chociaż ofiarami tego rodzaju aktywności padają na ogół osoby starsze, nie brakuje również przypadków dotyczących osób młodych. Przykładowo, w jednej ze spraw poszkodowany w wyniku rozmowy telefonicznej poniósł stratę w wysokości niemal 140 000 zł[146].

Jak zatem jednostki stają się ofiarami takich oszustw? Należy odrzucić często spotykane założenie, jakoby użytkownicy nie mieli świadomości zagrożeń wynikających z działalności cyberprzestępczej. Z dostępnych analiz psychologicznych dotyczących mechanizmów, które zwiększają podatność potencjalnych ofiar na tego typu zagrożenia, wynika, że oszuści: „opierają się na dowodach społecznych, wykorzystując nasze kręgi wpływów, aby przekonać innych do podjęcia decyzji lub inwestycji, których w innym przypadku by nie podjęli. Kiedy widzimy, że inni coś robią, chcemy ich naśladować"[147]. Ponadto, „stosują również wyrafinowane taktyki, aby oszukać swoje ofiary, a wiele osób po prostu nie jest świadomych różnych rodzajów oszustw" lub „wykorzystują emocjonalne bodźce, aby manipulować swoimi ofiarami. Tworząc poczucie pilności, strachu lub podekscytowania, oszuści osłabiają racjonalne myślenie i zmuszają osoby do podejmowania impulsywnych decyzji"[148].

Niektóre branże są bardziej narażone na tego typu oszustwa finansowe ze względu na swój charakter i sposób działania, na przykład: handel elektroniczny i rynki internetowe, takie jak sklepy internetowe, ze względu na liczbę przeprowadzanych transakcji online; usługi finansowe, które są głównym celem oszustw płatniczych, biorąc pod uwagę cenne dane finansowe, które posiadają; opieka zdrowotna ze względu na cenne dane osobowe i medyczne, a także hotelarstwo, zwłaszcza w sezonie, kiedy wolumen transakcji jest wysoki. Zrozumienie konkretnych zagrożeń, przed którymi stoi każda branża, ma kluczowe znaczenie dla wdrożenia skutecznych środków zapobiegania oszustwom.

Najpowszechniejsze sposoby oszustw były związane z przelewami i płatnościami kartą. Mogą to być w szczególności:

1. Techniki inżynierii społecznej i phishingu – „techniki inżynierii społecznej polegającej na wysyłaniu wiadomości e-mail zawierających treści zachęcające do kliknięcia linku zawartego w wiadomości";

2. Złośliwe oprogramowanie (*malware* – „każdy rodzaj złośliwego oprogramowania zaprojektowanego w celu wyrządzenia szkody systemowi informatycznemu lub kradzieży danych");

3. APT (*Advance Persistent Treats*) – to długotrwały cyberatak, który w sposób ukryty wykorzystuje luki w zabezpieczeniach w celu uzyskania i utrzymania nieautoryzowanego dostępu do sieci w celu ciągłej kradzieży danych;

4. Odmowa dostępu DDoS (*Denial Distribution of Service*) – „narzędzie służące do uszkodzenia lub uniemożliwienia prawidłowego działania infrastruktury ICT ofiary";

[144] https://rf.gov.pl/en/the-financial-ombudsman-intervenes-in-the-case-of-unauthorized-transactions/ [dostęp: 27 listopada 2025 r.].
[145] J. Alvilhiera, *How Banks Prevent Cyberfraud with Improved Threat Intelligence – Mastercard*, *Mastercard*, www.mastercard.com/us/en/news-and-trends/Insights/2025/how-banks-prevent-cyber-fraud-with-improved-threat-intelligence.html. Accessed 2 Oct. 2025 [dostęp: 30 września 2025 r.].
[146] https://rf.gov.pl/en/the-financial-ombudsman-intervenes-in-the-case-of-unauthorized-transactions/ [dostęp: 27 listopada 2025 r.].
[147] J. Langabeer, *Why Smart People Fall for Fraudulent Schemes How to Stop Falling Prey*, „Psychology Today", https://www.psychologytoday.com/us/blog/how-to-make-better-choices/202506/why-smart-people-fall-for-fraudulent-schemes?msockid=20ad3a77966460511d532c069795618f [dostęp: 27 listopada 2025 r.].
[148] V. Ticha, *Cracking the code: why people fall for scams*, https://www.unsw.edu.au/newsroom/news/2023/09/cracking-the-code--why-people-fall-for-scams [dostęp: 27 listopada 2025 r.].

5. Botnety – „zbiór urządzeń podłączonych do Internetu, które zostały wcześniej zaatakowane przez przestępców w celu przejęcia nad nimi kontroli bez wiedzy ofiary"[149].

Przykłady inicjatyw w tym zakresie przedstawił Rzecznik Finansowy w materiale dotyczącym nieautoryzowanych transakcji płatniczych, w którym opisano procedurę postępowania po wykryciu nieprawidłowości przez płatnika.[150] Według tego opracowania należy podjąć następujące działania:

1. Po wykryciu oszustwa transakcyjnego należy niezwłocznie powiadomić: swój bank, zespół CERT.PL (incydent.cert.pl), najbliższą jednostkę policji (zgłoszenie i uzyskanie zaświadczenia o popełnieniu przestępstwa);

2. Złożenie wniosku finansowego do banku o zwrot utraconych środków;

3. Jeśli bank nie odpowie w ciągu D + 1[151], należy złożyć skargę, która powinna zostać rozpatrzona w ciągu 15 dni roboczych;

4. Jeśli bank udowodni, że: a) transakcja została dokonana przez uwierzytelnioną osobę próbującą oszukać bank, b) płatnik naruszył swoje obowiązki umyślnie lub w wyniku rażącego niedbalstwa, płatnik będzie zobowiązany do zwrotu wcześniej zgłoszonych roszczeń finansowych;

5. W przypadku sporu z bankiem można złożyć wniosek o interwencję do Rzecznika Finansowego lub Rzecznika Praw Konsumentów. Jeśli chodzi o zalecenia skierowane zarówno do dostawcy usług płatniczych, jak i płatnika, ważnym elementem bezpieczeństwa są wytyczne i zalecenia opracowane przez Komisję Nadzoru Finansowego[152].

6.2. Skala i znaczenie oszustw finansowych w ujęciu globalnym

Zgodnie z najnowszym wydaniem Global Fraud Index, firma Sumsub stworzyła klasyfikację 112 państw pod względem odporności na cyfrowe oszustwa. W gronie „15 krajów najbardziej chronionych" znajdują się m.in. państwa Europy Zachodniej (Luxemburg, Dania, Finlandia, Norwegia, Holandia, Szwajcaria), Australia i Nowa Zelandia. Natomiast w grupie „15 państw najbardziej narażonych" plasują się kraje takie jak Pakistan, Nigeria, Indie, Indonezja, Tanzania czy Uganda[153]. W krajach o silnych instytucjach, rozwiniętej infrastrukturze cyfrowej i stabilnych regulacjach, gdzie wykazuje się dużą odporność na fraud cyfrowy – naturalnie występuje niższe ryzyko, że oszuści skutecznie przeprowadzą działania phishingowe lub inne oszustwa finansowe. W krajach o niskim poziomie ochrony często charakteryzujących się słabą infrastrukturą, niską zasobnością i ograniczoną skutecznością interwencji państwowej podatność na oszustwa pozostaje znacząco wyższa.

Agencje rządowe Stanów Zjednoczonych, takie jak CFPB (Consumer Financial Protection Bureau, czyli Biuro Ochrony Finansowej Konsumentów) i FTC (Federal Trade Commission, Federalna Komisja Handlu), działają na rzecz ochrony konsumentów i małych przedsiębiorstw poprzez regulowanie produktów i usług. Obejmuje to egzekwowanie przepisów dotyczących ochrony, nadzorowanie firm finansowych i zapewnianie zasobów edukacyjnych. Co istotne, z punktu widzenia niniejszego raportu, wymagają one od dużych firm technologicznych dostarczania danych na temat sposobu funkcjonowania ich systemów płatniczych. Nadzorując i ustalając ograniczenia dla dużych firm technologicznych, tworzą one bardziej sprawiedliwy i przejrzysty rynek dla przedsiębiorców, w tym tzw. start-upów. Nadzór ten buduje również zaufanie klientów, którzy nie posiadają tego typu wiedzy, i pomaga zapobiegać tworzeniu się monopoli[154].

Z drugiej jednak strony, nie brak negatywnych przykładów zagranicznych, pozwalających stwierdzić, że aktywność instytucji publicznych w ograniczony sposób przekłada się na bezpieczeństwo konsumentów i przedsiębiorców w sieci. I tak na przykład: w obecnej kadencji prezydent Donald Trump podjął kontrowersyjne działania w zakresie działalności CFPB, co może mieć negatywne konsekwencje dla

[149] P. Milik, G. Pilarski, *Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, Cybersecurity and Law nr 1 (9) 2023 , s. 112-113.

[150] https://rf.gov.pl/edukacja/baza-wiedzy/najczestsze-pytania-i-odpowiedzi-faq/transakcje-nieautoryzowane/, [dostęp: 30 września 2025 r.].

[151] Skrót „D + 1" w praktyce bankowej oznacza dzień następujący po dniu dokonania określonej czynności, przy czym: „D" tj. dzień zainicjowania zdarzenia (np. dzień zgłoszenia nieautoryzowanej transakcji przez klienta), „+1" tj. pierwszy dzień roboczy po tym dniu.

[152] P. Milik, G. Pilarski, *Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, „Cybersecurity and Law", 1(9)/2023 , s. 117.

[153] https://sumsub.com/newsroom/sumsub-releases-2nd-global-fraud-index-in-collaboration-with-statista-studying-fraud-trends-across-100-countries/?utm [dostęp: 28 listopada 2025 r.].

[154] https://www.consumerfinance.gov/about-us/the-bureau/ [dostęp: 28 listopada 2025 r.].

konsumentów, ale jednocześnie stanowić „ogromną szansę" dla dużych firm technologicznych. Trump mianował bowiem Russela Voughta nowym dyrektorem tymczasowym CFPB, którego już pierwsze zaskakujące działania wywołały wątpliwości co do profesjonalizmu i merytorycznego przygotowania do pełnienia tej odpowiedzialnej funkcji publicznej[155]. Obrońcy praw konsumentów ostrzegają, że może to oznaczać mniejszą ochronę przed potencjalnymi szkodami ze strony sektora usług finansowych.

Podobne problemy obserwuje się także w innych częściach świata. W Republice Południowej Afryki trwa szerokie dochodzenie prowadzone przez Audytora Generalnego (AGSA) dotyczące nadużyć w systemie świadczeń SASSA (South African Social Security Agency). Pomimo wdrożenia – jak deklarował obecny dyrektor generalny – 98% zaleceń naprawczych, agencja wciąż boryka się z systemowymi oszustwami wynikającymi z luk technologicznych oraz niewystarczających mechanizmów weryfikacji wniosków. SASSA była zmuszona zawiesić urzędników i podjąć współpracę ze specjalną jednostką śledczą (Hawks), wskazując jednocześnie na potrzebę wdrożenia biometrii, cyfryzacji danych i nowych procedur odzyskiwania nienależnych płatności. Przypadek ten potwierdza, że **nawet instytucje publiczne dysponujące ustawową kompetencją do ochrony obywateli przed nadużyciami mogą ponosić porażki w zakresie monitorowania ryzyka i identyfikacji fraudów**[156]. W szerszym ujęciu ukazuje to, że równie wysokie standardy należy stosować wobec podmiotów prywatnych – w tym bardzo dużych platform internetowych – które mają obowiązek minimalizowania ryzyk systemowych na mocy DSA.

Z kolei, w Chinach działania objęły wprowadzenie nowatorskich, a zarazem restrykcyjnych regulacji ram prawnych mających na celu ograniczenie oszustw finansowych i poprawę dyscypliny rynkowej – przy umocowaniu do działań w tym obszarze kilku organów władzy publicznej, w tym: Chińskiej Komisji Regulacyjnej ds. Papierów Wartościowych (CSRC), Ministerstwa Bezpieczeństwa Publicznego, Ministerstwa Finansów, Ludowego Banku Chin, Krajowej Administracji Regulacji Finansowej oraz Komisji Nadzoru i Administracji Aktywami Państwowymi Rady Państwa. Podkreśla on konieczność stałego przeciwdziałania nadużyciom na rynkach kapitałowych, w szczególności praktykom związanym z bezprawną emisją akcji i obligacji. Wskazuje również na potrzebę zdecydowanego zaostrzenia mechanizmów nadzorczych oraz procedur rejestracyjnych dotyczących wprowadzania i obrotu papierami wartościowymi[157].

Podkreślić trzeba, że rozwiązania chińskie – również w zakresie działań wprowadzających w błąd, jak i innych aktywności rynkowych mogących generować szkody dla innych uczestników rynku – cechuje **dalece posunięty rygoryzm charakteryzowany czasem jako „polityka 0 tolerancji" dla naruszycieli, w tym również dużych podmiotów zagranicznych**. Tytułem przykładu: w ramach obowiązującej polityki zerowej tolerancji wobec nadużyć finansowych, obejmujących m.in. rozpowszechnianie fałszywych informacji, przywłaszczenie lub niewłaściwe wykorzystanie środków finansowych oraz unikanie spłaty zobowiązań, jako przykład można wskazać przypadek, w którym największa na świecie firma audytorska PricewaterhouseCoopers (PwC) była zaangażowana w znaczące oszustwo finansowe. PwC Zhong Tian był audytorem giganta nieruchomościowego Evergrande. Organy regulacyjne stwierdziły, że firma dopuściła się oszustwa, znacznie zawyżając swoją kondycję finansową. Doszły one do wniosku, że PwC nie popełniło jedynie błędu, ale przez wiele lat aktywnie „tuszowało, a nawet tolerowało" to oszustwo, wydając pozytywne raporty z audytu pomimo oszustwa. W rezultacie PwC spotkała surowa kara. Nałożono na nią rekordową grzywnę w wysokości prawie 63 mln dolarów, zakazano jej przeprowadzania audytów kluczowych klientów w Chinach kontynentalnych przez sześć miesięcy, a jej biuro w Kantonie zostało zamknięte[158].

W Europie istnieją organy regulacyjne na szczeblu Unii Europejskiej, a także instytucje nadzorcze funkcjonujące w poszczególnych krajach. Europejski System Nadzoru Finansowego (ESFS) został wprowadzony w 2010 r. i rozpoczął działalność w styczniu 2011 r. Składa się on z Europejskiej Rady ds. Ryzyka Systemowego (ESRB) oraz trzech europejskich organów nadzoru (ESA): Europejskiego Urzędu Nadzoru Bankowego (EBA), Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych (ESMA) oraz Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA). W 2011 r. UE przyjęła dyrektywę Omnibus II w celu doprecyzowania uprawnień nowych organów, szczególnie w sektorze ubezpieczeń. ESFS działa w oparciu

[155] https://www.cnbc.com/2025/03/05/trump-administration-plans-to-wind-down-the-cfpb.html?utm_ [dostęp: 28 listopada 2025 r.].

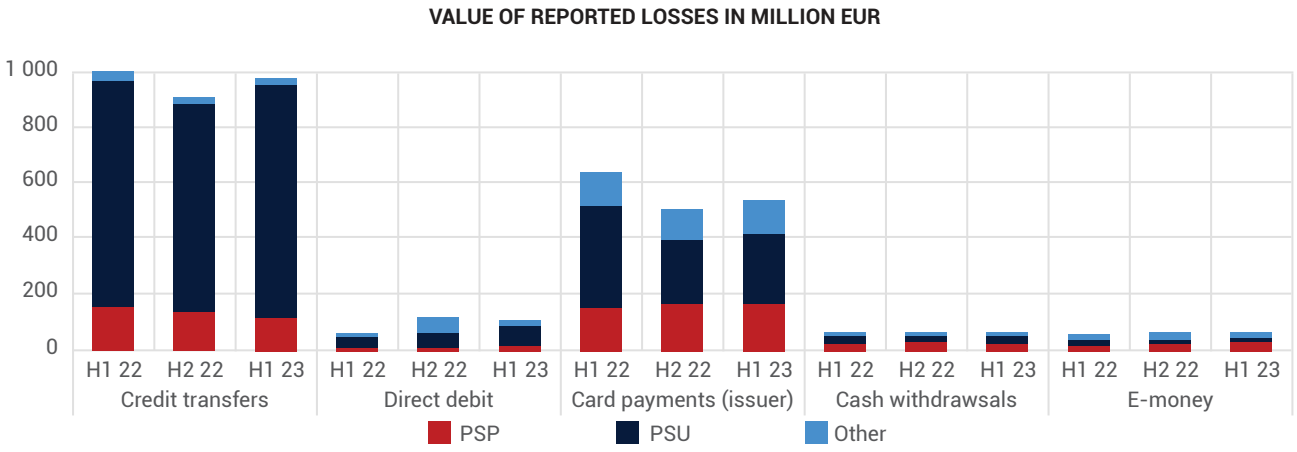
[156] R. Leathern, *HOW Agency and Law Enforcement Are Tackling SASSA Grant Fraud*, *The South African*, 22 Sept. 2025, www.thesouthafrican.com/lifestyle/how-agency-law-enforcement-tackling-sassa-grant-fraud-2025/. [dostęp: 28 listopada 2025 r.] .

[157] https://english.news.cn/20240705/d78edc7cd4074a8693a6f83e9f7cb4d4/c.html?utm [dostęp: 28 listopada 2025 r.].

[158] K. Nuthall, K. Kastner, S. Lewis, *China cracking down on weak auditing of accounting crime. International News Services*, z dnia 24 lutego 2025 r. https://www.internationalnewsservices.com/featured/china-cracking-down-on-weak-auditing-of-accounting-crime [dostęp: 28 listopada 2025 r.]

o pakiet aktów prawnych dostępnych na stronie internetowej Komisji Europejskiej. Europa dysponuje rozległą siecią agencji finansowych i organów regulacyjnych, które działają na rzecz ochrony praw konsumentów, zabezpieczają ich środki oraz chronią przed działalnością przestępczą. Dzięki zrozumieniu zasad funkcjonowania tych dobrze regulowanych instytucji konsumenci są w stanie podejmować świadome decyzje dotyczące tego, gdzie inwestować i komu powierzać swoje pieniądze.

Niemożliwe jest jednak całkowite wyeliminowanie oszustw, co zostało przedstawione na poniższych wykresach.



Wykres 1. Powyżej prezentuje łączną wartość zgłoszonych strat spowodowanych oszustwami według podmiotów ponoszących odpowiedzialność:

Źródło: Europejski Urząd Nadzoru Bankowego – Raport dotyczący oszustw płatniczych w 2024 r.

Wykres 1 przedstawia łączną wartość zgłoszonych strat poniesionych przez PSP (dostawców usług płatniczych), PSU (użytkowników usług płatniczych) i inne podmioty w 2022 r. i pierwszej połowie 2023 r. w odniesieniu do pięciu kluczowych instrumentów płatniczych. Jak widać, największe straty finansowe ponoszą PSU, zwłaszcza w przypadku przelewów i poleceń zapłaty.

Przelewy bankowe stanowią podstawową domenę oszustw związanych z tzw. autoryzowanymi płatnościami *push* (APP), w których użytkownicy mogą zostać oszukani poprzez autoryzowanie płatności, a ponieważ „autoryzowali płatność", odpowiedzialność często spoczywa na PSU. W przypadku poleceń zapłaty oszustwa prowadzą do strat z kont konsumentów, więc PSU ponosi większe straty niż PSP i inne podmioty. W przypadku płatności kartą PSP ponosi wysokie straty finansowe. Można uznać, że jest to zdarzenie, którego konsument nie był w stanie przewidzieć, a w konsekwencji stanowi ono stratę ponoszoną przez banki. Chociaż dokładne określenie wysokości wypłat jest trudne, to głównie banki odpowiadają za pokrycie takich strat, co zapewnia konsumentom wyższy poziom ochrony. Z kolei w przypadku użytkowników produktów bazujących na pieniądzu elektronicznym ochrona regulacyjna wydaje się mniejsza niż przy tradycyjnych płatnościach kartowych, co utrudnia precyzyjne oszacowanie ponoszonego ryzyka.

Tymczasem **banki w Wielkiej Brytanii permanentnie wzmacniają działania w zakresie zwalczania prania pieniędzy i finansowania terroryzmu, priorytetowo traktując sprawy wysokiego ryzyka, zwiększając specjalistyczną wiedzę oraz stosując proporcjonalne i odstraszające sankcje**. Lloyds Banking Group odkryła, że co siedem minut ktoś pada ofiarą oszustwa na platformie należącej do Meta i twierdzi, że platformy takie jak Facebook Marketplace i Instagram odpowiadają za prawie połowę wszystkich oszustw związanych z zakupami. Wprowadzono przepisy, zgodnie z którymi dostawcy usług płatniczych ponoszą odpowiedzialność za straty spowodowane oszustwami związanymi z aplikacjami, do kwoty 85 000 funtów. Banki postulują, by duże firmy technologiczne również ponosiły koszty oszustw płatniczych, do których dochodzi z powodu treści prezentowanych na ich platformach. Oszustwa często mają swoje źródło w serwisach społecznościowych[159].

[159] A. Quinio, M. Arnold, *Social media must do more to tackle payment fraud, says UK regulator. Financial Fraud*, https://www.ft.com/content/1e77ae86-a0c2-47ee-804b-cbe50765a9a8?amp%3Bsegmentid=7c8f09b9-9b61-4fbb-9430-9208a9e233c8 [dostęp: 28 listopada 2025 r.].

Pomimo podjętych działań przez rząd Wielkiej Brytanii w celu ograniczenia oszustw finansowych, w ocenie opinii publicznej oraz banków są one niewystarczające, bowiem stanowią aż 40% wszystkich przestępstw na terenie Anglii oraz Walii. W odpowiedzi **zaczęto zawierać porozumienia z krajami będącymi źródłem wielu oszustw, takimi jak Nigeria, oraz uruchomiono ogólnokrajową kampanię dla podnoszenia świadomości społecznej na temat przestępczości finansowej**. Przykładem jest inicjatywa *„Take Five to Stop Fraud"*[160] pod patronatem brytyjskiego Ministerstwa Finansów, której celem jest wspieranie osób fizycznych i przedsiębiorstw w identyfikowaniu podejrzanych działań i ochronie przed oszustwami finansowymi.

Na poziomie ponadnarodowym utworzono instytucję międzyrządową FATF (Financial Action Task Force), zorganizowaną w celu wypracowywania i określenia standardów w dziedzinie przeciwdziałania praniu pieniędzy, finansowaniu terroryzmu i innych powiązanych zagrożeń dla międzynarodowego systemu finansowego oraz promowanie skutecznego ich wdrażania[161].

Wydaje się zatem, że nie tylko Polska – bowiem problem ten dotyczy większości krajów europejskich i anglosaskich – stoi przed poważnymi wyzwaniami w zakresie podejmowania skutecznych środków w odniesieniu do tego rodzaju ryzyka. **Niska skuteczność występuje zazwyczaj wtedy, gdy rządy nie wdrożyły jeszcze polityk oraz nie koordynują działań z organami publicznymi i niepublicznymi w celu skutecznego reagowania na ryzyko, a także pozostają bierne w obszarze międzynarodowej współpracy, pozwalając przestępcom oraz globalnym Big Techom wykorzystywać zalety Internetu, trudność w egzekwowaniu obowiązków ze względu na siedzibę w innym kraju lub bycia pozwanym we własnej jurysdykcji**. Niemniej jednak inne kraje – co może być pewnym wzorem dla krajowych organów stanowiących i stosujących prawo – poczyniły znaczne postępy w zakresie ram nadzorczych przepisów i regulacji.

Porównując praktyki i ramy regulacyjne tych krajów, możemy ogólnie stwierdzić, że wszystkie kraje starają się złagodzić ten problem, przechodząc od procesów realizowanych przez człowieka do technologii opartych na sztucznej inteligencji, a także ustanawiając systemy nadzoru, takie jak Unia Europejska z DSA, DMA, aby chronić konsumentów i zabezpieczyć przedsiębiorców. Natomiast stosujące prawo organy powinny być surowe, nakładając surowe kary za oszustwa, brak staranności lub woli eliminacji działań przestępczych, uwzględniając siłę rynkową dużych firm technologicznych i zobowiązując je do ponoszenia kosztów finansowych oszustw. Negatywnie na tym tle – z uwagi na bieżące wydarzenia polityczne oraz politykę kadrową prezydenta – wypadają Stany Zjednoczone, gdzie zmiany polityczne w ostatnim czasie zagroziły stabilności i konsekwencji, ograniczając ochronę konsumentów i osłabiając jedyny organ regulacyjny, który przeciwdziała tego typu przestępstwom. W efekcie priorytetem staje się zysk przedsiębiorstw (zwłaszcza wielkich Big Techów) i krótkoterminowe korzyści ekonomiczne, a nie ochrona słabszych uczestników rynku.

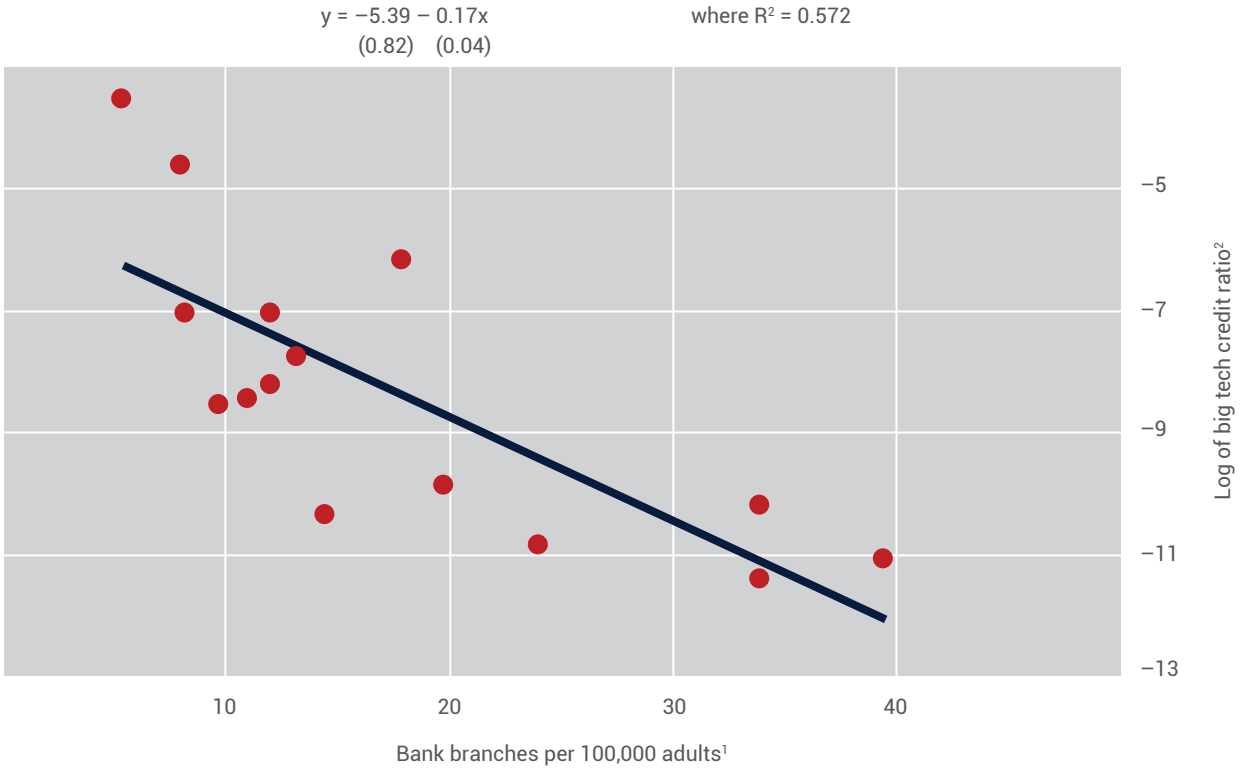
6.3. Wielkie firmy technologiczne na rynku finansowym

Duże firmy technologiczne czerpią korzyści z przewagi konkurencyjnej będącej wynikiem tzw. pętli analizy danych, efektów zewnętrznych sieci i powiązanych działań (DNA). W praktyce wygląda to następująco: im więcej użytkowników ma platforma, tym więcej danych generuje. Więcej danych z kolei stanowi lepszą podstawę do analizy danych, co usprawnia funkcjonowanie istniejących usług, a tym samym przyciąga więcej użytkowników. Ponadto platformy te mają możliwość monitorowania i zarządzania uczestnikami rynku danych, dysponując przy tym bazą milionów użytkowników gotowych do korzystania z ich najnowszych produktów i usług[162].

Ich obecność jest bardziej znacząca w Chinach (Alibaba Group) oraz w niektórych gospodarkach wschodzących i rozwijających się. Pandemia COVID-19 – z uwagi na wprowadzanie przez rządy zasad izolacji społecznej, co wymuszało również ograniczenia lub brak dostępu do banków w formie tradycyjnej (stacjonarnej) – również przyczyniła się do rozwoju usług i produktów finansowych dużych firm technologicznych. Pojawiły się wręcz badania, z których wynikało, że im mniej placówek bankowych, do których dostęp mieli klienci – tym większa popularność usług świadczonych alternatywnie w formie *online* przez konkurujące z bankami podmioty.

Poniżej przedstawiono wykres punktowy, na którym oś X przedstawia liczbę oddziałów banków na 100 000 dorosłych – co oznacza, że im większa liczba oddziałów banków, tym łatwiejszy jest dostęp do banków. Oś Y przedstawia natomiast logarytm

[160] https://www.takefive-stopfraud.org.uk/ [dostęp: 28 listopada 2025 r.].
[161] https://www.gov.pl/web/finanse/publikacje-fatf [dostęp: 28 listopada 2025 r.].
[162] Na ten temat: S. Doerr, J. Frost, L. Gambacorta, V. Shreeti, *Big Techs in finance*, „BIS Working Papers", 1129/October 2023, https://www.bis.org/publ/work1129.pdf [dostęp: 28 listopada 2025 r.].



Źródło: S. Doerr, J. Frost, L. Gambacorta, V. Shreeti, Big Techs in finance, „BIS Working Papers", 1129/October 2023, [dostęp: 28 listopada 2025 r.].

wskaźnika kredytów udzielanych przez duże firmy technologiczne, czyli udział dużych firm technologicznych w rynku kredytowym. Te dwie zmienne są ze sobą ujemnie powiązane, co oznacza, że wzrost jednej z nich powoduje automatyczny spadek drugiej. Tak więc za każdy dodatkowy oddział banku na 100 000 dorosłych logarytm wskaźnika kredytów udzielanych przez duże firmy technologiczne zmniejsza się o 0,17.

Kluczowym czynnikiem wpływającym na wysoką aktywność dużych firm technologicznych w sektorze finansowym jest wykorzystanie przez nie algorytmów *big data* i uczenia maszynowego, czyli programów obliczeniowych zaprojektowanych do identyfikowania wzorców lub prognozowania na podstawie danych. Są one tworzone poprzez szkolenie algorytmu uczenia maszynowego na zbiorze danych. Daje im to przewagę w zakresie udzielania kredytów, co może poprawić dokładność decyzji kredytowych. Ponadto wykazano, że techniki uczenia maszynowego przynoszą znaczną poprawę w zakresie zarządzania ryzykiem i zgodności z przepisami, umożliwiając lepsze wykrywanie oszustw, przestępstw finansowych i naruszeń przepisów. Dochodzi do tego oszczędność kosztów w postaci przeniesienia niemal całej aktywności do sieci (Internetu), pozwalając ograniczyć wydatki związane z koniecznością utrzymywania placówek stacjonarnych, czynnika ludzkiego (pracowników) i innych zasobów (wykorzystanie papieru, sprzętu itd.). Kolejnym czynnikiem kształtującym kredyty udzielane przez duże firmy technologiczne jest system regulacyjny danego kraju, tzn. łatwiej jest wprowadzać nowe produkty w bardziej liberalnym systemie, natomiast rygorystyczne regulacje mogą stanowić większe ograniczenie.

Po wejściu na rynek usług finansowych mogą one rozszerzyć swoją działalność o produkty kredytowe, ubezpieczeniowe, oszczędnościowe i inwestycyjne.

Zasoby oraz ograniczona odpowiedzialność (w porównaniu do tradycyjnych banków, podlegających w Europie zjawisku tzw. „tsunami regulacyjnego", co generuje poważne koszty i utrudnienia w funkcjonowaniu) dużych firm technologicznych mogą ułatwić im świadczenie usług finansowych i obniżyć ich koszty, co prowadzi do zwiększenia dostępności tych usług dla potencjalnych konsumentów. Tradycyjne banki opierają się na kosztownych i czasochłonnych procesach, natomiast duże firmy technologiczne wykorzystują algorytmy, które obniżają koszty operacyjne związane z udzielaniem kredytów. Tradycyjne banki często odmawiają udzielenia kredytu osobom, które nie mają historii kredytowej, natomiast duże firmy technologiczne mogą obsługiwać tę grupę klientów, korzystając z alternatywnych danych. Ważną cechą jest to, że usługi pomocnicze generują

cyfrowy ślad dla małych firm, który może być wykorzystany do generowania ocen kredytowych.

Duże banki i Big Techy różnią się istotnie pod względem danych, sieci i działalności finansowej. Banki dysponują zweryfikowanymi i wiarygodnymi danymi klientów z długą historią, jednak zakres tych danych jest ograniczony, a systemy IT – na tle amerykańskich Big Techów, zwłaszcza w przypadku banków zachodniej kontynentalnej Europy – często przestarzałe. Z kolei Big Techy gromadzą informacje o ogromnej liczbie użytkowników i łatwo łączą różne źródła danych, lecz dane te są krótsze w historii, mniej spójne, a ochrona prywatności bywa niżej traktowana. W kontekście sieci banki mają już rozbudowaną sieć działań finansowych, jednak regulacje i wysokie koszty obsługi nowych klientów ograniczają ich rozwój. Big Techy natomiast korzystają z efektów sieciowych dzięki szerokiemu ekosystemowi aktywności niefinansowych, choć muszą osiągnąć znaczną bazę klientów, aby w pełni wykorzystać potencjał sieci. Jeśli chodzi o działalność, banki oferują złożone, wysokomarżowe produkty, mają doświadczenie w zarządzaniu ryzykiem i dostęp do taniego finansowania, ale dziedziczne systemy IT utrudniają wprowadzanie nowych usług. Big Techy mogą oferować standaryzowane usługi przy niemal zerowym koszcie marginalnym, wykorzystując istniejące dane, jednak brakuje im doświadczenia w kluczowych usługach finansowych oraz ekspertyzy regulacyjnej. Podsumowując, banki mają przewagę w zaufaniu, regulacjach i doświadczeniu finansowym, natomiast Big Techy dysponują skalą, szeroką siecią i zdolnością do efektywnego wykorzystania danych, choć z ograniczeniami w specjalistycznych usługach finansowych.

Powyższe może prowadzić do wniosku, że działalność dużych platform na rynku finansowym może przynosić wymierne korzyści, jednak należy pamiętać, że jest to nierozerwalnie związane ze zwiększeniem ryzyka oraz niesie za sobą nowe problemy, w tym w zakresie oszustw finansowych. Zwłaszcza biorąc pod uwagę mnogość danych, jakimi dysponują Big Techy, a które następnie mogą być „pożywką" dla osób, które w sposób nielegalny takie dane przetwarzają. Przepisy finansowe i międzybranżowe skupiają się na konkretnych podmiotach prawnych wchodzących w skład dużych grup technologicznych lub na określonych rodzajach ich działalności, zamiast uwzględniać ryzyko wynikające z możliwych skutków ubocznych wszystkich działań prowadzonych przez te duże firmy technologiczne[163].

Duże firmy technologiczne mają zasadnicze znaczenie dla rozwoju rynku finansowego dzięki innowacjom opartym na danych, jednak stwarzają one poważne wyzwania rynkowe i polityczne. Wykorzystywanie przez nie dużych zbiorów danych i algorytmów do oceny zdolności kredytowej i zarządzania ryzykiem stanowi wyraźny postęp w stosunku do tradycyjnych, kosztownych metod. Jednak ta potęga niesie ze sobą ryzyko powstania monopolu. Dlatego też niezwykle ważne jest, aby decydenci polityczni stworzyli solidne, elastyczne ramy regulacyjne. Punktem wyjścia jest stosowanie tradycyjnych zasad finansowych, ale należy je uzupełnić nowymi przepisami opracowanymi specjalnie w celu zarządzania monopolami danych, zapewnienia konkurencji i ochrony praw konsumentów w tym nowym ekosystemie.

[163] S. Doerr, J. Frost, L. Gambacorta, V. Shreeti, *Big Techs in finance*. BIS Working Papers No WP1129, October 2023, s.22 na: https://www.bis.org/publ/work1129.pdf [dostęp: 28 listopada 2025 r.].

Ocena skuteczności obecnych ram regulacyjnych i ich wpływu na bezpieczeństwo użytkowników

Biorąc pod uwagę wnioski wynikające z wywiadów pogłębionych, analizy komparatystycznej (porównawczej), jak i literatury przedmiotu (zarówno naukowej, popularnonaukowej, jak i eksperckiej) – stwierdzić należy, że **aktualnie obowiązujący stan prawny jest dalece niesatysfakcjonujący, a także nieskuteczny (w sensie jego respektowania, tj. osiągania stanu zamierzonego przez prawodawcę) oraz nieefektywny (w rozumieniu ekonomicznej analizy prawa, w której porównuje się konsekwencje ekonomiczne regulacji, konfrontując generowane zyski i straty)**.

Wyrażona wyżej krytyczna konkluzja znajduje zastosowanie zarówno do prawa krajowego, jak i prawa Unii Europejskiej, które – mimo obowiązywania DSA oraz innych przepisów normujących odpowiedzialność Big Techów i innych podmiotów prowadzących działalność *online* z wykorzystaniem Internetu – nie zapewnia dostatecznej ochrony użytkownikom sieci (klientom, w tym konsumentom), a także bankom, zobowiązanym jednocześnie do partycypacji w stratach wywoływanych transakcjami oszukańczymi.

Jednocześnie – co akcentują wszyscy Respondenci, a znajduje potwierdzenie w ustaleniach badaczy zagranicznych i doświadczeniach innych państw członkowskich Unii Europejskiej – globalne platformy internetowe nie tylko niedostatecznie skutecznie (co nosi znamiona działań bezprawnych oraz niespełniających wymogu należytej staranności) weryfikują treści, w tym reklamy, a nawet nieraz w pełni świadomie promują je, kosztem innych podmiotów. Co więcej, jak wykazano, aktualny stan prawny nie tylko nie dostarcza należytej motywacji do zmiany tej nagannej postawy, ale wręcz zachęca – biorąc pod uwagę generowane zyski, „klikalność" użytkowników oraz fakt przerzucenia kosztu na bank (a zatem podmiot trzeci z punktu widzenia podmiotu typu Big Tech) – do utrzymywania dotychczasowej praktyki.

W konsekwencji tego stanu:

- cierpi nie tylko bank zwracający środki zgodnie z przepisami normującymi tzw. nieautoryzowane transakcje,
- uszczerbku doznaje bezpieczeństwo, wiarygodność oraz zaufanie społeczne do treści prezentowanych w internecie,
- rozwijają się technologie i sposoby wykorzystywane przez przestępców i ich organizacje, bazujące zarówno na metodach manipulacji emocjonalnej i inżynierii społecznej, a także nowoczesnych technologiach służących naruszaniu prawa,
- dochodzi do nieuzasadnionych gospodarczo i niesprawiedliwych transferów środków pieniężnych,
- na szwank narażany jest autorytet prawa oraz powaga organów władzy publicznej niezdolnych do wyegzekwowania obowiązków wobec międzynarodowych korporacji,
- pogłębia się stan nieuczciwej konkurencji pomiędzy podmiotami sektora bankowego a Big Techami na rynku usług i produktów finansowych,
- zwiększa się ryzyko inwestowania środków finansowych podejrzanego pochodzenia, inwestowanych wbrew procedurom AML, należących do grup przestępczych, zaangażowanych w finansowanie terroryzmu itd.,
- podnosi się stan nieufności względem nowoczesnych technologii, obrotu bezgotówkowego, transakcji na odległość itp.

Rekomendacje dotyczące przeciwdziałania zjawisku oraz poprawy efektywności regulacji

Mając na uwadze zidentyfikowane problemy, stwierdzone deficyty stanu prawnego oraz niesatysfakcjonujące działania organów władzy publicznej, rekomenduje się:

– podjęcie przez sektor bankowy, w tym przy zaangażowaniu Związku Banków Polskich oraz krajowych organów władzy publicznej (w tym: Prezesa UOKiK, Rzecznika Finansowego, Rzecznika Praw Obywatelskich, Prezesa UODO, Komisji Nadzoru Finansowego, Ministra Cyfryzacji, Ministra Spraw Zagranicznych, Ministra Finansów i Gospodarki, Ministra Sprawiedliwości, Prezesa NBP) działań na rzecz wypracowania koherentnych rozwiązań podnoszących bezpieczeństwo oraz wiarygodność treści udostępnianych w internecie na poziomie krajowym oraz Unii Europejskiej;

– podjęcie przez sektor bankowy, w tym przy zaangażowaniu Związku Banków Polskich, działań mających na celu integrację stanowiska sektora bankowego z innych krajów Unii Europejskiej w celu wywarcia presji na organy Unii Europejskiej oraz państw trzecich (zwłaszcza rząd Stanów Zjednoczonych) w celu wprowadzenia rozwiązań ograniczających działalność Big Techów w obszarze udostępniania i promocji treści (reklam) oszukańczych, prowadzących do nieautoryzowanych transakcji;

– stworzenie funduszu kompensacyjnego przez największe platformy cyfrowe, Big Techy, z którego pokrywane byłyby roszczenia odszkodowawcze wypłacane w związku z nielegalnymi reklamami lub treściami wprowadzającymi w błąd. Fundusz mógłby być zasilany coroczną składką obliczaną jako procent globalnych lub europejskich przychodów reklamowych danej platformy (w razie wystąpienia pozytywnych przesłanek, tj. uznania, iż dana reklama doprowadziła użytkownika do straty finansowej, zwłaszcza w powiązaniu z nieautoryzowaną transakcją płatniczą, odszkodowanie byłoby wypłacone z funduszu w sposób znacznie szybszy i bardziej automatyczny niż w obecnych procedurach reklamacyjnych. Jednocześnie, powyższe nie zwalniałoby Big Tech z ewentualnych sankcji administracyjnych);

– zainicjowanie precedensowych postępowań sądowych (przy współpracy europejskich kancelarii prawnych z kancelariami amerykańskimi) w celu uzyskania rozstrzygnięcia korzystnego, zasądzającego odszkodowanie lub inny rodzaj rekompensaty odpowiadającej stratom banków w związku z nieautoryzowanymi transakcjami, do których przyczyniły się oszukańcze treści (reklamy) w internecie;

– ścisła koordynacja pomiędzy bankami oraz organami władzy publicznej (Ministerstwo Cyfryzacji) w zakresie permanentnego monitorowania oraz publicznego informowania o aktywnościach oraz metodach działania podejrzanych reklamodawców, przestępców oraz treści publikowanych przez Big Techy;

– większa aktywność oraz bardziej rygorystyczna postawa krajowych organów odpowiedzialnych za ochronę konkurencji i konsumentów (zwłaszcza UOKiK) względem podmiotów typu Big Tech;

– podjęcie dyskusji nad zmianami legislacyjnymi (również w obszarze fiskalnym, w tym instytucji tzw. podatku cyfrowego) uzależniającymi zakres obowiązków publicznoprawnych od skali incydentów polegających na udostępnieniu informacji nieprawdziwych, oszukańczych reklam itd.;

– działania na rzecz wprowadzenia dodatkowej daniny publicznoprawnej, nałożonej na Big Techy, w prawie Unii Europejskiej – jako instrumentu „nacisku" na amerykańskie korporacje, zwłaszcza najczęściej dopuszczające się ignorowania europejskich standardów informowania, reklamy i praw konsumentów;

– udoskonalenie współpracy międzynarodowej (również przez resorty odpowiedzialne za sprawy wewnętrzne, zagraniczne, sprawiedliwość, gospodarkę i podatki) w obszarze wymiany informacji o nadużyciach Big Techów, reklamach oszukańczych, działalności przestępców w Internecie itd.;

– stworzenie centralnego rejestru rachunków wykorzystywanych do przestępstw oraz wprowadzenie procedur umożliwiających sprawne blokowanie środków;

– wprowadzenie obowiązkowych interfejsów API (ang. Application Programming Interface[164]) umożliwiających bezpośrednią komunikację między platformami a instytucjami finansowymi oraz organami ścigania;

– wydzielenie specjalnych grup złożonych z prokuratorów, ekspertów, reprezentantów banków oraz UKNF oraz funkcjonariuszy służb odpowiedzialnych za bezpieczeństwo państwa (ABW, AW, SKW, CBA) w celu działań prewencyjnych oraz skrócenie czasu potrzebnego na uzyskanie decyzji o blokadzie środków na podejrzanym koncie;

[164] Techniczny „kanał komunikacji" między systemami, który pozwala na automatyczne i natychmiastowe przesyłanie określonych informacji.

- wypracowanie europejskiego kodeksu etycznego normującego zasady działania platform internetowych, zwłaszcza w kontekście obowiązku weryfikowania reklamodawców i treści potencjalnie niebezpiecznych dla konsumentów oraz inwestorów;

- choć – mimo weta Prezydenta Rzeczypospolitej Polskiej wobec ustawy wdrażającej DSA – wszystkie obowiązki, które nakłada DSA obowiązują, a zawarte w niej regulacje wiążą bezpośrednio, utrudniona będzie egzekucja tych obowiązków (ponieważ ustawa dookreślała kompetencje proceduralne organów administracyjnych i sądowych, zwłaszcza w zakresie raportowania treści niedozwolonych i powiązanej procedury nadzoru nad wykonywaniem obowiązków platform), wobec czego: rekomenduje się podejmowanie przez sektor bankowy (szczególnie Związek Banków Polskich) działań mających na celu jak najszybsze przyjęcie ustawy, która doprecyzuje zakres praw, obowiązków oraz kształt krajowych procedur w celu zapewnienia pewności prawnej.

Scenariusz wywiadu pogłębionego w ramach badania pt. „*Problem nieautoryzowanych transakcji w kontekście odpowiedzialności Big Techów za reklamy – skala zjawiska, analiza ryzyk i procedur odzyskiwania środków oraz odpowiedzialności w systemach płatności. Propozycja optymalnego uregulowania*"

1. **Wprowadzenie (*szacowany czas: ok. 5 minut*)**

   a) Przedstawienie się ankietera.

   b) Opis badań (skład zespołu badawczego, cel badań, metody badań, cel wywiadu pogłębionego, podmiot finansujący badania: Warszawski Instytut Bankowości, sposób popularyzacji wyników badań: raport popularno-naukowy dostępny *open access online*).

   c) Zgoda na rejestrowanie wypowiedzi i wykorzystanie ich wybranych fragmentów w tekście raportu.

   d) Ewentualne dodatkowe pytania do ankietera.

2. **Sylwetka Respondenta (*ok. 5 minut*).**

   a) Proszę krótko (w kilku zdaniach, koncentrując się na pełnionych funkcjach, wykonywanych obowiązkach, latach doświadczenia, zrealizowanych projektach) opowiedzieć o swoich doświadczeniach zawodowych związanych z sektorem bankowym.

   b) Proszę ogólnie (w kilku zdaniach, skupiając się zwłaszcza na: pełnionych funkcjach, wykonywanych zadaniach, wykształceniu i ukończonych kursach itp.) opisać swoje doświadczenia w zakresie zastosowania/wdrażania sztucznej inteligencji w sektorze bankowym.

3. **Pytania główne – otwarte (*ok. 15-20 minut*)**

   a) Jaka jest z Pani/Pana/instytucji (banku) perspektywy obserwowana skala obserwowana zjawiska nieautoryzowanych transakcji? [*swobodna wypowiedź*].

   b) Jakie są najczęściej identyfikowane przez przyczyny tego zjawiska. [*swobodna wypowiedź*].

   c) Jak duża – w kontekście nieautoryzowanych transakcji – jest rola platform społecznościowych oraz firm technologicznych (tzw. *Big Tech*) dla działań przestępczych/bezprawnych w tym zakresie. [*swobodna wypowiedź*].

   d) Co Pani/Pana zdaniem należy zrobić, by skuteczniej niż obecnie przeciwdziałać zjawisku nieautoryzowanych transakcji, szczególnie w kontekście aktywności (reklam) platform społecznościowych oraz firm technologicznych (tzw. *Big Tech*) [*swobodna wypowiedź*].

   e) [*pytanie faktultatywne[165]] Jak ocenia Pani/Pan aktualny, obowiązujący w Polsce/Unii Europejskiej, stan regulacji prawnej w kontekście aktywności platform społecznościowych oraz firm technologicznych (tzw. *Big Tech*) i ich wpływu na nieautoryzowane transakcje? Czy jest Pani/Pan w stanie przedstawić ewentualne kierunki lub konkretne propozycje zmian legislacyjnych? [*swobodna wypowiedź*].

4. **Zamknięcie i podsumowanie wywiadu**

   Czy – poza poruszonymi zagadnieniami i odpowiedziami na dotychczas zadane pytania – widzi Pani/Pan inne istotne kwestie, które warto wskazać?

[165] Skierowane do respondentów, którzy wyrażą zgodę na pytania dotyczące zagadnień prawnych.

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY